# CWE-CAPEC ICS/OT Special Interest Group

## Wednesday, January 25, 2023

**THIS MEETING IS BEING RECORDED**

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# ICS/OT Special Interest Group Participants

1. **Aagam Shah**
2. **Aamir Khan,** Tata Power
3. **Abdelrahman Elsanose**
4. **Adam Hahn**
5. **Adrian Crespo-Ortiz,** Capgemni
6. **Ahmad Sharafi,**
7. **Albert Vartic,** OMV Petrom
8. **Alex Rodriguez**, PG&E
9. **Alfinie Bullock,**
10. **Amanda Kraus**
11. **Andres Fuentes-Fernandez,** Inetum
12. **Andrew Kling**, Schneider Electric
13. **Andy Kling,** Schneider Electric
14. **Anjel Jimenez**
15. **Anton Shipulin**
16. **Armada Sramek**
17. **Ashley McGlone,** Tanium
18. **Aw Landgraaf,**
19. **Ayman Alissa**, Mckinsey
20. **Barry Greene**, Senki
21. **Bayard Johnson**
22. **Bill Newhouse**
23. **Brandon Carter**,
24. **Ben Deering,** ODNI
25. **Ben Sooter**, EPRI
26. **Beverly Novak**, INL
27. **Bill Aubin,** Nozomi Networks
28. **Bill Kintz**, Invictus
29. **Bill Newhouse**
30. **Bob Hanson,** LLNL
31. **Bob Heinemann**,
32. **Bob Radvanovsky**
33. **Bradley Nickens**, GE
34. **Bryan Beckman,** INL
35. **Bryan Owen**, Aveva
36. **Cameron Burden,**
37. **Carl Mccants,** ODNI

# ICS/OT Special Interest Group Participants

38. **Carmen Zapata**, DHS
39. **Chris Charpentier**, GE
40. **Christopher Havey,** Applied Cybersecurity Engineering
41. **Christopher Sundberg**, Woodward
42. **Chris Humphrey**, Boeing
43. **Chris Levendis**,
44. **CJ Harvey,**
45. **Cody Kieltyka**,
46. **Craig Barrett,** Kinder Morgan
47. **Curtis Taylor**, CyManII
48. **Curt Wiggins**
49. **Cynthia Hsu,** DOE
50. **Dana Thomas**
51. **Dan Bennett,** NREL
52. **Dan Ehrenreich,** SCCE
53. **Danielle Jablanski**,
54. **Daniel Santos**, Forescout
55. **Daniel Stachan**
56. **Daryl Haegley**
57. **Dave Halla**
58. **Dave Keppler**
59. **David Hernandez**
60. **David Nicol**, UIUC & CyManII
61. **David Simpson**
62. **Deborah Kobza,** IACI
63. **Derek Hart**
64. **Dimple Shah**
65. **Dylan Sundy**
66. **Ed Hicks**
67. **Edward Liebig**
68. **Eric Cosman**
69. **Eric Mitchell,** NSA
70. **Eric Strief,** John Deere
71. **Erik Hrin**
72. **Espen Endal,** KraftCERT
73. **Evgeni Sabev**
74. **Faheem Ahmed (new)**
75. **Gabriela Ciocarlie,** CyManII (new)
76. **Gananand G Kini**
77. **Greg Ahira,** GE
78. **Greg Bastien**

# ICS/OT Special Interest Group Participants

79. **Greg Sanchez**
80. **Gus Serino**
81. **Hadeli Hadeli,** Hitachi Energy
82. **Haritha Srinivasan,** FM Global
83. **Harry Perper,** Cyber Architecture and Resiliency
84. **Herson Esquiviel-Vargas** (new)
85. **Howard Grimes,** CyManII
86. **Iain Deason,** DHS CISA
87. **Ismael Garcia,** NRC
88. **Jace Powell,** Fortress
89. **Jarvis Robinson**
90. **Jason Li,** TrustedST
91. **Jason Plant**
92. **Jason Robbins,** AT&T
93. **Jay Gazlay,** DHS CISA
94. **Jen Walker,** Water ISAC
95. **Jennifer Pedersen**
96. **Jeremy Mckeown**
97. **Jesper Johansson,** Nouryon
98. **Jess Smith,** PNNL
99. **Jodi Jensen**
100. **Joe Agres,** West Yost
101. **Joe McCormick**
102. **Joe Weiss**
103. **John Almlof**
104. **John Kingsley**
105. **John Repici**
106. **John Schneider**
107. **John Parmley,** Zuuliot
108. **John Ransom**
109. **Jon Terrell,** Hitachi Energy
110. **Jon White,** NREL
111. **Jonti Talukdar,** Duke
112. **Jordon Sims**
113. **Jose Jimenez,** Sothis
114. **Jose Perez,** Tenable
115. **Joseph Bessett,** Cynalytica (new)
116. **Joseph Cummings,** NYPA
117. **Joseph Januszewski,** E-Isac
118. **Joseph Matthews**

# ICS/OT Special Interest Group Participants

119. **Jude Desti,** Boeing
120. **Junya Fujita,**
121. **Justin Cain**
122. **Karen Wetzel**
123. **Ken Wang,** DOD
124. **Ken Cole**, Entergy
125. **Kerry Stuver,** GE
126. **Khalid Ansari,** FM Approvals
127. **Kimberly Denbow,**
128. **Krystel Castillo**
129. **Kumar**
130. **Kyle Hussey**
131. **Kyle Johnson,** GSOC
132. **Lee Szilagyi**, MITRE (new)
133. **Lindsey Cerkovnik,** DHS CISA
134. **Manoj Balachandran**
135. **Marc Sachs,** Auburn University
136. **Marco Ayala**
137. **Mark McCoy (new)**
138. **Mark Sullivan,** NSA
139. **Martijn Jansen,** Taqa
140. **Martin Kihiko**
141. **Martin Ring,** Bosch
142. **Martin Scheu,** Switch
143. **Marty Edwards**
144. **Matt Bishop,** UC Davis & CyManII
145. **Matt Sexton,** Hexagon
146. **Marie Stanley Collins**
147. **Matthew Bohne**
148. **Matthew Knoll,** ArcelorMittal
149. **Max Wandera,** Eaton
150. **Megan Samford**
151. **Melissa Vice,** Air Force
152. **Michael Chaney,** CyManII
153. **Michael Hok,** Hitachi Energy
154. **Michael Toecker**
155. **Michalis Pavlidis,** University of Brighton
156. **Mike Iapalucci (new)**
157. **Mike Cohen** (new)
158. **Mina Todorova**

