NIST SPECIAL PUBLICATION 1800-32B

Securing the Industrial Internet of Things:

Cybersecurity for Distributed Energy Resources

Volume B:
Approach, Architecture, and Security Characteristics

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

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

April 2021

PRELIMINARY DRAFT

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-32B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-32B, 44 pages, (April 2021), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Public comment period: April 22, 2021 through May 24, 2021

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

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 issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information and operational technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

The Industrial Internet of Things, or IIoT, refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy, and other critical infrastructure sectors. In the energy sector, distributed energy resources (DERs) such as solar photovoltaics and wind turbines include sensors, data transfer and communications systems, instruments, and other commercially available devices that are networked together. DERs introduce information exchanges between a utility's distribution control system and the DERs to manage the flow of energy in the distribution grid.

This practice guide explores how information exchanges among commercial- and utility-scale DERs and electric distribution grid operations can be monitored and protected from certain cybersecurity threats and vulnerabilities.

The NCCoE built a reference architecture using commercially available products to show organizations how several cybersecurity capabilities, including communications and data integrity, malware detection, network monitoring, authentication and access control, and cloud-based analysis and visualization can be applied to protect distributed end points and reduce the IIoT attack surface for DERs.

KEYWORDS

data integrity; distributed energy resource; industrial internet of things; malware; microgrid; smart grid

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Mike Brozek	Anterix
Mark Poulin	Anterix
Doug Johnson	BlackRidge Technology
John Walsh	BlackRidge Technology (now with Bedrock Systems)
Michael Harttree	Cisco
Peter Romness	Cisco
Shanna Ramirez	CPS Energy
Pete Tseronis	Dots and Bridges
Candace Suh-Lee	Electric Power Research Institute
TJ Roe	Radiflow

Name	Organization
Gavin Nicol	Spherical Analytics
Chris Rezendes	Spherical Analytics
Jon Rezendes	Spherical Analytics
Scott Miller	Sumo Logic
Doug Natal	Sumo Logic
Rusty Hale	TDi Technologies
Bill Johnson	TDi Technologies
Samantha Pelletier	TDi Technologies
Don Hill	University of Maryland
Kip Gering	Xage Security
Andy Sugiarto	Xage Security

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Product
Anterix	LTE infrastructure and communications on wireless broadband

Technology Partner/Collaborator	Product
BlackRidge Technology	Transport Access Control
Cisco	Cisco Identity Services Engine; Cisco Cyber Vision
Dots and Bridges	subject matter expertise
Radiflow	iSID Industrial Threat Detection
Spherical Analytics	Immutably™, Proofworks™, and Scrivener™
Sumo Logic	Sumo Logic Enterprise
TDi Technologies	ConsoleWorks
University of Maryland	campus DER microgrid infrastructure
Xage Security	Xage Security Fabric

Contents

List of Figures

List of Tables

1 Summary

An increasing number of distributed energy resources (DERs) are connecting to the distribution grid. These DERs introduce two-way information exchanges between a utility's distribution control system and the DERs, or an aggregator, 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 conventional utility systems. Managing, trusting, and securing the information exchanges between and among DERs present significant challenges.

The National Institute of Standards and Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE) collaborated with stakeholders in the electricity sector, the University of Maryland (UMD), and cybersecurity technology vendors to build a laboratory environment that represents a distribution utility interconnected with a campus DER microgrid. Using this environment, we are exploring how information exchanges between commercial- and utility-scale DERs and the electric distribution grid can be monitored, trusted, and protected.

The goals of this NIST Cybersecurity Practice Guide are to help organizations:

- remotely monitor and control utility-owned and customer-managed DER assets
- protect and trust data and communications traffic of grid-edge devices and networks
- capture an immutable record of control actions across DERs
- support secure edge-to-cloud data flows, visualization, and continuous intelligence

For ease of use, the following provides a short description of each section in this volume.

Section 1, Summary, presents the challenge addressed by this NCCoE project, including our approach to addressing the challenge, the solution demonstrated, and the benefits of the solution.

Section 2, How to Use This Guide, explains how business decision makers, program managers, information technology (IT) and operational technology (OT) professionals might use each volume of the guide.

Section 3, Approach, offers a detailed treatment of the scope of the project, the risk assessment that informed the solution, and the technologies and components that industry collaborators supplied to build the example solution.

Section 4, Architecture, specifies the components of the example solution and details how data and communications flow between and among DERs and the distribution grid.

Section 5, Security Characteristic Analysis, provides details about the tools and techniques used to test and understand the extent to which the project example solution meets its objective of demonstrating that information exchanges among DERs and electric distribution grid operations can be monitored and protected from certain cybersecurity compromises.

Section 6, Future Project Considerations, is a brief treatment of other applications that NIST might explore in the future to further protect DER communications.

The appendixes provide acronyms, a glossary of terms, and a list of references cited in this volume.

1.1 Challenge

Small-scale DERs—such as wind and solar photovoltaics—are growing rapidly and transforming the power grid. 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 both the DERs' power production assets and various wireless networks. These edge devices have an embedded level of digital intelligence that allows DER assets to be monitored and tracked, and through the edge devices, share data on their status and communicate with other devices across DER networks and beyond.

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 control the operating points and monitor the status of these devices. Many companies are not equipped to provide secure access to DERs and to monitor and trust the rapidly growing amount of data coming from them or flowing into them. The ability of utilities and DER operators to trust these information exchanges is essential to these companies' business. Any disruption or manipulation of the data could have negative consequences on utility and DER operations, and on their customers. 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.

1.2 Solution

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

- **communications and data integrity** to ensure that information is not modified in transit
- **authentication and access control** to ensure that only known, authorized systems can exchange information
- **command register** that maintains an independent, immutable record of information exchanges between distribution grid and DER operators

- **malware detection** to monitor information exchanges and processing to identify potential malware infections
- **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 from our project collaborators. The solution aligns with the security standards and guidelines of the NIST Cybersecurity Framework; NIST Interagency or Internal Report 7628 Revision 1: *Guidelines for Smart Grid Cybersecurity* [1]; 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* [2].

1.3 Benefits

The NCCoE's 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 NIST and industry standards
- provide integrity of energy transactions by monitoring and protecting IIoT digital communications
- enhance reliability and stability of the grid by better protecting DERs from a cyber attack
- assure that distribution operators retain control of DERs independent of a cyber event
- provide an immutable record of commanded actions and responses across all utility-owned and customer-managed DERs

2 How to Use This Guide

This is a preliminary draft of Volume B of a NIST Cybersecurity Practice Guide. Implementation of the example solution at the NCCoE is ongoing. The NCCoE is providing this preliminary draft to gather valuable feedback and inform stakeholders of the progress of the project. Organizations should not attempt to implement this preliminary draft.

When finalized, this NIST Cybersecurity Practice Guide will demonstrate a standards-based reference architecture and provide users with the information they need to replicate secure and trusted information exchanges in a DER environment. This reference architecture will be modular and can be deployed in whole or in part.

This guide will contain three volumes:

- NIST Special Publication (SP) 1800-32A: *Executive Summary*

- NIST SP 1800-32B: *Approach, Architecture, and Security Characteristics*–what we built and why **(you are here)**
- NIST SP 1800-32C: *How-To Guides*–instructions for building the example solution **(planned for early summer 2021 release)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-32A, which describes the following topics:

- challenges that enterprises face in monitoring, protecting, and trusting information exchanges among and between DERs
- example solution built at the NCCoE and UMD
- cybersecurity benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-32B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.3, Risk, provides a description of the risk analysis we performed
- Section 3.4.4, Security Control Map and Technologies, maps the security characteristics of this reference architecture to cybersecurity standards and best practices and the technologies used in our example solution

You might share the *Executive Summary,* NIST SP 1800-32A, with your leadership team members to help them understand the importance of adopting standards-based cybersecurity for DERs.

IT and OT professionals who want to implement an approach such as this will find the entire practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-32C, to replicate all or parts of the example solution created in our lab. The how-to portion of the guide will provide specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT and OT professionals have experience implementing security products within the enterprise. While we are using a suite of commercial products to address this challenge, this guide does not endorse these particular products. 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 the reference architecture to provide a high level of assurance in the integrity of the data for secure information exchanges between DERs and utilities. Your organization's security experts should identify the products that will best integrate with your existing tools and IT, OT, and related grid monitoring and control system infrastructure. Section 3.4.4, Security Control Map and

Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference architecture.

A NIST Cybersecurity Practice Guide does not describe a "single" solution but rather a possible solution. This is a preliminary draft guide. We seek feedback on its contents and welcome your input. Comments and suggestions will improve subsequent versions of this guide. Please contribute your thoughts to energy_nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

IIoT devices within DERs can communicate and exchange information across the open internet. Absent private communications networks, these information exchanges expand the attack surface of traditional energy generation and distribution networks and the assets that connect to them. To address this challenge, the NCCoE offers a risk-based approach to cybersecurity and proactive cybersecurity defense mechanisms that organizations can use to assure that information exchanges between and among DERs can be monitored, secured, and trusted.

The NCCoE collaborated with an Energy Sector Community of Interest that included technology and cybersecurity vendors, subject matter experts from the electric power industry, academia, and government to define the project scope and cybersecurity challenges, DER use cases, data flows and information exchanges, and a reference architecture.

We then assembled a team of cybersecurity vendors and subject matter experts to refine the solution and build a laboratory prototype of the reference architecture. The prototype example solution uses a combination of logical and physical infrastructure at the NCCoE and on the UMD campus.

