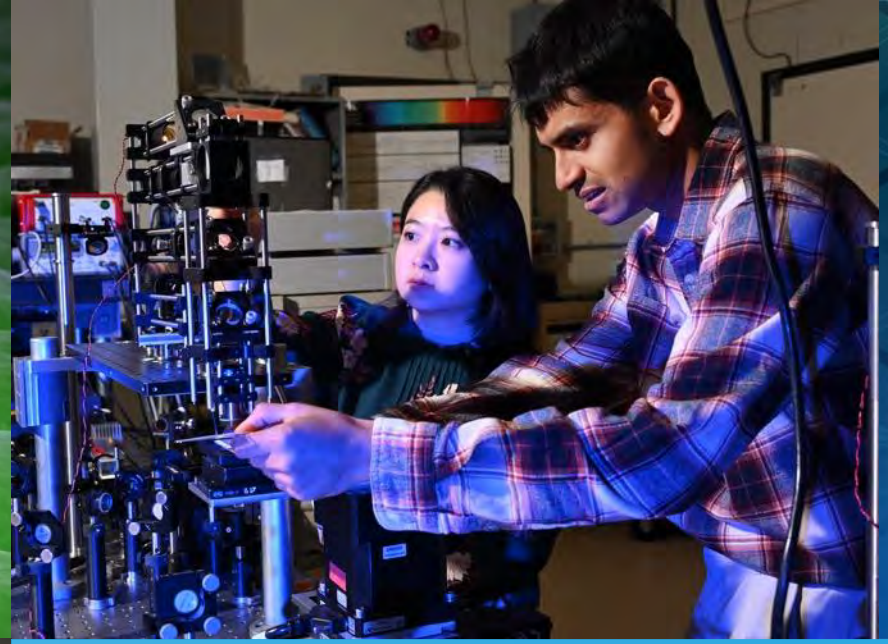


April 1, 2026

Dr. Jonathan Tacke

Center for Securing Digital Energy Technology

Securing Every Link in the Supply Chain

Supply Chain Security for Battery Energy Storage Systems

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

Idaho National Laboratory

Agenda

Grid modernization landscape and growth of IBRs

- Interconnected challenges
- Digital energy landscape
- Use of BESS to solve modernization challenges
- Deployment Trends

Threat landscape

- Threats
- Vulnerabilities
- Consequences

Supply chain security: BESS deep dive

- Domestic supply challenges
- Supply chain security concerns
- Risk-based mitigation approach

Grid Modernization Landscape and Growth of IBRs

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

Idaho National Laboratory

The National Security Challenge

Behind the headlines and accelerating investments …

The U.S. digital supply chain is not built or sourced with secure design in mind.

Lack of unified standards for cybersecurity of emerging energy technology.

The rapid growth in digital energy players has resulted in a burgeoning industrial base that is not well-understood.

Converging Paradigms & Needs

Why Now

- Broad digital transformations in technology
- Digital technologies and data hold tremendous potential
- It is not just about changing the sources of energy, but also revolutionizing the entire energy infrastructure to be more resilient, controllable, and agile
- This security paradigm must be built into the new system
- By elevating cybersecurity practices and improving overall system integrity, we strive for a system that can survive major events and thrive in enabling affordable and secure supply of energy

Interconnected Challenges of Grid modernization

Digital Energy Transformation

- Dispatchability & Increasing Base Load

- AI in action

- Wide-scale sensing for optimized performance

- Increased control over energy use, consumer choice and bills

- Better management of existing assets

- Predictive maintenance for equipment

- More accurate forecasts

- Better supply chain management

Overall Threat Landscape in Energy

Notable Energy Sector Cyber Incidents in 2024-2025

(January) Schneider Electric Ransomware

(February) EV charging infrastructure compromised

(April) Purported attack on US energy HMIs and related water/waste-water system

(May) Duke Energy Florida experienced data breach

(September) Alleged attack on PV monitoring

(December) RECOPE ransomware

(December) Electrica ransomware

(January) Iowa electric utility lost sensitive personal info in ransomware

(February) Varta ransomware

(March) Hydroelectric dam in France reportedly attacked

(May) Solar devices used in bank fraud

(August) Halliburton data breach

(November) Deye inverters reportedly disabled in U.S.

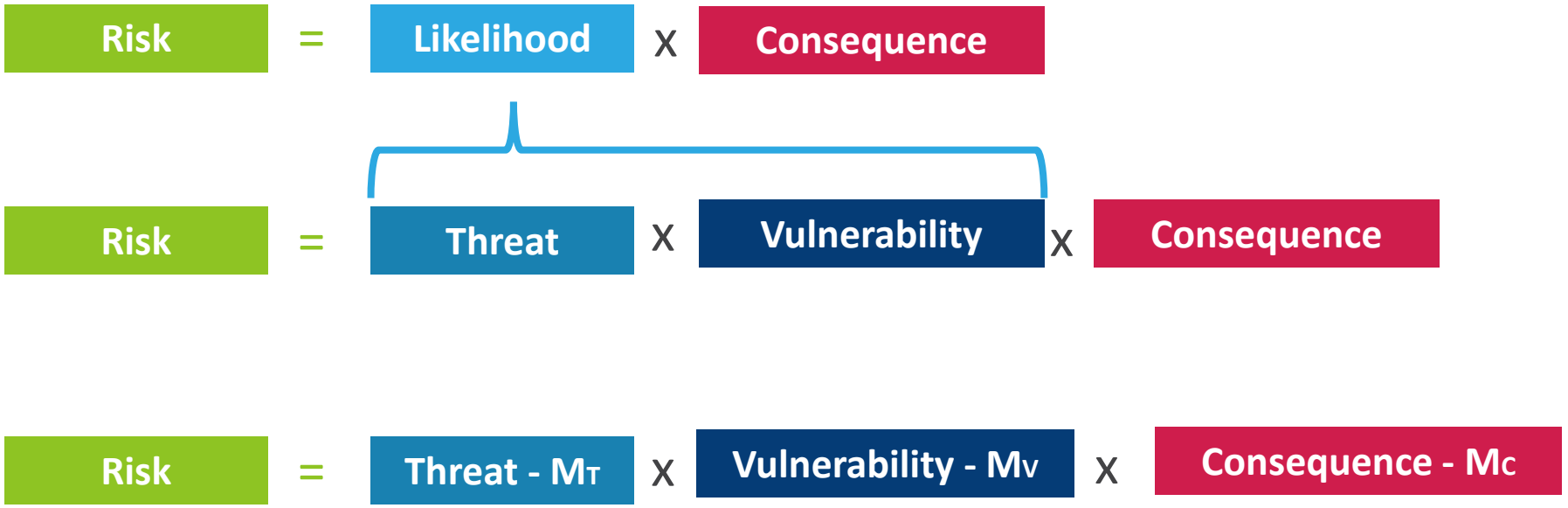
(December-January) ENGlobal ransomware

Government warnings on expanding threats to emerging energy sources

- Agencies in Denmark, Germany, India, Australia, and the U.S. have highlighted importance

https://innovationorigins.com/en/emergency-bell-for-cybersecurity-of-dutch-solar-energy/
https://www.rechargenews.com/wind/germany-plans-cyber-security-scrutiny-of-every-wind-turbine-says-top-energy-official/2-1-1715184
https://topsectorenergie.nl/nl/kennisbank/maatregelen-cyberveiligheid-zonpv/
https://www.bankinfosecurity.com/australia-focuses-on-threat-chinese-attack-on-solar-power-a-23395
https://industrialcyber.co/threats-attacks/fbi-warns-of-increased-cyber-threats-to-expanding-us-renewable-energy-sector/