# ICS/OT Special Interest Group Participants

159. **Monika Akbar,** UTEP & CyManII
160. **Muhammed Shaban**
161. **Nik Urlaub,** MITRE
162. **Niyu Ogunniyi,** Corteva
163. **Oystein Brekk-Saunderud,** Norma Cyber
164. **Patrick Dale**
165. **Patrick Obruba**
166. **Patti Escatel,** DHS CISA
167. **Paul Martyak,** EPRI
168. **Paul Peix,** Headmind
169. **Paul Zawada**
170. **Pete Tseronis**
171. **Peter Colombo**
172. **Peter Jackson,** SGS
173. **Peter Pongracz,** MOL
174. **Philip Huff, UALR**
175. **Pierre Janse van Rensburg,** BBA
176. **Piotr Pedziwiatr,** Arcelor Mittal
177. **Ralph Ley**
178. **Raymond Savarda**
179. **Renan**
180. **Rex Wempen,** DOE
181. **Rezaur Rahman**
182. **Rich Piazza,** MITRE
183. **Richard Robinson,** Cynalytica
184. **Rita Ann Foster**
185. **Robert Garry,** GE Gas Power
186. **Robert Heinemann**, MITRE
187. **Robert Murphy**
188. **Robert Sadler**, MITRE (new)
189. **Roger Johnson,** Novelis
190. **Ronald Atwater**
191. **Ruben Aguilar (new)**
192. **Ryan Bays,** PNNL
193. **Ryan Gagliastre,** HF Sinclair
194. **Sabri Khemissa**
195. **Sachin Shah,** Armis
196. **Saleh Almaghrabi**
197. **Salman Salman,** Aerospace Corporation
198. **Sam Thom**
199. **Samuel Chanoski,** INL

# ICS/OT Special Interest Group Participants

200. **Sandeep Shukla,** Virginia Tech
201. **Sarah Fluchs,** Admeritia
202. **Shane Stailey**
203. **Shannon Hughes**
204. **Shadya Maldonado,** Sandia
205. **Sharin Crane,** Boeing
206. **Sharla Artz**
207. **Sherry Hunyadi**
208. **Steve Battista**
209. **Steve Chapin**
210. **Steve Granda,** NREL
211. **Stephanie Saravia**
212. **Stephen Trachian,** Hitachi Energy
213. **Susan Farrell**, ObjectSecurity
214. **Ted Wittmer**
215. **Thomas Ruoff,** DHS CISA
216. **Timothy Isaacs,** NuScale Power
217. **Todd Riley, Goodyear**
218. **Tom McGoogan**
219. **Tony Turner,** Fortress
220. **Tonya Riley,** Cyberscoop
221. **Tracy Briggs,** CyManII
222. **Travis Ashley,** PNNL
223. **Vivek Ponnada**
224. **Wayne Austad,** CyManII
225. **Wayne Cantrell**
226. **William Kintz** (Added)
227. **William Welch**
228. **Vadim Nerovnia (new)**
229. **Yasoda Ramchune,** Chevron
230. **Zachary Rogan,** Xage

# ICS/OT Special Interest Group Leadership and Support

1. **Aeriel Lane,** Nexight Group
2. **Alec Summers,** MITRE
3. **Andrew Kresses,** Nexight Group
4. **Cheri Caddy,** DOE-CESER
5. **Chris Coffin**, MITRE (new)
6. **Daisyareli Martin,** Nexight Group
7. **Greg Kerr,** Nexight Group
8. **Greg Shannon,** CyManII
9. **Ginger Wright,** INL
10. **Jeff Hahn,** INL
11. **Jeff Mitchell,** INL
12. **Jennifer Ekperigin,** Nexight Group
13. **Katie Baker,** Nexight Group
14. **Karsten Daponte,** Nexight Group
15. **Lindsay Kishter,** Nexight Group
16. **Matthew Luallen,** UI
17. **Stephen Bolotin,** Nexight Group
18. **Steve Christey,** MITRE

# Agenda

| Eastern Time | Activity |
|---|---|
| 3:00 – 3:05 pm | **Login and Roll Call** |
| 3:05 – 3:10 pm | **Opening Remarks**<br>• Review meeting objectives<br>• Review material covered in last meeting |
| 3:10 – 3:25 pm | **CWE and CAPEC Updates Related to ICS/OT Weaknesses**<br>• CWE 4.10 updates from January 2023<br>• CAPEC 3.9 updates from January 2023 |
| 3:25 – 3:40 pm | **SIG Exhibition Space at S4x23 ICS Security Event in Miami Beach**<br>• Survey results<br>• Activity planning<br>• Seeking SME volunteers<br>• Onboarding new participants |
| 3:40 – 4:25 pm | **Progress Updates from SIG Sub-Working Groups**<br>• "Boosting CWE Content" subgroup update by chair Howard Grimes<br>• "Mapping CWE to 62433" subgroup update by co-chairs Khalid Ansari and Bryan Owen |
| 4:25 – 4:30pm | **Wrap-Up**<br>• Closing remarks<br>• Major milestones<br>• Next SIG meeting – Wed 2/22 @ 3pm ET<br>• Action Items |
| 4:30 pm | **Meeting Ends** |

# Opening Remarks

# Opening Remarks

## Meeting Objectives

1. Review CWE 4.10 and CAPEC 3.9 updates related to ICS/OT weaknesses
2. Plan for upcoming SIG Exhibition Space at S4x23 ICS Security Event
3. Share progress updates from SIG sub-working groups

## Review of Last Meeting 11/30

- MITRE presented upon the updated definition of a “weakness” in CWE/CAPEC
- MITRE reviewed CWE 4.9 updates for Oct 2022 and CAPEC 3.8 updates for Sep 2022
- “Boosting CWE Content” co-chair Howard Grimes presented on subgroup’s progress
- “Mapping CWE to 62443” co-chair Khalid Ansari presented on subgroup’s progress

# Housekeeping/Announcements

- **LIVE POLL: Who is receiving emails via the ICS/OT SIG listerv?**
  - Email address is: cwecapec-ics-ot-sig-list@mitre.org
- **Announcing new co-chair from CyManII:**
  - Greg Shannon, *Chief Science Officer @ CyManII*, stepping down
  - Matt Luallen, *Vice President for Cyber Vulnerability Awareness @ CyManII*, assuming duties of co-chair