3.1 Audience

This guide is intended for individuals and organizations responsible for the safe, secure, responsive, and efficient operation and interconnection of DERs with the distribution grid. This could include distribution utilities, investor-owned utilities, municipal utilities, utility cooperatives, independent power producers, distribution and microgrid owners and operators (including their investors and insurers), DER aggregators, and DER vendors. The guide may also be of interest to anyone in industry, academia, or government who seeks general knowledge of DER cybersecurity.

3.2 Scope

This NCCoE project and reference architecture demonstrate an approach for improving the overall security of IIoT in a DER environment and 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 occur
- the mechanisms that can be used for protecting both system and data transmission components
- data-driven cybersecurity analytics to help DER owners and operators securely perform necessary tasks

3.3 Assumptions

This project is guided by the following assumptions:

- The solution is being developed in a lab environment to mimic commercial- and utility-scale DERs connecting to the distribution grid. We did not interconnect with an actual distribution utility as part of the project.
- An organization has access to the skills and resources necessary to implement the cybersecurity capabilities highlighted in the project.

- The IIoT components and devices used in the project are trustworthy (i.e., there are no supply chain cybersecurity concerns) on initial connection to the lab environment.

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—material that is available to the public. The Risk Management Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks and evaluate the security characteristics of the reference architecture, example solution, and this guide.

We performed two types of risk assessment in this project:

- Initial analysis of the risk factors based on discussions with the Energy Sector Community of Interest and key stakeholders in the electric power industry, academia, and the cybersecurity technology domain. This analysis led to creating the *Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources* project description.
- Analysis of how to secure the components, connections, and information exchanges within the reference architecture and to minimize any vulnerabilities they might introduce. See Section 5, Security Characteristic Analysis.

3.4.1 Threats

NIST SP 800-30 Revision 1 defines a threat as, "… any circumstance or event with the potential to adversely impact organizational operations." For this project, threats are viewed from the standpoint of cybersecurity and the cyber events that could impact or compromise the integrity or control of DER information exchanges.

DERs employ industrial control systems (ICS). The Cybersecurity and Infrastructure Security Agency (CISA) ICS-Computer Emergency Readiness Team (CERT) defines cyber-threat sources to ICS as "persons who attempt unauthorized access to a control system device and/or network using a data communications pathway" [3]. CISA ICS-CERT, along with NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, identifies malicious actors who may pose threats to ICS infrastructure, including foreign intelligence services (i.e., national government organizations whose intelligence-gathering and espionage activities seek to harm U.S. interests), criminal groups such as organized crime groups that seek to attack for monetary gain, and hackers.

The Electric Power Research Institute (EPRI) outlined several potential cybersecurity threats to DERs in its December 2015 publication *Electric Sector Failure Scenarios and Impact Analyses—Version 3.0*. EPRI's threat events influenced the scope of this NCCoE project. Specifically, our reference architecture addresses several scenarios where a malicious actor attempts to gain access to DER systems to deploy malware, to manipulate or disrupt data and information exchanges, or to assume control of a utility or microgrid management system. These "attacks" could happen independently or together as part of a larger effort to ultimately gain control of the distribution grid or a utility's business network. As such, our reference architecture is being built and tested to address threats to data integrity, industrial control malware protection and detection, and device and data authenticity.

3.4.2 Vulnerabilities

NIST defines a vulnerability as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." A vulnerability may exist inherently within a device or within the design, operation, installation, and architecture of a system. This project does not specifically address vulnerabilities related to devices, software, hardware, or networks used in the example solution or to the cybersecurity policies that a distribution grid operator has in place. We encourage a consistent and comprehensive approach to detecting vulnerabilities. While we understand the constraints of scanning and patching industrial networks and devices, we also believe that overlooking known vulnerabilities increases cybersecurity risk. The chances of a malicious actor gaining unauthorized access increase if an exploitable vulnerability is left unaddressed. NIST SP 800-82 categorizes ICS vulnerabilities into the following categories with examples:

- **policy and procedure–**incomplete, inappropriate, or nonexistent security policy, including its documentation, implementation guides (e.g., procedures), and enforcement
- **architecture and design–**design flaws, development flaws, poor administration, and connections with other systems and networks
- **configuration and maintenance–**misconfiguration and poor maintenance
- **physical–**lack of or improper physical access control, malfunctioning equipment
- **software development–**improper data validation, security capabilities not enabled, inadequate authentication privileges
- **communication and network–**nonexistent authentication, insecure protocols, improper firewall configuration

Performing vulnerability management and remediation tasks can provide the DER or utility operator at least some level of assurance that they have reduced or mitigated the possibility of an exploit. Vulnerabilities will vary from network to network, and even those specific to particular devices may vary depending on the disposition or deployment of that device in an operating environment.

Finally, knowledge of deployed assets is paramount in securing an organization's ICS infrastructure and mitigating risks associated with asset-based vulnerabilities. NIST Special Publication 1800-23, *Energy Sector Asset Management*, describes a solution for monitoring and managing deployed OT assets.

3.4.3 Risk

Risk management is the ongoing process of identifying, assessing, and responding to risk as it relates to an organization's mission objectives. To manage risk, organizations should understand the likelihood that an event will occur and its potential impacts. An organization should also consider statutory and policy requirements that may influence or inform cybersecurity decisions.

Information system-related security risks are those risks that arise from loss of confidentiality, integrity, or availability of information or information systems and that reflect potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. For the energy sector, a primary risk to OT networks is the loss of power production and distribution assets. As described in the threats section earlier, loss in the trustworthiness of the data, loss of control of the industrial network, or introduction of malware into OT can have serious consequences.

This practice guide is informed by cybersecurity risk management processes. We provide part of the information needed to make informed decisions—based on business needs and risk assessments—to select and prioritize cybersecurity activities that are deemed necessary by your organization.

3.4.4 Security Control Map and Technologies

Table 3-1 maps the security characteristics of our reference architecture to the NIST Cybersecurity Framework [4] security Functions, Categories, and Subcategories that it supports. The technologies used in this project are mapped to the Cybersecurity Framework Subcategories they support. We selected the Subcategories that address the threats, vulnerabilities, and risks discussed above. Your organization can use Table 3-1 to identify the corresponding NIST SP 800-53 Rev 5 controls necessary to achieve the desired outcomes. While our reference architecture focuses on the Protect and Detect Functions of the Cybersecurity Framework, there are more Functions, Categories, and Subcategories in the framework than appear here. Your organization should select the Cybersecurity Framework Subcategories and controls that help mitigate your business-specific cybersecurity risks.

411 **Table 3-1 Security Characteristics and Controls Mapping—NIST Cybersecurity Framework**

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
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.	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12	**Cisco Identity Services Engine (ISE)** provides identity and access management capabilities; determines whether users are accessing the network on an authorized, policy-compliant device, and allows access to services based on associated policy.
				TDi ConsoleWorks manages the privileged access credentials for systems. These credentials are never seen or used directly by privileged users.
				Xage Security Fabric manages identities and credentials for users, applications, and devices. .
		PR.AC-3: Remote access is managed.	AC-1, AC-17, AC-19, AC-20, SC-15	**BlackRidge Gateway** provides first-packet authentication of incoming transmission control protocol (TCP) connections and enforces network access control policy, preventing unauthorized TCP connections through the gateway to protected devices and services.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
				Xage Security Fabric provides policy creation for fine-grained, multiparty access control and authentication of all the human, machine, and application/hardware assets within the utility.
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	**Anterix** provides a wireless broadband network capability for the campus microgrid over a long-term evolution (LTE) network. The solution includes LTE's extensive authentication and access control features for communications that traverse the network.
				Cisco ISE provides identity and access management capabilities.
				TDi Technologies ConsoleWorks manages privileged user access permissions. Privileged users authenticate to ConsoleWorks by either using local authentication capabilities or leveraging external authentication technologies and are then given access to systems they are supposed to manage.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
				Xage Security Fabric provides policy creation capabilities for fine-grained multiparty access control and authentication of all the human, machine, and application/hardware assets within the utility. Fine-grained access control policies are created, and authentication is enforced for every asset. This includes authentication and authorization of peer-to-peer connections between various control systems within utility systems. Failed access requests, rogue device detection, and OT device tampering are logged.
				BlackRidge Transport Access Control (TAC) Gateway provides first-packet authentication of incoming TCP connections and enforces network access control policy, preventing unauthorized TCP connections through the gateway to protected devices and services.
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	AC-4, AC-10, SC-7, SC-10, SC-20	**Xage Security Fabric** provides fine-grained access control policies and authentication enforcement for every asset. This includes authentication and authorization of peer-to-peer connections between various control systems within the utility and between the utility and microgrid operators.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
				Spherical Analytics Immutably provides data-integrity and availability technologies that protect data at rest or in transit, detects data-integrity violations, and ensures data authenticity.
	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.	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28	**Anterix** provides an LTE-based broadband network that includes LTE's data encryption and integrity features for data in transit.
		PR.DS-2: Data in transit is protected.	SC-8, SC-11	**Spherical Analytics Immutably** provides data-integrity technologies that protect data at rest or in transit, detects data-integrity violations, and ensures data authenticity.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7, SI-10	**Spherical Analytics Immutably** provides data-integrity technologies that protect data at rest or in transit, detect data-integrity violations, and ensure data authenticity.
				Sumo Logic Enterprise provides protections to ensure data encryption at rest and in transit. Logs are immutable.
				Xage Security Fabric provides data integrity via fingerprinting for every interaction within the campus microgrid network. In addition, data authenticity to and from both the DER microgrid and the utility network is guaranteed.
				Cisco Cyber Vision learns the expected traffic flows and establishes those as the baseline.
				TDi Technologies ConsoleWorks monitors for assets that have been newly discovered on a network and can leverage that information to create new devices in ConsoleWorks.
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.	AC-4, CA-3, CM-2, SC-16, SI-4	**Radiflow iSID** learns the expected traffic flows and establishes those as the baseline.
				TDi Technologies ConsoleWorks monitors for assets that have been newly discovered on a network and can leverage that information to create new devices in ConsoleWorks.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
				Cisco Cyber Vision provides network anomaly detection for operational technology traffic.
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6, CA-7, RA-5, IR-4, SI-4	**Radiflow iSID** provides operational technology network monitoring to detect potentially malicious activity.
				Sumo Logic Enterprise provides analysis and visualization capabilities to collect and process monitoring data from communications, management systems, and control systems to detect anomalies and identify anomalies that represent potential malicious activity via outlier detection. Behavioral monitoring capabilities measure 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.
				Cisco Cyber Vision provides network anomaly detection for operational technology traffic.
		DE.AE-3: Event data are collected and correlated	AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4	**Radiflow iSID** collects operational technology network events and analyzes them to identify potential indicators of compromise.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
		from multiple sources and sensors.		**Sumo Logic Enterprise** provides analysis and visualization capabilities to collect and process monitoring data from communications, management systems, and control systems to detect anomalies and identify anomalies that represent potential malicious activity via outlier detection. Behavioral monitoring capabilities measure 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.
				Cisco Cyber Vision provides alert thresholds for reporting anomalies.
		DE.AE-5: Incident alert thresholds are established.	IR-4, IR-5, IR-8	**Radiflow iSID** provides alert thresholds for reporting anomalies.
				Cisco Cyber Vision provides network anomaly detection for operational technology traffic.
	Security Continuous Monitoring (DE.CM): The information system and	**DE.CM-1:** The information system and assets are monitored to identify	AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	**Radiflow iSID** provides operational technology network monitoring to detect potentially malicious activity.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
	assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	cybersecurity events and verify the effectiveness of protective measures.		**TDi Technologies ConsoleWorks** monitors for changes to asset configurations, either on demand or on a schedule. Collected configuration information is compared with an established configuration baseline to identify changes. If changes are found, an alert is generated. Configuration information collected depends on asset type but can include information such as open ports, active services, accounts, current software, or firmware versions.
				NIST physical access control systems control access to the NCCoE building and the IIoT DER Lab. UMD physical access control systems control access to the Clark Hall engineering building and spaces housing the emergency power systems. Interfaces to the solar arrays at the Regents and Terrapin Trail parking garages are in locked equipment rooms that require physical keys for access.
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	CA-7, PE-6, PE-20	**Cisco Cyber Vision** provides network anomaly detection for operational technology traffic.

