NREL
Transforming ENERGY

Improving Cyber-Physical Security for Critical Infrastructure—Technology, Standards, and R&D

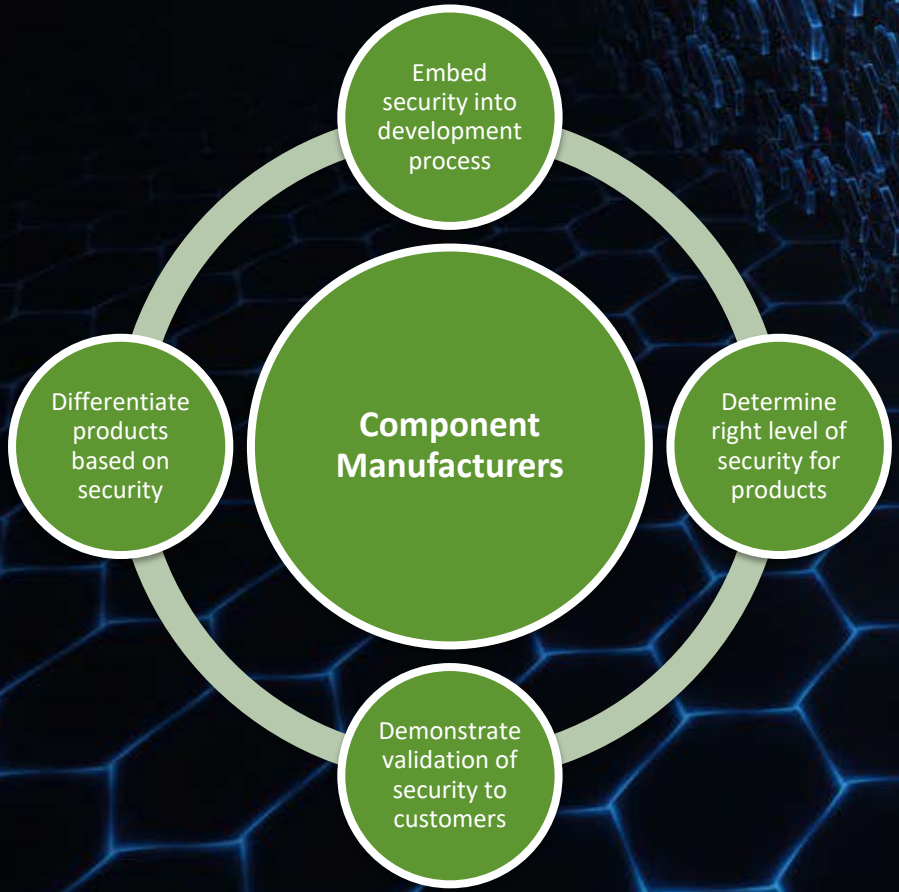
Danish Saleem, National Renewable Energy Laboratory

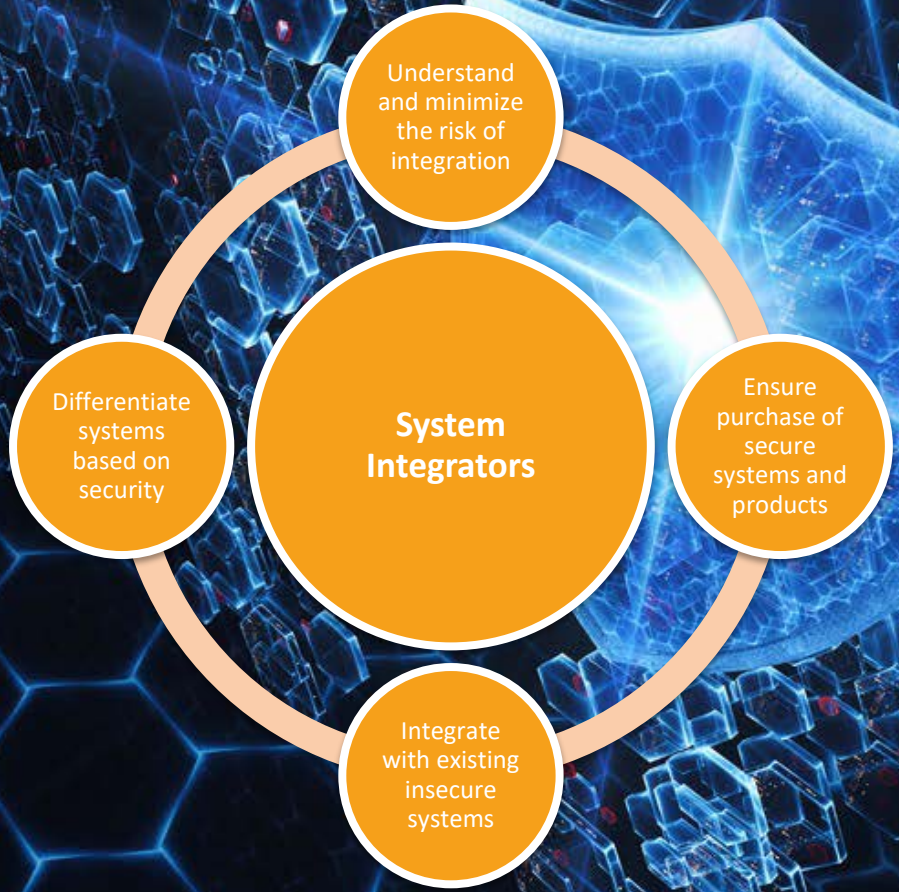
DOE Cybersecurity and Technology Innovation Conference, June 15, 2022

Agenda

1. Challenges and Blind Spots for Cybersecurity
2. Module-OT
3. Named Data Networking
4. Blockchain for Energy Sector
5. Cybersecurity Certification
6. Important Principles of Cyber-Physical Security

