NIST SPECIAL PUBLICATION 1800-32A

Securing the Industrial Internet of Things:

Cybersecurity for Distributed Energy Resources

Volume A:
Executive Summary

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Eileen Division
Don Faatz
Nik Urlaub
John Wiltberger
The MITRE Corporation
McLean, Virginia

April 2021

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/iiot

Executive Summary

Protecting Industrial Internet of Things (IIoT) devices at the grid edge is arguably one of the more difficult tasks in cybersecurity. There is a wide variety of devices, many of which are deployed and operate in a highly specific manner. Their connectivity—the conduit through which they can become vulnerable—represents a growing cyber threat to the distribution grid. In this practice guide, the National Cybersecurity Center of Excellence (NCCoE) applies standards, best practices, and commercially available technology to protect the digital communication, data, and control of cyber-physical grid-edge devices. We demonstrate how to monitor and detect unusual behavior of connected IIoT devices and build a comprehensive audit trail of trusted IIoT data flows.

CHALLENGE

The use of small-scale distributed energy resources (DERs)—grid-edge devices such as wind and solar photovoltaics—is growing rapidly and transforming the traditional power grid. As the use of DERs expands, the distribution grid is becoming a multisource grid of interconnected devices and systems driven by two-way data communication and power flows. These data and power flows often rely on IIoT technologies that are connected to wireless networks, given a level of digital intelligence that allows them to be monitored and tracked and to share data on their status and communicate with other devices.

A distribution utility may need to remotely communicate with thousands of DERs—some of which may not even be owned or configured by the utility—to monitor the status of these devices and control the operating points. Many companies are not equipped to offer secure access to DERs and to monitor and trust the rapidly growing amount of data coming from them. Securing DER communications will be critical to maintain the reliability of the distribution grid. Any attack that can deny, disrupt, or tamper with DER communications could prevent a utility from performing necessary control actions and could diminish grid resiliency.

This practice guide can help your organization:

- **develop a risk-based approach for connecting and managing** DERs and other grid-edge devices that is built on National Institute of Standards and Technology (NIST) and industry standards
- **protect data and communications traffic** of grid-edge devices and networks
- **support secure edge-to-cloud data flows,** visualization, and continuous intelligence
- **remotely monitor and control** utility and nonutility DERs
- **capture an immutable record of control actions** across DERs that can be shared with DER management systems, regulators, auditors, financiers, or grid operators
- **advance the cybersecurity workforce skills needed** to support DER and smart grid growth
- **build the business case,** functional requirements, and test plan for a similar solution within your own environment

SOLUTION

The NCCoE collaborated with stakeholders in the electricity sector, the University of Maryland, and cybersecurity technology providers to build an environment that represents a distribution utility interconnected with a campus DER microgrid. Within this ecosystem, we are exploring several scenarios in which information exchanges among DERs and electric distribution grid operations can be protected from certain cybersecurity compromises. The example solution demonstrates the following capabilities:

- **authentication and access control** to ensure that only known, authorized systems can exchange information
- **communications and data integrity** to ensure that information is not modified in transit
- **malware detection** to monitor information exchanges and processing to identify potential malware infections
- **command register** that maintains an independent, immutable record of information exchanges between distribution and DER operators
- **behavioral monitoring** to detect deviations from operational norms
- **analysis and visualization** processes to monitor data, identify anomalies, and alert operators

The example solution documented in the practice guide uses technologies and security capabilities (shown below) from our project collaborators. The solution is mapped to security standards and guidelines of the NIST Cybersecurity Framework; NIST Interagency or Internal Report 7628 Rev 1: *Guidelines for Smart Grid Cybersecurity*; and the Institute of Electrical and Electronics Engineers (IEEE) 1547-2018, *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*.

Collaborator	Security Capability or Component
Anterix	Offers long-term evolution infrastructure and communications on wireless broadband for campus DER microgrid communications
BlackRidge TECHNOLOGY	Provides trusted authentication of DER devices and enforces the network access control policy
CISCO	Detects process anomalies or unwanted IIoT device modifications; provides identity and access management capabilities
DOTS AND BRIDGES	Serves in an advisory role in smart grid and critical infrastructure cyber-physical security
radiflow Secure your Assets	Provides operational technology network monitoring to detect malicious activity

Collaborator	Security Capability or Component
S|A SPHERICAL ANALYTICS	Affords data integrity and maintains a distributed ledger that gives an immutable audit trail for all data exchanges between the utility and the microgrid
sumo logic	Offers cloud-based DER device log management and metrics that leverage big data analytics to produce real-time insights and actionable intelligence
tdi technologies	Manages privileged user permissions and access
UNIVERSITY OF MARYLAND	Delivers live data feed from on-campus solar arrays
xage SECURITY	Allows multiparty, fine-grained policy creation, authentication, and secure access control and data sharing for human, machine, and application interactions across utility and DER operations

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT or operational technology (OT) system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers, can use this part of the guide, NIST Special Publication (SP) 1800-32A: *Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use NIST SP 1800-32B: *Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security control mappings.

Information technology (IT) or operational technology (OT) professionals who want to implement an approach like this can use NIST SP 1800-32C: *How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/iiot. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at energy_nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order 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 NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.