PROJECT DESCRIPTION

SECURING THE INDUSTRIAL INTERNET OF THINGS

Scenario-Based Cybersecurity for the Energy Sector

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

Don Faatz
Eileen Division
The MITRE Corporation

DRAFT

May 2019

Energy_nccoe@nist.gov

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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. To learn more about the NCCoE, visit http://www.nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a particular problem that is relevant across the energy sector and especially to distributed energy resources. NCCoE cybersecurity experts will address this challenge through collaboration with members of the energy sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by energy sector organizations.

ABSTRACT

This project will explore various scenarios in which information exchanges among interconnected energy infrastructures can be protected from cybersecurity compromises. Components of these infrastructures form what is commonly known as the Industrial Internet of Things (IIoT). In this project, the IIoT comprises interconnected sensors, data transfer and communications systems, instruments, and other commercial off-the-shelf (COTS) devices networked together. This project focuses on demonstrating data integrity and malware prevention, detection, and mitigation for scenarios in which information exchanges occur between distributed energy resources and the distribution grid. These information exchanges create the potential for increased cybersecurity risk.

This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

data integrity, distributed energy resource, industrial control system, Industrial Internet of Things, malware, microgrid, smart grid

DISCLAIMER

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://www.nccoe.nist.gov.

Comments on this publication may be submitted to Energy_NCCoE@nist.gov.

Public comment period: May 6, 2019, to June 5, 2019

TABLE OF CONTENTS

1 Executive Summary

Purpose

Public feedback is being solicited for this draft document, which describes a National Cybersecurity Center of Excellence (NCCoE) project focused on providing cybersecurity guidance to help energy companies secure information exchanges with distributed energy resources (DERs) in their operating environments. As an increasing number of DERs are being connected to the grid, this growth provides a pertinent opportunity to examine its impact on the cybersecurity of these connections.

This project is focused specifically on data integrity and malware prevention, detection, and mitigation within industrial control systems (ICS). Major consideration is given to DERs—particularly commercial-scale and utility-scale solar power installations—and their interconnection with the electricity distribution grid.

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 Industrial Internet of Things (IIoT) technologies 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. Introduction of 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 present significant challenges.

This project aims to develop a reference architecture to address these challenges and to demonstrate the architecture with an example solution built with commercially available technologies. Utilities facing these challenges will be able to adopt all or part of the reference architecture to help secure their operating environments.

Publication of this Project Description is the beginning of a process to identify project collaborators as well as standards-based, commercially available, and/or open-source hardware and software components. These components will be deployed, integrated, and configured in a laboratory environment to create an open, standards-based, modular, end-to-end reference design that addresses the cybersecurity challenges of data integrity and malware attacks within the energy sector. The approach will include a reference architecture, a logical design, a proof-of-concept implementation, security analysis of the architecture, implementation testing, security control mapping, and adoption considerations. This project will result in a publicly available National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Scope

The objective of this project is to demonstrate a proposed approach for improving the overall security of IIoT in a DER environment and to address the following areas of interest:

- the information exchanges between and among DER systems and distribution facilities/entities and the cybersecurity considerations involved in these interactions

- the processes and cybersecurity technologies needed for trusted device identification and communication with other devices
- the ability to provide malware prevention, detection, and mitigation in operating environments where information exchanges are occurring
- the mechanisms that can be used for protecting both system and data transmission components
- data-driven cybersecurity analytics to help owners and operators securely perform necessary tasks

Assumptions

This project makes the following assumptions:

- An IIoT lab infrastructure is in place and can adequately reflect components that are representative of an IIoT environment.
- Numerous commercially available technologies exist to demonstrate the example solution.

Challenges

IIoT as a concept can be defined in many ways. NIST does not seek to authoritatively define IIoT, but rather to provide examples of what are generally accepted to be IIoT applications in the real world and the commensurate cybersecurity challenges that may arise. The lab environment will not contain all the devices that would typically be found in a real-world setting. This project will demonstrate effective cybersecurity practices in an applied manner.