# CWE and CAPEC Updates Related to ICS/OT Weaknesses

# Recent CWE/CAPEC Content Changes

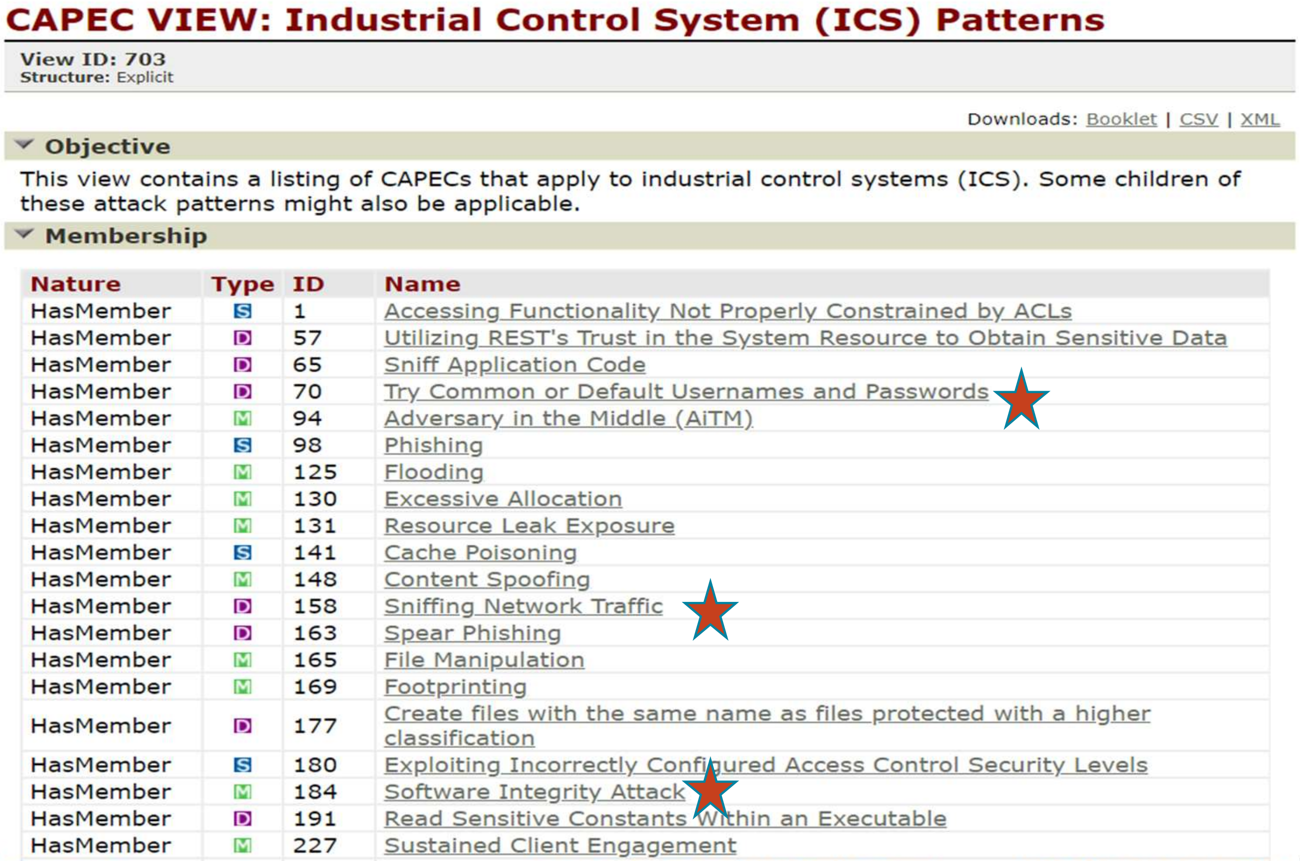
Steve Christey Coley

January 25, 2023

# CAPEC 3.9

- Released yesterday, January 24, 2023
- New view: “Industrial Control System (ICS) Patterns”
- https://capec.mitre.org/data/definitions/703.html
- 46 attack patterns
- Created in part by utilizing the ATT&CK ICS Matrix

# New CAPEC View



## CAPEC VIEW: Industrial Control System (ICS) Patterns

**View ID: 703**
**Structure:** Explicit

Downloads: Booklet | CSV | XML

**Objective**

This view contains a listing of CAPECs that apply to industrial control systems (ICS). Some children of these attack patterns might also be applicable.

