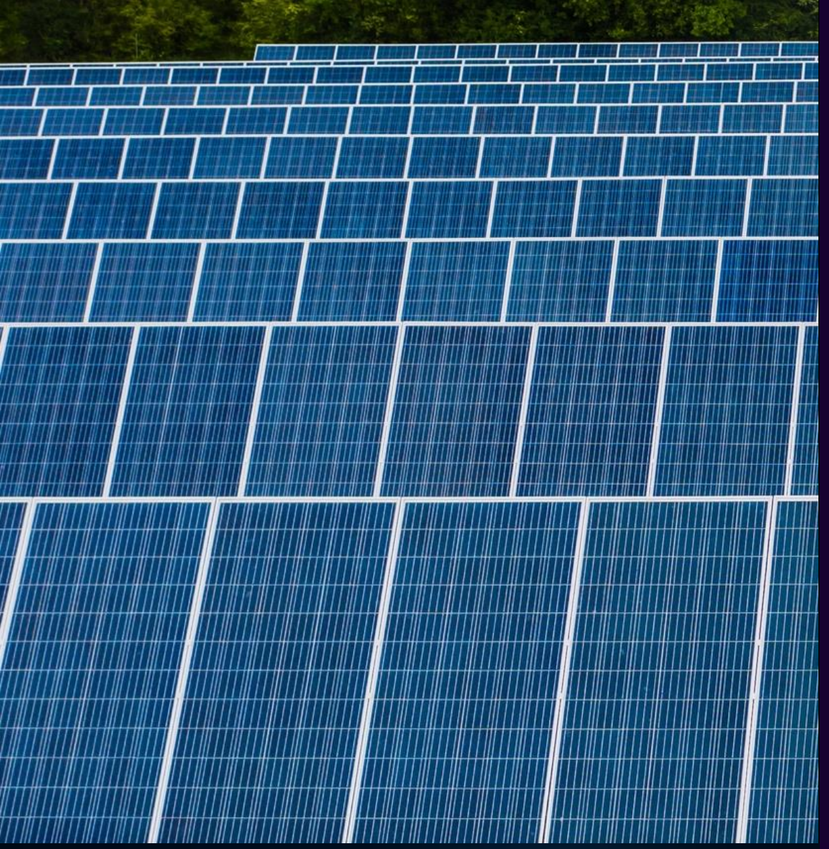


STEMPRISE

CYBERSECURITY

RE+ 25 SEIA Codes and Standards Symposium
November 2025

Marissa Morales-Rodriguez, Ph.D
Founder and Technology Security Strategist
STEMPRISE

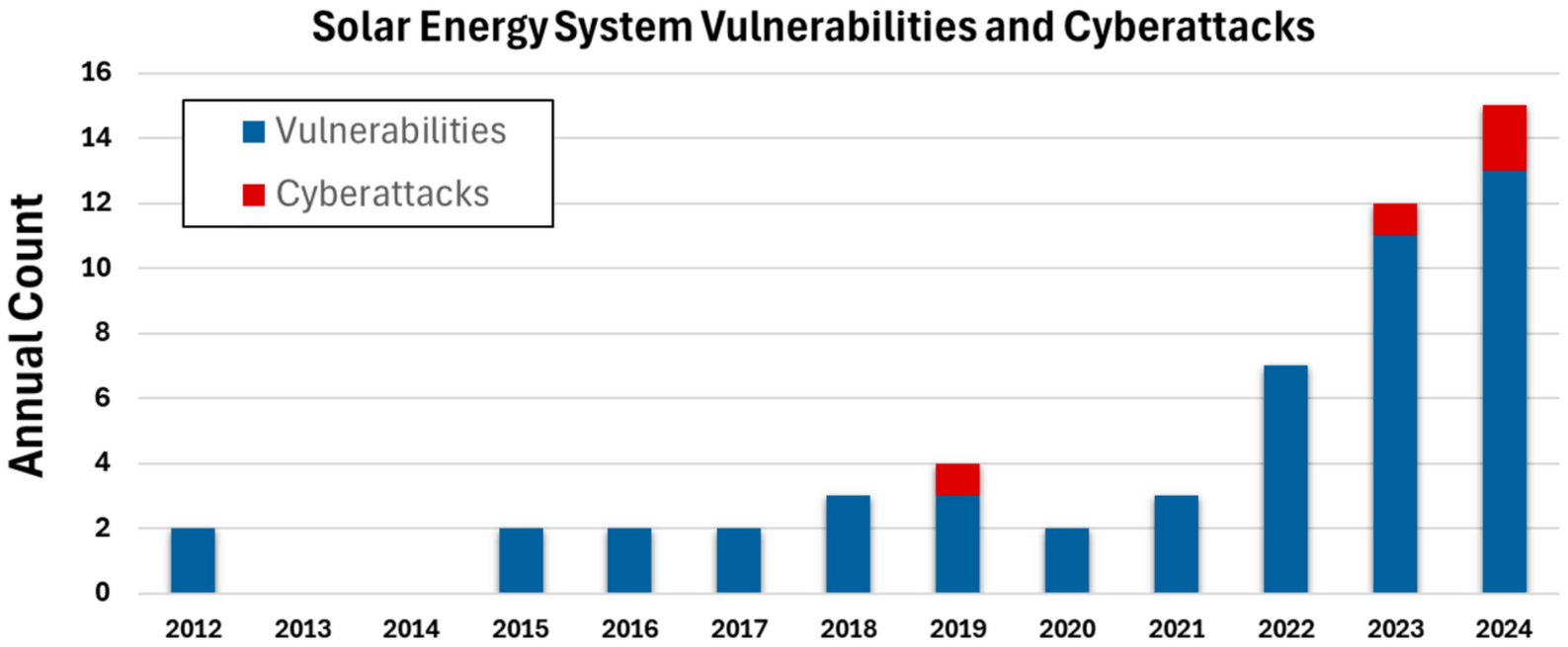
INTRODUCTION

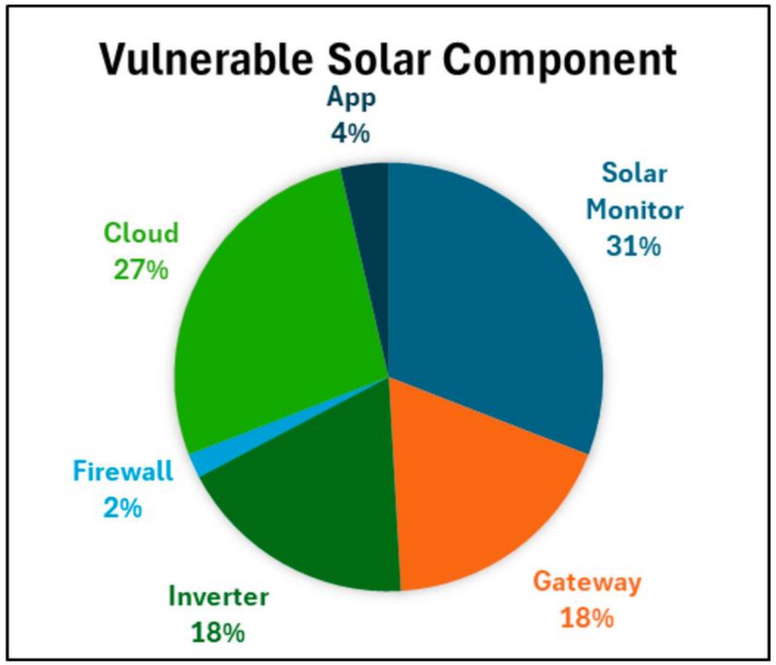
Why Cybersecurity Matters

Cybersecurity is critical for distributed energy resources because they rely on digital tools to operate, with a decentralized nature directly integrated into the electric grid. An orchestrated attack on inverters could disrupt grid operations and cause cascading failures. Adopting and implementing standards, codes and best practices is essential to maintaining reliability and avoiding critical failures.

- **Ensure System Reliability**
- **Protect Grid Integrity**
- **Build Trust & Compliance**

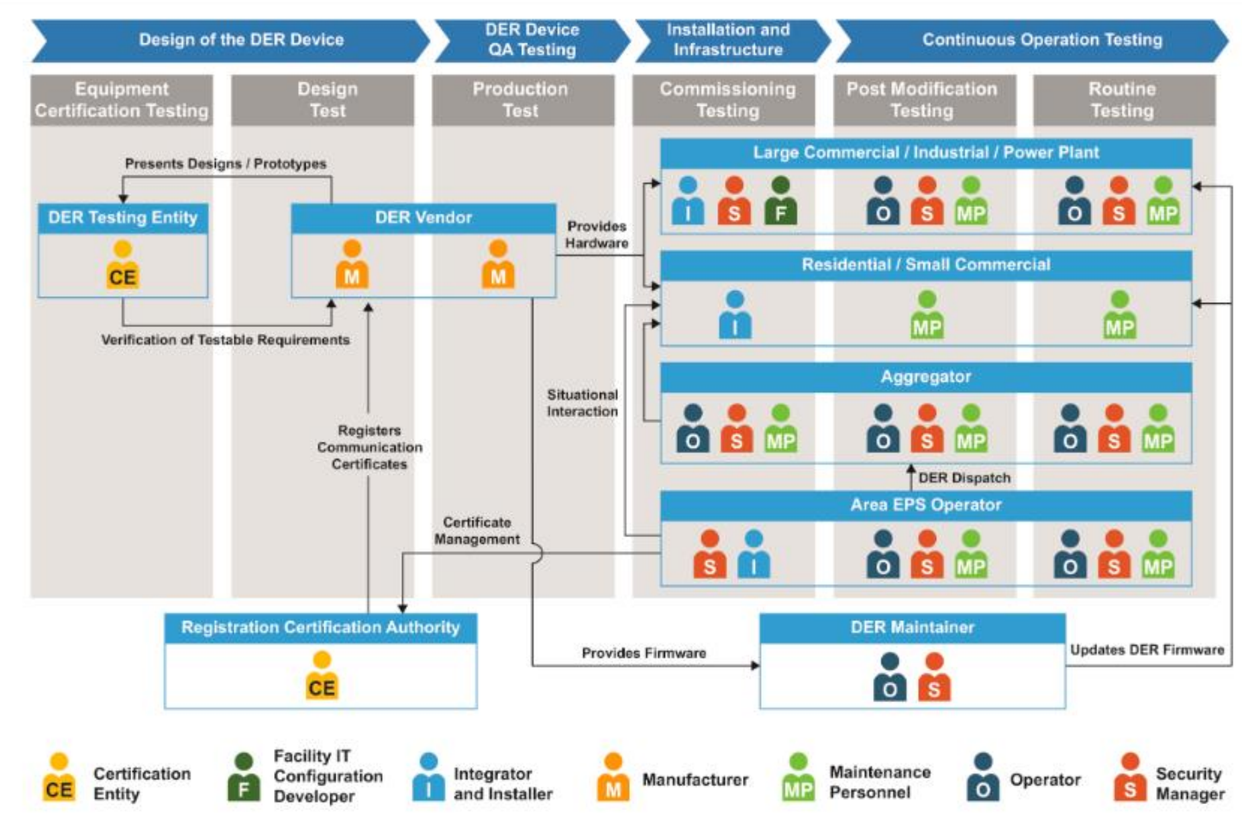
SOLAR THREAT LANDSCAPE

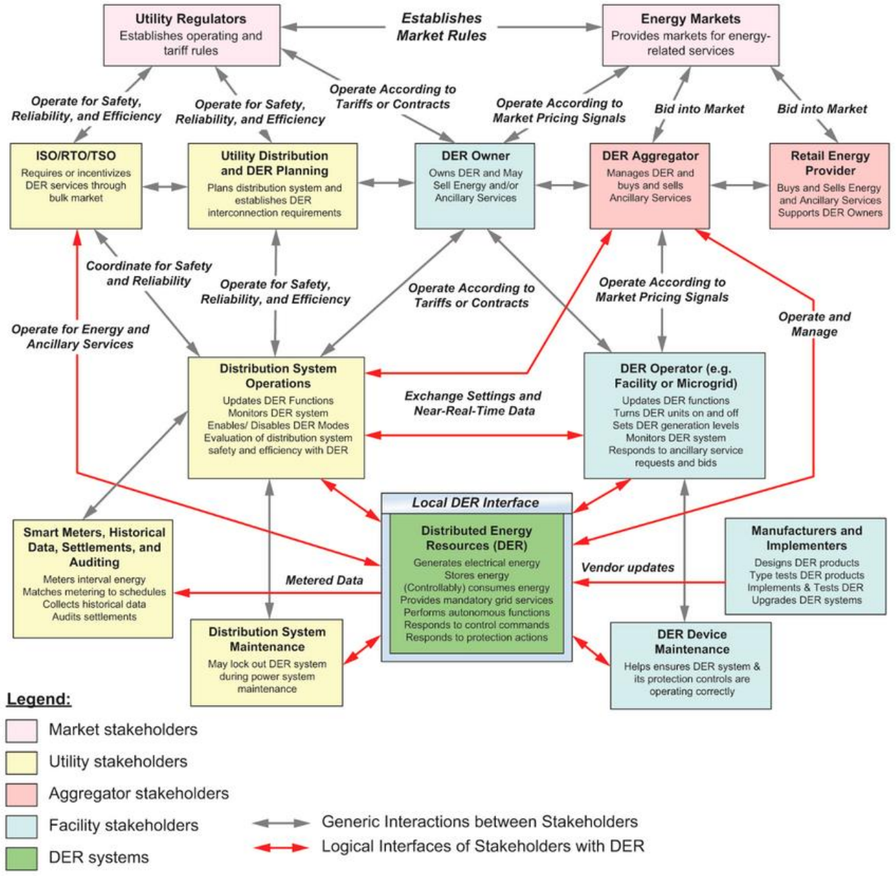




Source: Public History of Solar Energy Cyberattacks and Vulnerabilities, DER Security, 2024

DER STAKEHOLDERS





Source: IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems, 2023

CYBERSECURITY

Standards, Codes and Best Practices

Stakeholder	Mandatory (Enforced)	Voluntary / Guidance
Utilities	NERC CIP, state DER interconnection rules (CA Rule 21, HI), FERC orders, contracts	NIST CSF, DOE CIE, IEEE 1547.3 (end-to-end security, protocol hardening, joint IR/DR)
Vendors (OEMs)	Where required UL 2900 (software), inverter certification, utility/developer contracts	IEC 62443, IEC 62351 (IEC 61850), IEEE 1547.3 secure comms (DNP3-SA, TLS for 2030.5), secure-by-design, SBOMs, emerging UL 2941* (DER cybersecurity),
Developers	IEEE 1547 (as adopted), utility/financier/insurer contracts	DOE CIE design integration, IEEE 1547.3 supply chain posture, NIST CSF, insurance best practices
EPC Firms	Utility/developer contract requirements	DOE CIE, IEC 62443-3-3, IEEE 1547.3 commissioning practices
Operators (O&M)	Service contracts with utilities/asset owners	IEEE 1547.3 Respond/Recover playbooks; NIST CSF monitoring; CIE resilience practices
Aggregators / VPPs	Market participation & utility program agreements	IEEE 1547.3: secure cloud integration (TLS, DNP3-SA); strong RBAC; near-real-time alerts; DOE CIE; emerging UL 2941* compliance in device fleets
Regulators / PUCs	NERC CIP, state DER mandates	Can adopt IEEE 1547.3 & DOE CIE into DER interconnection standards
Investors / Insurers	Financing/insurance contracts	Can require UL 2941* device compliance; NIST CSF, IEC 62443, DOE CIE in due diligence
End Users	Utility interconnection agreements (IEEE 1547)	Cyber hygiene, Secure defaults (MFA, updates), IEEE 1547.3 awareness, DOE CIE resilience mindset

Notes:
This table is not exhaustive. Some standards are mandatory today (NERC CIP, state interconnection rules, contracts), while others are voluntary guidance or emerging practices (IEEE 1547.3, DOE CIE, UL 2941).
*UL2941 is under development

TAKEAWAYS

Cyber threats will continue to rise. The security of DERs and utility assets is a shared responsibility. To ensure system reliability and increased resilience, each stakeholder must adopt necessary standards and best practices.

Ensuring Compliance

Follow guidelines to protect systems. Provide continuous training to stay up to date with evolving standards and guides.

Harmonization

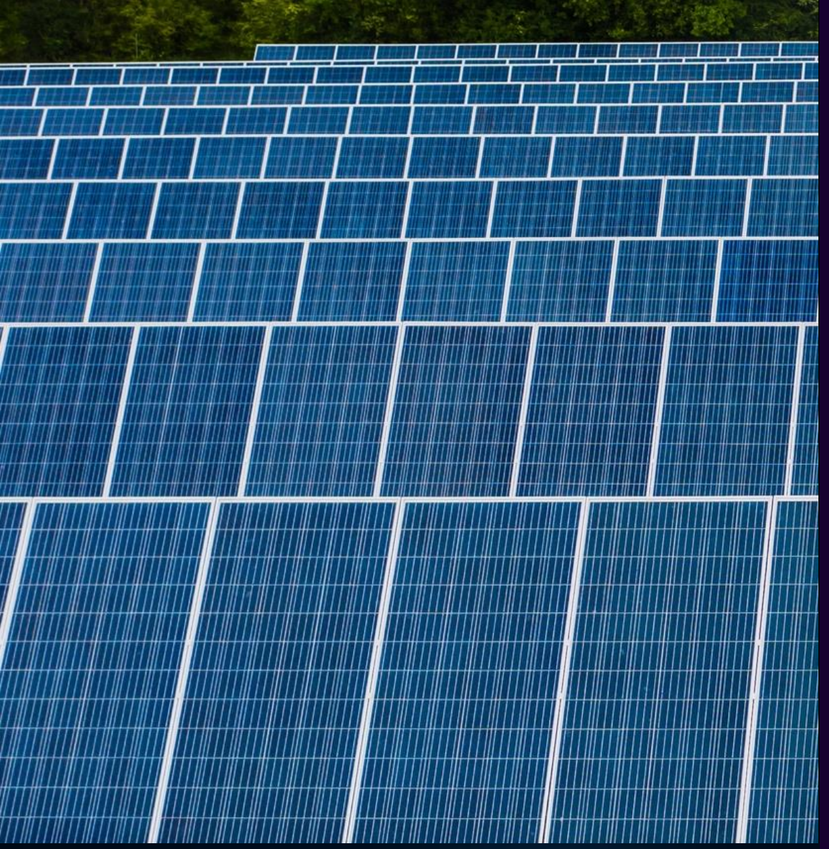
Standards, codes and best practices must be harmonized to avoid conflicting requirements.

Security by Design

Addressing security at the design phase will increase system protection.

Threat Visibility

Stay informed on the latest vulnerabilities and mitigation strategies.



STEMPRISE

THANK YOU!

www.stemprise.com

marissa.morales@stemprise.com

Marissa Morales-Rodriguez, Ph.D
Founder and Technology Security Strategist
STEMPRISE