Risk Management Architecture: Intro to Threats, Vulnerabilities and Consequence



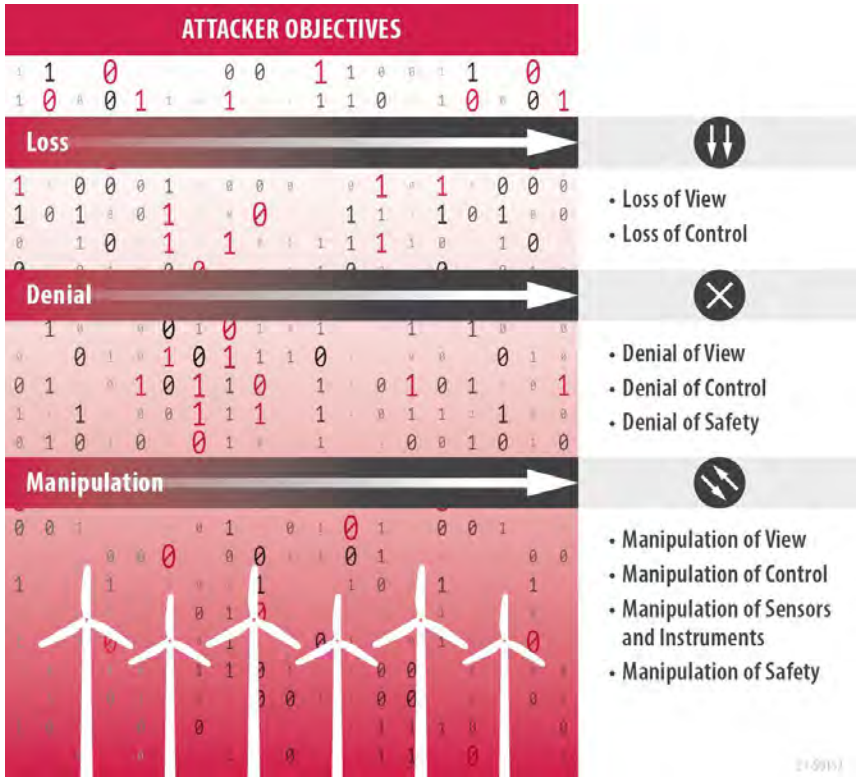
- Risk management comes from mitigating each element individually
- Cyber resilience measures can apply to any element

Risk Management Architecture: Cyber Threats

Threat = **Intent** x **Capability** x **Opportunity**

- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding
- **Opportunity:** Access to a target

Capability	Example
Hacker	Spower Firewall DoS attacker
Insider	AWEA technician
Organized group	Ransomware gangs
Hostile nation-state or terrorist	Nation-state sponsored APT



Attack Vectors

Physical Access

- Physical device access
  - Takes time to respond to intrusions

Transient Access

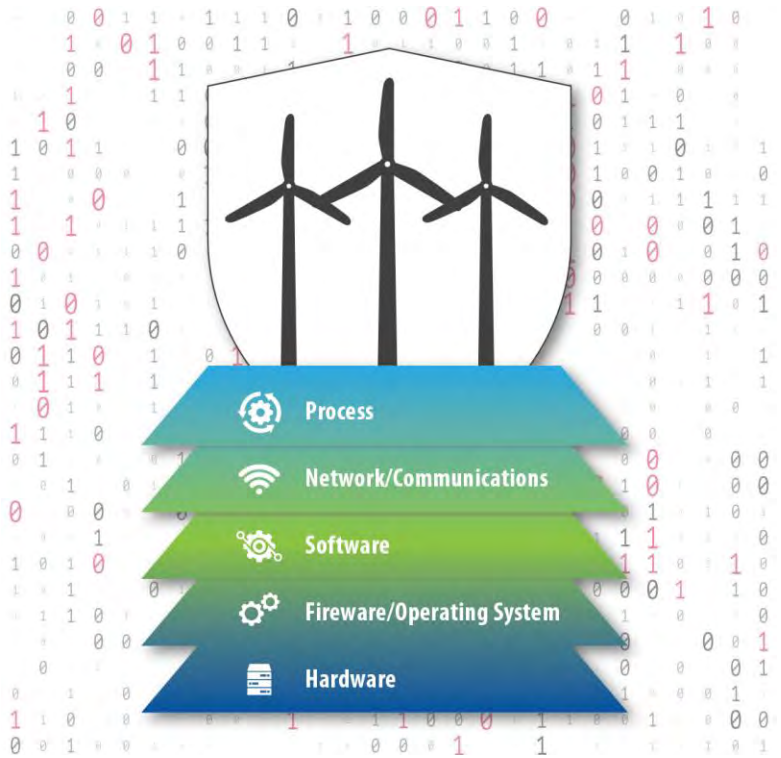
- Authorized external devices
- Infected technician equipment

Cyber Access

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

Risk Management Architecture: Vulnerabilities

- **What is a Vulnerability:** a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system
- May be a flaw in either design or implementation
- Can occur at any layer of the system



Trends in Targeting and Vulnerability Exploitation in Digital Energy Infrastructure

- 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
- Proof-of-concept for exploits of known vulnerabilities can be posted on many forums, including video walk throughs and source code
- Cybersecurity research firms look for exposed systems for devices with known vulnerabilities
  - Sometimes it is possible to discern whether devices are patched or updated

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

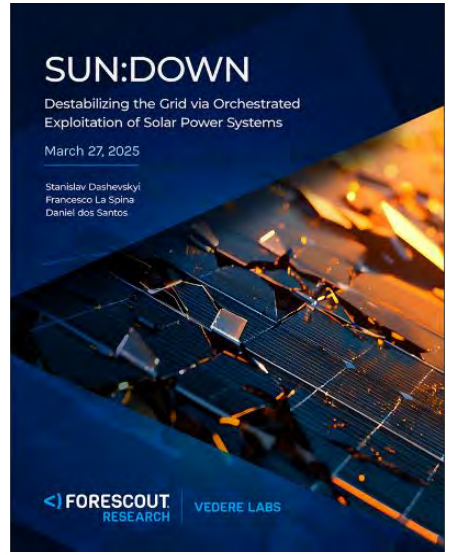
Solar App Vulnerabilities – Weak Passwords

- Enphase Envoy
  - CVE-2020-25754: Custom PAM module uses password derived from the MD5 hash of the username and serial number. Serial number can be retrieved by an unauthenticated remote user.
  - CVE-2020-25753: Default admin password for certain versions set to the last 6 digits of the serial number, which can be retrieved by an unauthenticated remote user.
  - CVE-2020-25752: Hardcoded web-panel login passwords for the installer and Enphase accounts. Users are unable to change these passwords
  - CVE-2019-7676: Weak password vulnerability discovered in Envoy R3
- Contec SolarView
  - CVE-2023-27512 use of hard-coded credentials may allow remote authenticated attacker to login with administrative privilege
- Fronius
  - CVE-2019-19228: Solar inverter allows attackers to bypass authentication because the password is stored in a plaintext file

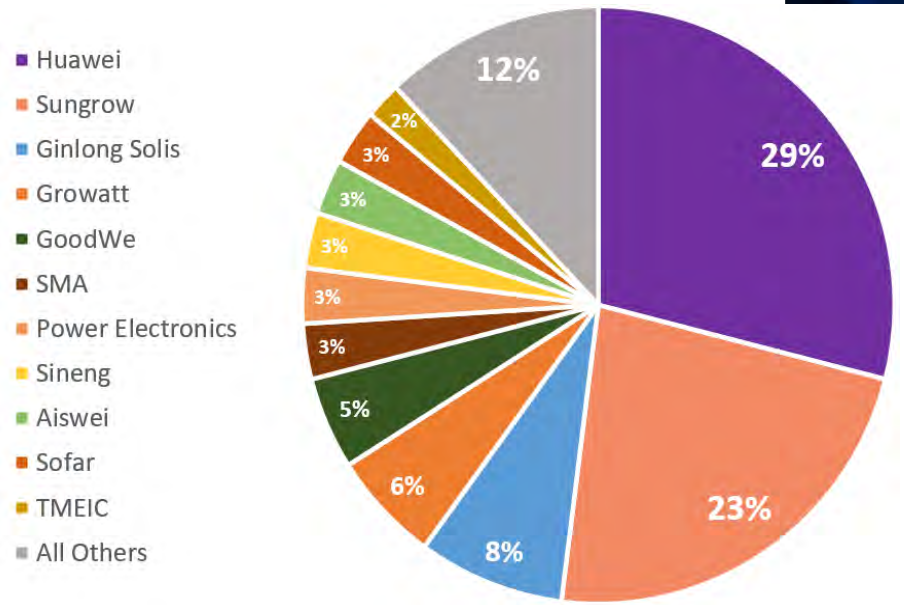
Takeaways for Inverters:

- Require strong passwords and store them correctly

SUN:DOWN – Inverter Vulnerabilities



- Forescout's SUN:DOWN report highlighted critical vulnerabilities within SMA, Growatt, and Sungrow inverters
- SMA, Sungrow and Growatt provide a combined total of **approximately 32%** of **global inverters**
- Vulnerability disclosure summary:
  - 46 Total CVEs: Growatt accounted for 30 of these vulnerabilities,
    SMA for 1, and Sungrow for 15.
  - 39 of the vulnerabilities were related to web applications and
    Android applications (Mobile and web applications are not just used for residential inverters)
  - 7 of the vulnerabilities were related to an SMA gateway

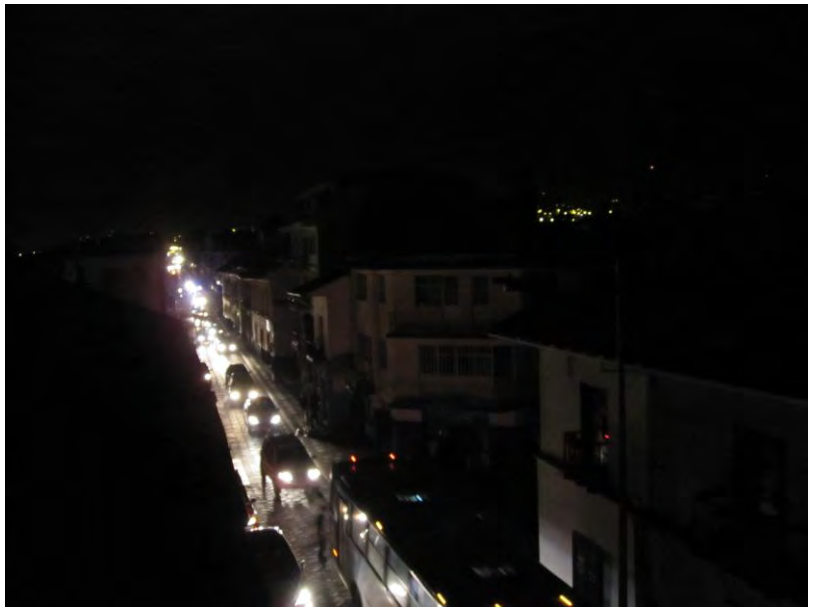


Source: UnivDatos Market Insights | US Solar Inverter Market (2023-2030)

https://www.forescout.com/research-labs/sun-down-a-dark-side-to-solar-energy-grids/

Consequences – Aggregation & Impact

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



- Volatge stability
- Power dispatch
- Reputational damage

Potential Impacts of Attacks on Batteries - Asset Health, Site Damage, Environment

- Site (uncontrolled) Fire
- Loss of preventative/proactive disconnect
- Damage to Battery Components & Site
- Damage to Battery Site Capacity
- Environmental Discharge / Damage

Likelihood vs Difficulty point: Single Site - Medium, Mass Event – Low L Very High D

Potential Impacts of Attacks on Batteries - Loss of visibility

- Loss of status monitoring
- Loss of capacity monitoring
- Loss of activation or inactivation control
- Loss of physical access alarms

Viasat

- Attack against the ViaSat KA-SAT network
  - Russian state-sponsored actors in attack coordinated with invasion of Ukraine
- DoS caused by an attacker exploiting a VPN appliance misconfiguration
  - Allowed for rewriting of flash on customer modems
  - Required replacement devices
- Caused loss of remote monitoring of 5,800 ENERCON wind turbines

Likelihood vs Difficulty point: Mass Event – high L, Med D

Potential Impacts of Attacks on Batteries - Electric Grid/Bulk Impact

- Loss of Control (doing the opposite)
- Power system stability & ancillary services
- Emergency Dispatch failure/loss of load
- Reputational damage
- Uncontrolled re-energization
- Loss of life
- Financial Loss

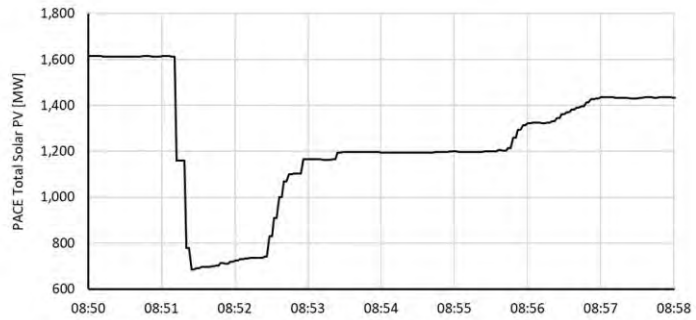


Figure I.2: PACE BPS-Connected Solar PV during Disturbance

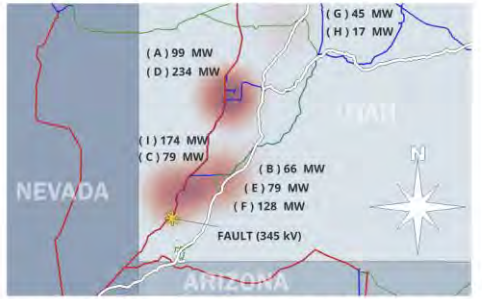


Figure I.3: Map of Fault Location and Affected Solar PV Facilities

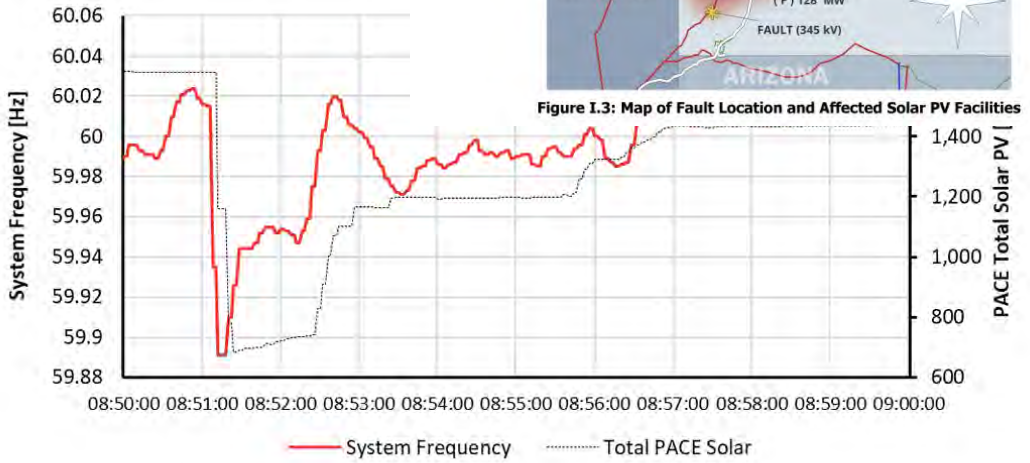


Figure I.4: WECC System Frequency

Likelihood vs Difficulty point: Mass Event – Low L, Very High D

Overall Attack Trends

- Notable increase in attacks targeting solar industry and renewable sector at large
- No strong evidence that renewables being targeted because they're renewables or for operational impact
  - Active exploitation of vulnerabilities just uses devices for computing power for other attacks
- Ransomware and data breaches continue to be some of most common attacks.
  - Ransomware remains a top cyber threat across sectors
  - Targets include utilities, manufacturers, and service providers
  - Median payment in energy, oil & gas, and utilities ransomware events was $2.5M (Sophos)
- Operational impact seen most as denial-of-service.
  - Level of impact depends on stakeholder affected and criticality of assets.
- Attacks targeting third parties (OEMs, maintenance, etc.)
- APT activity detected before OT attack executed

Key Challenges with Growth

- Aggregators are growing but **lack** clear **oversight**
  - Aggregators typically outside of NERC CIP scope (especially when behind-the-meter)
  - DERs lack standardized cybersecurity baselines
- Little to no network monitoring within DERs
- Lack of federal-level incident reporting for DER cyber events
- No mandatory software checks for aggregator services
- Vulnerability management is often ignored
  - Partially because its difficult for utilities and aggregators to keep up
- Third-party and foreign component dependencies
- Patch Management
  - Inverter vendors rarely push timely patches; customers often unaware of risks

Supply Chain Security for BESS: Deep Dive

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

Idaho National Laboratory

Criticality of Battery Energy Storage Systems

Rapid Response

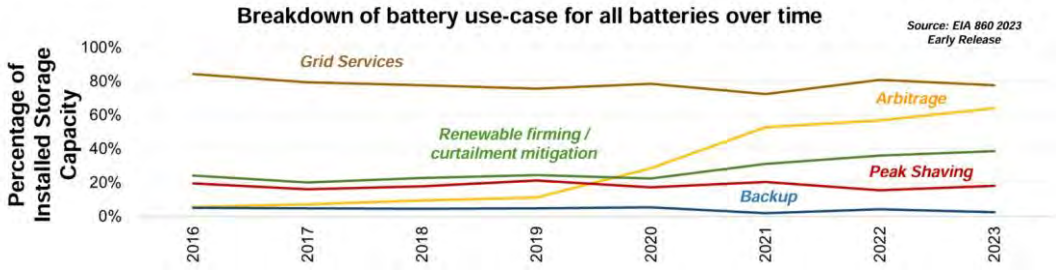
- Fast ramping that matches natural gas in performance
- Avoided bulk outages through emergency dispatch
- Doubling installed capacity year over year

Reliable

- HI – KES BESS project can serve 17% of Oahu's demand for 3 hours at peak load
- 17%+ of CA load is served by BESS
- TX and CA are 72% of deployed BESS, 62% of BESS in development

Resilient

- ~9GW in CA
- ~6 GW in TX
- ~108 MW in HI (2020)
- Doubling in 2024
- Expected to double again in 2025