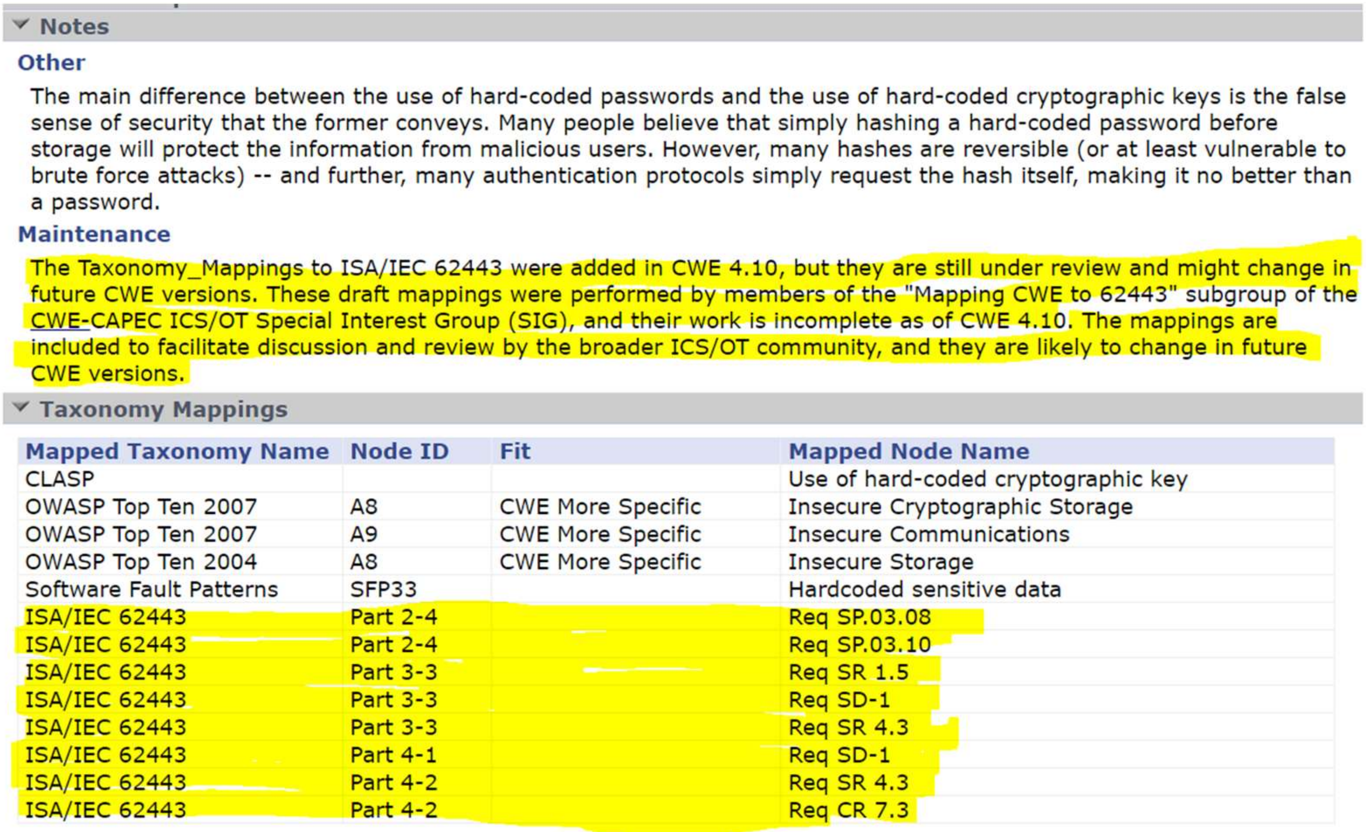
**Membership**

| Nature | Type | ID | Name |
|---|---|---|---|
| HasMember | S | 1 | Accessing Functionality Not Properly Constrained by ACLs |
| HasMember | D | 57 | Utilizing REST's Trust in the System Resource to Obtain Sensitive Data |
| HasMember | D | 65 | Sniff Application Code |
| HasMember | D | 70 | Try Common or Default Usernames and Passwords |
| HasMember | M | 94 | Adversary in the Middle (AiTM) |
| HasMember | S | 98 | Phishing |
| HasMember | M | 125 | Flooding |
| HasMember | M | 130 | Excessive Allocation |
| HasMember | M | 131 | Resource Leak Exposure |
| HasMember | S | 141 | Cache Poisoning |
| HasMember | M | 148 | Content Spoofing |
| HasMember | D | 158 | Sniffing Network Traffic |
| HasMember | D | 163 | Spear Phishing |
| HasMember | M | 165 | File Manipulation |
| HasMember | M | 169 | Footprinting |
| HasMember | D | 177 | Create files with the same name as files protected with a higher classification |
| HasMember | S | 180 | Exploiting Incorrectly Configured Access Control Security Levels |
| HasMember | M | 184 | Software Integrity Attack |
| HasMember | D | 191 | Read Sensitive Constants Within an Executable |
| HasMember | M | 227 | Sustained Client Engagement |

# CWE 4.10 – Main relevant ICS/OT changes

- **To be released January 31, 2023**
- **Hundreds of descriptions changed from "software" to "product"**
  - More directly includes hardware, ICS, etc.
- **Updated SEI ETF category descriptions to quote directly from the paper**
- **Integrated (some) changes from Boosting and Mapping subgroups**
  - Votes by sub-WG members were strongly in favor
  - Taxonomy mappings to 62443
  - New members of some SEI-ETF categories
  - Flagging CWEs as affecting ICS/OT
- **Finished observed examples (CVEs) covered by OT:ICEFALL**
- **New entry for "Reliance on Vulnerable Third-Party Component"**

# Example Changes from Mapping-CWE Sub-WG (CWE-321: Hard-coded Cryptographic Key)



**Notes**

**Other**

The main difference between the use of hard-coded passwords and the use of hard-coded cryptographic keys is the false sense of security that the former conveys. Many people believe that simply hashing a hard-coded password before storage will protect the information from malicious users. However, many hashes are reversible (or at least vulnerable to brute force attacks) -- and further, many authentication protocols simply request the hash itself, making it no better than a password.

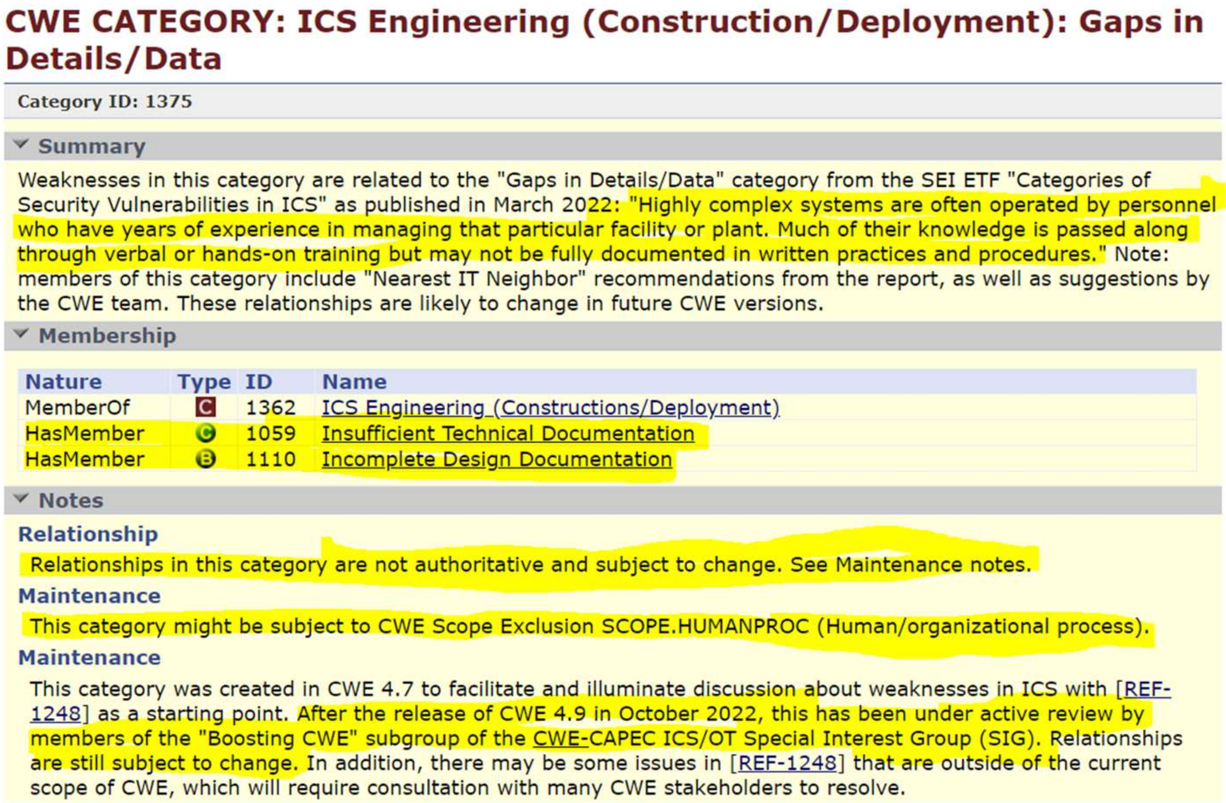
**Maintenance**

The Taxonomy_Mappings to ISA/IEC 62443 were added in CWE 4.10, but they are still under review and might change in future CWE versions. These draft mappings were performed by members of the "Mapping CWE to 62443" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG), and their work is incomplete as of CWE 4.10. The mappings are included to facilitate discussion and review by the broader ICS/OT community, and they are likely to change in future CWE versions.

**Taxonomy Mappings**

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| CLASP | | | Use of hard-coded cryptographic key |
| OWASP Top Ten 2007 | A8 | CWE More Specific | Insecure Cryptographic Storage |
| OWASP Top Ten 2007 | A9 | CWE More Specific | Insecure Communications |
| OWASP Top Ten 2004 | A8 | CWE More Specific | Insecure Storage |
| Software Fault Patterns | SFP33 | | Hardcoded sensitive data |
| ISA/IEC 62443 | Part 2-4 | | Req SP.03.08 |
| ISA/IEC 62443 | Part 2-4 | | Req SP.03.10 |
| ISA/IEC 62443 | Part 3-3 | | Req SR 1.5 |
| ISA/IEC 62443 | Part 3-3 | | Req SD-1 |
| ISA/IEC 62443 | Part 3-3 | | Req SR 4.3 |
| ISA/IEC 62443 | Part 4-1 | | Req SD-1 |
| ISA/IEC 62443 | Part 4-2 | | Req SR 4.3 |
| ISA/IEC 62443 | Part 4-2 | | Req CR 7.3 |

# Example Changes from Boosting-CWE Sub-WG



## CWE CATEGORY: ICS Engineering (Construction/Deployment): Gaps in Details/Data

**Category ID: 1375**

**Summary**

Weaknesses in this category are related to the "Gaps in Details/Data" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Highly complex systems are often operated by personnel who have years of experience in managing that particular facility or plant. Much of their knowledge is passed along through verbal or hands-on training but may not be fully documented in written practices and procedures." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

**Membership**

| Nature | Type | ID | Name |
|---|---|---|---|
| MemberOf | C | 1362 | ICS Engineering (Constructions/Deployment) |
| HasMember | C | 1059 | Insufficient Technical Documentation |
| HasMember | B | 1110 | Incomplete Design Documentation |

**Notes**

**Relationship**

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

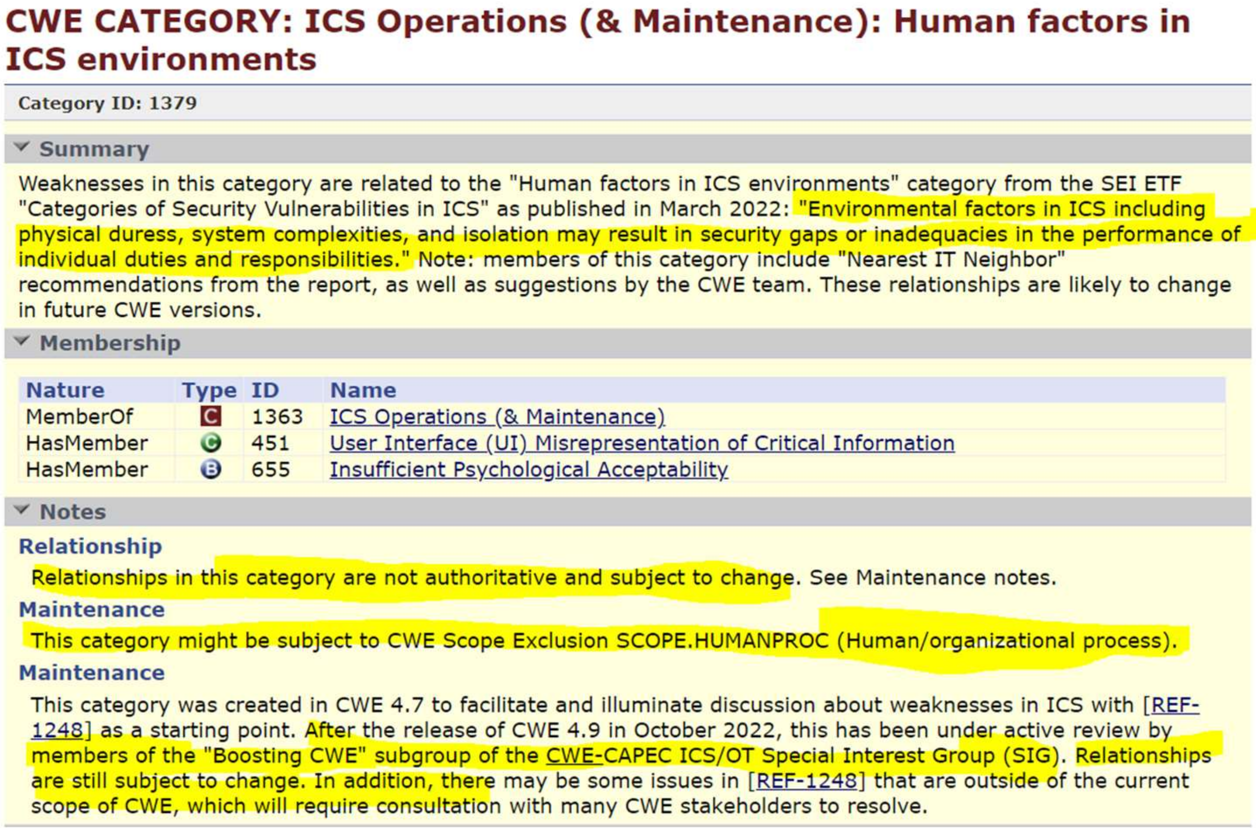
**Maintenance**

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

**Maintenance**

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

# Example Changes from Boosting-CWE Sub-WG (2)



## CWE CATEGORY: ICS Operations (& Maintenance): Human factors in ICS environments

Category ID: 1379

### Summary

Weaknesses in this category are related to the "Human factors in ICS environments" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Environmental factors in ICS including physical duress, system complexities, and isolation may result in security gaps or inadequacies in the performance of individual duties and responsibilities." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

