INL/CON-24-77490-Revision-0

CyberSHIELD: Securing Renewable Energy Infrastructure Against Cyber Attacks 2024 Spring O&M Users Group Meeting

April 2024

Daniel Alan Ricci, Jake P Gentle

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-24-77490-Revision-0

CyberSHIELD: Securing Renewable Energy Infrastructure Against Cyber Attacks 2024 Spring O&M Users Group Meeting

Daniel Alan Ricci, Jake P Gentle

April 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

April 16, 2024

Jake Gentle
Portfolio Manager

Dan Ricci
Power Systems Security Engineer/Researcher

CyberSHIELD: Securing Renewable Energy Infrastructure Against Cyber Attacks

2024 Spring O&M Users Group Meeting

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

Idaho National Laboratory

INL/CON-24-77490

Jake P. Gentle

Portfolio Manager;
Staff Supervisor;
Secure Renewables and Grid Integration

About Me

- M.S., Measurement and Controls Engineering – Idaho State University
- B.S., Electrical Engineering – Idaho State University
- Professional Affiliations:
  - The International Council on Large Electric Systems (CIGRE)
  - Institute of Electrical and Electronics Engineers (IEEE)
    - IEEE Power & Engineering Society
    - IEEE Standards Association
    - IEEE Overhead Lines Subcommittee
  - Smart Electric Power Alliance
    - Cybersecurity Working Group Co-Chair

What I work on:

- Lead multiple programs focused on the secure integration of clean energy technologies including:
  - Cybersecurity roadmap for wind technologies
  - Wind and solar cybersecurity threat assessments
  - Resiliency and security of distributed energy technologies in microgrid applications
  - Deployable wind and solar energy technologies for defense applications
  - Enhanced methodologies of bare overhead line ratings, and facilitating the global advancement of transmission innovation
  - Verification and validation of Grid Enhancing Technologies like dynamic line rating

Dan Ricci

Technical leadership and Cybersecurity

About Me

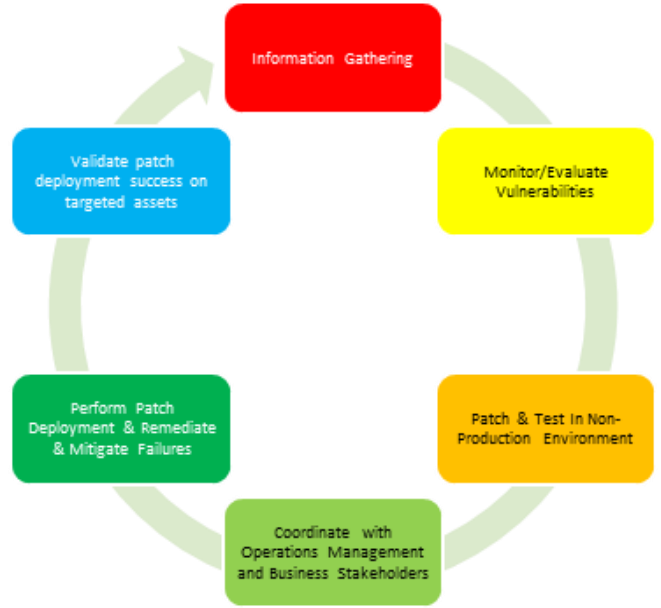
- 21-year Navy Veteran
- M.S. Computer Science from Lewis University
  - Focus in Cybersecurity Operations
- ISA99 Member for ISA/IEC 62443
- Remote to Idaho Falls facilities
- Local to Washington, D.C. DOE Facilities

What I work on:

- Cyber Defense Operation & Incident Response for Navy Afloat & Shore Networks
- Network Intelligence and Analysis in Support of DoD Cyber-enabled Operations
- Project Management of DoD Acquisition Category (ACAT) I & II Programs
- Commercial & DoD ICS/SCADA Cyber Risk Assessments for Building Automation, Energy Management, Medium-Power, Process Control, and Water Treatment Systems
- Design & implementation of Vulnerability Management programs for Manufacturing Execution Systems (MES)
- Building Cybersecurity & Physical Security Programs
- Founder of ICS Advisory Project to provide open-source data visualization of ICS vulnerabilities for small & medium size asset owners