Emerging energy markets are transforming…

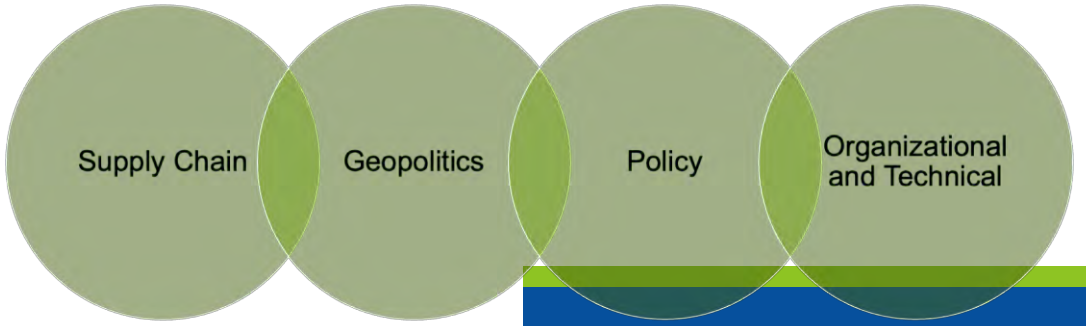
- Utility-Scale batteries are increasingly operated by non-traditional utilities.
- Any batteries divested by U.S. utilities will end up serving grid interests from 3rd party entities.
- Many battery contracts which affect the next 5 years of installation have already been let.

https://www.eia.gov/analysis/studies/electricity/batterystorage/

Threats and Risk Convergence in Emerging Technology Supply Chain and IBR

BESS & IBR, transformers, breakers - all provide critical reliability, resilience, and rapid response capabilities

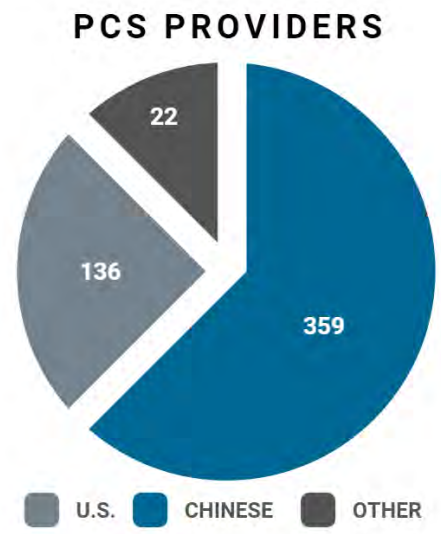
Many (90 – 95%) of the digital components available currently for control systems have a FEOC made, owned, derived control, hardware or software component



BESS Supply Chain is highly dependent on non-domestic OEMs

Nearly 100% of battery material and over 70% of power electronic control systems for batteries are produced by the People's Republic of China (PRC). Nearly all BESS sites in the United States will have 1+ PRC-made component.

81+ battery/BESS suppliers **with approved safety/standards**	~90–95% use PRC-manufactured equipment / material
73+ named inverter manufacturers **meet U.S. (safety/operational) standards**	70% are PRC owned/operated 90% have some manufacture in PRC
There are around 10 top integrators **for PRC-made equipment** The integrator relationship has a significant influence on security factors, and can drastically change risk	50% are PRC-owned integrators / 50% are U.S.-owned integrators



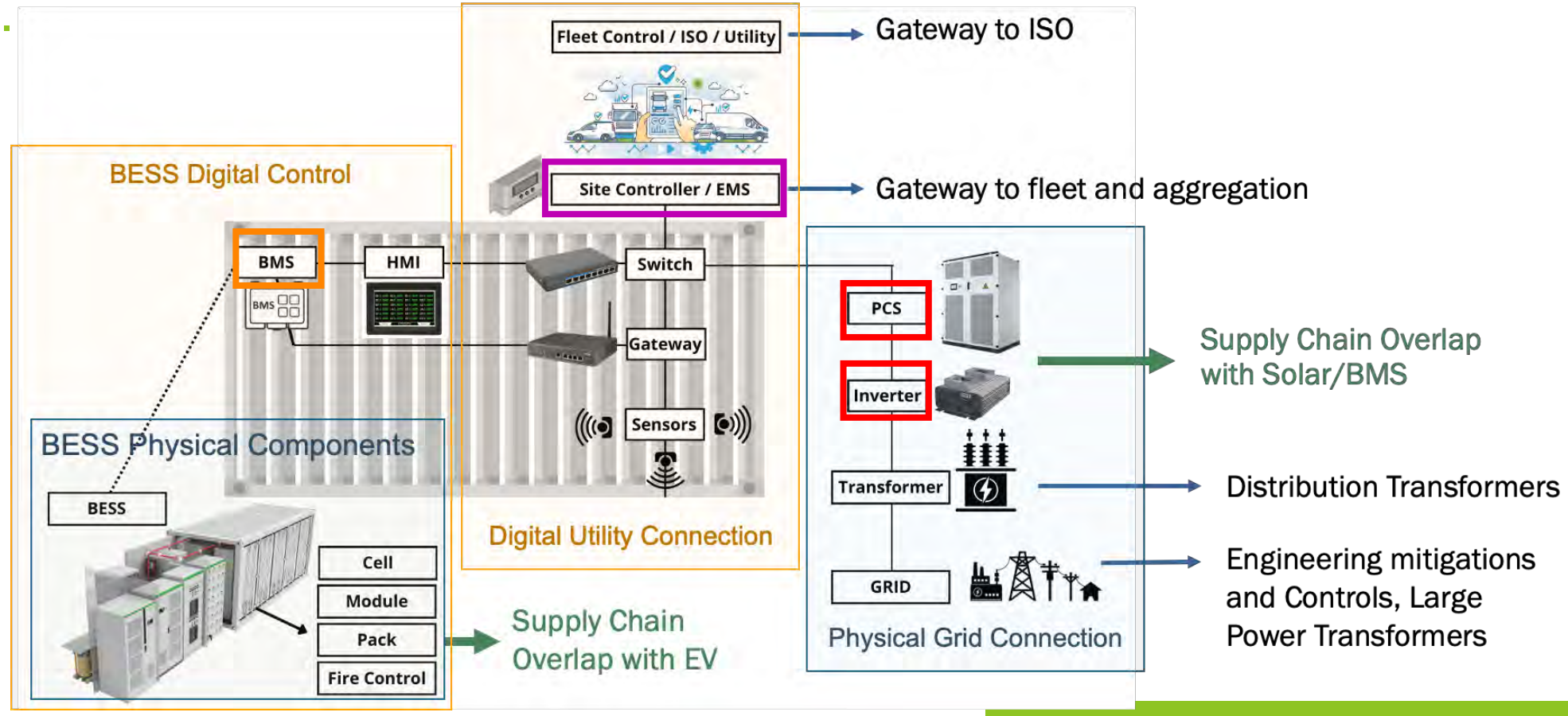
> 20 new players entered this market between 2021 – 2026

Complex BESS, ADMS and IBR Supply Chain Extends across Energy Ecosystem

Battery component OEMs have evolved to be integrators and suppliers across the energy ecosystem, not just BESS. Integrator and supplier relationships create a complex web that obfuscates hardware origin and foreign influence.

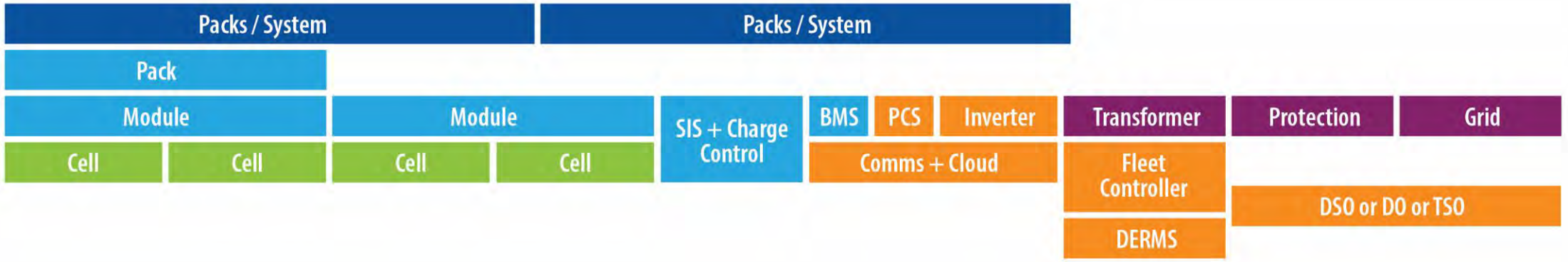
Supply chain reports are challenging to interpret as they mix:

- Integrator vs. Core Supplier
- OEM products and "white-labeled" products
- EV & BESS components



Roles & responsibilities in the BESS and inverter sector

- Many stakeholders involved in a single BESS site
- All may have a need for digital access of some degree



Local distribution utility

Independent power producer (IPP)

Developer/Integrator

OEM 2

OEM 1

Example of a BESS stakeholder ecosystem.

Why is this a problem?

Integrated Markets

- Market power imbalance
- Dependency on global supply chain
- Reduced domestic innovation

White labeling

- Quality control issues
- Brand dilution
- Supply chain disruptions

Contracts

- Regulatory compliance
- Financial liabilities
- Limited negotiation power

Ownership

- High total cost of ownership (TCO)
- Reshoring challenges
- Displacement by imports

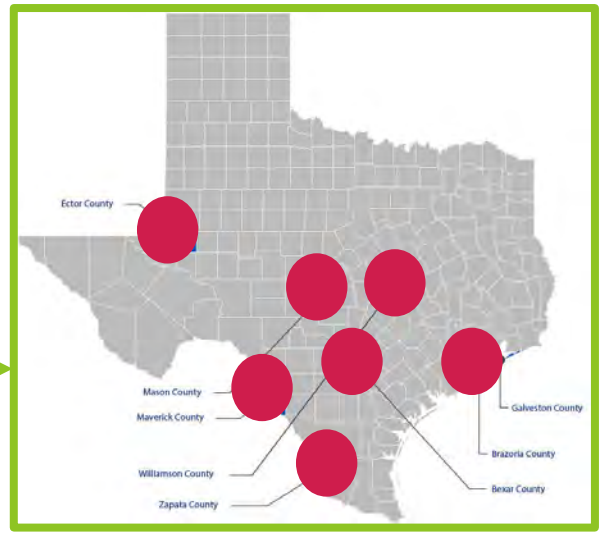
Organizational Risk: Complex Web

Interconnection Slot

Developer/Owner 1

Utility Receives/Approves Electric Grid Study

buys power through PPA



Sold Site

Owns over 800MW of BESS generation

Developer/Owner 2 (Finance Company)

Developer bought out

Developer/ Owner 3 (France)

Develops Sites With PRC Integrator

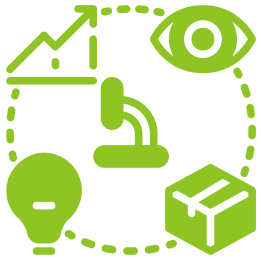
PRC BESS Company

PRC Inverter Company

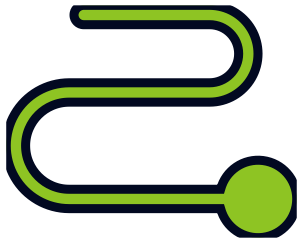
4th party O&M

Connected to RTO & Market via Fiber

We have technical and policy solutions, we need to use them

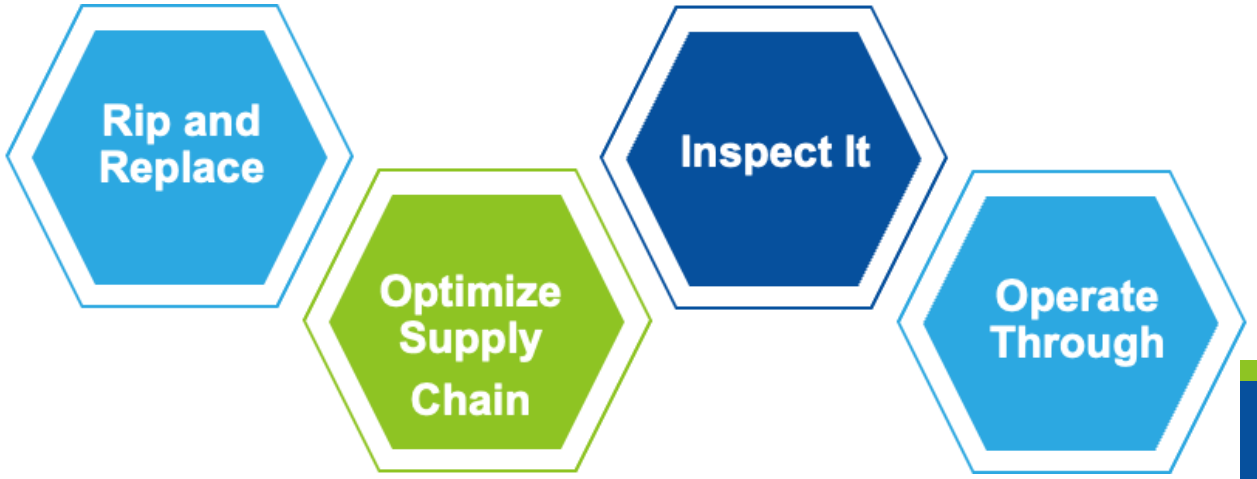


Solutions, analysis, and research **MUST** take a system-of-systems approach to reduce risk

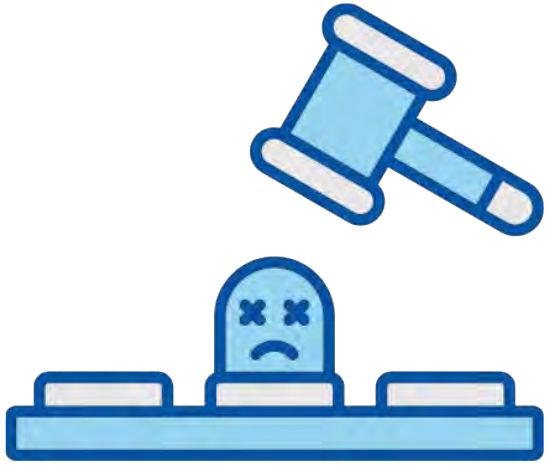


There is no fast path to limiting suppliers domestically

Most direct approach is implementing a cyber-informed engineering approach to secure systems and mitigate risk



Rip and Replace vs. Secure Around and Through



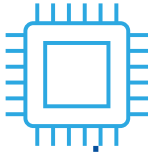
Ban and Replace

Secure around and Through

- $4B, 4 years to replace one US state's batteries alone
- $12B for US Installed Supply Currently
- 70+ options currently for PRC BESS
- But what about quality and safety metrics?
- Huawei are still here, 5 years later

- Domestication of the Supply Chain
- Secure By Design
- Policy and Regulatory Solutions
- Cyber Informed Engineering Design
- Maintain demand signal

Supply Chain Challenges & Securing Digital Assets: Common Global Challenges - Procurement & Integration

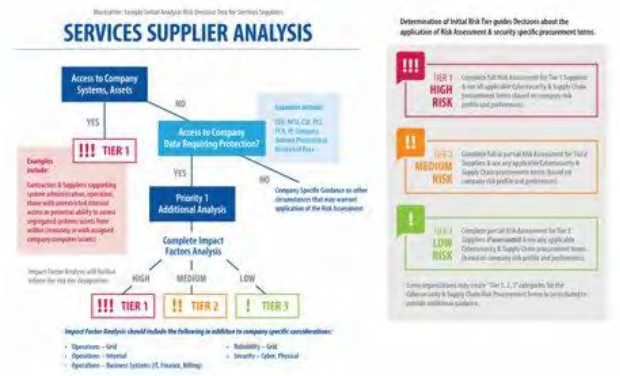
1. Failing Chips 
2. Persistent Communications 
3. Hardcoded and Weak Passwords 
4. Direct Connection to OEM for Firmware and Condition Management
5. White Labeled Products 
6. Mass Orchestration via Offshore Cloud and Third-Party Platforms 
7. Bad Documentation and/or no SBOMs or HBOMs
8. Unknown Supply Chain ‘Spiderweb’ for Integrated Systems 
9. Limited Threat and Consequence Modeling Capabilities

Navigating Supply Chain Challenges

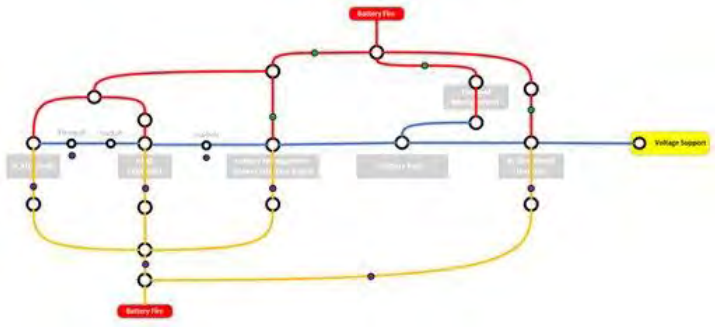
Building Resilient Systems for Electric Grid Modernization

Technical Assistance		
Policy	Technical Tools	Digital SCRM
Procurement and Contracting Guidance Interconnection Requirements	Cyber-Informed Engineering Design Equipment Inspection Network Analysis	SBOM/HBOM escrow Supply Chain Influence Analysis and Visualization

- Technical Assistance and information sharing used to:
  - Mature state policies and requirements
  - Make resources available to electric utilities and related stakeholders within a state



Ex: risk decision tree for services suppliers

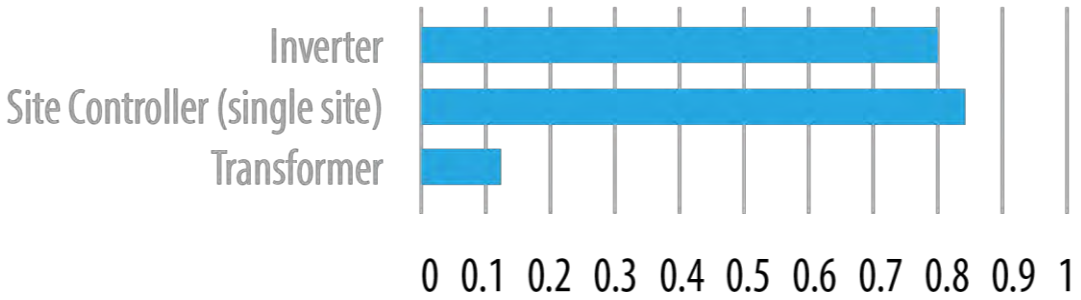


Ex: function consequence analysis for CIE analysis of BESS

Cyber Informed Engineering Design Guide for BESS and Microgrids

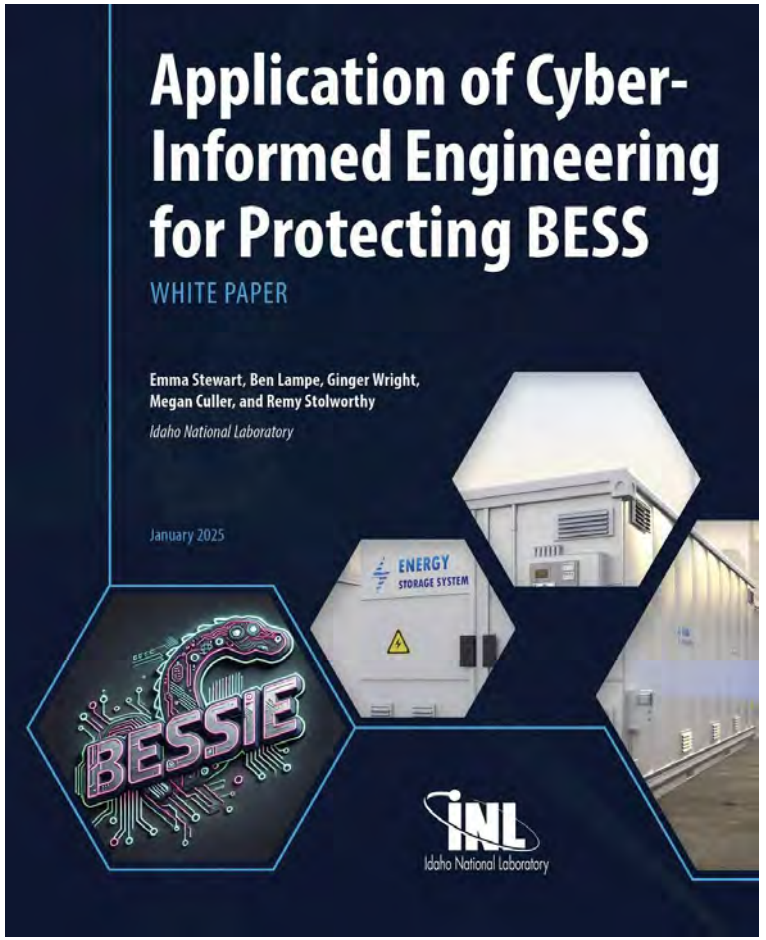
1 ANALYZE SYSTEM SERVICES 2 ANALYZE CONSEQUENCES 3 ANALYZE CIE MITIGATIONS

CRITICALITY OF BESS COMPONENTS



Goal: Help asset owners design their BESS integrations securely
3 industry partners have tested and used the process successfully

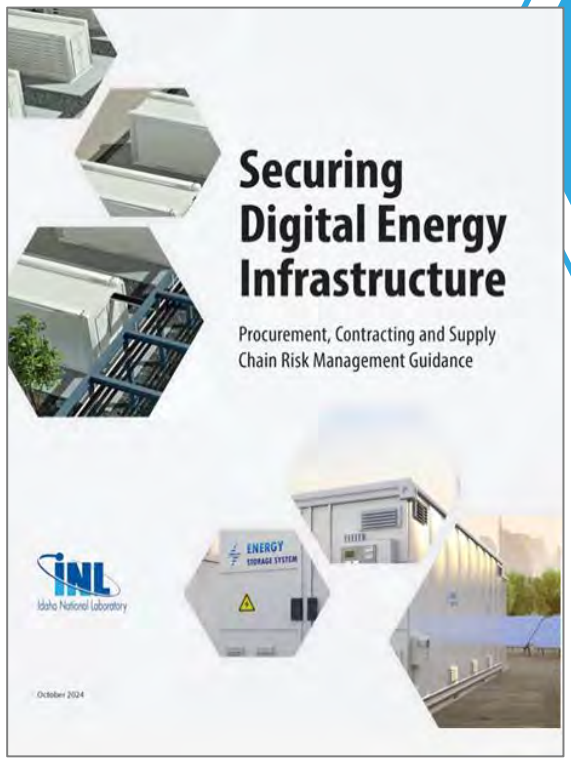
- Successful Case Study with US BESS Company: Business Case for Utilizing CIE in US integrated manufacture



Contract teeth: Configuration, Design Requirements & Supply Chain

Better configurations could mitigate ~70 to 80% of the biggest consequences

- Strong password requirements
- Firewall and Firmware DMZs
- Don’t put it on the internet
- US Based O&M
- Monitor it
- External sensing for highest consequence scenarios
- Make contracts and procurement your friend



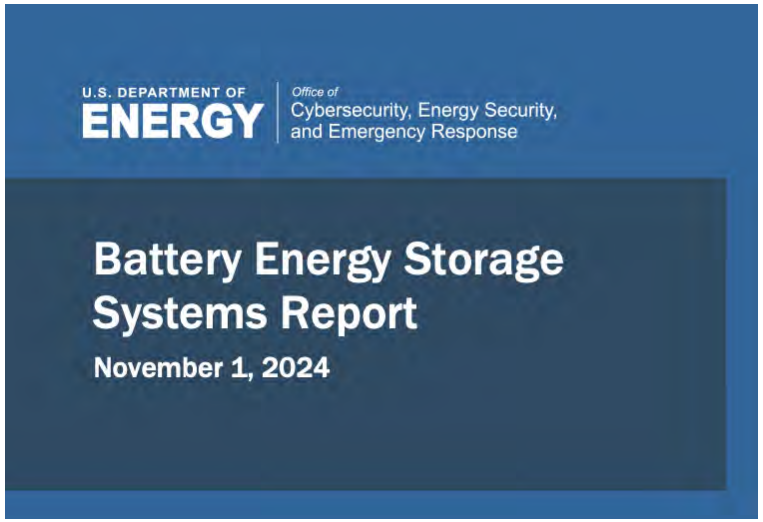
Summary

- The adoption of digital and emerging sources is increasing across all critical infrastructure sectors, such as hospitals, communication systems, water, transportation, military installations, and large loads
- The presence of adversarial entity suppliers in the supply chain is a significant concern, but not going away
- Solutions extend to many scenarios – not just BESS
- We can fix this, both in the short and long term
- Policy and Technical mitigations need to align

1. Force inspection and assessment
2. Rationalize regulation and oversight around the “new school”
3. Configure it right….
4. We can safely integrate this equipment, we don’t have a choice, we need the right structure and services to do it (we just need to use them)

Links Programs and Info

- https://csdet.inl.gov/bess/
- https://www.energy.gov/ceser/articles/new-ceser-report-offers-supply-chain-mitigation-strategies-battery-storage-systems
- **Cyber Informed Engineering** – https://www.energy.gov/ceser/cyber-informed-engineering
  - Products in IBR, Interconnection, Microgrids and BESS to guide secure configuration
- **Cyber Testing for Resilient Industrial Control Systems (CYTRICS)** – https://cytrics.inl.gov/
  - Equipment assessment strategy
- **Energy Cyber Sense -** https://www.energy.gov/ceser/energy-cyber-sense-program
  - Principles Targeted as Guidelines for IBR & BESS Manufacture
  - Analysis and Assessment Combined
- **Cyber Labeling (Inverters) -** https://energy.sandia.gov/programs/electric-grid/cyber-security-for-electric-infrastructure/cyber-labeling-research-initiative/
- **Liberty Eclipse** – https://www.energy.gov/ceser/liberty-eclipse
  - Battery Assessments in GMLC
- **CyberStrike (STORMCLOUD)** – https://inl.gov/national-security/cyberstrike/
- **Energy Threat Analysis Center (ETAC)** – https://www.energy.gov/ceser/energy-threat-analysis-center-0
- **CESER OT Defender** – https://otdefender.inl.gov/



Technical Assistance for Digital Assurance

Core Challenge. Many of the inverters, BESS, management platforms, and software packages have a limited domestic supply chain

We must **enable** the **resilient deployment**, while also providing mitigations, training, support and security solutions for digital controls

GDO enlisted INL to develop and deliver a **component security evaluation** and **mitigation technical assistance program** for key digital energy components

Technical Assistance (TA) is being offered to all states to support education, planning, and evaluation efforts

Program Enrollment. This program has open enrollment and sign up links are included on this slide.

TA Sign up here (for more info):
https://inl.gov/csdet-technical-assistance-and-training/
Or contact:
CSDET.TA@inl.gov

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.