### Membership

| Nature | Type | ID | Name |
|---|---|---|---|
| MemberOf | C | 1363 | ICS Operations (& Maintenance) |
| HasMember | C | 451 | User Interface (UI) Misrepresentation of Critical Information |
| HasMember | B | 655 | Insufficient Psychological Acceptability |

### Notes

**Relationship**

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

**Maintenance**

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

**Maintenance**

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

# After CWE 4.10

- **Continue to adapt/refine work from both subgroups**
  - Integrate into CWE when applicable
- **ICS/OT SIG members could engage in public discussion / community review of CWE's "Scope Exclusions"**

# SIG Exhibition Space at S4x23 ICS Security Event in Miami Beach

# Activity Planning for S4 – Wed 2/15, 8am – 1pm

- **Activities being explored by leadership (order by vote in survey)**
  1. Identify opportunities to collaborate with other activities in the ICS/OT space
  2. Expand SIG and subgroup participation
  3. Conduct one-on-one interviews
  4. Conduct mini focus groups
  5. Conduct real-time surveys (in person or via the Whova app)
- **Ideas gathered from the survey**
  1. Bring case studies (to demonstrate purpose and benefit)
  2. Pick a theme (for clear messaging)
  3. Pull-out posters (for highlighting subgroup activities and successes)
  4. On last day, there is an "unsolicited response" session where anyone can speak on stage for 5 min (use to summarize S4 activities and surveys conducted)
  5. Hand out "swag" such as stickers
  6. Host dinner gather for SIG and subgroup members to attend
  7. *What ideas do you have?*

# Seeking SME Volunteers

- **SURVEY RESULTS:**
  - 12 SIG participants have indicated they are planning to attend S4
  - 6 volunteered to be SMEs
  - Recognizing not everyone is receiving listerv emails, we’re going to poll this group now
- **LIVE POLL:** If you are planning to attend S4, would you be willing to volunteer as a subject matter expert for technical questions about the SIG and/or subgroups?

# Onboarding New Participants

- **S4 is likely to attract new SIG and subgroup participants**
- **The next ICS/OT SIG will convene on Wed 2/22 @ 3pm ET**
- **We will use this meeting to:**
  - Onboard new participants
  - Take stock of where we've been and where we're going
  - Gather live feedback on how the SIG and subgroups are operating and find opportunities for improvement
  - Perhaps adjust the cadence of SIG and subgroup meetings

# Progress Updates from SIG Sub-Working Groups

# “Boosting CWE Content” Subgroup

# Boosting CWE Content Group Participants

1. **Howard Grimes**, CyManII (co-chair)
2. **Haritha Srinivasan,** FM Global (co-chair)
3. **Steven Christey Coley**, MITRE
4. **Adrian Crespo-Ortiz**, Capgemini
5. **Alec Summers**, MITRE
6. **Beverly Novak**, INL
7. **Brandon Tarr**, CISA (new)
8. **Bryan Owen**, Aveva
9. **Chris Coffin**, MITRE
10. **Curtis Taylor**, CyManII
11. **Daniel Ehrenreich**
12. **David Hernandez**, Takeda
13. **Edward Liebig**, Hexagon
14. **Evgeni Sabev**, SAP
15. **Gabreila Ciocarlie**, CyManII
16. **Greg Shannon,** CyManII
17. **Gus Serino**, Dragos
18. **Iain Deason**, DHS
19. **Ismael Garcia**, NRC
20. **John Kingsley, Hitachi**
21. **John Repici, DoD**
20. **Joseph Giampapa**, Arm Institute
21. **Joseph Januszewski**, E-ISAC
22. **Julia Turkevich**, CISA
23. **Junya Fujita**, Hitachi
24. **Kyle Hussey**, TDI
25. **Marco Ayala**, 1898
26. **Matt Luallen,** UIUC
27. **Melissa Vice**, Air Force
28. **Michael Chaney**, INL
29. **Monica Akbar**, CyManII
30. **Oystein Brekke-Saunderud**, Norma Cyber
31. **Paul Peix**, HeadMind
32. **Ryan Bays, PNNL**
33. **Sean Gordon** LLNL
34. **Steven Grzesiak**, Lift
35. **Wayne Austad**, CyManII

36. **Aeriel Lane**, Nexight Group
37. **Greg Kerr**, Nexight Group
38. **Katie Baker**, Nexight Group
39. **Stephen Bolotin**, Nexight Group

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# Work Plan From Subgroup Charter

✓ 1. **Define the problem space and identify the stakeholders that need to be involved**
   - What is the problem we are trying to solve?
   - What is the value proposition for this effort?

2. **Reach consensus on how to move the state of the practice forward**

3. **Establish project plan including key tasks, subtasks, and milestones**

✓ a. Expand participants with outreach to manufacturers

b. Review of SEI ETF 20 Categories of Security Vulnerabilities in ICS/OT and conduct a deeper analysis than MITRE had done. ICS/OT experts will provide input and insights into whether these are event appropriate mappings.

c. Examine common architectural weaknesses in ICS/OT/SCADA (including connections to Cyber-Informed Engineering).

# Work Plan From Subgroup Charter

3. **Establish project plan including key tasks, subtasks, and milestones**

   d. Examine OT:ICEFALL vulnerabilities and determine if CWEs exist but may not be findable/understandable for ICS/OT. This activity may involve additional content in CWEs and/or explicitly labeling for ICS/OT

   e. Wrestle with scope questions. It may be important or useful to expand CWE's scope to include additional types of weaknesses. Previous tasks may produce certain proposals for the expansion of CWE's scope. For important findings outside of CWE's scope, explore how to represent them in ways that make them more accessible to ICS manufacturers and practitioners.

   f. Nominate existing CVEs for ICS/OT issues that CWE does not have coverage for.