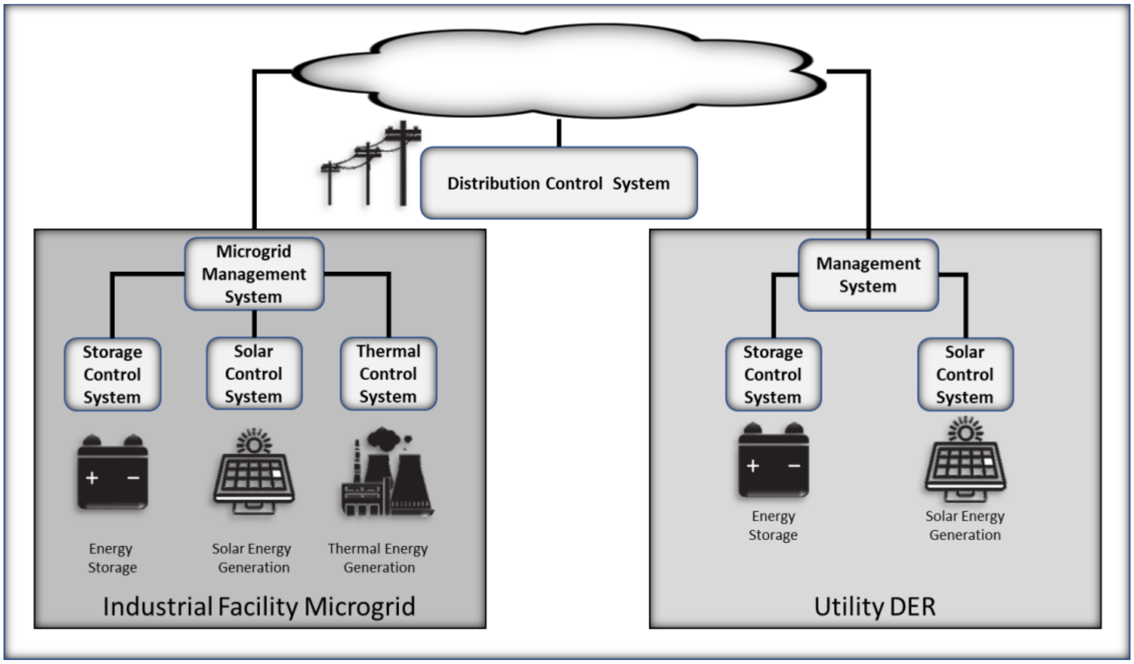
Background

The need for proactive cybersecurity defense mechanisms is a key concern in the energy sector as DERs and IIoT introduce new connections and expand the attack surface of traditional energy generation and distribution networks. The NCCoE, in association with members of industry, academia, and government, was prompted to engage in this effort to assist energy providers with mitigating cybersecurity risks of innovation in critical infrastructure, such as IIoT for energy management.

2 Conceptual Architecture

Figure 1 shows the conceptual architecture of an industrial facility microgrid, a utility-managed DER, and their tie-in to a distribution control system (distribution grid). The scenarios described in Section 3 reference the components of this conceptual architecture.

Figure 1: Example DER Infrastructure



An industrial facility has added a solar array and battery storage capability to its campus microgrid to both augment its natural gas cogeneration plant and further reduce its dependence on the local utility. Additionally, the solar array will allow the facility to sell excess power back to the local utility.

The campus microgrid has several control systems for its various components. The solar array, the battery storage, and the cogeneration plant each has its own control system. Each individual control system interacts with human operators and with an overall microgrid management system. The microgrid management system interacts with human operators and with the local utility's distribution control center.

These control systems communicate on campus by using a combination of wired Ethernet and Wi-Fi connections. The microgrid management system communicates with the local utility by using a connection over the internet.

The local utility operates a DER facility with both a solar array and a battery storage capability. The power from this facility augments the utility's supply from other sources and reduces its costs in meeting peak power demand. The utility's system has control systems like those in the industrial facility's microgrid. However, all utility-operated control systems interact over wired Ethernet connections.