EERE projects:

- WindSHIELD
- WaterSHIELD
- SolarSHIELD (S2G)
- Long Duration Energy Storage (LDES) Tiger Team



Recent Renewable Energy Cyber Attacks

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

Examples of Internal Threat Actors & Known Incidents

AOO	OEM	Utility	Maintainers	Integrators & other third-parties
• Disgruntled employee • Phishing victim	• (March 2022) Nordex SE hit by ransomware • (Nov. 2023) Vestas hit by ransomware	• (May 2023) Danish utilities compromised by coordinated attack, forcing islanded operations	• (2018) U.S. technician accidentally downloaded malware from hotel, later plugged into wind plant network and turbines stopped working.	• Software as a Service (SaaS) providers • Data collectors • Installers • Developers

Examples of External Threat Actors & Known Incidents

Benign external actors	Activist groups	Criminal organizations	Nation-state actors
• Landowners • Land tenants • Land staff • General public	• (2019) Anti-wind protestors in Hawaii disrupt construction • Rise in eco-terrorist attacks in Europe	• Ransomware groups affected 3 wind companies within 6 months • Exploiting known vulnerabilities • Ex: (2019) IPP sPower affected by denial-of-service on comms equipment	• Reconnaissance activity and advanced persistent threats (APTs) • Russian attack on SATCOM infrastructure affected 5800 turbines • Chinese espionage targeting offshore wind in Strait of Taiwan and India

Attack Vectors

Physical Access

- Physical device access
  - Takes time to respond to intrusions

Transient Access

- Authorized external devices
- Infected technician equipment

Cyber Access

- VPN exploitation
- Wireless
- Temporary access points
- Pivoting from enterprise network

Impacts

- Asset health and damage
- Loss of remote monitoring
- Power system stability

Critical failures can lead to severe physical damage.

- Ancillary services
- Power dispatch
- Reputational damage

Cyber SHIELD Overview: Program Initiatives

Cyber ***S****ecurity through* ***H****ardware* ***I****ntegration,* ***E****ducation, and* ***L****ayered* ***D****efense:*

Industry Impact

Cyber SHIELD is an impactful program (people/tools) for industry and support the “raise the floor” objectives, the initial focus has been deployment across renewable sectors (Wind/Water/Solar) with three initiative options for participating engagement partners.

- Cyber Program Assessment
- Architecture Basics
- Asset Interaction Analysis

Each initiative is supported leveraging DOE-INL tools + INL team members to integrate with asset owners/operators existing operations.

Program Evolution

This, like most INL tools and resource program is a constantly improving iterative process that builds upon successes and setbacks, but dependent on industry engagements

Measuring Success

Measuring the success of this effort is truly dictated by the ability to have an impact within industry and drive investment by renewable sector in cybersecurity as a priority.

*Cybersecurity Evaluation and Risk Tool – (CERT)

INL Cyber SHIELD-INL CERT

INL Cybersecurity Evaluation and Risk Tool

Key Challenges Targeted

Provide insight and guidance for better informed, broader, risk-based investment decisions for renewable asset owners/operators IT and OT cybersecurity programs through Cybersecurity Evaluation and Risk Tool (CERT)

Key features:

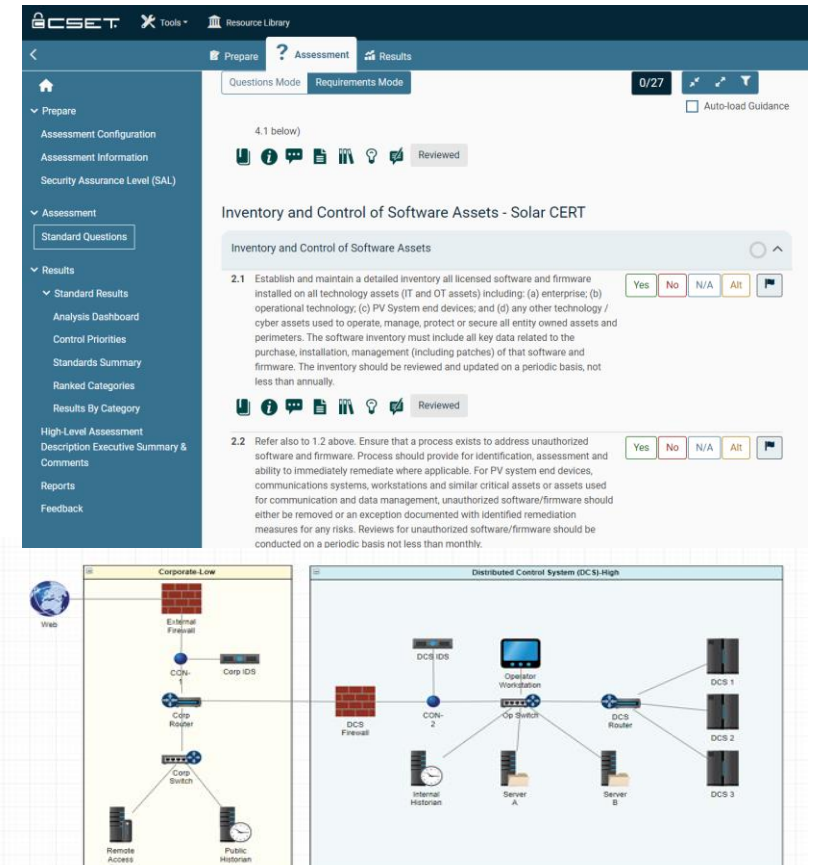
- ✓ Renewable Sector Focused Capability
- ✓ Open-Source and tuned for renewable industry
- ✓ Identifies gaps in Cybersecurity process and procedures

Top 3 Benefits:

1. Guided cybersecurity assessment and risk-based report
2. Map network architecture within the assessment to control areas to help identify or validate asset owner/operator cyber posture
3. Support cyber program and resource planning to more quickly meet asset owner/operator maturity objectives by providing document templates and process flows to integrate with existing organization configuration management, maintenance, incident response/recovery procedures

CERT
Program Assessment

CERT
Architecture Basics



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Network Diagram

SHIELD–Malcolm

Asset Interaction Analysis

Key Challenges Targeted

Provide asset owners/operations with initial baseline of assets linked to operational technology (OT) and business processes. Detect and visualize threats and vulnerability identification/analysis for renewable OT environments.

Key features:

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

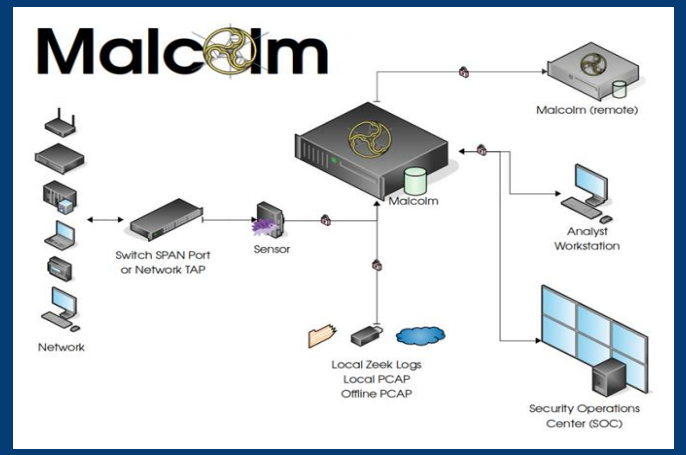
Top 3 Benefits:

1. Know assets, view of asset risk levels based on devices, protocols, misconfigurations.
2. Identify potential attacks, vulnerabilities, and active exploits impacting assets/devices.
3. Increases network visibility to make informed decisions and improve operational reliability.

Asset Interaction Analysis

Malcolm

Malcolm Key Benefits & Deployment Overview



Threat Monitoring and Analytics

SHIELD Tools Links

- CSET Renewable as its own branch: cset-renewables-download.inl.gov
- Malcolm site for industry to interact with dashboards and view functionality: https://training.malcolm.fyi/dashboards
- Malcolm GitHub Site for industry to download and install on local hardware or virtual machine: https://github.com/cisagov/Malcolm
- CyberSHIELD Industry Engagement Website: https://resilience.inl.gov/inlcybershield/
- Email for specific program contacts: CYBERSHIELD@INL.GOV

Thank you!