4. **Execute on the project schedule, reporting out progress to the ICS/OT SIG at key milestones**

5. **Review final deliverables and identify additional channels of dissemination**

# Boosting CWE Content Meetings

- **Task groups from SEI ETF 20 “Categories of Security Vulnerabilities in ICS”**
  - ICS Communications
  - ICS Dependencies
  - ICS Supply Chain
  - ICS Engineering
  - ICS Operations
- **Boosting CWE Content Subgroup met 1/18/23**

# Task Group Volunteers

### ICS Communications

- Ian Deason
- Kyle Hussey
- Oystein Brekke-Sanderud

### ICS Dependencies

- Iain Deason
- John Kingsley
- Kyle Hussey
- Haritha Srinivasan

### ICS Supply Chain

- Ismael Garcia
- John Repici
- Melissa Vice
- Joseph Giampapa

### ICS Engineering

- Monika Akbar
- Gabreila Ciocarlie
- Curtis Taylor

### ICS Operations

- Beverly Novak
- John Kingsley
- Kyle Hussey
- Michael Chaney
- Oystein Brekke-Sanderud
- Ed Liebig
- Haritha Srinivasan

# Super Category: ICS Communications (CWE-1359)

- **1. Zone Boundary Failures (CWE-1364)**
  - CWE-668: Exposure of Resource to Wrong Sphere
  - CWE-669: Incorrect Resource Transfer Between Spheres
  - CWE-754: Improper Check for Unusual or Exceptional Conditions
- **2. Unreliability (CWE-1365)**
  - CWE-1384: Improper Handling of Physical or Environmental Conditions
- **3. Frail Security in Protocols (CWE-1366)**
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm
  - CWE-358: Improperly Implemented Security Check for Standard

# Super Category: ICS Dependencies (& Architecture) (CWE-1360)

- **4. External Physical Systems (CWE-1367)**
  - CWE-1338: Improper Protections Against Hardware Overheating
  - CWE-1357: Reliance on Uncontrolled Component
- **5. External Digital Systems (CWE-1368)**
  - CWE-610: Externally Controlled Reference to a Resource in Another Sphere
  - CWE-1357: Reliance on Uncontrolled Component

# Super Category: ICS Supply Chain (CWE-1361)

- **6. IT/OT Convergence/Expansion (CWE-1369)**
  - CWE-636: Not Failing Securely ('Failing Open')
- **7. Common Mode Frailties (CWE-1370)**
  - CWE-329: Generation of Predictable IV with CBC Mode
  - CWE-1357: Reliance on Uncontrolled Component
- **8. Poorly Documented or Undocumented Features (CWE-1371)**
  - CWE-912: Hidden Functionality
  - CWE-1059: Insufficient Technical Documentation
  - CWE-1242: Inclusion of Undocumented Features or Chicken Bits

# Super Category: ICS Supply Chain (CWE-1361)

- **9. OT Counterfeit and Malicious Corruption (CWE-1372)**
  - CWE-1198: Privilege Separation and Access Control Issues
  - CWE-1231: Improper Prevention of Lock Bit Modification
  - CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit
  - CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques

# Super Category: ICS Engineering (Constructions/Deployment) (CWE-1362)

- **10. Trust Model Problems (CWE-1373)**
  - CWE-269: Improper Privilege Management
  - CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data
  - CWE-807: Reliance on Untrusted Inputs in a Security Decision
- **11. Maker Breaker Blindness (CWE-1374)**
- **12. Gaps in Details/Data (CWE-1375)**
- **13. Security Gaps in Commissioning (CWE-1376)**
  - CWE-276: Incorrect Default Permissions
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
- **14. Inherent Predictability in Design (CWE-1377)**
  - CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques

# Super Category: ICS Operations (& Maintenance) (CWE-1363)

- **15. Gaps in obligations and training (CWE-1378)**
- **16. Human factors in ICS environments (CWE-1379)**
  - CWE-451: User Interface (UI) Misrepresentation of Critical Information
  - CWE-655: Insufficient Psychological Acceptability
- **17. Post-analysis changes (CWE-1380)**
- **18. Exploitable Standard Operational Procedures (CWE-1381)**

# Super Category: ICS Operations (& Maintenance) (CWE-1363)

- **19. Emerging Energy Technologies (CWE-1382)**
  - CWE-20: Improper Input Validation
  - CWE-285: Improper Authorization
  - CWE-295: Improper Certificate Validation
  - CWE-296: Improper Following of a Certificate's Chain of Trust
  - CWE-346: Origin Validation Error
  - CWE-406: Insufficient Control of Network Message Volume (Network Amplification)
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
- **20. Compliance/Conformance with Regulatory Requirements (CWE-1383)**

# Summary of Findings

- **SEI ETF categories not always perfect fit for CWEs, but a great start**
- **Group considering drafting a commentary document regarding SEI ETF paper**
  - Some descriptions are not clear
  - Recommendations
  - SEI ETF paper is not fluid
- **Several new CWEs are proposed as members of CWE categories**
  - Some may incorporate into CWE 4.10
- **Human factor categories (ICS Operations) – often no direct CWE mapping**
- **Next step: finish and validate the work that has been completed**

# “Mapping CWE to 62443” Subgroup

# “Mapping” Subgroup Participants

1. **Bryan Owen**, AVEVA (co-chair)
2. **Khalid Ansari**, FM Approvals (co-chair)
3. **Alec Summers**, MITRE (CWE-CAPEC program rep)
4. **Michael Thompson**, MITRE
5. **Dave Morse**, MITRE
6. **Philip Taggart**, MITRE
7. **Steve Christey Coley**, MITRE
8. **Oystein Brekke-Sanderud**, NORMA Cyber
9. **Paul Peix**, HeadMind Partners
10. **Marco Ayala**, 1898 & Co.
11. **Martin Scheu**, SWITCH
12. **Matt Knoll**, ArcelorMittal
13. **Junya Fujita**, Hitachi Energy
14. **Stephen Trachian**, Hitachi Energy
15. **John Kingsley**, Hitachi Energy
16. **Kyle Hussey**, TDI Technologies
17. **Edward Liebig**, Hexagon
18. **Sam Chanoski**, INL
19. **Beverly Novak**, INL
20. **Jose Luis Jimenez Izquierdo**, SOTHIS
21. **Jose Miguel Perez Vergara**, SOTHIS
22. **Ruben Aguilar Rives**, SOTHIS
23. **Susan Farrell**, ObjectSecurity
24. **Melissa Vice**, DoD Cyber Crime Center (DC3)
25. **John Repici**, DoD Cyber Crime Center (DC3)
26. **Ismael Garcia**, NRC
27. **Christopher Sundberg**, Woodward, Inc.
28. **Curtis Taylor**, CyManII
29. **Mike Chaney**, CyManII
30. **Greg Shannon**, CyManII
31. **Mina Todorova**, ITARICON GmbH
32. **Adrian Crespo**, Capgemini
33. **Daniel Ehrenreich**, Secure Communications and Control Experts
34. **Richard Robinson**, Cynalytica
35. **Joseph Bessette**, Cynalytica
36. **Sean Gordon**, LLNL
37. **James “Jake” Jones**
38. **Tony Turner,** Fortress
39. **Chris Coffin,** MITRE
40. **Stephen Bolotin**, Nexight Group
41. **KatherineAnne Baker**, Nexight Group
42. **Greg Kerr,** Nexight Group
43. **Aeriel Lane**, Nexight Group