Figure 1 contains the following components:

- **distribution control system:** a system that controls the operation of the local utility's distribution grid
- **microgrid management system:** a system that controls the operation of the microgrid, including distribution of energy from the available sources, storage, solar, thermal, and the local utility

- **management system:** a system that controls the operation of the utility's distributed energy resources
- **storage control system:** a system that manages the flow of power going into and out of the battery bank
- **solar control system:** a system that manages solar energy generation
- **thermal control system:** a system that manages thermal energy generation
- **solar energy generation:** photovoltaic modules that generate and supply solar electricity
- **energy storage:** a battery bank that stores energy
- **thermal energy generation:** a natural gas electricity generation plant

3 Scenarios

The specific scenarios included in this section are derived from the DER failure scenarios presented by the Electric Power Research Institute [1]. The example scenarios described below illustrate some of the challenges that this project may address, along with the security requirements/outcomes that this project will aim to demonstrate. In Section 5, Security Control Map, the scenarios are mapped to the relevant Categories and Subcategories of the NIST Cybersecurity Framework.

Scenario 1: Industrial Control Malware Protection and Detection

During efforts to correct a software problem, the microgrid management system is given limited access to the internet. During this interval, a malicious actor gains access to the microgrid management system. Using this access, the malicious actor locates a connection to the business network that is used to provide information from the microgrid to a system that interacts with energy markets.

The malicious actor makes configuration changes that give persistent remote access to the microgrid management system.

Using this persistent access, the malicious actor implants malware to gather information about the microgrid. Over time, the malicious actor can understand the architecture of the microgrid control systems and learn the typical information exchanges among them. This information is used to compromise the battery and solar control systems.

With an understanding of the architecture and data exchanges, the attacker conducts subtle tests at manipulating the controls by injecting information into the data exchanges.

Security requirements/outcomes:

- Demonstrate protections to either prevent malware infections or render delivered malware ineffective.
- Demonstrate techniques to detect malware that circumvents protections.

Scenario 2: Data Integrity

From the foothold in the microgrid's control systems, the malicious actor spoofs monitoring data messages to the utility's distribution control system. The malicious actor monitors the utility's response to the changed monitoring data, learns how the system responds, and observes the command streams issued. With the information gained from these observations within the microgrid, the malicious actor uses internet access from outside the microgrid to attempt spoofing commands from the utility's distribution management system to the utility's DER systems. These invalid commands to the utility's DER systems increase software error reports from the utility's DER control systems.

Security requirements/outcomes: Demonstrate methods that can protect the integrity and ensure the authenticity of information used to monitor and control DERs.

Scenario 3: Device and Data Authenticity

As a result of these experiments, the threat actor learns how to masquerade as the distribution control system and create and deliver valid commands to microgrids and utility DERs connected to the distribution system.

Security requirements/outcomes:

- Demonstrate methods to protect DER management systems from compromise.
- Detect potential compromise.
- Detect DER management system behavioral and performance anomalies.

Desired Cybersecurity Capabilities

Based on the security requirements/outcomes for the scenarios mentioned above, the specialized cybersecurity components and capabilities that collaborating vendors will need to provide include:

- non-interactive device authentication with policy/rule enforcement to enable asset/end point cloaking, assured identity, and segmentation/segregation
- authenticated identity to improve or enhance monitoring and detection, which is compatible with security information and event management protocols
- state engines for workflows and data flows
- network graph analytics and machine learning
- domain-specific predictive analytics
- sensors, data acquisition devices, and intelligent sensor gateways
- ICS data integrity validation capabilities
- visualization capabilities to provide situational awareness

Figure 2 shows how the desired cybersecurity capabilities may be deployed to protect the DER.

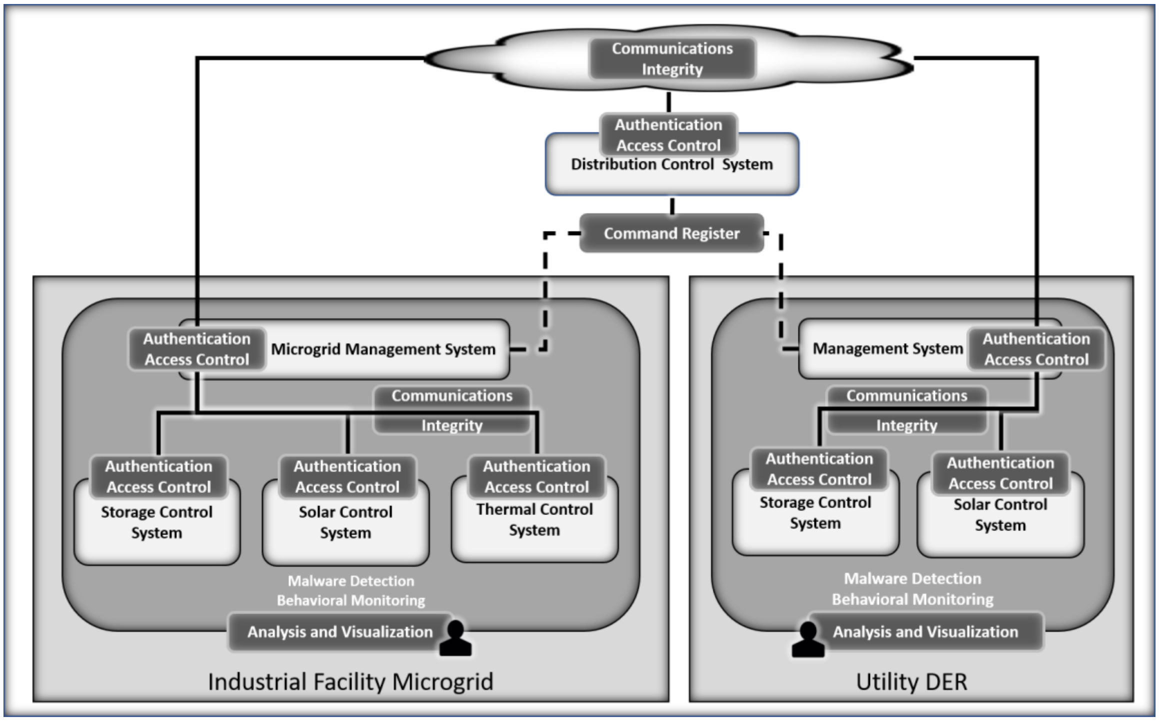
The analysis and visualization capabilities collect and process monitoring data from communications, management systems, and control systems to detect anomalies, identify anomalies that represent potential malicious activity, and alert human operators.

The authentication and access control capabilities are used on all communication between management and control systems. These capabilities ensure that only known, authorized systems can exchange information. Further, these capabilities may limit the types of information exchanged. Attempted unauthorized communication or attempted communication by unknown systems is detected and reported to the analysis and visualization capabilities.

The behavioral monitoring capabilities examine behavioral characteristics of the management and control systems. Measurements are compared with expected or normal behavioral characteristics that have been learned over time. Anomalies are reported to the analysis and visualization capability.

The command register capability records transactions between the distribution control system and control systems managing the DER. This capability allows both the utility and the DER operator to verify information exchanges. Information exchanges may be commands from the utility to the DER or status information from the DER to the utility.

Figure 2: Cybersecurity Capabilities Deployed in the Example DER Infrastructure



The communications integrity capabilities ensure that information is not modified in transit between the sender and receiver. If the information is modified, the capabilities detect the modification and notify the analysis and visualization capabilities.

The malware detection capabilities monitor information exchanges among the management and control systems and processing by the management and control systems, looking for signatures of known malware. If a malware signature is detected, the analysis and visualization capability is notified.

4 Relevant Standards and Guidance

- NIST Cybersecurity Framework
  https://www.nist.gov/programs-projects/cybersecurity-framework
  Outlines the best cybersecurity practices to minimize risk to critical infrastructure
- NIST Special Publication (SP) 1108 Revision 3: *Framework and Roadmap for Smart Grid Interoperability Standards*
  https://www.nist.gov/sites/default/files/documents/smartgrid/NIST-SP-1108r3.pdf
  Provides a road map for the open architecture of smart grid technologies and their software systems, for interaction with other systems and technologies

- NIST Interagency/Internal Report 7628: *Guidelines for Smart Grid Cyber Security*
  https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
  Companion document to the NIST SP 1108 Revision 1; describes a high-level conceptual reference model for the smart grid, identifies standards that are applicable, and specifies a set of high-priority, standards-related gaps and issues
- NIST SP 800-82 Revision 2: *Guide to Industrial Control Systems (ICS) Security*
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
  Provides guidance on how to secure ICS, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as programmable logic controllers, while addressing their unique performance, reliability, and safety requirements
- International Electrotechnical Commission (IEC) 60870-5: *Tele-control equipment and systems—Part 5: Transmission protocols*
  Standard for power system monitoring, telecontrol, tele-protection, and associated telecommunications for electric power systems
- IEC 60870-6: *Tele-control equipment and systems—Part 6: Tele-control protocols compatible with ISO standards and ITU-T recommendations*
  Specified by utility organizations throughout the world to provide data exchange over wide area networks among utility control centers, utilities, power pools, regional control centers, and nonutility generators that are compatible with ISO standards and ITU-T recommendations
- Institute of Electrical and Electronics Engineers (IEEE) 1815-2012: *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*
  Defines DNP3 protocol structure, functions, and interoperable application options
- IEEE 1815.1-2015: *IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]*
  Addresses a selection of features, data classes, and services of the two use cases: 1) mapping between an IEEE 1815-based master and an IEC 61850-based remote site and 2) mapping between an IEC 61850-based master and an IEEE 1815-based remote site
- IEEE C37.240-2014: *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*
  Provides technical requirements for substation cybersecurity and presents sound engineering practices that can be applied to achieve high levels of cybersecurity of automation, protection, and control systems independent of the voltage class or criticality of cyber assets. Cybersecurity includes trust and assurance of data in motion, data at rest, and incident response.
- IEEE 1547-2018: *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*
  Standard for testing the interconnection and interoperability between utility electric power systems and DERs
- IEEE 2030-2011: *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*
  Provides alternative approaches and best practices for achieving smart grid interoperability

- IEEE 2030.5-2018: *SEP2–Smart Energy Profile 2.0*
  Defines the application layer with transmission control protocol/internet protocol providing functions in the transport and internet layers to enable utility management of the end user energy environment, including demand response, load control, time of day pricing, management of distributed generation, electric vehicles, etc.
- National Energy Reliability Council (NERC) Reliability Guideline: *Cyber Intrusion Guide for System Operators*
  Provides assistance for system operators in recognizing events that may indicate a cyber attack, and how and when to share information with others
- NERC Reliability Guideline: *Situational Awareness for the System Operator*
  Provides guidance for organizations to have a process in place for assessing and increasing the effectiveness of the situational awareness to their operators in electric systems
- NERC Critical Infrastructure Protection Standard Series
  Imposes rules that address power system security, and specifies the minimum security requirements for the bulk power systems

5 Security Control Map

Table 1 maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity, and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet your industry’s requirements for regulatory approval or accreditation.

Table 1 Security Control Map

Function	Category	Subcategory	Scenario Applicability
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	1, 2, 3
		PR.AC-3: Remote access is managed.	1
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	3
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	2, 3
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected.	2
		PR.DS-2: Data-in-transit is protected.	2
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	1, 2
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	3
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	1, 3
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	3
		DE.AE-5: Incident alert thresholds are established.	
	Security Continuous Monitoring (DE.CM): The	**DE.CM-1:** The information system and assets are	3

	information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	
		DE.CM-4: Malicious code is detected.	1
		DE.CM-5: Unauthorized mobile code is detected.	
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	3
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	3

APPENDIX A REFERENCES

[1] *Electric Sector Failure Scenarios and Impact Analyses–Version 3.0*, Electric Power Research Institute, National Electric Sector Cybersecurity Organization Resource, Dec. 2015. Available: http://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf.

331 # Appendix B Acronyms and Abbreviations

COTS	Commercial Off-the-Shelf
DER	Distributed Energy Resource
ICS	Industrial Control System
IIoT	Industrial Internet of Things
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology