INL/CON-24-78143-Revision-0

Threats to DERs and Tools to Mitigate Them

May 2024

Megan Jordan Culler, Daniel Alan Ricci, Scott Mix

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-78143-Revision-0

Threats to DERs and Tools to Mitigate Them

Megan Jordan Culler, Daniel Alan Ricci, Scott Mix

May 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

May 15, 2024

Megan Culler
Infrastructure Security

Threats to DERs and Tools to Mitigate Them

Securing Solar for the Grid (S2G)

SEIA's Security and Reliability Forum

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

INL/CON-24-78143:

Recent Renewable Energy Cyber Attacks

- Increased renewable sector influence
- Primary U.S. adversaries
  - China
  - Russia
  - Iran
  - North Korea
- Development of more sophisticated attacks

Key Trends

- Exploitation of disclosed vulnerability
- Limited visibility and asset inventories
- Weak / hardcoded / plaintext storage of passwords
- OT systems are not the only target
- Denial-of-view and denial-of-service are common impacts
- OT security needs consideration of embedded IT systems
- Increased access to OT networks exposes a larger attack surface

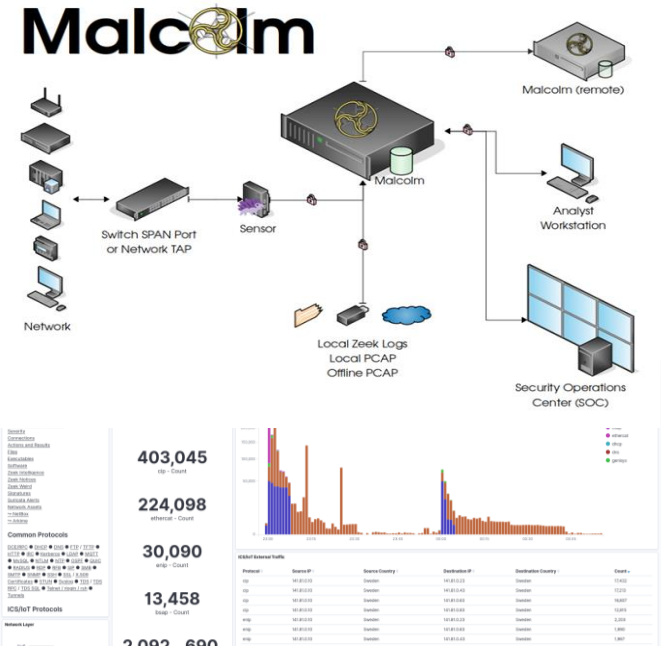
Vulnerability Exploitation in Clean Energy

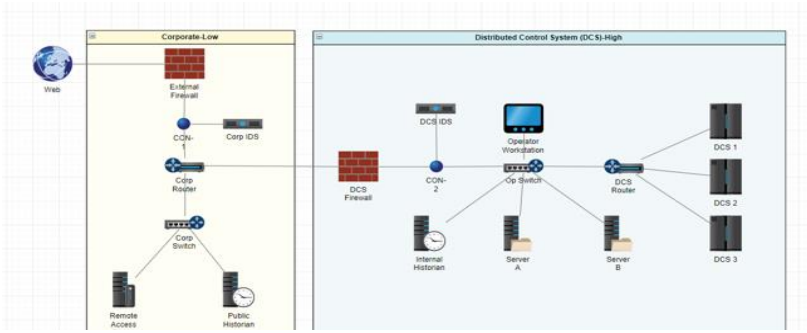
- Weak credentials
  - Weak requirements
  - Hard-coded credentials
  - Passwords derived from available information
  - Plaintext storage
  - Weak encryption or authentication
- Web page vulnerabilities allowing arbitrary code execution
- Cross-site scripting vulnerabilities
- Unauthorized access to sensitive files
- Web apps were the most targeted service type followed by remote management protocols
- 5 OT protocols were constantly targeted (Modbus was a third of attacks, DNP3 was about 18%)
- RATs and information stealers were the most popular malware types

- Make sure the fix is really a fix
- Best practices for storing sensitive information (i.e. passwords)
- Web portal security

Cyber SHIELD

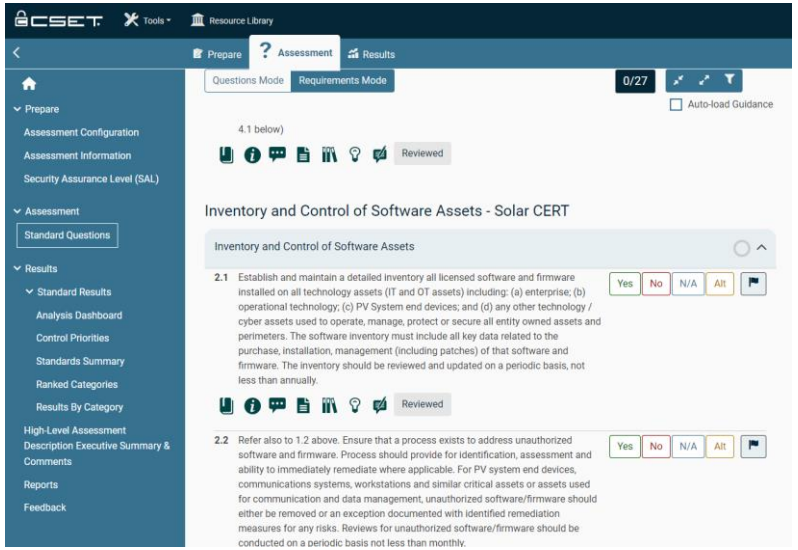
Cyber Security through Hardware Integration, Education, and Layered Defense





CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Network Diagram



Malcolm + Asset Interaction Analysis (AIA)

- ✓ OT Asset to business processes mapping
- ✓ Log collection & analysis tool suite
- ✓ Increases cyber maturity by adding visibility of assets and threats

CSET – Cyber Security Evaluation Tool

- ✓ Renewable Sector Focused Capability
- ✓ Tuned for renewable industry
- ✓ Identifies gaps in Cybersecurity process and procedures

S2D-C2M2

- Secure Design and Development Cybersecurity Capability Maturity Model – SD2-C2M2
  - **Guided self assessment** of a **manufacturer or developer internal processes** for design, development, manufacture, and support of Operational Technology products
  - Assess over **800 Practice Statements** for implementation as:
    - Not Implemented (**NI**), Informally Implemented (**II**), Documented (**D**), Formally Implemented (**FI**)
  - Each Practice Statement **assigned a maturity level** of:
    - MIL 1 – Basic; MIL 2 – Intermediate; MIL 3 – Advanced

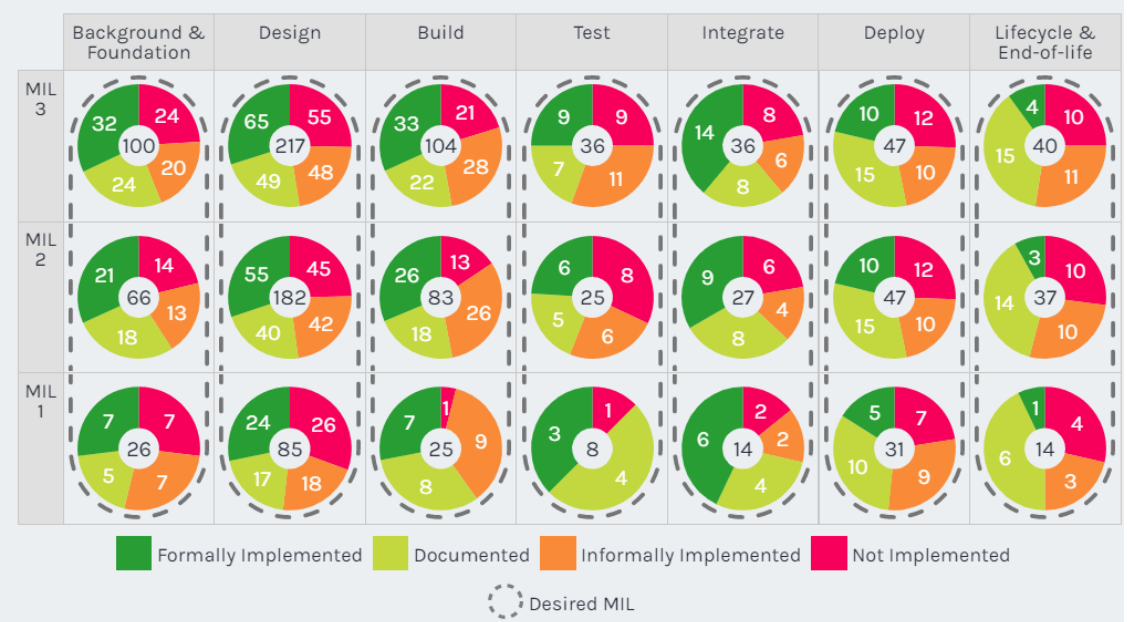
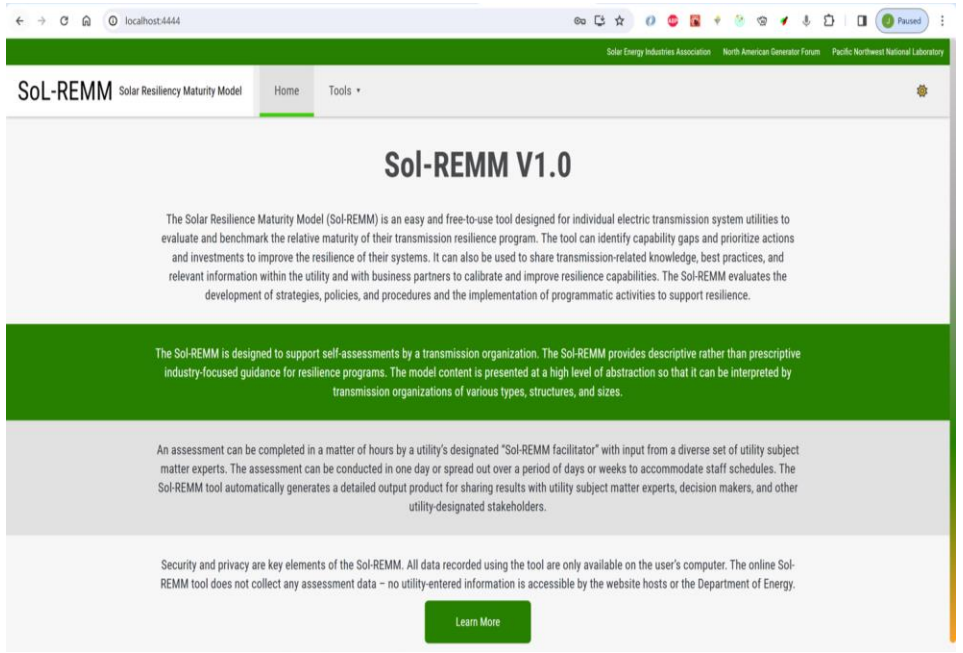


Figure 3: Pie Summary of Answer Input by MIL and Domain

MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to *Figure 5* in *Appendix B.*

Sol-ReMM

- Solar Power Resilience Maturity Model (Sol-ReMM)
  - Tool under development to assess **resilience of solar operator's cybersecurity operational practices**
    - Utility-scale, commercial, and industrial facilities
  - Includes Cybersecurity, Operational Security, and Physical Security
  - Self-evaluating the level of maturity of key components of their resilience program and **identifying programmatic improvements** to achieve resilience goals.
    - Management tool to determine desired maturity levels based on business drivers
  - **Compare assessments over time** to measure progress in addressing gaps
  - Modeled after existing maturity model tools (C2M2 tool suite),



Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.