# Defining the Problem Space & Value Proposition

- **Defining the Problem Space**
  - There is not a direct relationship between current CWEs associated with OT vulnerabilities and 62443 security requirement (both product and system requirements/enhancements). Further, there is a need to design-out weaknesses in products, but this is hampered by a gap in terminology between CWE and 62443.
- **Articulating the Value Proposition**
  - Help organization in their application of standards by outlining how CWEs can be addressed, especially in terms of improving design quality of products commonly used in critical infrastructure.

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# Work Plan from Subgroup Charter

## Tasking & Major Milestones

1. Identify failure examples to be referenced in applicable CWEs (and SEI ETF 20 categories of security vulnerabilities with CWE updates)
   - 1st Month Milestone: Determine top-10 CWEs (most exploited) in ICS/OT ✓
   - 2nd Month Milestone: Determine top CWEs for subsequent rounds of mapping (potentially 2-4 more) ✓
   - 3rd Month Milestone: Identify gaps in CWE relevant to ICS/OT for the "Boosting" subgroup to consider
2. Tier ISA/IEC 62443 requirements (must have, nice to have, if there is time) as candidates to enrich CWE
   - 1st Month Milestone: Determine top 62443 security requirement **parts** (must haves) ✓
   - 2nd Month Milestone: Map top-10 CWEs to specific requirements of 62443 (e.g., 62443-4-2 CR 2.1) ✓
   - 3rd Month Milestone: Map remaining CWEs to 62443, and identify areas where 62443 does not address top weaknesses in ICS/OT
3. Provide recommendations to CWE to add cross references to ISA/IEC 62443 requirements/guidance based including the example case(s)

## Accessing ISA/IEC 62443 requirements

- ISA-99 committee has provided the following 62443 sections for this mapping exercise: 1-1, 2-1, 2-2, 2-4, 3-2, 3-3, 4-1, 4-2, TR99

## Additional Suggested Tasking

- Identifying a comprehensive list of threats beyond threats currently listed in 62443
- Consider reaching out to other Standards Development Organizations (e.g., IEEE) based on the outcome of this effort

# Small Group Pairings & CWE Assignments

1. Beverly Novak, Stephen Trachian, Sandeep Kumar Shukla, Sean Gordon
   - **CWE-287:** ***Improper Authentication***
2. Ismael Garcia, Tony Turner, Junya Fujita, John Kingsley
   - **CWE-321:** ***Use of Hard-coded Cryptographic Keys***
3. Mike Chaney, Mina Todorova, Ruben Aguilar Rives, Martin Scheu
   - **CWE-657:** ***Violation of Secure Design Principles (parent of CWE-636)***
4. Susan Farrell, Edward Liebig, James "Jake" Jones, Jose Miguel Perez Vergara, Daniel Ehrenreich
   - **CWE-798:** ***Use of Hard-coded Credentials***
5. John Repici, Joseph Bessette, Jose Luis Jimenez, Richard Robinson, Monika Akbar
   - **CWE-319:** ***Cleartext Transmission of Sensitive Information***
6. Michael Thompson, Curtis Taylor, Oystein Brekke-Sanderud, Marco Ayala, Paul Peix
   - **CWE-327:** ***Use of a Broken or Risky Cryptographic Algorithm***
7. Sam Chanoski, Matt Knoll, Iain Deason, Kyle Hussey, Christopher Sundberg
   - **CWE-400:** ***Uncontrolled Resource Consumption***

# Prioritized Spreadsheet of CWEs

# CWE-62443 Master Mapping List

# Wrap-Up

# Milestones

- **Sub-Working Groups meet bi-weekly**
  - "Boosting" subgroup next meets Wednesday 2/1 from 10:30 to 11:30am ET
  - "Mapping" subgroup next meets Tuesday 1/31 from 1:00 to 2:00pm ET
- **ICS/OT SIG normally meets bimonthly**
  - Next meeting Wednesday 2/22 from 3:00 to 4:30pm ET
- **CWE/CAPEC publish content on quarterly basis**
  - Next major update for CWE 4.10 – Jan 2023
  - Next major update for CAPEC 3.9 – Jan 2023

# Action Items

1. **Insert Text**

MITRE

MITRE’s mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org

YouTube

# Survey Results

## Thank you for your responses!

1. 11 participants indicated that they are planning to attend S4 – we will see you there! We will reach out individually to the 6 folks who volunteered to support as subject matter experts.
2. Exhibit Activities (priority ranking) and associated recommendations
   1. Identify opportunities to collaborate with other activities in the ICS/OT space
      - Key to expand our messaging!
      - Engage with ACT-IAC Cybersecurity COI and INSA Critical Infrastructure Subcommittee
   2. Expand SIG and subgroup participation
      - Get the word out in a concise and attractive way to bring more members in and get industry's perspective
   3. Conduct one-on-one interviews and mini focus groups
      - Focus groups to see what consensus is among manufacturers and other ICS representatives on subgroup topics
   4. Conduct real-time surveys
      - May be too granular
      - Ensure any survey is not vendor-influenced or biased
      - Tablet-based quick surveys on awareness of CWE, 62443, subgroup activities, perceived benefits, what else could the SIG do, would you like to join
3. Additional recommendations
   1. Have some use case studies available to help demonstrate the purpose and benefit
   2. May be beneficial to pick a theme for messaging
   3. On the last day of the conference there is an ‘unsolicited response’ session where anyone can speak on stage for 5 minutes. We can take this opportunity to summarize the SIG activities ad surveys conducted at S4
   4. Pull-out posters highlighting subgroup activities and successes
   5. “Swag” such as stickers would be nice
   6. Informal dinner gathering for SIG members who attend