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	Product by Function in Project
		DE.CM-4: Malicious code is detected.	SC-44, SI-3, SI-4, SI-8	**Radiflow iSID** provides operational technology network monitoring to detect potentially malicious activity.
				Spherical Analytics provides graph analytics, machine learning, behavioral monitoring, and predictive analytics that aid in detecting malware and data-integrity violations.
				Cisco Cyber Vision provides network anomaly detection for operational technology traffic.
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4	**Radiflow iSID** provides operational technology network monitoring to detect potentially malicious activity.

3.4.5 Cybersecurity Workforce Considerations

Table 3-2 identifies the cybersecurity work roles that most closely align with the Cybersecurity Framework security Categories and Subcategories demonstrated in our reference architecture. The work roles are based on the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework). Note that the work roles shown may apply to more than one NIST Cybersecurity Framework Category.

More information about NICE and other work roles can be found in NIST SP 800-181 Revision 1, *Workforce Framework for Cybersecurity (NICE Framework).*

Table 3-2 Cybersecurity Work Roles Aligned to Reference Architecture

NICE Work Role ID	NICE Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
OM-ADM-001	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g., installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).	Operate and Maintain	Systems Administration	PR.AC-1, PR.AC-3, PR.AC-4
SP-SYS-001	Information Systems Security Developer	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.	Securely Provision	Systems Development	PR.AC-5, PR.DS-1, PR.DS-2, PR.DS-6, DE.AE-1
PR-CDA-001	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their	Protect and Defend	Cyber Defense Analysis	DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-4, DE.CM-7

NICE Work Role ID	NICE Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Frame-work Subcate-gory Mapping
		environments and to miti-gate threats.			
OM-ANA-001	Systems Secu-rity Analyst	Responsible for the analysis and development of the inte-gration, testing, operations, and maintenance of systems security.	Operate and Main-tain	Systems Analysis	DE.AE-1, PR.AC-1, PR.AC-3

4 Architecture

The IEEE standard 1547-2018, *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces* requires that a DER have a communication interface to exchange monitoring and control information with the area electric power systems (EPS) operator. The standard defines the minimum set of information that the DER must be able to exchange with the area EPS operator. This architecture addresses the security of these information exchanges.

This architecture helps ensure that both the DER operator and the local utility have confidence that the information exchanges are legitimate. This publication refers to the area EPS operator as a local utility.

4.1 Architecture Description

The project reference architecture demonstrates the following capabilities to protect, monitor, and audit DER information exchanges.

- All information exchanges are by and between authenticated and authorized entities.
- The networks used to exchange information are monitored, and suspicious activity is detected and reported.
- A distributed ledger of information exchanges is maintained by a third party to allow both DER operators and the utility to independently verify the information exchanges.
- A DER operator log collection and analysis capability provide controlled results sharing with the utility and other DER operators.

Figure 1 depicts the reference architecture used to protect information exchanges.

Figure 1 Reference Architecture

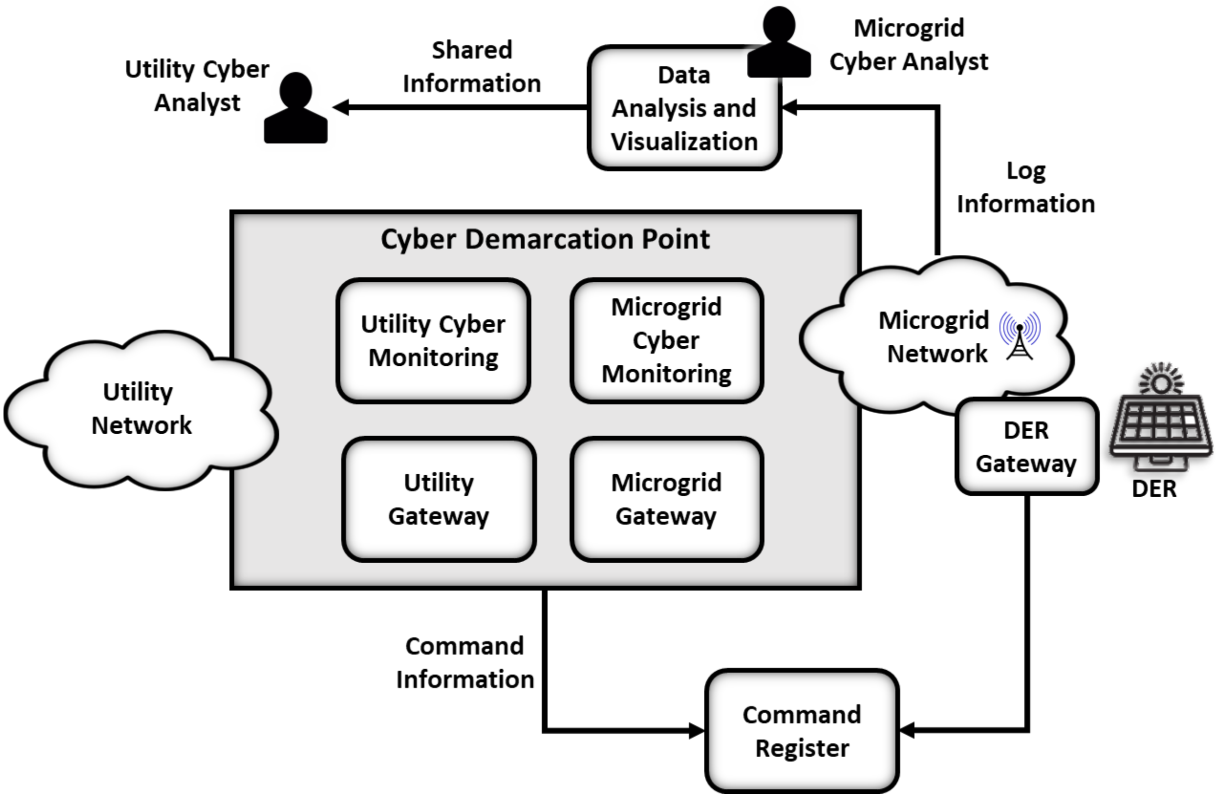


Figure 1 shows the elements of the reference architecture. The core element is the cyber demarcation point. The cyber demarcation point separates a utility network and a microgrid network—a network that is owned and controlled by a DER operator. The cyber demarcation point is responsible for independently enforcing two distinct security policies—the utility's security policy and the microgrid owner's security policy. There is a cyber demarcation point at each DER operator site. It contains the following:

- The **utility gateway** component implements the utility's access policy. It verifies the identity of any entity on the utility network attempting to exchange information with microgrid-based DERs and allows access based on the utility's defined access policy. This gateway is owned, managed, and operated by the utility. We assume all information exchanges originate on the utility network via a request from the utility to a DER on the microgrid network.
- The **microgrid gateway** component implements the microgrid access policy. It receives information requests from the utility gateway and passes authorized requests into the microgrid network. This gateway is owned, managed, and operated by the microgrid operator.

- The **utility cyber monitoring** component examines network and application traffic on the utility network and alerts utility cybersecurity personnel if suspicious activity is detected. This component is owned, managed, and operated by the utility.
- The **microgrid cyber monitoring** component examines network and application traffic on the microgrid network and alerts microgrid cybersecurity personnel if suspicious activity is detected. This component is owned, managed, and operated by the microgrid operator.

This architecture allows both the utility and the microgrid operator to control access to DERs on the microgrid. Both must agree to allow access to a DER. Similarly, both the utility and the microgrid operator can detect suspicious activity. There is no requirement for the utility or the microgrid operator to use the same products to implement these capabilities. There is a potential security benefit in each organization choosing different products, which provides a degree of diversity in an implementation. The selected products, however, must be able to exchange information via defined protocols. IEEE 1547-2018 identifies three TCP/internet protocol-based protocols that may be used for information exchanges.

The microgrid network in Figure 1 connects to the customer-owned DER devices. It may be a combination of wired and wireless network segments. A DER gateway protects each DER device. This gateway controls access to the DER device. Using a device gateway allows the microgrid gateway to implement coarse-grained policies that are not device specific. The microgrid gateway can allow a request independent of device. The device gateways can then implement fine-grained policies that are device specific. This allows the microgrid gateway policies to be independent of the specific devices currently accessible on the microgrid network. Note that the reference architecture allows but does not require the microgrid gateway policy to be independent of the specific devices on the microgrid network.

The reference architecture assumes the DER microgrid is neither owned nor operated by the utility. The microgrid operator and the utility may both independently collect audit trails that record information exchanges. As such, there is no single authoritative record of these exchanges. A complete audit trail would have to be constructed by combining audit records from the utility and the microgrid operator.

Each gateway in the reference architecture records the information exchanges it handles in a command register. The command register is a distributed ledger operated by a trusted third party. It provides an accurate, immutable record of all information exchanges that may be reviewed by both the utility and the microgrid operator. The ledger provides an authoritative source for determining who said what to whom and when and is a complete audit trail of information exchanges.

Last, the reference architecture provides collection and analysis of the log files from systems on the microgrid network and sharing select analysis results with the utility. This provides a degree of shared situational awareness. Log information is collected from source systems and sent to a cloud analytics platform. The microgrid operator's cyber defense analysts have full access to all the log information and analysis results. The microgrid operator may choose to share select results with the utility. It is easier to realize this selective sharing by using a cloud platform than it would be by using an on-premises analysis platform. The cloud analytics platform can also enable select information sharing between and among microgrid operators.

4.2 Example Solution Description

A laboratory prototype instance of the reference architecture, called an "example solution," is being constructed to verify the design. The example solution consists of a combination of logical and physical infrastructure at the NCCoE and on the UMD campus. This preliminary draft describes the intended implementation of the example solution. At the time of writing this preliminary draft, the design is not fully implemented, and some details may change.

The utility network and the cyber demarcation point are represented in the example solution by virtual infrastructure in the NCCoE lab.

The microgrid network is represented by three distinct components: a virtual network in the NCCoE lab, the UMD campus network, and an LTE network installed on the UMD campus.

4.2.1 Cyber Demarcation Point

The components of the cyber demarcation point were each implemented using different products. Therefore, the utility and microgrid components are described separately. Figure 2 illustrates the products and services used to implement the utility components of the cyber demarcation point. Figure 3 illustrates the products and services used to implement the microgrid operator components of the cyber demarcation point.

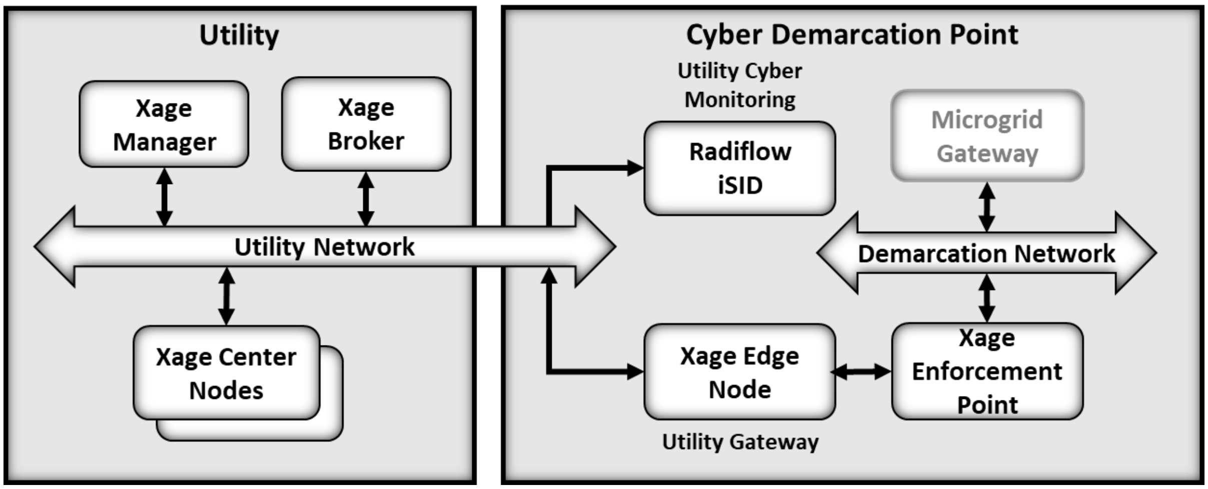
4.2.1.1 Utility Gateway and Cyber Monitoring

We used the Xage Security Fabric for the utility gateway component. This product is composed of five services:

- The Xage Manager configures users, devices, and access policies. The policies are then sent to Xage Broker. There is one Xage Manager operated by the utility and used to configure security policies for access to all DERs.
- The Xage Broker is the authoritative source for security policy information. Xage Broker can store the policy locally or use enterprise services such as a lightweight directory access protocol directory or Microsoft Active Directory. In the NCCoE example solution, all information is stored locally in the broker. There is one Xage Broker operated by the utility to store and distribute access policies for all DERs.
- The Xage Center Nodes use a distributed ledger to provide a geographically distributed information store that is tamperproof. The Xage Broker distributes policy information to the Xage Center Nodes. This distributed information store provides policy information for the Xage Edge Nodes.

- A Xage Edge Node is in the cyber demarcation point at each microgrid operator site. The Xage Edge Node retrieves security information for its site from the Xage Center Nodes and stores it locally within the cyber demarcation point.
- The Xage Enforcement Point (XEP) in the cyber demarcation point uses the security information to allow or deny access to DERs on the microgrid network.

Figure 2 Utility Gateway and Cyber Monitoring



The utility uses the Xage Manager to configure its security policy for each DER site. These policies are distributed by the Xage Broker to the Xage Center Nodes. The Xage Edge Node at a DER site retrieves its security information from a Xage Center Node and provides that security information to the DER site's XEP. When the utility exchanges information with a DER site, the XEP verifies the exchange by using the security information from its Xage Edge Node and allows authorized exchanges to pass to the microgrid gateway and ultimately to the intended DER device.

The combination of the Xage Center Nodes and Xage Edge Node storage of security information provides redundancy that ensures that the security information to authorize information exchanges is always available. Using a distributed ledger by the Xage Center Nodes ensures the integrity of the stored security information.

We used Radiflow iSID for the utility cyber monitoring component. Radiflow iSID is a passive monitoring, analysis, and detection platform that can be provided as either a physical or logical appliance. iSID learns the basic topology and behavior of the industrial control devices on the networks that it monitors. A typical deployment places an iSID appliance at a central location on the utility network and deploys iSAP Smart Collectors to each cyber demarcation point. To simplify the NCCoE lab example solution, a single virtual appliance was deployed that acts as both the analysis and detection engine and the network sensor.

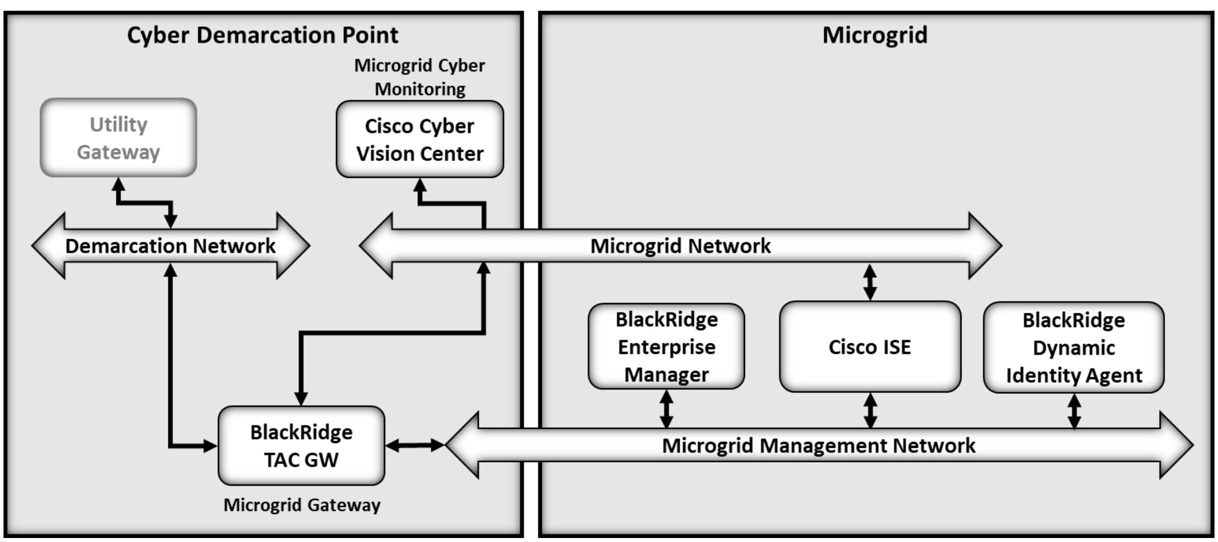
iSID allows the utility to see all devices connected to the utility network, detect anomalous behavior on the network, and detect policy violations in communications occurring over the network with DERs. This information is made available to utility cyber analysts through a collection of dashboards that provide both high-level and drill-down views and visualization of the monitoring and alert data.

