INL/CON-24-79387-Revision-0

Assessment and Coordination of DER Cybersecurity Standards

July 2024

Megan Jordan Culler, Chelsea Neely, Danish Saleem, Jenna deCastro

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-24-79387-Revision-0

Assessment and Coordination of DER Cybersecurity Standards

Megan Jordan Culler, Chelsea Neely, Danish Saleem, Jenna deCastro

July 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

Assessment and Coordination of DER Cybersecurity Standards

DOE Grid Modernization Initiative

Megan Culler | Idaho National Laboratory

INL/CON-24-79387

What is a distributed energy resource (DER)?

What is a distributed energy resource (DER)?

For us: DERs are any energy resource connected at the distribution level at 20MW and under.

DER

- Demand response
- Smart devices
- EVs
- Diesel generator




IBR

- Rooftop solar
- Distributed wind
- Battery storage
- Fuel Cell
- EV chargers

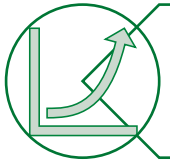



- Utility Scale wind
- Utility Scale solar
- Offshore wind
- Utility battery storage
- Fuel Cell H2

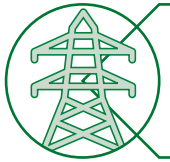



Need for DER Cybersecurity Standards

Why do we care about this niche topic?

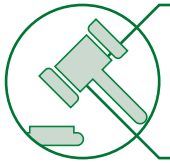


Rapidly developing technology

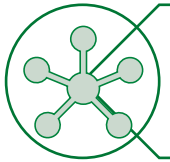


Increasing reliance on DERs for grid stability

Diverse and complex stakeholder landscape



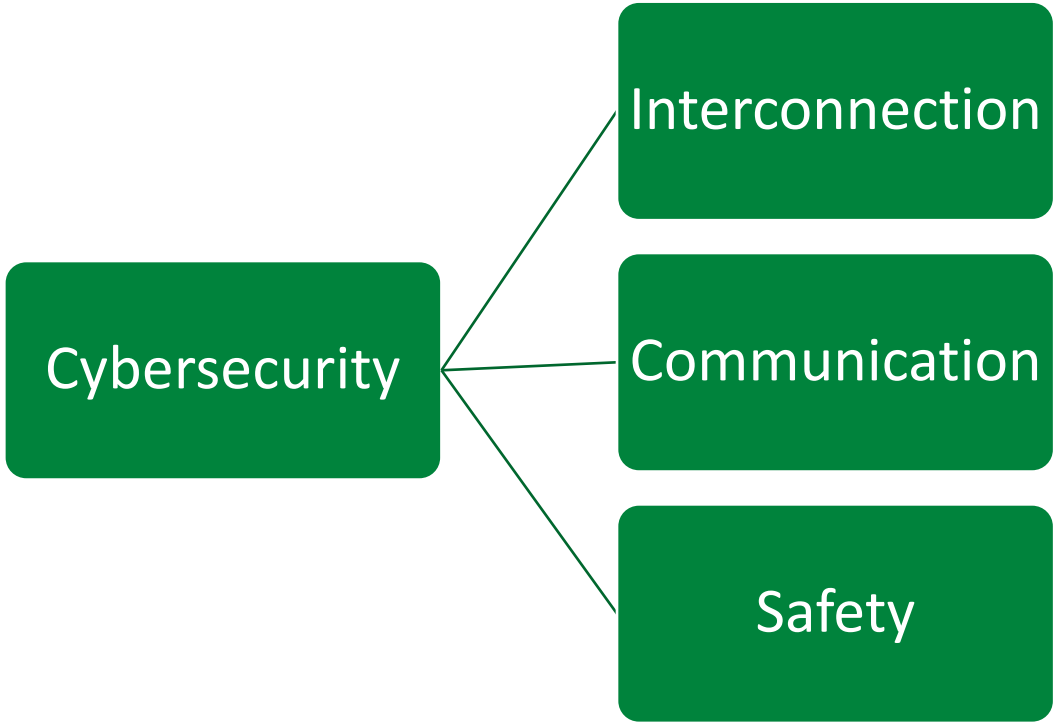
Not in reach of federal regulation



Distributed and digital go hand-in-hand

DER Cybersecurity Standards

- Few standards directly address cybersecurity for DERs
- Some broader cybersecurity standards apply
- Adjacent areas may include cybersecurity requirements



DER Standards Library

Key questions to answer with the library:

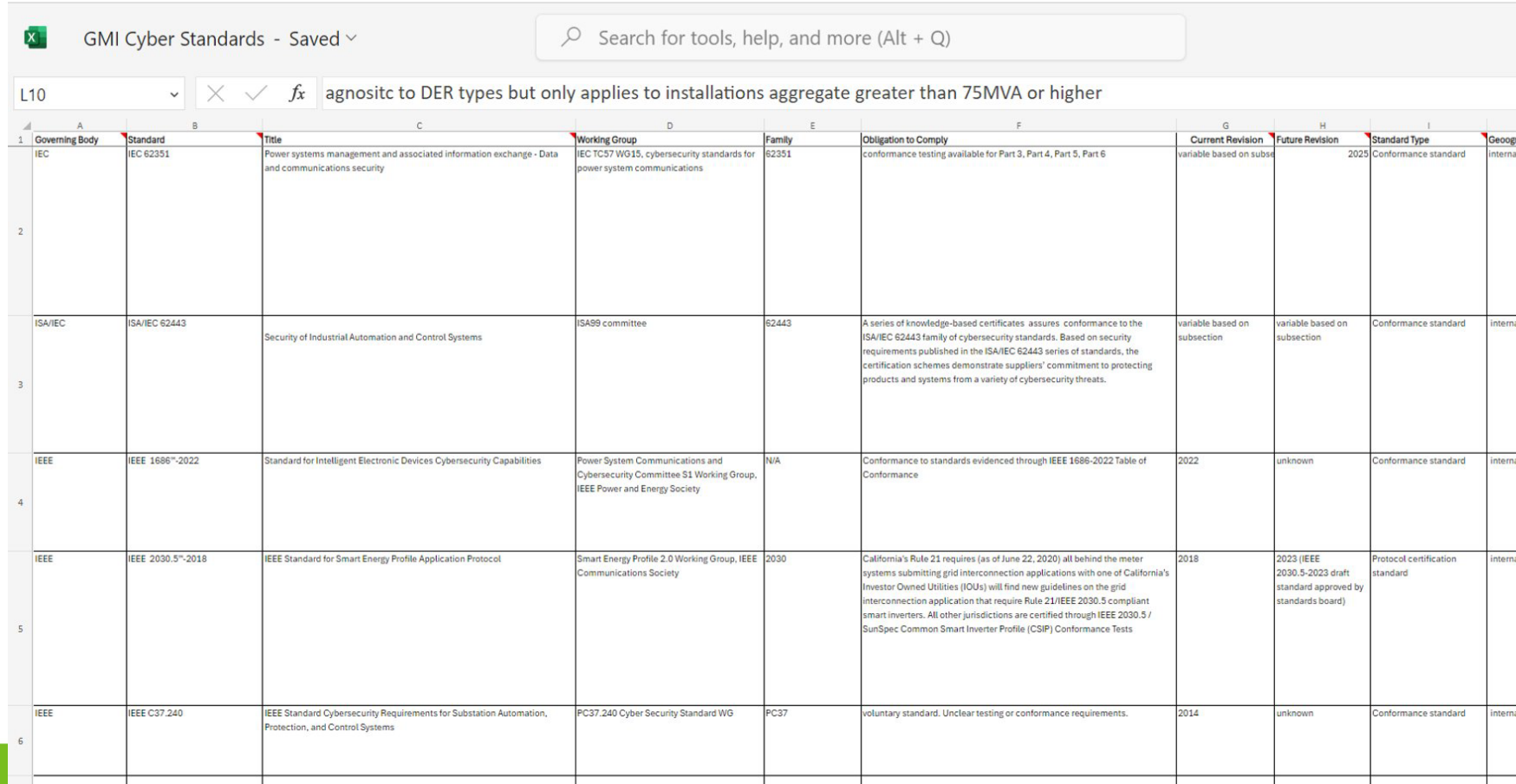
- What do they apply to?
- How are they commonly used?
- Where are they commonly used?
- How do they tie to one another?

Cybersecurity	Interconnection	Communications	Safety
IEEE 1547.3	IEEE 1547	IEC 61850	UL 1741
UL 2941	IEEE P2800	IEEE 1815 (DNP3)	UL 9540
NIST SP 800-82	IEC TR 62351	Modbus	IEC 62109-1
IEEE P2658	CA Rule 21	IEEE 2030.5	IEEE 2030.2
ISO/SAE 21434	Hawaii Electric Rule 14H	REST	
		Open ADR	

Sample of DER Cyber Standards Database + Data Dictionary

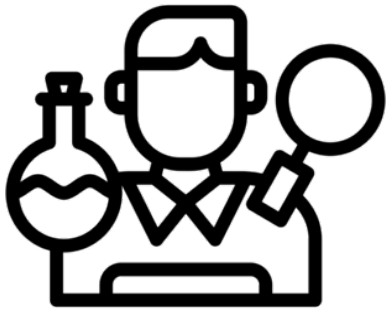
Categories were chosen based on relevancy to the user of the library and are meant to add value to the standards library.

- Standard Name/Number
- Issuing Organization
- Last updated
- Next release expected
- Standard Type
- Function
- Applicability to DER Type
- Encryption type
- Device Authentication
- Key Exchange Algorithms
- Specific Requirement
- Criteria for applicability
- Nationality of Standard
- Compliance Notes
- Source/Link
- Keywords



Governing Body	Standard	Title	Working Group	Family	Obligation to Comply	Current Revision	Future Revision	Standard Type	Geoog
IEC	IEC 62351	Power systems management and associated information exchange - Data and communications security	IEC TC57 WG15, cybersecurity standards for power system communications	62351	conformance testing available for Part 3, Part 4, Part 5, Part 6	variable based on subse	2025	Conformance standard	interna
ISA/IEC	ISA/IEC 62443	Security of Industrial Automation and Control Systems	ISA99 committee	62443	A series of knowledge-based certificates assures conformance to the ISA/IEC 62443 family of cybersecurity standards. Based on security requirements published in the ISA/IEC 62443 series of standards, the certification schemes demonstrate suppliers' commitment to protecting products and systems from a variety of cybersecurity threats.	variable based on subsection	variable based on subsection	Conformance standard	interna
IEEE	IEEE 1686™-2022	Standard for Intelligent Electronic Devices Cybersecurity Capabilities	Power System Communications and Cybersecurity Committee S1 Working Group, IEEE Power and Energy Society	N/A	Conformance to standards evidenced through IEEE 1686-2022 Table of Conformance	2022	unknown	Conformance standard	interna
IEEE	IEEE 2030.5™-2018	IEEE Standard for Smart Energy Profile Application Protocol	Smart Energy Profile 2.0 Working Group, IEEE Communications Society	2030	California's Rule 21 requires (as of June 22, 2020) all behind the meter systems submitting grid interconnection applications with one of California's Investor Owned Utilities (IOUs) will find new guidelines on the grid interconnection application that require Rule 21/IEEE 2030.5 compliant smart inverters. All other jurisdictions are certified through IEEE 2030.5 / SunSpec Common Smart Inverter Profile (CSIP) Conformance Tests	2018	2023 (IEEE 2030.5-2023 draft standard approved by standards board)	Protocol certification standard	interna
IEEE	IEEE C37.240	IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems	PC37.240 Cyber Security Standard WG	PC37	voluntary standard. Unclear testing or conformance requirements.	2014	unknown	Conformance standard	interna

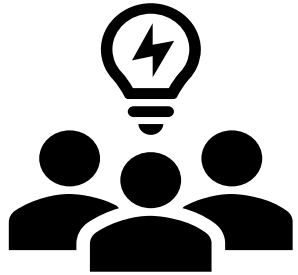
User groups for the Standards Library



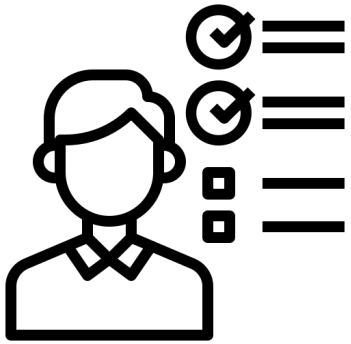
Lab researchers

Government/DOE

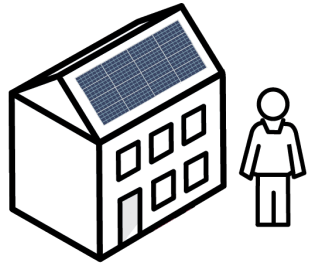
Manufacturers



SDOs



Regulators



Asset owner/ operator; utility

Developer/integrators/contractors

User stories for the Standards Library (so far)

As an SDO/manufacturer/developer I want to figure out what cybersecurity standards and requirements apply to DER assets.

As a library user I want know when a standard last updated so I can choose the right standard and participate in future revisions.

As an SDO, I want to understand what other SDOs are creating to avoid duplication and find opportunity to address security gaps.

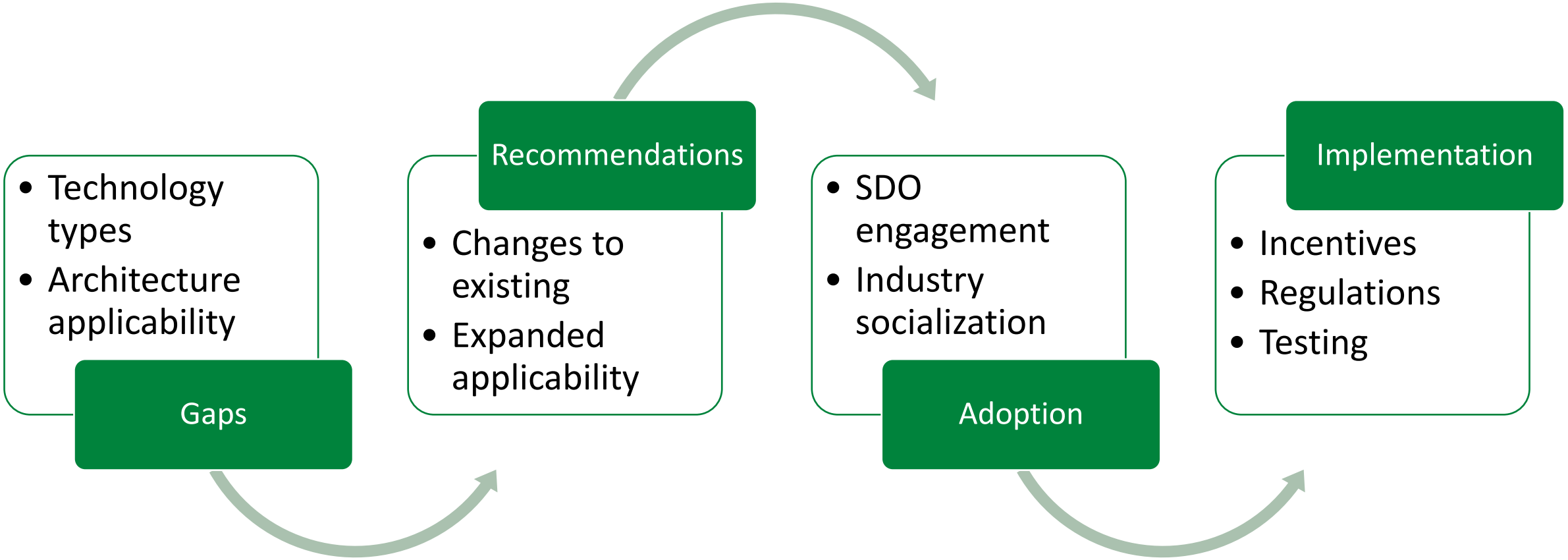
As a manufacturer, I want to understand the details of the standards ecosystem so I can decide what level of security I should provide.

As a manufacturer/asset owner, I want to understand my options or tradeoffs in design when comparing different standards so that I can optimize resources.

As a lab/DOE/regulator I want to understand the nexus to cybersecurity in related standards (communications, interconnection, safety, etc) to harmonize requirements and advance DER security.

As DOE/lab I want to...

What does standards harmonization look like?

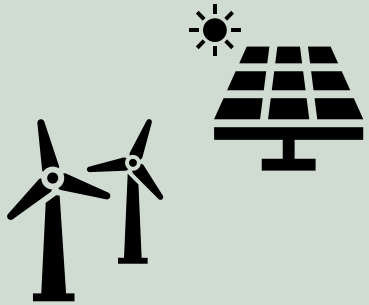


Gaps in standards coverage

Using the library to inform a harmonization strategy

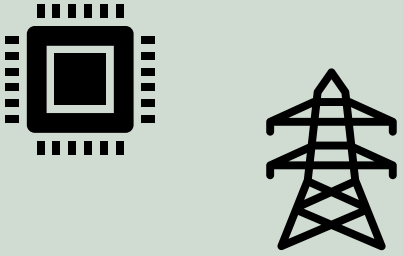
Technology adoption

- e.g. wind commonly uses IEC 61850, but solar commonly uses Modbus



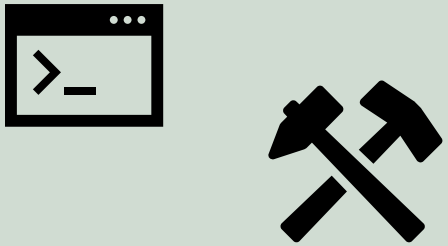
Architecture applicability

- e.g. device standards and interconnection standards may leave gaps in local communications network design



Technology development

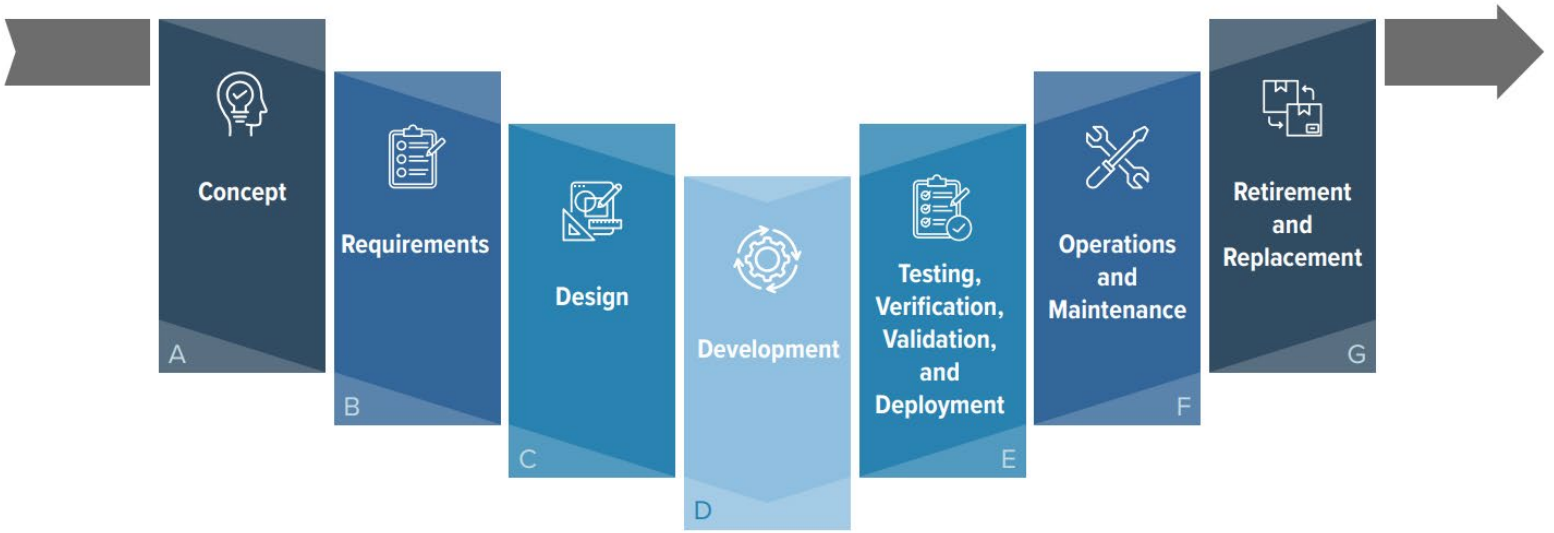
- Software development
- Device design
- Supply chain
- Manufacturing



Cyber-Informed Engineering (CIE)

Identifying recommendations for addressing gaps

- CIE deepens the cybersecurity protections for critical infrastructure by providing guidance to allow defenses from cyber attack to be engineered in from the early design lifecycle of infrastructure systems.
  - Mitigate worst consequences of cyber-attack
  - Proactively secure existing infrastructure
  - Uses design decisions and engineering controls to prioritize defenses



CIE systems engineering lifecycle model

Cyber-Informed Engineering (CIE)

- Standards can be used to inform mitigations associated with many of the CIE design principles
- Some controls need to be customized to the deployment

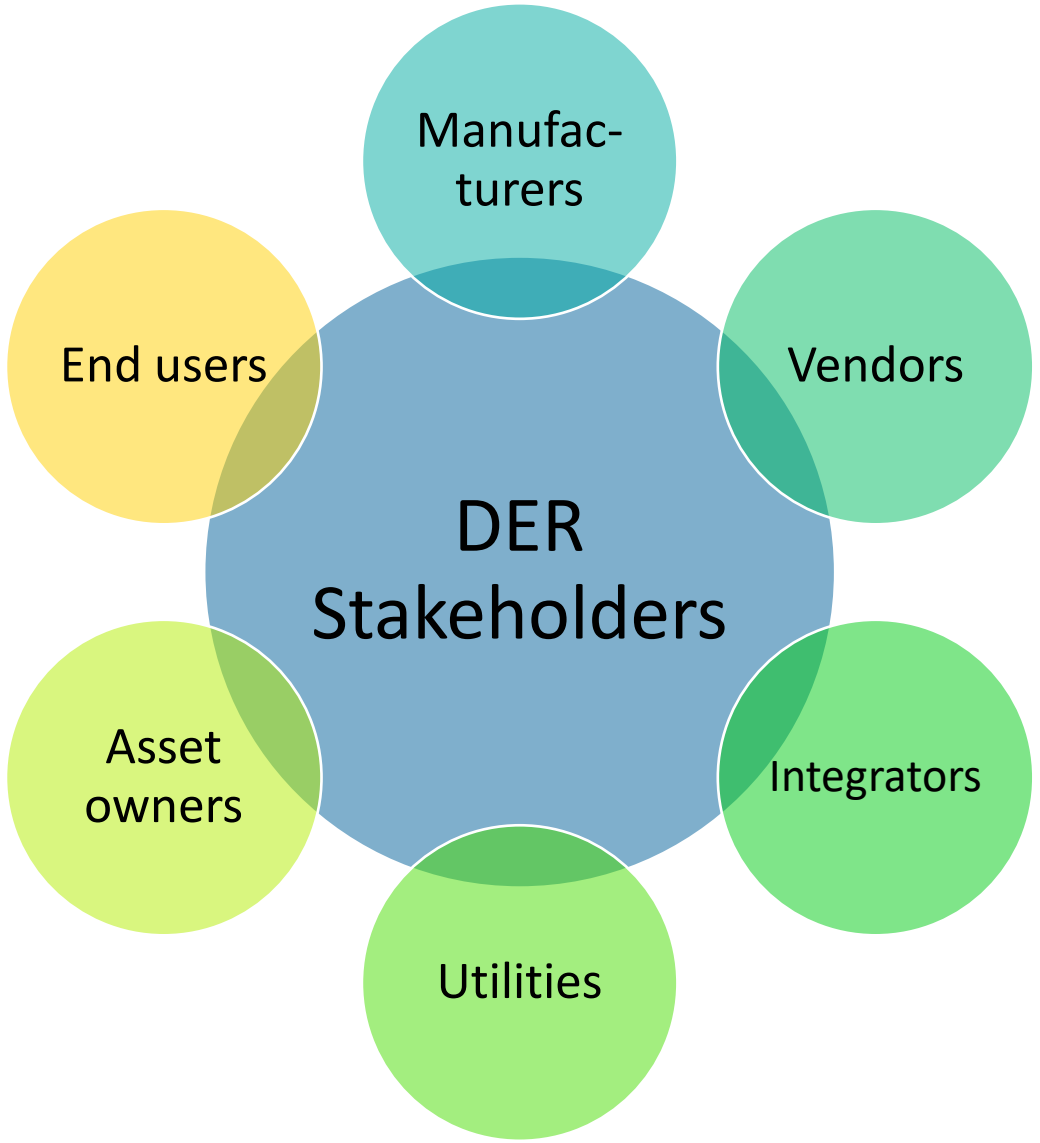
CIE Design Principles

- Consequence focused-design
- Engineered controls
- Secure information architecture
- Design simplification
- Layered defenses
- Active defense
- Interdependency evaluation
- Digital asset awareness
- Cyber-secure supply chain controls
- Planned resilience
- Engineered information control
- Organizational culture

Stakeholder Roles

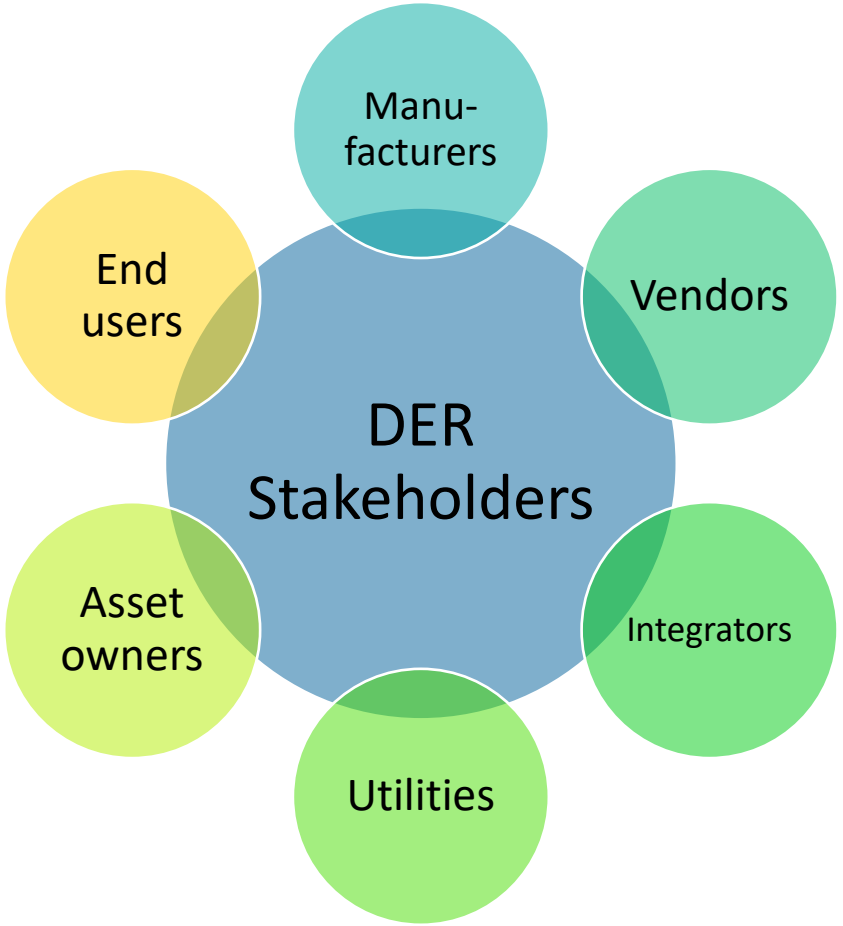
Adoption of standards

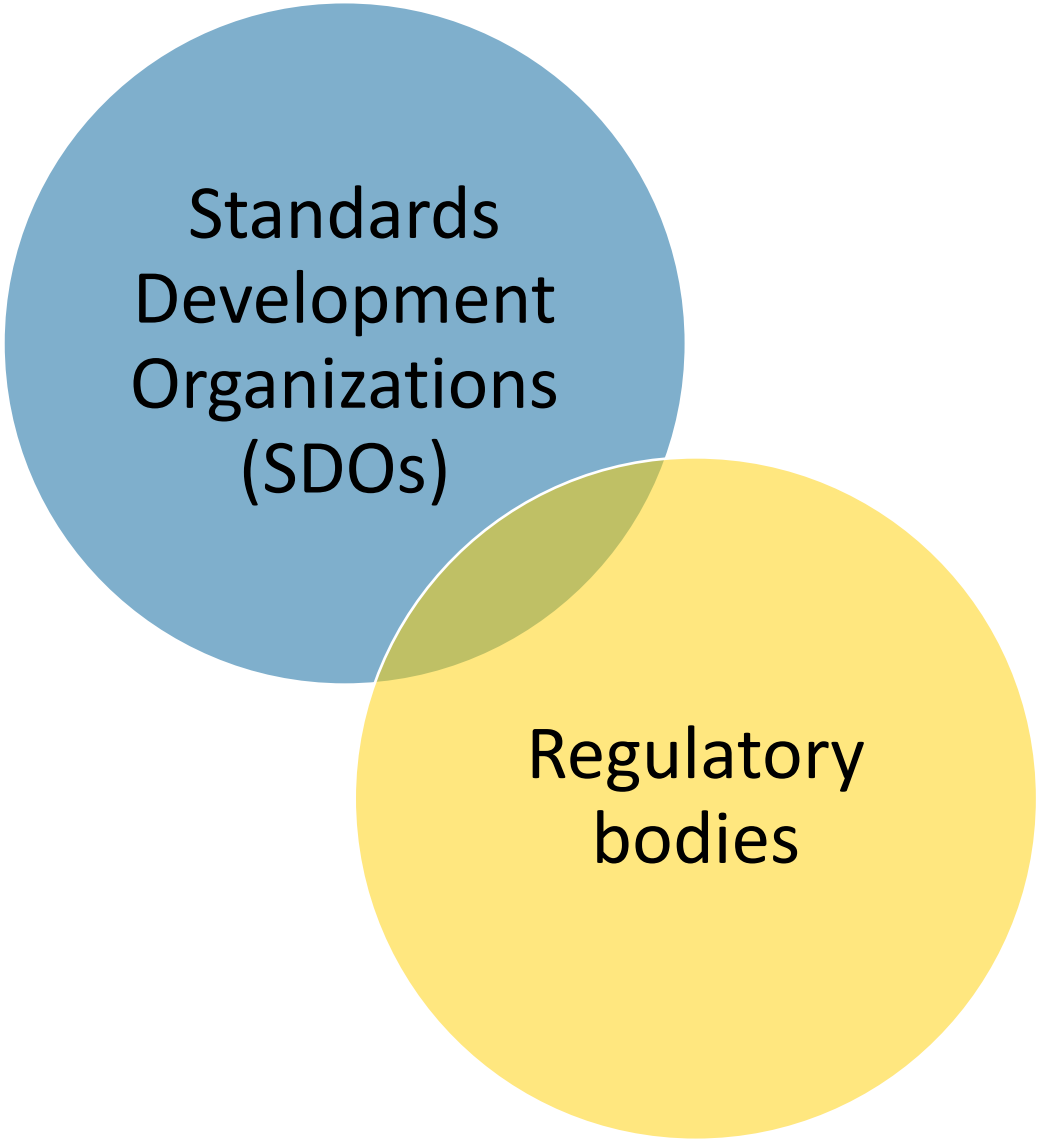
- Roles and responsibilities vary across the DER ecosystem.
- Not all instances may have all stakeholders involved.
- Are responsibilities appropriately tied to assumed risk?



Stakeholder roles

Implementation of standards





Thank you

Megan Culler
megan.culler@inl.gov