Industry Cybersecurity Challenges

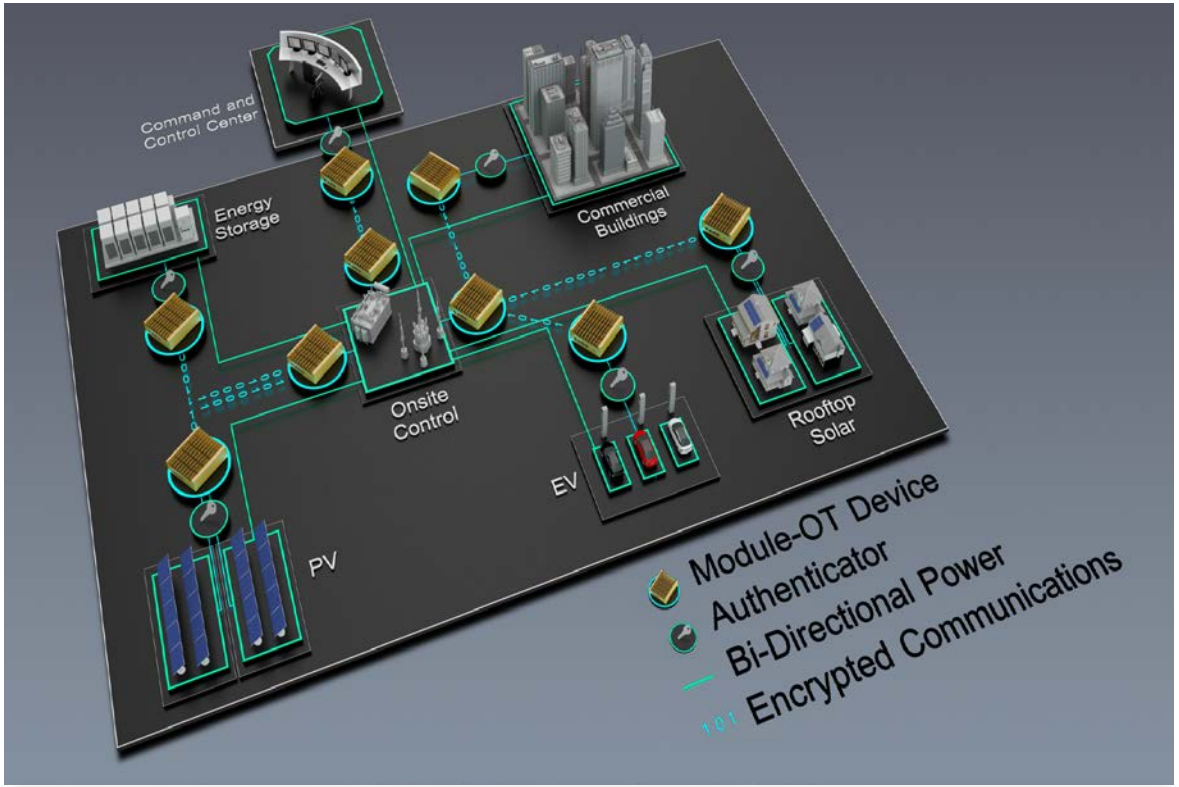




Blind spots and challenges for electric utilities

- Lack of visibility into operating assets
- Lack of investment in workforce development
- Lack of security alignment between OT and IT
- Pace of advancements in technology and threats
- Accessibility of threat and risk information