In the NCCoE example solution, we placed iSID on the utility network in the cyber demarcation point. This placement provides information about all of the activity across the utility network. A sensor could also be placed on the demarcation network of the cyber demarcation point to provide insight into network traffic traversing the utility gateway.

4.2.1.2 Microgrid Gateway and Cyber Monitoring

We implemented the microgrid gateway by using BlackRidge Technology's TAC product. The product consists of two services: the BlackRidge Enterprise Manager and the BlackRidge TAC Gateway (GW). The gateways control access based on the identity of the entity attempting to communicate through the gateway. An identity token is inserted into the header of the first packet sent to open a TCP connection. If the gateway recognizes the identity and the identity is authorized to send information through the gateway, the gateway accepts the connection request. If the identity is not recognized or is not authorized, the connection request is ignored. To the requester, it appears that there is no device at the address to which the request was directed.

Figure 3 Microgrid Gateway and Cyber Monitoring



A request from the utility gateway entering the microgrid through the cyber demarcation point has an identity token assigned to it by the BlackRidge TAC GW implementing the microgrid gateway. Identities within the microgrid are managed by the Cisco ISE. The BlackRidge Dynamic Identity Agent provides an interface between Cisco ISE and the BlackRidge Enterprise Manager. Via this interface, the Enterprise

Manager can determine identity and access information to configure the TAC GW implementing the microgrid gateway.

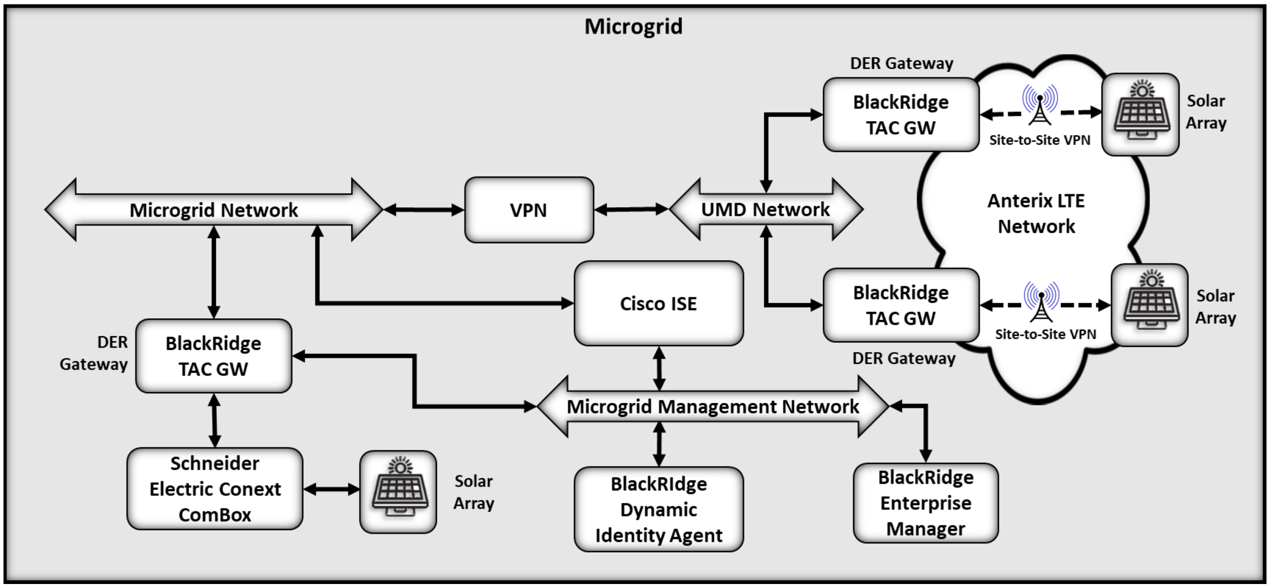
We implemented the microgrid cyber monitoring component by using Cisco Cyber Vision. Cisco Cyber Vision is a passive monitoring, analysis, and detection platform that can be provided as either a physical or logical appliance. Cyber Vision learns the basic topology and behavior of the industrial control devices on the networks that it monitors. A typical deployment places a Cyber Vision appliance at a central location on the microgrid network and deploys Cyber Vision sensors to various locations of interest on the microgrid network. In the example solution, for example, we could have placed sensors at UMD and in the NCCoE lab. To simplify the NCCoE lab example solution, a single virtual appliance was deployed in the NCCoE lab that acts as both the analysis and detection engine and the network sensor.

Cyber Vision allows the microgrid operator to see all devices connected to the microgrid network, detect anomalous behavior on the network, and detect policy violations in communications occurring over the network with DERs. This information is made available to microgrid cyber analysts through a collection of dashboards that provide both high-level and drill-down views and visualization of the monitoring and alert data.

In the NCCoE example solution, Cyber Vision was placed on the microgrid network. This placement provides information about all the activity on the microgrid network, including traffic entering the network from the cyber demarcation point. A sensor could also be placed on the demarcation network to observe traffic entering the microgrid gateway from the utility network to provide insight into network traffic traversing the microgrid gateway.

4.2.2 Microgrid Network, DER Gateway, and DER

Figure 4 Microgrid Network



We implemented the microgrid network as a combination of a virtual network in the NCCoE lab, a wired network in the NCCoE lab, a wired network on the UMD campus, and an LTE network. The virtual network in the NCCoE lab is connected via a physical network switch to a physical BlackRidge TAC GW. This BlackRidge TAC GW controls access to a Schneider Electric Conext ComBox. The ComBox is the communication interface to an inverter connected to four solar panels in the NCCoE lab. Communication with the ComBox is via SunSpec Modbus over TCP.

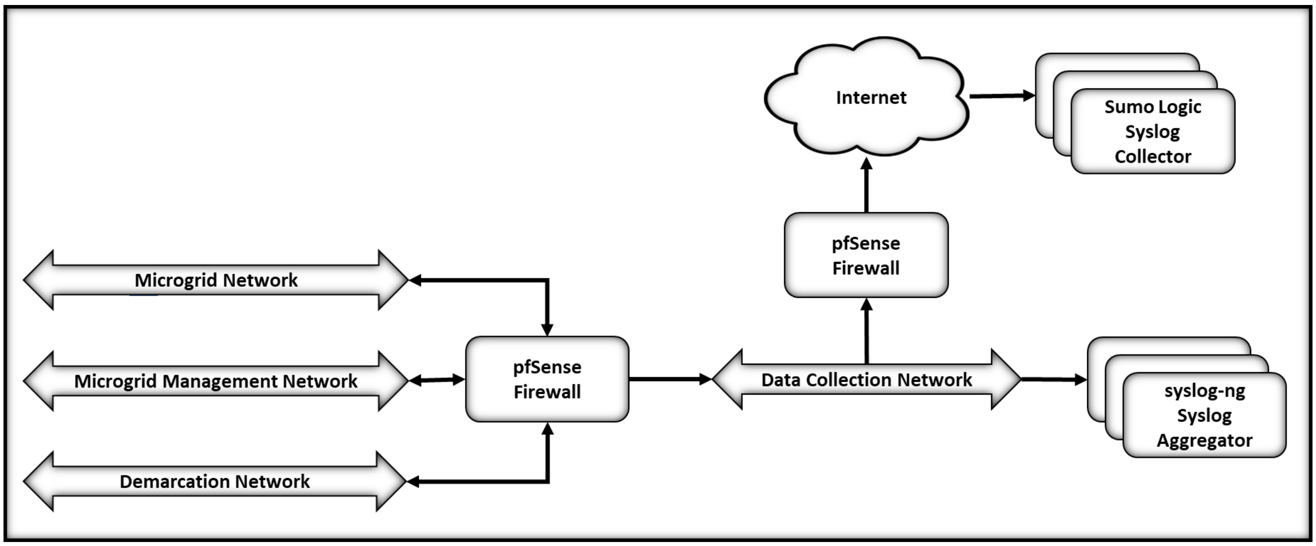
A virtual private network (VPN) using pfSense firewalls connects the virtual network in the NCCoE lab to the UMD campus network. Two virtual BlackRidge TAC GWs are installed at UMD to control access to two solar arrays at UMD. The UMD campus network does not reach the two parking garages where the solar arrays are installed. An Anterix LTE network connects each of the parking garage solar arrays to the UMD campus network. Point-to-point VPNs over the LTE network connect each TAC GW to a solar array. Communication with the solar arrays uses Modbus over TCP. Figure 4 shows how these products and services are assembled into an example of the microgrid network element in the reference architecture.

A Modbus command from the utility destined for either the UMD solar arrays or the NCCoE lab solar array enters the microgrid network through the cyber demarcation point. The BlackRidge TAC GW in the cyber demarcation point assigns an identity to the command and connects it to the appropriate DER gateway. That connection will succeed only if the BlackRidge TAC Gateway, used as the DER gateway, recognizes the identity assigned in the cyber demarcation point. If there is no assigned identity, or if the identity is not authorized to communicate with the solar array, no TCP connection will be made to the DER gateway.

As described for the microgrid gateway in the cyber demarcation point, the BlackRidge Dynamic Identity Agent provides an interface between Cisco ISE, which manages identities and access policy, and the BlackRidge Enterprise Manager, which configures the TAC GWs implementing the DER gateways.

4.2.3 Data Analysis and Visualization

Figure 5 Data Analysis and Visualization



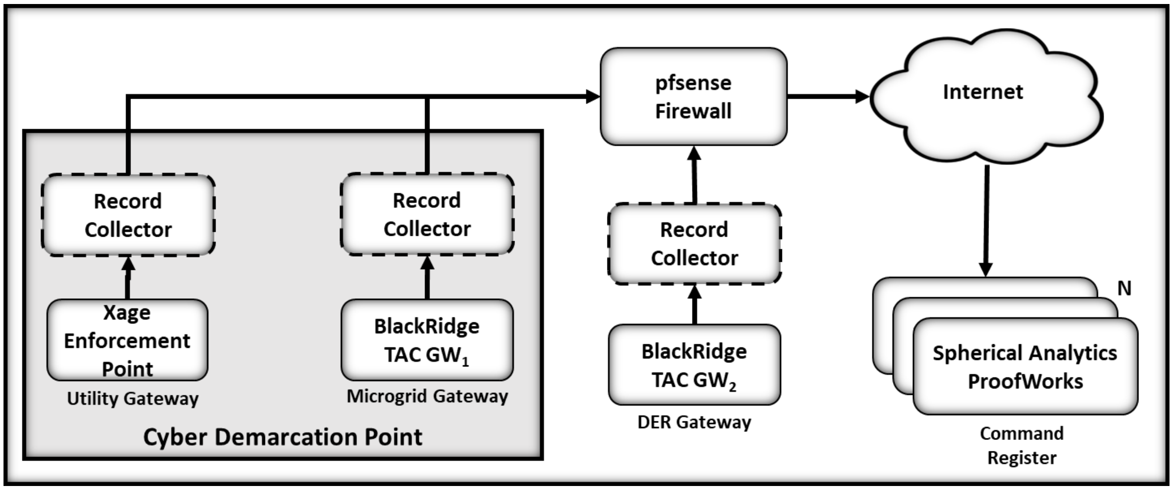
We plan to implement data analysis and visualization using Sumo Logic's cloud analytics platform as shown in Figure 5. We will collect syslog data from products and services on the microgrid network, the microgrid management network, and the demarcation network. This log information will be uploaded to Sumo Logic for analysis and presentation of results via a dashboard.

Three syslog aggregators, implemented using syslog-ng, will be placed on a dedicated data collection network. Syslog data sources on the two microgrid networks and the demarcation network will send their syslog data to one of the three aggregators. Each of these aggregators in turn will forward the collected syslog data to syslog collectors at Sumo Logic that will ingest the data into the analytics platform.

The pfSense firewalls will be used to segregate the data collection network from the microgrid and demarcation point networks and to control connections between the syslog aggregators and the internet. While not shown in Figure 5, the NIST and NCCoE corporate firewalls and network monitoring tools will also protect the connection from the log collection network to the internet.

4.2.4 Command Register

Figure 6 The Command Register



We plan to implement the command register by using Spherical Analytics Immutably service as shown in Figure 6. Immutably can receive records of information exchanges from all the gateways—the utility gateway, the microgrid gateway, and the DER gateway. It will digitally sign the records, augment them with information from notaries providing time stamps and source information, and place them on a distributed ledger, which will provide an immutable audit trail of information exchanges between the utility and DER operator devices.

None of the gateways natively support sending records of information exchanges to a third-party ledger system. For each gateway, a record collector will be developed to extract records of information exchanges and send them to Immutably. The record collectors will use an Immutably representational state transfer (REST) application programming interface to send the records. The record collector for the XEP uses a Xage-provided REST interface to extract records from the enforcement point. The BlackRidge record collector will use a BlackRidge-provided interface to extract records from the TAC Gateways. The instructions for implementing the record collectors will be provided as an appendix to Volume C of this document [anticipated in early summer 2021).

The records in the ledger will be cryptographically chained together to provide tamper detection. The utility and all participating microgrid operators will be able to read and verify the audit trail maintained by the Immutably distributed ledger.

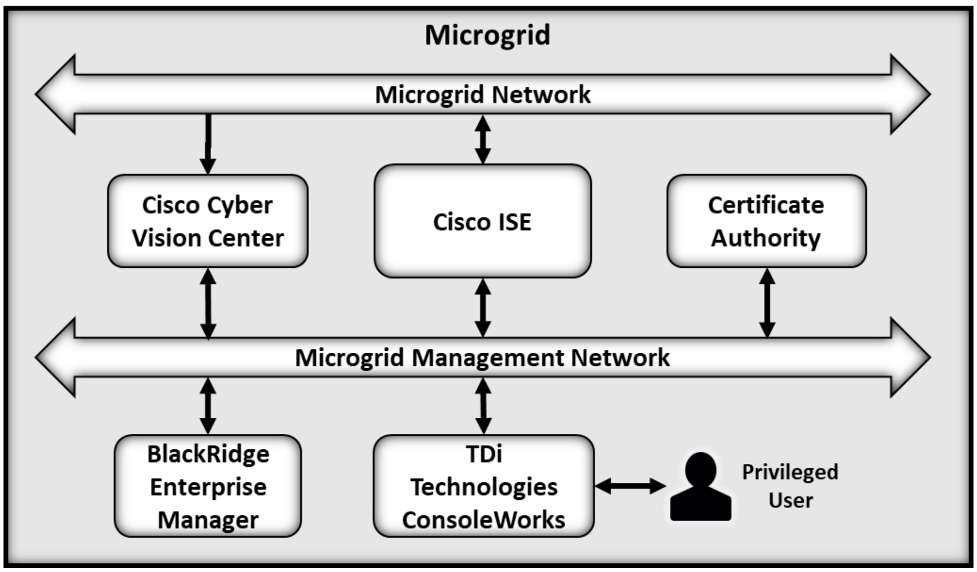
4.2.5 Privileged User Access and Management

Privileged user management capabilities protect privileged access credentials, control access to management interfaces, and provide accountability for all privileged user actions in managing products on the microgrid.

Privileged users manage the configuration of infrastructure and security devices to determine how the devices function and what operations they will allow. In the example solutions, privileged users must configure user, create and manage user credentials, manage user access permissions, determine alert thresholds, and determine what is captured in audit trails.

Cisco ISE, Cisco Cyber Vision, and BlackRidge Enterprise Manager have dedicated interfaces for configuration and management. Additionally, the BlackRidge Enterprise Manager uses a certificate authority for configuring the BlackRidge TAC Gateways. The certificate authority does not need to be accessible from the microgrid or cyber demarcation point. These dedicated management interfaces and the certificate authority are connected to a dedicated microgrid management network as shown in Figure 7.

Figure 7 Microgrid Management Network



Privileged users do not have direct access to the microgrid management network, the products' dedicated management interfaces, or privileged access credentials for the products. TDi Technologies ConsoleWorks provides privileged user management. ConsoleWorks maintains the credentials used to access the dedicated management interfaces. Privileged users have credentials that allow them to access ConsoleWorks. ConsoleWorks uses "user profiles" to define the management interfaces that each privileged user can access and the credentials used to access that interface. ConsoleWorks authenticates authorized user to product management interfaces and records all privileged user actions in an audit trail.

Additional information about privileged user management can be found in NIST SP 1800-18, *Privileged Account Management for the Financial Services Sector*. Although written for the financial sector, this guidance is applicable to other environments.

5 Security Characteristic Analysis

This section discusses the results of a comprehensive security evaluation of the reference architecture shown in Figure 1 and how it supports the Cybersecurity Framework Subcategories that we identified and mapped in Table 3-1. The purpose of the security characteristic analysis is to understand the extent to which the project example solution meets its objective of demonstrating that information exchanges among DERs and electric distribution grid operations can be monitored and protected from certain cybersecurity compromises. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- The analysis is not a comprehensive test of all security components nor a red-team exercise.
- The analysis cannot identify all weaknesses.
- The analysis does not include the lab infrastructure. We assume that the IT infrastructure used in the example solution is configured securely and properly managed. Testing this infrastructure would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.
- Because this is a preliminary draft, testing the example solution is not complete. The content provided in this section is preliminary and incomplete.
- The analysis considers only those product capabilities explicitly used in the example solution. Products may have additional capabilities that are not considered.
- The products used to implement the utility, microgrid, and DER gateways use identity to grant or allow access. The gateways are not firewalls and do not provide network protocol-level access control.
- While identities are used to control access, identity and access management technologies and processes are not addressed in the reference architecture or the example solution. See NIST SP 1800-2, *Identity and Access Management for Electric Utilities*, for more information.
- The example solution includes a limited privileged user management capability. NIST SP 1800-18, *Privileged Account Management for the Financial Services Sector*, provides additional guidance on managing privileged user access.

5.2 Example Solution Testing

Example solution testing verifies that the products we integrated in the lab environment work together as intended. For this project, we designed six test scenarios that are defined in Table 5-1 through Table 5-6.

5.2.1 Test Scenario 1: Communication Between the Utility and a DER Is Secure

This test case will verify that authenticated and authorized systems on the utility network can communicate with a DER connected to the microgrid network.

Table 5-1 Test Procedures: Communication Between the Utility and a DER Is Secure

Procedure	▪ Within the NCCoE lab (utility network), the utility can access the lab's solar array (DER) through the cyber demarcation point; only authenticated and authorized users are given access. ▪ At UMD over the LTE network (microgrid network), the utility can access the UMD DERs through the cyber demarcation point; only authenticated and authorized users are given access.
Architectural Requirements	▪ Within the NCCoE lab, identity-based access management allows authenticated and authorized users. ▪ At UMD, the LTE network has access to DERs connected to the microgrid network, and data-integrity analytics detect integrity violations and ensure data authenticity.
Capabilities/ Requirements	▪ LTE connectivity with embedded encryption through LTE point-to-point VPN ▪ Identity engine manages and distributes authenticated and authorized identities.
Expected Results	▪ Devices and users with proper authentication and authorization can communicate between the utility and the DER. ▪ Devices and users without proper authentication and/or authorization are unable to communicate between the utility and the DER.
Actual Results	▪ to be determined
Overall Results	▪ to be determined

5.2.2 Test Scenario 2: Integrity of Command Register Data and Communication Is Verified

This test case will verify data providence and integrity across the system for commands being exchanged between the utility and the DER microgrid.

Table 5-2 Test Procedure: Integrity of Command Register Data and Communication Is Verified

Procedure	▪ Communication through the cyber demarcation point is captured in the command register. ▪ The utility and the microgrid operator can verify communication through the cyber demarcation point. ▪ Devices along the communication path store commands in a distributed ledger.
Architectural Requirements	Within the NCCoE lab’s utility network, the microgrid network, and at UMD over the LTE network: ▪ Devices can generate audit trails for all privileged user activities. ▪ An audit trail of information exchanged between devices is provided. ▪ Audit logs are delivered to the command register.
Capabilities/ Requirements	▪ Logging capabilities exist across the entire communications architecture. ▪ Logs are captured in command register. ▪ Command register is capable of cross-checking and verifying log integrity.
Expected Results	▪ Command register verifies integrity of events throughout individual communication life cycles. ▪ Command register notifies of integrity failure in events throughout individual communication life cycles.
Actual Results	▪ to be determined
Overall Results	▪ to be determined

5.2.3 Test Scenario 3: Log File Information Can Be Captured and Analyzed

This test case will verify the capabilities of capturing and analyzing log data within the microgrid network.

725 **Table 5-3 Test Procedure: Log File Information Can Be Captured and Analyzed**

Procedure	▪ Log file data is captured by the syslog aggregators on the NCCoE lab data collection network. ▪ Log files are routinely transferred by the syslog aggregators to Sumo Logic for analysis. ▪ Log file analysis results are presented to microgrid cyber analysts via a Sumo Logic dashboard.
Architectural Requirements	▪ ability for log data to be captured and stored somewhere in the network ▪ ability to transfer log data to analytics engine
Capabilities/ Requirements	▪ All microgrid applications and services can record data in an exportable and accessible log. ▪ ability to analyze log files based on predetermined audit logic
Expected Results	▪ Log data is collected across the utility and microgrid networks. ▪ Log data is successfully transferred to analysis engine. ▪ Analysis engine can read and interpret all logs that are ingested.
Actual Results	▪ to be determined
Overall Results	▪ to be determined

726 ### 5.2.4 Test Scenario 4: Log File Analysis Can Be Shared

727 This test case will verify that the log analysis findings can be shared through proper channels.

728 **Table 5-4 Test Procedure: Log File Analysis Can Be Shared**

Procedure	▪ A subset of analysis and/or log file data can be shared among utility and microgrid operators' Sumo Logic user accounts.
Architectural Requirements	▪ A workstation can connect to Sumo Logic for reviewing log analysis.
Capabilities Requirements	▪ analytical capabilities to interpret results from log files

Expected Results	▪ Log analysis is used to understand system health and detect suspicious behavior. ▪ Log events are communicated to an analyst.
Actual Results	▪ to be determined
Overall Result	▪ to be determined

729 ### 5.2.5 Test Scenario 5: Malicious Activity Is Detected

730 This test case will verify the system's ability to detect anomalous or malicious behavior on the network.

731 **Table 5-5 Test Procedure: Malicious Activity Is Detected**

Procedure	▪ Suspicious activity on the utility network is identified and alert(s) is generated. ▪ Suspicious activity is captured in log files. ▪ Suspicious activity in the cyber demarcation point is identified, and an alert(s) is generated.
Architectural Requirements	▪ Holistic monitoring is enabled across the system. ▪ Logging is completed and delivered to log collector through secure means. ▪ Log analysis is performed.
Capabilities Requirements	▪ ability to monitor device and network activities ▪ ability to collect logs on devices and across the networks ▪ ability to deliver logs to analysis engine ▪ proper analysis of logs ▪ notification of events found within logs
Expected Results	▪ Log analysis is successfully completed, and any potentially malicious events are detected and alerts are created for an analyst.
Actual Results	▪ to be determined

Overall Result	▪ to be determined

5.2.6 Test Scenario 6: Privileged User Access Is Managed

This test case will verify that privileged users are authenticated and authorized to access only those devices to which they have been given proper privileges.

Table 5-6 Test Procedure: Privileged User Access Is Managed

Procedure	▪ Access the applications and services on the microgrid management network through ConsoleWorks.
Architectural Requirements	▪ ConsoleWorks system is placed at network access points for privileged users. ▪ ConsoleWorks system controls all privileged user interaction
Capabilities Requirements	▪ ability to identify approved users for ConsoleWorks ▪ ConsoleWorks will control access based on authentication and authorization of privileged users. ▪ ConsoleWorks will be able to route privileged user interaction successfully to proper devices.
Expected Results	▪ Privileged users will be able to access the devices they are authorized to access. ▪ Users will not be able to access devices they are not authorized to access.
Actual Results	▪ to be determined
Overall Results	▪ to be determined

5.3 Scenarios and Findings

Security evaluation of the reference architecture involves assessing how well the architecture addresses the security characteristics that it is intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment. Using the Cybersecurity Framework Subcategories as a basis for organizing the analysis allows systematic consideration of the reference architecture's support for the intended security characteristics.

In the project description, we described a sequence of events that could lead to a malicious entity being able to masquerade as either a utility operator or a DER operator. If that were to occur, the utility could not trust the information that it would receive from the DER operators. Likewise, the DER operators could not trust the utility's information exchange.

This section analyzes the example solution in terms of the Cybersecurity Framework's specific Subcategories supported, creating trust in information exchanges between the utility and the microgrid operation. The example solution has not been completed. Therefore, the security characteristic analysis in this preliminary draft is incomplete.

5.3.1 Identity Management, Authentication, and Access Control

5.3.1.1 PR.AC-1: Identities and Credentials Are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes

This Cybersecurity Framework Subcategory is supported in the example solution by the Xage Security Fabric, Cisco ISE, and ConsoleWorks. The utility can establish identities and credentials by using the Xage Manager. These identities and credentials are used by the utility gateway in the cyber demarcation point. The utility gateway is implemented by the Xage Edge Node and Xage Enforcement Point. The microgrid operator can verify identities and credentials by using Cisco ISE. These permissions are used by the microgrid gateway in the cyber demarcation point and by the DER gateway on the microgrid. These gateways are implemented in the example solution by BlackRidge Technologies TAC Gateways.

ConsoleWorks manages the privileged access credentials used to access the management interfaces of Cisco ISE, the BlackRidge Enterprise Manager, and Cisco Cyber Vision.

5.3.1.2 PR.AC-3: Remote Access Is Managed

This Cybersecurity Framework Subcategory is supported by the reference architecture's cyber demarcation point. The cyber demarcation point uses identity to control access by the utility to DER devices on the microgrid network. The reference architecture has two separate policy domains: the utility domain and the microgrid operator domain. The cyber demarcation point consists of a utility gateway and a microgrid gateway. The utility controls the identities used and the access policy enforced by the utility gateway. The microgrid operator controls the identities used and the access policy enforced by the microgrid gateway. These two gateways control remote access by the utility to DER devices on the microgrid network.

5.3.1.3 PR.AC-4: Access Permissions and Authorizations Are Managed, Incorporating the Principles of Least Privilege and Separation of Duties

This Cybersecurity Framework Subcategory is supported in the example solution by the Xage Security Fabric, Cisco ISE, Anterix, and TDi ConsoleWorks. The utility can establish access permissions using the

Xage Manager. The permissions are used by the utility gateway in the cyber demarcation point. The utility gateway is implemented by the Xage Gateway and Xage Enforcement Point. The microgrid operator can configure access permissions using Cisco ISE. These permissions are used by the microgrid gateway in the cyber demarcation point and by the DER gateway on the microgrid. These gateways are implemented in the example solution by BlackRidge Technologies TAC Gateways.

The Anterix LTE network at UMD uses LTE's access control features to determine what devices are allowed to access the wireless network.

ConsoleWorks manages privileged user access permissions that determine who has access to the management interfaces of Cisco ISE, Cisco Cyber Vision, and BlackRidge enterprise manager. The access permission also details what actions a user is allowed to perform on each of these systems.

5.3.1.4 PR.AC-5: Network Integrity Is Protected (e.g., Network Segregation, Network Segmentation)

This Cybersecurity Framework Subcategory is supported by the reference architecture's cyber demarcation point and by network segmentation within the microgrid.

The utility is not exchanging information directly with the microgrid, but it is exchanging information through the cyber demarcation point. The reference architecture provides gateways to represent the microgrid and utility independently. Thus, the utility would manage communications and security interactions through its gateway; the microgrid operator would also manage its gateway and the assets on its side.

The microgrid implemented in the example solution has several distinct networks as shown in Figure 5: Data Analysis and Visualization. These networks are separated by pfSense virtual firewalls that isolate each network and control traffic and access among the networks.

5.3.2 Data Security

5.3.2.1 PR.DS-1: Data at Rest Is Protected

This Cybersecurity Framework Subcategory is supported by the reference architecture's command register capability. The command register provides protection at rest for the audit trail of information exchanges between the utility and microgrid operator. The ledger ensures the integrity of the audit trail records. The distributed nature of the ledger ensures availability of the audit trail records. In the example solution, the command register is implemented using Spherical Analytics' Immutably services. As records are received, Immutably invokes notaries that sign the records and attest to attributes of the records such as time received and source. This realizes the objective of a distributed, immutable audit trail of information exchanges.

The Xage Security Fabric uses a distributed ledger to protect security information, such as credentials and access permissions, that are needed by the Xage Edge Nodes and Xage Enforcement Points. The distributed ledger protects the integrity and availability of this information.

5.3.2.2 PR.DS-2: Data in Transit Is Protected

This Cybersecurity Framework Subcategory is supported using VPNs to encrypt traffic between the NCCoE lab and the solar arrays located on parking garages at UMD.

The example solution includes two physically separate sites—the NCCoE lab and the UMD infrastructure. Data in transit between the NCCoE and UMD is protected by a VPN by using two pfSense virtual firewalls that encrypt all traffic between the NCCoE lab and UMD.

The example solution also includes an LTE network that carries traffic from the termination point of the pfSense VPN in a UMD campus building to the solar arrays' control systems at two parking garages. Separate point-to-point VPNs over the LTE network connect each solar array to the pfSense VPN connection to the NCCoE lab. The point-to-point VPNs encrypt traffic from the UMD campus building to the solar array control systems at the parking garages. The LTE network itself also provides data encryption and data-integrity protection features.

A utility implementing its own private LTE network can choose to adopt additional security features to improve its security posture, as it deems most appropriate to its own mission and business considerations.

5.3.2.3 PR.DS-6: Integrity-Checking Mechanisms Are Used to Verify Software, Firmware, and Information Integrity

This Cybersecurity Framework Subcategory is supported by the reference architecture's command register.

The command register provides an immutable, fully distributed audit trail accessible by all parties involved in information exchanges. Using the command register, the full sequence of events between the utility and DER operators is observable by all parties.

In the example solution, the command register is implemented using a distributed ledger system. Each DER operator and the utility create a partial audit trail that is aggregated by the ledger to record all steps in an information exchange. The integrity of the ledger is verifiable, ensuring the integrity of the recorded audit trail.

5.3.3 Anomalies and Events

5.3.3.1 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and Systems Is Established and Managed

This Cybersecurity Framework Subcategory is supported by the utility cyber monitoring and microgrid cyber monitoring components of the cyber demarcation point in the reference architecture. The cyber monitoring components are self-training. They monitor network traffic and observe the normal behavior and flow of information into and out of the cyber demarcation.

In the example solution, the cyber monitoring components are implemented by Radiflow iSID and Cisco Cyber Vision. Each of these systems independently learns the expected traffic flows. If the flows are intentionally changed from those initially learned, the monitoring components can relearn the flows, or the expected flows can be manually configured to include changes.

5.3.3.2DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods

This Cybersecurity Framework Subcategory is supported by the utility cyber monitoring and microgrid cyber monitoring components of the cyber demarcation point and data analysis and visualization in the reference architecture.

In the example solution, the cyber monitoring components are implemented by Radiflow iSID and Cisco Cyber Vision. Each of these products has multiple analytic and reporting capabilities that can identify known cyber-attack techniques and help cyber analysts understand new attack methods and targets.

Data analysis and visualization analyzes log data from services on the microgrid network to identify suspicious behavior and to alert analysts. Log data is compared with the expected normal behavioral characteristics that are learned over time. Deviations from the expected normal behavior are reported as events.

5.3.3.3 DE.AE-3: Event Data Are Collected and Correlated from Multiple Sources and Sensors

This Cybersecurity Framework Subcategory is supported by the reference architecture's data analysis and visualization capability. The data analysis and visualization capability collects log information from multiple sources within the microgrid network and sends this data to a cloud analytics platform. At the cloud analytics platform, the log data is analyzed to identify evidence of malicious or unexpected activity.

In the example solution, this capability is implemented using syslog-ng syslog aggregators and the Sumo Logic cloud analytics platform. Systems and applications within the microgrid send their syslog records to one of three syslog-ng aggregators. The aggregators forward the log data to the Sumo Logic cloud analytics platform for analysis.

While not incorporated in the example solution, the cloud analytics platform allows controlled sharing of information from the DER operators to the utility. The utility can also share analytic results with the DER operators.

This Cybersecurity Framework Subcategory is supported by the utility monitoring and microgrid monitoring components of the cyber demarcation point. These components can collect monitoring data from multiple locations within the cyber demarcation point for correlation. In the example solution, this does not happen because Cisco Cyber Vision and Radiflow iSID, which implement the microgrid and utility cyber monitoring, are each configured to use a single sensor.

This Cybersecurity Framework Subcategory is supported by the command register in the reference architecture. The command register captures a complete audit trail of information exchanges between a utility and DER operators who provide power to the utility. This audit trail can be analyzed for anomalies in the way information exchanges occur. In the example solution, Spherical Analytics Immutably supports such analysis and reporting.

5.3.3.4 DE.AE-5: Incident Alert Thresholds Are Established

This Cybersecurity Framework Subcategory is supported by the utility cyber monitoring and microgrid cyber monitoring components of the cyber demarcation point as well as by the log analysis capability. Each of these monitoring and analysis capabilities has established thresholds for detecting anomalies and generating alerts.

5.3.4 Security Continuous Monitoring

5.3.4.1 The Information System and Assets Are Monitored to Identify Cybersecurity Events and Verify the Effectiveness of Protective Measures

This Cybersecurity Framework Subcategory is supported by the utility cyber monitoring and microgrid cyber monitoring components of the cyber demarcation point, and by the log analysis capability. Each of these monitors aspects of the system and identifies cybersecurity events.

5.3.4.2 DE.CM-2: The Physical Environment Is Monitored to Detect Potential Cybersecurity Events

This Cybersecurity Framework Subcategory is supported by the physical security systems at the NCCoE and UMD. Both the NCCoE and UMD have physical access control systems in place to control and monitor access to the physical locations where the example solution components are installed. NIST monitors the NCCoE physical access control system. UMD monitors its physical security system.

5.3.4.3 DE.CM-4: Malicious Code Is Detected

This Cybersecurity Framework Subcategory is supported by the utility cyber monitoring and microgrid cyber monitoring components of the cyber demarcation point. These components can detect some malicious code types based on analysis of monitored network traffic. In the example solution, these components are implemented by Radiflow iSID and Cisco Cyber Vision, each of which has some malicious-code-detection capability.

5.3.4.4 DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software Is Performed

This Cybersecurity Framework Subcategory is supported by the microgrid cyber monitoring component of the cyber demarcation point in the reference architecture. Additionally, it is supported by Cisco ISE in the example solution.

The microgrid cyber monitoring component, implemented in the example solution by Cisco Cyber Vision, develops a model of the expected devices and information flows. Unexpected devices or connections are detected and reported. Additionally, Cisco ISE is used to manage identities and network access to the microgrid network. Unauthorized attempts to connect to or use the microgrid network are detected and reported.

6 Future Project Considerations

The NCCoE recognizes that the example solution described in this practice guide demonstrates some of the tenets and principles of a zero trust architecture as defined in [NIST SP 800-207, Zero Trust Architecture](). While most discussions around zero trust architectures focus on implementations for IT business networks and use cases, future NCCoE Energy Sector projects might consider implementing a zero trust architecture in an ICS environment. For example, we might consider extending this example solution to include dynamic access control for DERs or other grid-edge devices connecting to the distribution grid.

Appendix A List of Acronyms

CISA	Cybersecurity and Infrastructure Security Agency
DER	Distributed Energy Resource
EPRI	Electric Power Research Institute
EPS	Electric Power System
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems–Computer Emergency Readiness Team
IIoT	Industrial Internet of Things
IT	Information Technology
LTE	Long-Term Evolution
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OT	Operational Technology
UMD	University of Maryland
VPN	Virtual Private Network

Appendix B References

[1] The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee, *Guidelines for Smart Grid Cybersecurity*, National Institute of Standards and Technology (NIST) Interagency or Internal Report 7628 Revision 1, Gaithersburg, Md., Sept. 2014, 290 pp. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[2] Institute of Electrical and Electronics Engineers (IEEE) Standards Coordinating Committee 21, IEEE 1547-2018: *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, April 6, 2018. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=8332110

[3] Cybersecurity and Infrastructure Security Agency, Industrial Control Systems Cyber Emergency Response Team, "Cyber Threat Source Descriptions." Available: https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions.

[4] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, Gaithersburg, Md., Apr. 16, 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf