NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURING THE INDUSTRIAL INTERNET OF THINGS

Cybersecurity for Distributed Energy Resources

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of securing the industrial internet of things (IIoT) in and among distributed energy resources (DERs) through collaborative efforts with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Securing the Industrial Internet of Things project description, including background and challenge, goals, and potential benefits. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge, please contact us at energy_nccoe@nist.gov.

BACKGROUND

Use of DERs—such as wind and solar photovoltaics—is growing rapidly and is transforming the traditional power grid. As the use of DERs expands, the distribution network is changing from a single-source radial network to a multi-source grid of devices and systems. Proper management of these devices and their power flows is heavily dependent on digital communication and control across public communication networks. DER integration—driven by IIoT devices, data flow, and information management—poses a widening attack surface and growing cybersecurity challenge for the energy sector.

CHALLENGE

Distributed energy resources introduce information exchanges between a utility's distribution control system and the DERs to manage the flow of energy in the distribution grid. These information exchanges often employ IIoT devices that lack the communications security present in traditional utility systems. Additionally, the operating characteristics of DERs are dynamic and significantly different from those of traditional generation capabilities. Timely management of DER capabilities often requires a higher degree of automation. Introducing additional automation into the management and control systems can also introduce cybersecurity risks. Managing the automation, the increased need for information exchanges, and the cybersecurity associated with these presents significant challenges for electric power providers and distribution companies.

GOALS

This NCCoE project aims to improve the overall cybersecurity of IIoT devices in a DER environment by:

- ensuring authenticity of all information exchanges between distribution control systems and DERs
- providing malware prevention, detection, and mitigation in DER operating environments
- providing trusted identification of DER devices and distribution control systems

BENEFITS

The potential business benefits of the solution explored by this project include:

- enhancing reliability and stability of the grid by better protecting DERs from a cyber attack
- assuring that distribution operators retain control of DERs independent of a cyber event
- providing an immutable record of commanded actions and responses across all DERs
- ensuring integrity of energy transactions by monitoring and protecting IIoT digital communications with demand response programs

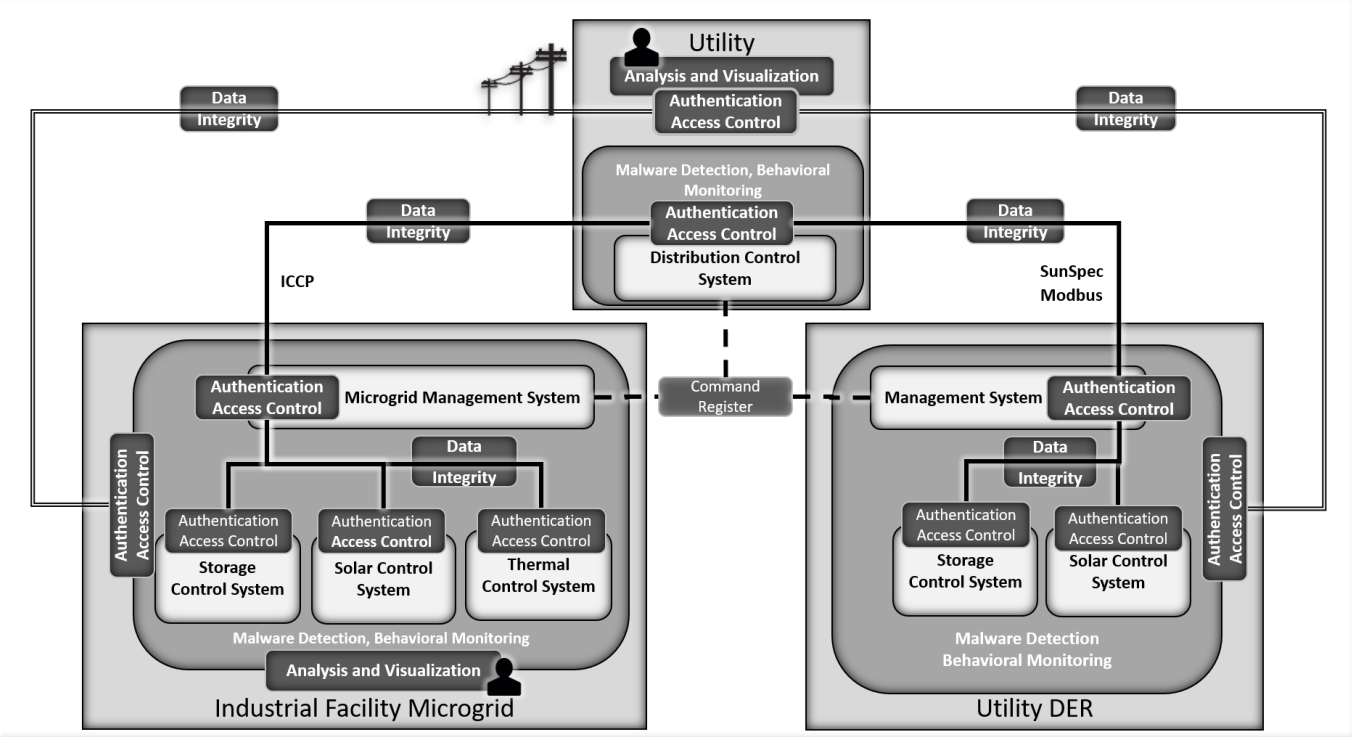
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
https://www.nccoe.nist.gov.

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

Below is a conceptual architecture of an industrial facility microgrid, a utility-managed DER, and their tie-in to a distribution control system (distribution grid). The cybersecurity capabilities that the NCCoE hopes to demonstrate in this architecture include analysis and visualization, authentication and access control, behavioral monitoring, a command register, data integrity, and malware detection.



TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution. Technology collaborators on this project are…

Anterix

BlackRidge TECHNOLOGY

CISCO

DOTS AND BRIDGES

radiflow Secure your Assets

SPHERICAL ANALYTICS

sumo logic

tdi technologies

xage SECURITY

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the work underway to strengthen the security of IIoT in a distributed energy resource environment. For more details, download the project description by visiting https://www.nccoe.nist.gov/projects/use-cases/energy-sector/iiot.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the Energy Sector Community of Interest, please email to energy_nccoe@nist.gov.