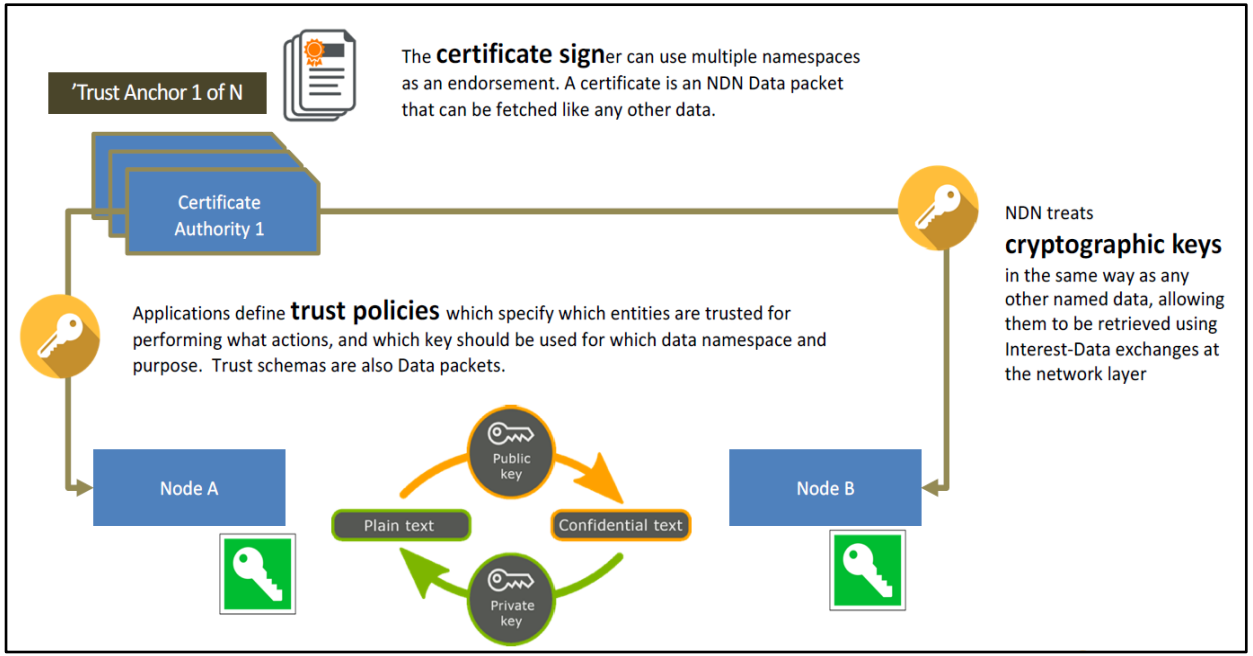
Module-OT

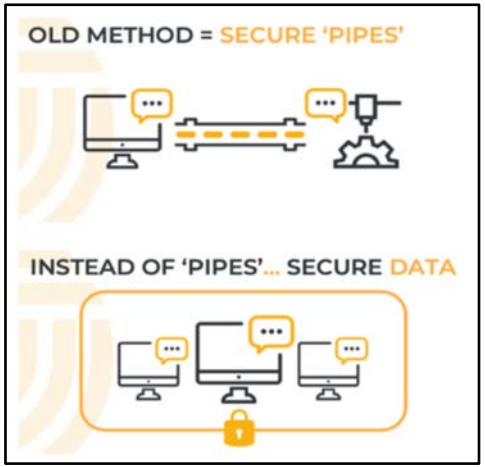


Cyber intrusions to industrial control systems (ICS) and distributed energy resource (DER) systems, particularly at scale, could have significant effects on grid performance and reliability.

- Modular security for operational technology
- Plug-and-play solution for defense against vulnerabilities that exist in highly interconnected electric power systems
- Developed to secure critical infrastructure communications
- Designed to protect legacy protocols and aging devices against common cyberattacks while creating minimal obstruction to normal operations
- Cost-effective, bump-in-the-wire technology for communication security across wide-area network
- Provides data integrity, confidentiality, authorization, and authentication
- Tested in a high-fidelity, utility-grade environment with 500-KW photovoltaic + storage site
- Offers system owners, electric utilities, and aggregators a better option to secure the critical energy infrastructure with minimal changes
- For more information on how Module-OT can work for you, please visit: https://www.nrel.gov/security-resilience/module-ot.html.

Named Data Networking



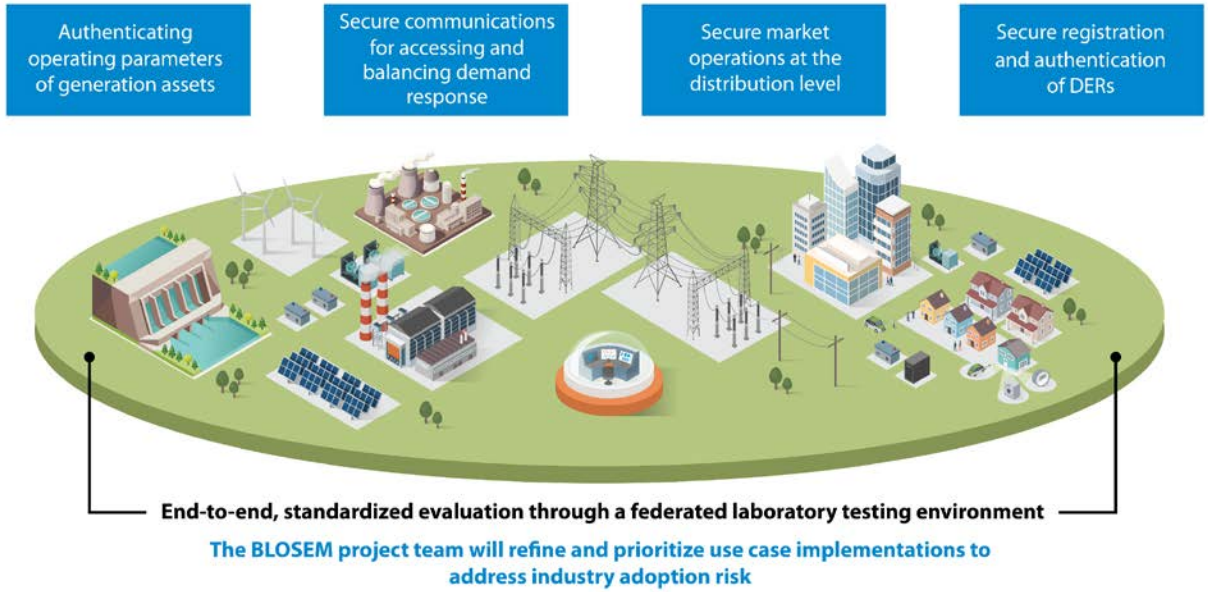


Named data networking (NDN) is a new internet architecture that enables secure end-to-end communications without depending on the security or topology of underlying channels.

Instead of defending only data channels, named data networking directly secures data by uniquely naming the data packets and by securely binding those names to the data packets using cryptographic signatures.

Source: https://operantnetworks.com/

BLOSEM



The U.S. energy sector needs an integrated strategy to evaluate, assess, and mature blockchain-based technologies for cybersecurity.

- Blockchain for Optimized Security and Energy Management (BLOSEM)
- Explores the potential for blockchain to be an enabler of new market structures, expanding the value of ICS and DER systems with enhanced security
- Ensures domain expertise and informs blockchain technology solutions for the energy sector
- Accelerates the pipeline of validated cyber-physical security concepts from the laboratory to the utility sector, de-risking and reducing costs through standardized metrics and testing
- Multi-laboratory project developed through the Grid Modernization Laboratory Consortium that fills a need for blockchain technology assessments for the energy sector.

Cybersecurity Certification Standard

- The requirements will provide a single unified approach for testing and certification of DERs *in advance* of deployment.
- The certification will be applicable to generation and energy storage technologies.
- UL and NREL are actively developing the outline of investigation.
- We will welcome participation from industry.

A national or international cybersecurity certification standard can aid industry stakeholders to evaluate and validate the cybersecurity posture of their DER or IBR devices before they are connected to the electric grid.

https://www.nrel.gov/security-resilience/cybersecurity-standards.html

PRESS RELEASE

UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources

UL and the National Renewable Energy Laboratory will complete an Outline of Investigation as a precursor to the first cybersecurity certification standard for distributed energy resources.

Home > News > UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources

March 7, 2022

NORTHBROOK, Illinois – March 7, 2022 – UL, a global safety science leader, has released a report, co-authored with the U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory (NREL), titled "Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources." The report includes recommendations that enable distributed energy resources (DER) and inverter based resources (IBRs) to maintain a strong cybersecurity posture.

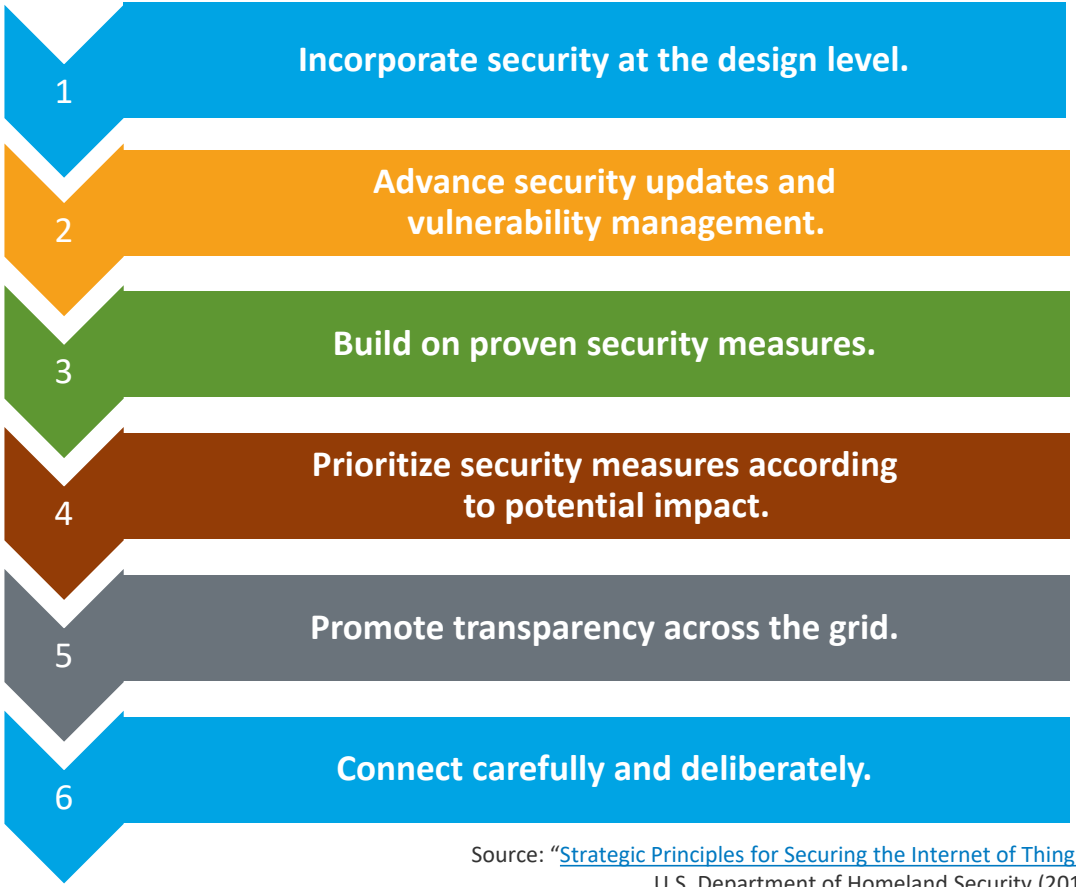
With support from DOE's Solar Energy Technologies Office, UL will continue working with NREL on developing requirements to support cybersecurity certification standards for DERs and IBRs. NREL and UL are currently working on an Outline of Investigation for a standard that will apply to energy storage and generation technologies on the distribution grid, including photovoltaic inverters, electric vehicle chargers, wind turbines, fuel cells and other resources essential to advancing grid operations. These new requirements will prioritize cybersecurity enhancements for power systems dealing with high penetration inverter-based resources, including those interfacing with bulk power systems for periods of instantaneous high wind, solar and hybrid/storage generation. It will also help ensure cybersecurity is designed into new IBR and DER systems.

"Currently, there are no cybersecurity certification requirements to which manufacturers and vendors can certify their DER and IBR devices against an established and widely adopted cybersecurity certification program. The development of these new cybersecurity certification requirements will provide a single unified approach that can be taken as a reference for performing the testing and certification of DERs before being deployed and while in the field," said Kenneth Boyce, senior director for Principal Engineering, Industrial, group at UL. "Drafting comprehensive certification requirements with peer review requires effective leadership and stakeholder participation. We are pleased to be working with NREL in this effort to bring additional performance-based security to electrical grid infrastructure."

Think Before You Connect

Implement **security by design** and practice basic **cyber hygiene.**

- Change default passwords.
- Use two-factor authentication.
- Install updates, e.g., authentication, TLS 1.2 or higher
- Consider security of underlying infrastructure during patch management or remote connection.
- Monitor both consumer devices and vendor-managed devices.
- If possible, add code-signing and roll-back firmware.
- Use vendors with cyber hygiene.
- DO NOT connect printers or other similar devices to the operations network.



Source: "Strategic Principles for Securing the Internet of Things," U.S. Department of Homeland Security (2016)

Road Map of Next Steps

- Establishing the principle of “security by design” for new industrial control systems
- Better coordination between government agencies and industry stakeholders to enhance ICS security
- Acceleration of public awareness, education, and training for stakeholders about risks associated with ICS
- Identification of risks and addition of incentives-based programs to incorporate ICS security
- Development of a cybersecurity certification to ensure security by design for new ICS.

Thank You!

Let’s work together!

Danish.Saleem@nrel.gov

NREL/PR-5R00-83048

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NREL
Transforming ENERGY