NIST Special Publication 1800-7B

SITUATIONAL AWARENESS

For Electric Utilities

Volume B:
Approach, Architecture, and Security Characteristics for CIOs, CISOs, and Security Managers

Jim McCarthy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani
The MITRE Corporation
McLean, VA

February 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use_cases/situational_awareness

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-7B
Natl Inst. Stand. Technol. Spec. Publ. 1800-7B, 86 pages (February 2017)
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: February 16, 2017 through April 17, 2017

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
Mailstop 2002

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 or broad, cross-sector technology challenges. Working with technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily 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 Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

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

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) 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 more easily 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

Through direct dialogue between NCCoE staff and members of the energy sector (comprised mainly of electric power companies and those who provide equipment and/or services to them) it became clear that energy companies need to create and maintain a high level of visibility into their operating environments to ensure the security of their operational resources (OT), including industrial control systems, buildings, and plant equipment. However, energy companies, as well as all other utilities with similar infrastructure and situational awareness challenges, also need insight into their corporate or information technology (IT) and physical access control systems (PACS). The convergence of data across these three often self-contained silos (OT, IT, and PACS) can better protect power generation, transmission, and distribution.

Real-time or near real-time situational awareness is a key element in ensuring this visibility across all resources. Situational awareness, as defined in this use case, is the ability to comprehensively identify and correlate anomalous conditions pertaining to industrial control systems, IT resources, access to buildings, facilities, and other business mission-essential resources. For energy companies, having mechanisms to capture, transmit, view, analyze, and

store real-time or near-real-time data from industrial control systems (ICS) and related networking equipment provides energy companies with the information needed to deter, identify, respond to, and mitigate cyber attacks against their assets.

With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remediate them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping to demonstrate compliance with information security standards. This NCCoE project's goal is ultimately to improve the security of operational technology through situational awareness.

This NIST Cybersecurity Practice Guide describes our collaborative efforts with technology providers and energy sector stakeholders to address the security challenges energy providers face in deploying a comprehensive situational awareness capability. It offers a technical approach to meeting the challenge, and also incorporates a business value mind-set by identifying the strategic considerations involved in implementing new technologies. The guide provides a modular, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how we met the challenge using open source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case is based on an everyday business operational scenario that provides the underlying impetus for the functionality presented in the guide. Test cases were defined with industry participation to provide multiple examples of the capabilities necessary to provide situational awareness.

While the example solution was demonstrated with a certain suite of products, the guide does not endorse these products. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost effectively with an energy provider's existing tools and infrastructure.

KEYWORDS

cybersecurity; energy sector; information technology; physical access control systems; security event and incident management; situational awareness; operational technology, correlated events

ACKNOWLEDGMENTS

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

Name	Organization
Robert Lee	Dragos
Justin Cavinee	Dragos
Jon Lavender	Dragos
Gregg Garbesi	Engie
Steve Roberts	Hewlett Packard Enterprise
Bruce Oehler	Hewlett Packard Enterprise
Gil Kroyzer	ICS^2
Gregory Ravikovich	ICS^2
Robert Bell	ICS^2
Fred Hintermeister	NERC
Paul J. Geraci	OSIsoft
Mark McCoy	OSIsoft
Stephen J. Sarnecki	OSIsoft
Paul Strasser	PPC
Matt McDonald	PPC
Steve Sage	PPC
T.J. Roe	Radiflow
Ayal Vogel	Radiflow
Dario Lobozzo	Radiflow
Dave Barnard	RS2
Ben Smith	RSA, a Dell Technologies business
Tarik Williams	RSA, a Dell Technologies business
David Perodin	RSA, a Dell Technologies business
George Wrenn	Schneider Electric
Michael Pyle	Schneider Electric
AJ Nicolosi	Siemens
Jeff Foley	Siemens

Name	Organization
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Clyde Poole	TDi Technologies
Eric Chapman	University of Maryland, College Park
David S. Shaughnessy	University of Maryland, College Park
Don Hill	University of Maryland, College Park
Mary-Ann Ibeziako	University of Maryland, College Park
Damian Griffe	University of Maryland, College Park
Mark Alexander	University of Maryland, College Park
Nollaig Heffernan	Waratek
James Lee	Waratek
John Matthew Holt	Waratek
Andrew Ginter	Waterfall Security Solutions
Courtney Schneider	Waterfall Security Solutions
Tim Pierce	Waterfall Security Solutions
Kori Fisk	The MITRE Corporation
Tania Copper	The MITRE Corporation

The technology vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products 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	Build Involvement
Dragos	CyberLens
Hewlett Packard Enterprise	ArcSight
ICS^2	OnGuard
OSIsoft	Pi Historian
Radiflow	iSIM
RS2 Technologies	Access It!, Door Controller
RSA, a Dell Technologies business	Archer Security Operations Management
Schneider Electric	Tofino Firewall

Technology Partner/Collaborator	Build Involvement
Siemens	RUGGEDCOM CROSSBOW
TDi Technologies	ConsoleWorks
Waratek	Waratek Runtime Application Protection
Waterfall Security Solutions	Unidirectional Security Gateway, Secure Bypass

The NCCoE also wishes to acknowledge the special contributions of The University of Maryland, for providing us with a real-world setting for the Situational Awareness build; PPC (Project Performance Company), for their dedication in assisting the NCCoE with the very challenging and complex integration in this build; and the NCCoE EPC (Energy Provider Community), for their support and guidance throughout the lifecycle of this project.

Contents

List of Figures

List of Tables

1 Summary

Situational Awareness (SA) is "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[1] The intent of SA is to know what is happening around you and how it might affect your activities. For electric utilities, this means understanding what is happening in the environment that might affect delivery of electricity to customers. Traditionally, this has involved knowing the operating status of generation, transmission, and delivery systems, as well as physical challenges such as weather and readiness to respond to outages. As computers and networks have been incorporated in grid operations, awareness of the cyber situation is becoming increasingly important to ensuring that the lights stay on.

The National Cybersecurity Center of Excellence (NCCoE) met with energy sector stakeholders to understand key cybersecurity issues impacting operations. We were told that they need a more efficient means of comprehensively detecting potential cybersecurity incidents directed at their Operational Technology (OT) or Industrial Control Systems (ICS), Information Technology (IT) or corporate networks, and their physical facilities such as sub-stations and corporate offices.

The NCCoE's example solution provides a converged and correlated view of OT, IT, and physical access resources. In our reference design, we collect sensor data from these resources and provide alerts to a platform that produced actionable information.

This example solution is packaged as a "How To" guide that demonstrates how to implement standards-based cybersecurity technologies in the real world based on risk analysis and regulatory requirements. The guide might help the energy industry gain efficiencies in SA while saving research and proof-of-concept costs.

1.1 Challenge

Energy companies rely on operational technology to control the generation, transmission, and distribution of power. While there are a number of useful products on the market for monitoring enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of control system networks. ICS and IT devices were designed with different purposes in mind. Attempting to use IT security applications for ICS, although in many cases useful, still does not properly account for the availability requirements of ICS networks. A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots and provide real-time SA.

To improve overall SA, energy companies need mechanisms to capture, transmit, view, analyze, and store real-time or near-real-time data from ICS and related networking equipment. With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remediate them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time or near-real-time data from networks also has the benefit of helping organizations demonstrate compliance with information security standards or regulations.

There is a definite need to improve a utility's ability to detect cyber-related security breaches or anomalous behavior, in real or near-real time. The ability to do this will result in earlier detection of cybersecurity incidents and potentially reduce the severity of the impact of these incidents on a utility's operational infrastructure. Energy sector stakeholders noted that a

1. Endsley, M.R. (1995b). Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32-64

robust situational awareness solution also must be able to alert for both individual and correlated events or incidents. To address these needs, we considered a scenario in which a dispatcher at an operations center sees that a relay has tripped at a substation and begins to investigate the cause. The dispatcher uses a single software interface that monitors system buses, displays an outage map, correlates operational network connections to the bus and outage maps, and indexes logs from operational network devices and physical security devices. The dispatcher begins their investigation by querying network logs to determine whether any ICS devices received commands that might have caused the trip. If the answer is yes, then, using the same interface, the dispatcher can automatically see logs of the most recent commands and network traffic sent to the relevant devices. This information allows the technician to easily extend the investigation to internal systems and users who communicated with the suspect devices. To extend the scenario, a technician on the IT network receives notification that a server is down. The technician conducts an investigation across the network and is alerted of the tripped substation relay. Are the anomalies connected? Use of our SA solution would answer this question in addition to achieving the needs described above. Additional benefits of the solution are addressed in Section 1.4.

1.2 Solution

This NIST Cybersecurity Practice Guide demonstrates how commercially available technologies can meet your utility's need to provide comprehensive real-time or near-real time SA.

In our lab at the NCCoE, we built an environment that simulates the common devices and technologies found in a utility such as IT, OT, and physical access control systems (PACS). In this guide, we show how a utility can implement a converged alerting capability to provide a comprehensive view of cyber-related events and activities across silos by using multiple commercially available products. We identified products and capabilities that, when linked together, provide a converged and comprehensive platform that can alert utilities to potentially malicious activity.

The guide provides:

- a detailed example solution and capabilities that address security controls
- a demonstration of the approach using multiple, commercially available products
- how-to instructions for implementers and security engineers with instructions on integrating and configuring the example solution into their organization's enterprise in a manner that achieves security goals with minimum impact on operational efficiency and expense

Commercial, standards-based products such as the ones we used are readily available and interoperable with existing information technology infrastructure and investments. While our simulated environment might be most similar in breadth and diversity to the widely distributed networks of large organizations, this guide is modular and provides guidance on the implementation of unified SA capabilities to organizations of all sizes. These organizations include but are not limited to corporate and regional business offices, power generation plants, and substations.

This guide lists all the necessary components and provides installation, configuration, and integration information with the intent that an energy company can replicate what we have built. The NCCoE does not particularly endorse the suite of commercial products used in our reference design. These products were used after an open call to participate via the Federal Register. Your utility's security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your company can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

1.3 Risks

This practice guide addresses risk using current industry standards, such as the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards, as well as taking into account risk considerations at both the operational and strategic levels.

At the strategic level, you might consider the cost of mitigating these risks and the potential return on your investment in implementing a product (or multiple products). You might also want to assess if a converged SA platform can help enhance the productivity of employees, minimize impacts to your operating environment, and provide the ability to investigate incidents in order to mitigate future occurrences. This example solution addresses imminent operational security risks and incorporates strategic risk considerations.

Operationally, the lack of a converged SA platform, especially one with the ability to collect and correlate sensor data from all silos, can increase both the risk of malicious cyber attacks being directed at your organization, or worse, the resulting damage that might ensue should such attacks go undetected. At a fundamental level, SA provides alerts to potential malicious behavior, which includes detection, prevention, and reporting mechanisms to ensure that proper remediation and investigation take place should these events occur.

Adopting any new technology, including this example SA solution, can introduce new risks to your enterprise. However, by aggregating sensor data from the silos (OT, PACS, and IT), a utility can increase its ability to identify a potentially malicious event that might otherwise go undetected or unreported. The lack of ability to see across the silos and correlate event data yields a potential blind spot to the safe and secure operation of utilities' most critical business assets.

1.4 Benefits

The NCCoE, in collaboration with our stakeholders in the energy sector, identified the need for a network monitoring solution specifically adapted for control systems. The following are what we determined to be the key (but not exclusive) benefits for implementing this solution:

- improves a utility's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of critical incidents on energy delivery, thereby lowering overall business risk
- increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- improves accountability and traceability, leading to valuable operational lessons learned
- simplifies regulatory compliance by automating generation and collection of a variety of operational log data

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the example solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-7a: *Executive Summary*
- NIST SP 1800-7b: *Approach, Architecture, and Security Characteristics* - what we built and why **(you are here)**
- NIST SP 1800-7c: *How-To Guides* - instructions for building the example solution

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 1800-7a)*, which describes the:

- challenges energy sector organizations face in maintaining cross-silo situational awareness
- example solution built at the NCCoE
- 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 1800-7b*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment and Mitigation, provides a description of the risk analysis we performed
- Section 3.4.2, Security Characteristics and Controls Mapping, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-7a*, with your leadership team members to help them understand the importance of adopting standards-based situational awareness solution.

Industrial Control Systems and Information Technology Security professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-7c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate 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 professionals have experience implementing security products within the enterprise. While we have used 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 a solution including PACS, OT, IT systems, and business processes. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

2.1 Typographical Conventions

The following table presents typographic conventions used in this volume.

Table 2.1 Typographical Conventions

Typeface/Symbol	Meaning	Example
italics	▪ filenames and pathnames ▪ references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*.
bold	names of menus, options, command buttons, and fields	Choose **File > Edit**
`Monospace`	command-line input, on-screen computer output, sample code examples, 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 National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

3 Approach

The NCCoE initiated this project because security leaders in the energy sector told us that a lack of cross-silo SA was a primary security concern to them. As we developed and refined the original problem statement, or use case, on which this project is based, we consulted with chief information officers, chief information security officers, security management personnel, and others with financial decision-making responsibility (particularly for security) in the energy sector.

Energy sector colleagues shared that they need to know when cybersecurity events occur throughout the organization. Additionally, the information generated about such events should be used to correlate data between various sources before arriving at a converged platform. Security staff need to be aware of potential or actual cybersecurity incidents in their IT, OT and PACS systems, and to view these alerts on a single converged platform. Furthermore, it is essential that this platform has the ability to drill down, investigate, and subsequently fully remediate or effectively mitigate a cybersecurity incident affecting any or all of the organization.

The example solution in this guide uses commercially available capabilities designed to perform these critical functions. Though security components and tools already exist in most utilities, the value of this NCCoE build can be seen in its ability to span across all silos and correlate sensor data. Currently, utilities rely on separate, and perhaps disparate, systems to provide security data. It is time consuming for staff to comb through OT or IT device event logs, physical access data, and other system data in order to trace anomalies to their source. A real-time SA platform with a well-developed alerting mechanism can speed up the process of detecting potentially malicious events, providing the information necessary to focus an investigation, making a determination regarding the potential issue, and remediating or mitigating any negative effects.

We constructed an end-to-end SA platform that includes many of the components necessary to eliminate or mitigate the impact of attacks directed at utilities. The solution employs the use of actual grid data sent to numerous applications and devices to increase cybersecurity. The solution includes:

- asset inventorying (especially for ICS devices)
- data-in-transit encryption
- advanced security dashboard views
- configuration change alerts
- behavioral anomaly detection
- SIEM capability
- unidirectional gateway functionality for ICS network protection
- single source timestamping and log transmission capability
- Structured Query Language (SQL) injection detection
- intrusion detection/prevention

3.1 Audience

This guide is intended for individuals or entities who are interested in understanding the architecture of the end-to-end situational awareness platform the NCCoE has designed and implemented to enable energy sector security staff to receive correlated information on cybersecurity events that occur throughout their IT, OT, and PACS systems on a single, converged platform. It may also be of interest to anyone in the energy sector, industry, academia, or government who seeks general knowledge of an original design and benefits of a situational awareness security solution for energy sector organizations.

3.2 Scope

The focus of this project is to address the risk of not being able to prevent, detect, or mitigate cyberattacks against OT, IT, and PACS infrastructure in a timely manner, a topic indicated by the energy sector as a critical cybersecurity concern. In response, the NCCoE drafted a use case that identified numerous desired solution characteristics. After an open call in the Federal Register for vendors to help develop a solution, we chose participating technology collaborators on a first come, first served basis.

We scoped the project to produce the following high-level desired outcomes:

1. provide a real-time, converged SA capability that includes sensor data from OT, IT and PACS networks and devices
2. provide a variety of cyber attack prevention, detection, response, reporting, and mitigation capabilities
3. correlate meaningful sensor data between silos, or between devices within individual silos, that will produce actionable alerts
4. provide a single view of this correlated alerting platform data which can be customized to accommodate the needs of individual organizations

The objective is to perform all four capabilities and display on a single interface that can serve as the authoritative source for security analysts monitoring the security of the assets on an energy provider's facilities, networks, and systems.

3.3 Assumptions

This project is guided by the following assumptions, which should be considered when evaluating whether to implement the solution in your organization.

3.3.1 Security

The SA example solution supports data monitoring, collection, aggregation, and analysis, with the goal of enabling a robust SA capability.

In the security analysis, we assume that all potential adopters of the build or of any of its components already have in place some degree of network security. Therefore, we focus only on new security protections provided by the reference design and new vulnerabilities that might be introduced if organizations implement the reference design. The security analysis cannot be expected to identify all weaknesses, especially those that might be introduced in a specific deployment or by specific commercial off-the-shelf products.

3.3.2 Existing Infrastructure

We assume that you already have some combination of the capabilities discussed in this example solution. A combination of some of the components described here, or a single component, can improve your overall security posture for OT, IT and PACS, without requiring you to remove or replace your existing infrastructure. This guide provides both a complete end-to-end solution and options you can implement based on your needs.

This example solution is made of many commercially available components. The solution is modular in that you can swap one of the products we used for one that is better suited for your environment.

3.3.2.1 Technical Implementation

The guide is written from a "how-to" perspective. Its foremost purpose is to provide details on how to install, configure, and integrate components, and how to construct correlated alerts based on the capabilities we selected. We assume that an energy provider has the technical resources to implement all or parts of the example solution, or has access to integrator companies that can perform the implementation.

3.3.3 Capability Variation

We fully understand that the capabilities presented here are not the only security capabilities available to the industry. Desired security capabilities will vary considerably from one company to the next. As mentioned in the scope, our key here is to provide SA utilizing sensor data from OT, IT and PACS. We selected what we believe to be a basic and fundamental approach to SA.

3.4 Risk Assessment and Mitigation

We performed two types of risk assessment: the initial analysis of the risk posed to the energy sector as a whole, which led to the creation of the use case and the desired security characteristics, and an analysis to show users how to manage the risk to components introduced by adoption of the solution.

3.4.1 Assessing Risk Posture

According to NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of the Risk Management Framework (RMF)[1] material available to the public.

Using the guidance in NIST's series of SPs concerning the RMF, we performed two key activities to identify the most compelling risks encountered by energy providers. The first activity was a face-to-face meeting with members of the energy community to define the main security risks to business operations. This meeting identified a primary risk concern: the lack of a comprehensive or cross-silo SA capability, particularly one that would include sensor data from OT networks and devices. We then identified the core risk area, SA, and established the core operational risks encountered daily in this area.

We deemed the following as tactical risks:

- lack of data visualization and analysis capabilities that help dispatchers and security analysts view control system behavior, network security events, and physical security events as a cohesive whole
- lack of analysis and correlation capabilities that could help dispatchers and security analysts understand and identify security events and predict how those events might affect control system operational data from a variety of sources
- inability to aggregate and correlate logs, traffic, and operational data from a variety of sources in OT, IT, and PACS device networks
- inability to allow dispatchers and security analysts to easily automate common, repetitive investigative tasks

Our second key activity was conducting phone interviews with members of the energy sector. These interviews gave us a better understanding of the actual business risks as they relate to the potential cost and business value. NIST SP 800-39, *Managing Information Security Risk*, focuses particularly on the business aspect of risk, namely at the enterprise level. This foundation is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. Below is a summary of the strategic risks:

- impact on service delivery
- cost of implementation
- budget expenditures as they relate to investment in security technologies
- projected cost savings and operational efficiencies to be gained as a result of new investment in security
- compliance with existing industry standards
- high-quality reputation or public image
- risk of alternative or no action
- successful precedents

Undertaking these activities in accordance with the NIST RMF guidance yielded the necessary operational and strategic risk information, which we subsequently translated to security characteristics. We mapped these characteristics to NIST's SP 800-53 Rev.4 controls where applicable, along with other applicable industry and mainstream security standards.

1.National Institute of Standards and Technology (NIST), Risk Management Framework (RMF) http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/

3.4.2 Security Characteristics and Controls Mapping

As explained in Section 3.4.1, we derived the security characteristics through a risk analysis process conducted in collaboration with our energy sector stakeholders. This is a critical first step in acquiring or developing the capability necessary to mitigate the risks as identified by our stakeholders. Table 3.1 presents the desired security characteristics of the use case in terms of the subcategories of the Framework for Improving Critical Infrastructure Cybersecurity. Each subcategory is mapped to relevant NIST standards, industry standards, controls, and best practices. We did not observe any example solution security characteristics that mapped to Respond or Recover Subcategories.

Table 3.1 Security Characteristics and Controls Mapping—NIST Cybersecurity Framework (CSF)

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU family	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	CSC-6	CIP-006-6

Table 3.1 Security Characteristics and Controls Mapping—NIST Cybersecurity Framework (CSF)

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Detect	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, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6
	DE.AE-4: Impact of events is determined	CP-2, IR-4, RA-3, SI-4			CIP-008-5
	DE.AE-5: Incident alert thresholds are established	IR-4, IR-5, IR-8			CIP-008-5
	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4			CIP-005-5 CIP-007-6
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20			CIP-006-6
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	A.12.4.1		CIP-006-6
	DE.CM-4: Malicious code is detected	SI-3	A.12.2.1	CSC-5	CIP-007-6
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4			CIP-005-5

a. Mapping taken from “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014

b. Mapping taken from “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014

c. Mapping prepared using “The CIS Security Controls for Effective Cyber Defense, Version 6.0,” Center for Internet Security, October 15, 2015

d. Mapping prepared using http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

3.5 Technologies

Table 3.2 lists all of the technologies used in this project and provides a mapping between the generic application term, the specific product used, and the security control(s) that the product provides in the example solution[2]. Table 3.2 describes only the functions and CSF subcategories implemented in the example solution. Products may have functionality not described in the table. Refer to Table 3.1 for an explanation of the CSF Subcategory codes.

Table 3.2 Products and Technologies

Component	Product	Function	CSF Subcategories
Security Information and Event Management (SIEM)	HPE ArcSight	▪ aggregates all IT, windows, OT (ICS) and physical access monitoring, event, and log data collected by the reference design ▪ acts as a data normalization and correlation point and enables queries to be developed and executed to detect potential security incidents ▪ serves as the central location at which the analyst can access all data collected	DE.AE-3, DE.AE-5 Related Subcategories: PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-7
Network Tap	IXIA TP-CU3 Tap	▪ collects data from specific locations on the ICS network and send it to the monitoring server via the ICS firewall ▪ the taps are passive, so if they lose power or otherwise fail, they will not adversely affect the ICS network ▪ collects data via monitor ports that are inherently unidirectional (and so do not pose any threat of information leaking from the tap onto the ICS network)	DE.CM-1

2.Note that two instances of the log collector component are present in the reference design: one in the reference design's monitoring/data collection sub-architecture and another in its data aggregation/analysis sub-architecture. Integrity seals that are applied by a log collector can only be verified at that log collector. Therefore, the log collector that is in the operations facility does not apply an integrity seal to its entries because these integrity seals cannot be verified in the enterprise.

Table 3.2 Products and Technologies

Component	Product	Function	CSF Subcategories
Log Collector/ Aggregator	TDi Technologies ConsoleWorks	▪ log collection and aggregation ▪ adds a time stamp and integrity seals the log entries ▪ log collection in the operations facility protects against potential data loss in the event that the communications channel between the operations and enterprise facilities fails ▪ aggregating the log entries of all monitoring components at the operations log collector/aggregator ensures that this log data gets buffered in the operations facility and can be transferred later in the event that network connectivity to the enterprise network is lost	PR.DS-6, PR.DS-6, PR.PT-1, DE.AE-3
ICS Asset Management System	Dragos Security CyberLens	▪ monitors ICS traffic and maintains a database of all ICS assets of which it is aware ▪ this enables it to detect new ICS devices, ICS devices that disappear, and changes to known ICS devices	ID.AM-1
Network Visualization Tool	Dragos Security CyberLens	▪ displays a depiction of network devices, connectivity, and traffic flows	Does not directly support a CSF subcategory. Related Subcategory: ID.AM-3
Physical Access Control System	RS2 Access It!	▪ controls user access to doors ▪ detects and reports door open/close events and user identity	PR.AC-2
Physical Access Sensor	RS2 door controller	▪ senses door close/open events ▪ generates alerts when door open and close events occur	DE.CM-2
ICS Network Intrusion Detection System (IDS)	Radiflow iSIM	▪ identify, monitor, and report anomalous ICS traffic that might indicate a potential intrusion	DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-7

Table 3.2 Products and Technologies

Component	Product	Function	CSF Subcategories
Historian	OSIsoft Pi Historian	▪ serves as a data repository that essentially replicates the database of collected ICS values on the ICS network's Historian ▪ can be configured to generate alerts when changes to certain ICS process values occur	Does not support a CSF subcategory in and of itself. It provides the data to be monitored by the ICS behavior monitor (next item). Related Subcategories: DE.AE-5, DE.CM-1
ICS Behavior Monitor	ICS^2 On-Guard	▪ monitor ICS process variable values in the Historian to assess application behavior, detect process anomalies, and generate alerts	DE.AE-5, DE.CM-1
Application Monitor & Protection	Waratek Runtime Application Protection	▪ monitors & protects a running application, analyzes the data it collects, and detects and reports unusual application behavior, e.g., it might generate an alert if it detects a potential SQL injection attack against the SIEM	DE.AE-2, DE.AE-4, DE.AE-5, DE.CM-4
Analysis Workflow Engine	RSA Archer Security Operations Management	▪ automates workflow associated with review and analysis of data that has been collected at the SIEM ▪ enables orchestration of various analytic engines	DE.AE-2
Unidirectional gateway	Waterfall unidirectional security gateway	▪ allows data to flow in only one direction	PR.AC-5, PR.PT-4
Visualization Tool	RSA Archer Security Operations Management	▪ provides data reduction and a dashboard capability for the data in the SIEM, as well as risk analysis	This component does not support a CSF subcategory in and of itself. Related Subcategory: ID.AM-3

Table 3.2 Products and Technologies

Component	Product	Function	CSF Subcategories
Electronic Access Control and Monitoring Systems (EACMS)	TDi Technologies ConsoleWorks	▪ authenticates system managers ▪ provides role-based access control of system management functions ▪ implements a “protocol break” between the system manager and the managed assets ▪ records all system management actions	PR.AC-3, PR.AC-4, PR.MA-2, PR.PT-1, PR.PT-3, DE.CM-3
	Siemens RUGGEDCOM CROSSBOW	▪ authenticates system managers ▪ provides role-based access control of system management functions ▪ implements a “protocol break” between the system manager and the managed assets ▪ records all system management actions	PR.AC-3, PR.AC-4, PR.MA-2, PR.PT-1, PR.PT-3, DE.CM-3
	Waterfall Secure Bypass	▪ provides time-limited network connectivity to perform system management functions	PR.AC-5, PR.PT-4
	Schneider Electric Tofino Firewall	▪ controls network connectivity for performing system management functions	PR.AC-5, PR.PT-4

3.6 Situational Awareness Test Cases

Table 3.3 Situational Awareness Test Cases

Test Case	Purpose	Operational Description	Events	Desired Outcome
SA-1: Event Correlation for OT and PACS	This test case focuses on the possibility of correlated events involving OT and PACS that might indicate compromised access.	This test case considers the correlation of events from two silos, which provides an indication of a potential security issue to the SIEM. A technician entering a sub-station is inconsequential and expected behavior. However, if a device goes down and triggers alarms within a certain time frame, there is a possible correlation of these two events. It should not automatically be assumed that malicious behavior is the cause. There might be scheduled maintenance to be performed on a certain device, which would provide a perfectly reasonable explanation for this test case. The key here is the correlation of the activity, which provides an indicator that could narrow possibilities and start an investigation into the activity more quickly than having an analyst looking at individual events and attempting to correlate them manually. To learn more about the data fields used to create the alert, see section 3.2.1 of NIST SP 1800-7c, Test Cases.	▪ technician accesses sub-station/ control-station ▪ OT device goes down	▪ alert of anomalous condition that correlates to a physical and ICS network event

Table 3.3 Situational Awareness Test Cases

Test Case	Purpose	Operational Description	Events	Desired Outcome
SA-2 Event Correlation - OT & IT	SQLi injection detection	This test case demonstrates how SQL injections (SQLi) can be detected. In this instance, the baseline assumption is that applications in the IT (corporate/enterprise) network can conduct limited communication with some devices in the OT network to generate information needed by corporate operations on usage, billing, accounting, or some other type of business information. This is a common scenario-typically a specific Historian would be dedicated for this purpose, perhaps in a network demilitarized zone (DMZ). This scenario is definitely preferable, but there are too many variations in networks to account for all of them. The example we provide is focused on the detection of SQLi, specifically directed at OT devices or devices connected to OT devices. To learn more about the data fields used to create the alert, see section 3.2.1 of NIST SP 1800-7c, Test Cases.	▪ detection of SQLi on IT device interconnected with OT device	▪ alert sent to SIEM on multiple SQLi attempts

Table 3.3 Situational Awareness Test Cases

Test Case	Purpose	Operational Description	Events	Desired Outcome
SA-3 Event Correlation - OT & IT / PACS-OT	Unauthorized access attempts detected and alerts triggered based on connection requests from a device on the Supervisory Control and Data Acquisition (SCADA) network destined for an internet protocol (IP) that is outside of the SCADA IP range. This test case focuses on the possibility of a malicious actor attempting to gain access to an OT device via the Enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.	Unauthorized access attempts can be made in numerous ways. For test case 3, we demonstrate an alerting capability that triggers when an ICS device located on the OT network attempts to communicate with an IT device outside of the authorized parameters. A key assumption here is that proper security measures have been instituted on the OT network to detect and alert for false connection requests. This scenario can also be correlated with PACS and OT, where numerous failed login attempts on a particular device trigger alerts to the SIEM. Since the origination of the connection attempt starts within the OT network, one must first investigate internally to determine the location of the device and who had access to the location where all of this activity occurred. To learn more about the data fields used to create the alert, see section 3.2.1 of NIST SP 1800-7c, Test Cases.	▪ inbound/outbound connection attempts from devices outside of authorized and known inventory	▪ alert to SIEM showing IP of unidentified host attempting to connect, or identified host attempting to connect to unidentified host

Table 3.3 Situational Awareness Test Cases

Test Case	Purpose	Operational Description	Events	Desired Outcome
SA-4 Data Infiltration Attempts:	Examine behavior of systems; configure SIEM to alert on behavior which is outside the normal baseline. Alerts can be created emanating from OT, IT and PACS. This test case seeks alerting based on behavioral anomalies, rather than recognition of IP addresses, and guards against anomalous or malicious inputs.	Baselining the proper operations and communications of an OT network is essential to being able to detect behavioral anomalies. Inserting security capabilities to confirm the normal operation of the OT network and alert to the detection of anomalous behavior provides an essential SA capability to the operator. Anomalous behavior can include any type of security or operational issue which falls outside of pre-defined thresholds. Here, we seek to focus specifically on anomalous behavior as it relates to data changes in the ICS protocols that could provide an indication of a security concern; whether it be data infiltration (rogue data inputs and/or malicious data manipulation), or some other variance that falls outside of the what is considered to be the normal baseline. To learn more about the data fields used to create the alert, see section 3.2.1 of NIST SP 1800-7c, Test Cases.	▪ anomalous behavior falling outside defined baseline	▪ alert sent to SIEM on any event falling outside of what is considered normal activity based on historical data
SA-5 Configuration Management	Unauthorized (inadvertent or malicious) uploading of an ICS network device configuration. Alert will be created to notify SIEM this has occurred. Detection method will be primarily based on inherent device capability (i.e. log files).	For this test case, we focused on the unauthorized loading of a new configuration on a networking or security device in the ICS network. If a firewall, switch, or router configuration change is made, the SA solution can detect the change and send an alert to the SIEM. The SIEM provides awareness of these changes to those concerned with the security of the OT network and devices. Once they have the information, they can determine whether or not the change was authorized. Malicious changes to the OT network or devices, if undetected, can pave the way for numerous exploits and reintroduce significant risk to the OT network. To learn more about the data fields used to create the alert, see section 3.2.1 of NIST SP 1800-7c, Test Cases.	▪ configuration change on Tofino FW, Cisco 2950	▪ alert will be created to notify SIEM this has occurred

Table 3.3 Situational Awareness Test Cases

Test Case	Purpose	Operational Description	Events	Desired Outcome
SA-6 Rogue Device Detection	Alerts are triggered by the introduction of any device onto the ICS network that has not been registered with the asset management capability in the build.	A primary concern of ICS owners and operators is the introduction of unauthorized devices onto the OT network. This test case focuses on the introduction of a device that has not been previously registered to the asset management tool. This test case assumes the absolute necessity of having an ICS asset management tool in place, and properly maintaining inventory throughout the lifecycle of all the devices. It is essential that this be in place, as determining the difference between authorized and unauthorized devices will be extremely difficult without one. To learn more about the data fields used to create the alert, see section 3.2.1 of NIST SP 1800-7c, Test Cases.	■ unidentified device appears on ICS network	■ alert will be created to notify SIEM this has occurred

4 Architecture

"Cyber situational awareness involves the normalization, de-confliction, and correlation of disparate sensor data and the ability to analyze data and display the results of these analyses."[1] This guide presents an architecture for instrumenting the ICS network of a utility's OT silo with sensors to collect cyber events. These events are then sent to a SIEM system where they are normalized and correlated with cyber events from the IT silo and physical access events. Once collected in the SIEM, events from all three silos can be analyzed to provide a converged picture of the cyber situation. Relevant information from this converged picture can then be provided to OT, IT, and physical security personnel.

This section describes both an example solution for providing converged situational awareness across OT, IT and physical security and a prototype implementation or "lab build" of the example solution constructed by NCCoE to validate the example solution.

- Section 4.1, Example Solution Description, describes the logical components that make up the example solution.
- Section 4.2, Example Solution Monitoring, Data Collection, and Analysis, provides details of the components used to monitor and collect data from operations, transmit the data to the enterprise services, and analyze the collected data to identify events of interest and detect potential cyber incidents.
    - Section 4.2.1, Example Solution Monitoring and Data Collection Lab Build, describes the lab prototype of the Monitoring and Data Collection portion of the example solution.
    - Section 4.2.2, Example Solution Data Aggregation and Analysis Lab Build, describes the lab prototype of the Data Aggregation and Analysis portion of the example solution.
- Section 4.3, Example Solution Remote Management Connection, provides details of the components that comprise the on-demand limited-access remote management connection.
    - Section 4.3.1, Example Solution Operations Remote Management Lab Build, describes the lab prototype of remote management for Operations facilities.
    - Section 4.3.2, Example Solution Enterprise Remote Management Lab Build, describes the lab prototype of remote management for Enterprise services.

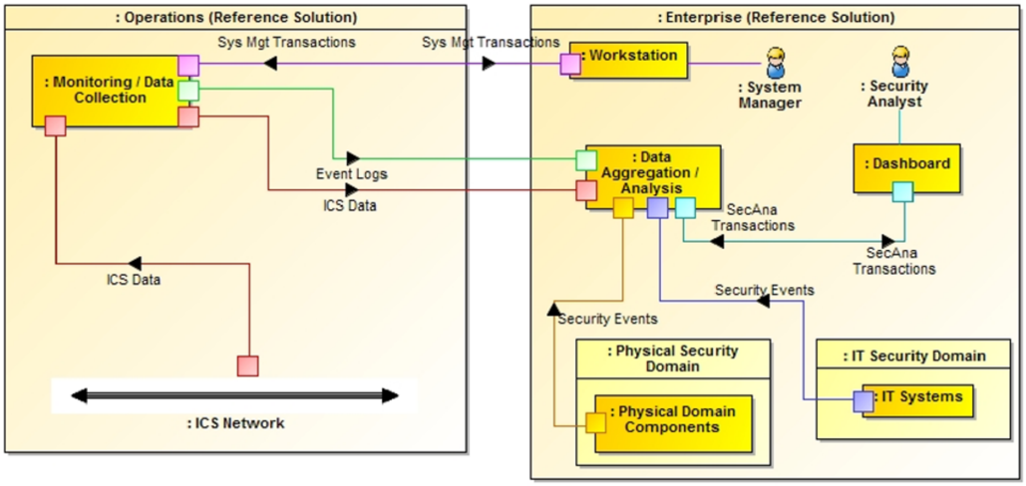
4.1 Example Solution Description

A high-level view of the example solution is depicted in Figure 4.1. The solution consists of a Monitoring/Data Collection component, which is deployed to Operations facilities such as substations and generating plants, and a Data Aggregation/Analysis component that is deployed as a single service for the enterprise. Data is collected from the ICS network by the Monitoring/Data Collection component, and sent to the Data Aggregation/Analysis component. To protect the ICS network and the Operations facility, the flow of data is restricted to be unidirectional out of Operations and into the Enterprise services.

At the Enterprise Data Aggregation/Analysis component data from the ICS network is combined with data from physical security monitoring and business systems monitoring. Combining monitoring data from Operations, physical security, and business systems is the basis for providing comprehensive cyber situational awareness.

1.http://itlaw.wikia.com/wiki/Cyber_situational_awareness

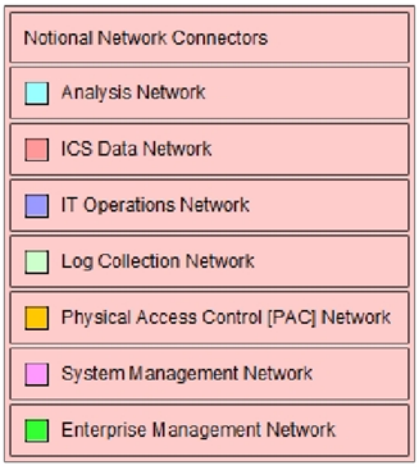
Figure 4.1 High-level Example Solution Architecture



In addition to the unidirectional flow of monitoring data out of operations, an on-demand, limited-access bidirectional system management connection is provided from the enterprise to each operations facility. This connection provides remote access to manage the software that monitors the ICS network and operations components.

Figure 4.2 provides a color-coded legend identifying the different types of network connections portrayed in diagrams throughout section 4.

Figure 4.2 Network Connections Color Code



- Analysis network - connects situational awareness analysis functions
- ICS Data Network - connects ICS monitoring functions
- IT Operations Network - connects IT business systems
- Log Collection Network - connects log collection and aggregation functions
- Physical Access Control (PAC) Network - connects physical access control functions

- System Management Network - provides system managers remote access to ICS monitoring functions
- Enterprise Management Network - provides vendor remote access to the NCCoE energy sector lab

4.2 Example Solution Monitoring, Data Collection, and Analysis

Figure 4.3 depicts the monitoring and data collection components deployed in operations and the data aggregation and analysis components deployed as enterprise services. Operations has five main sources of monitoring information:

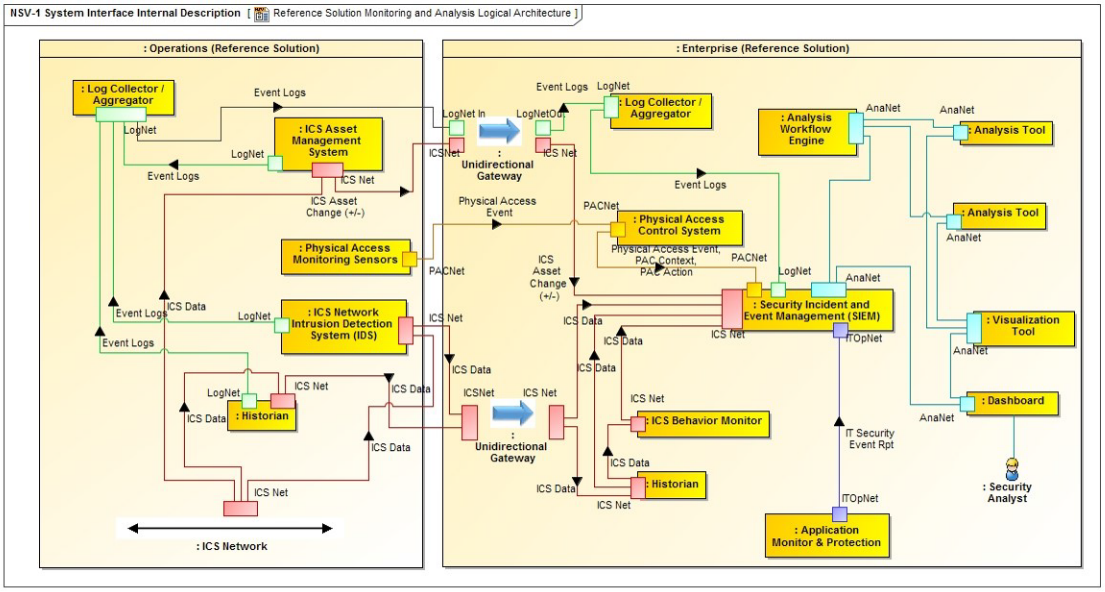
- ICS Asset Management System - this component monitors the ICS network to identify the devices connected to and communicating over the network. It sends an event to the enterprise Security Information and Event Management (SIEM) system when a new device is identified on the ICS network, or if a known device disappears from the network.
- ICS Network Intrusion Detection system - this component monitors ICS network traffic for traffic that matches a signature of known suspicious activity. When suspicious activity is detected, an event is sent to the enterprise SIEM.
- Historian - this component collects parameter values from the industrial control systems in operations and replicates them to a second Historian in enterprise. The operations Historian is assumed to be an existing ICS component.
- Log Collector/Aggregator - this component collects log data from all of the other monitoring components in operations, stores them locally, and replicates the log data to another log collector aggregator in enterprise. Logs are captured and stored locally to prevent loss of log data should communications between operations and enterprise be disrupted.
- Physical Access Monitoring Sensors - these components monitor physical access to the operations facility. They detect events such as doors opening or closing and report those events to the PACS in enterprise.

A unidirectional gateway connects monitoring functions in Operations to analysis functions in Enterprise. This ensures data flows in only one direction, out of Operations.

Enterprise contains the following components:

- Log Collector/Aggregator- this component receives log data from the operations facilities and sends it to the SIEM.
- Physical Access Control System (PACS) - this component monitors physical access to all facilities and generates events to the SIEM when physical access occurs, such as doors or windows being opened and closed.

Figure 4.3 Monitoring, Data Collection, and Analysis Example Solution



- Historian - this component receives replicated ICS data from the operations Historian.
- ICS Behavior Monitor - this component compares ICS data from the Historian with expected values based on normal operations. It sends events to the SIEM when ICS data deviates from normal behavior on a particular ICS network.
- Application Monitor & Protection - this component monitors IT applications for suspicious behavior and sends events to the SIEM
- Security Information and Event Management (SIEM) system - this component receives and stores events from sensors, normalizes the data, correlates events from multiple sensors, and generates alerts.
- Analysis Workflow Engine - to the extent feasible, this component automates the execution of courses of action related to events collected in the SIEM.
- Analysis Tools - these components implement algorithms that examine data from the SIEM to identify events of interest and potential cyber incidents. These components report this information to security analysts via the visualization tool.
- Visualization Tool - this component provides alerts and other cyber SA information to security analysts and allows them to examine the underlying data that lead to an alert.

Enterprise components serve one of two primary responsibilities, collect event data from operations into a common repository, the SIEM, or analyze data in the SIEM to detect suspicious events and potential cyber incidents.

A unidirectional gateway is used to ensure the data flows from the components in Operations that monitor the ICS network are one-way data flows from Operations to Enterprise.

4.2.1 Example Solution Monitoring and Data Collection Lab Build

Figure 4.4 shows the products used to build an instance of the monitoring and data collection portion of the example solution. The instance was constructed at the University of Maryland's (UMd) power cogeneration plant. As a result of this collaboration with UMd, the NCCoE was able to utilize real grid data and process it through our build collaborator's security devices and applications. Though this certainly added to the complexity of the build, we believe using UMd's grid data provides an actual real-life implementation of ICS network security solutions that can be replicated at other utilities. The NCCoE energy sector lab provides the enterprise facility described in the example solution. A Virtual Private Network (VPN) is used in the lab build to protect data in transit between the operations facility and the enterprise facility. The VPN was established using a Siemens RUGGEDCOM RX1501 (O1) at the cogeneration facility and a Siemens RUGGEDCOM RX1400 at the NCCoE. The RX1501 includes firewall capabilities to control which TCP ports are available to communicate with the NCCoE.

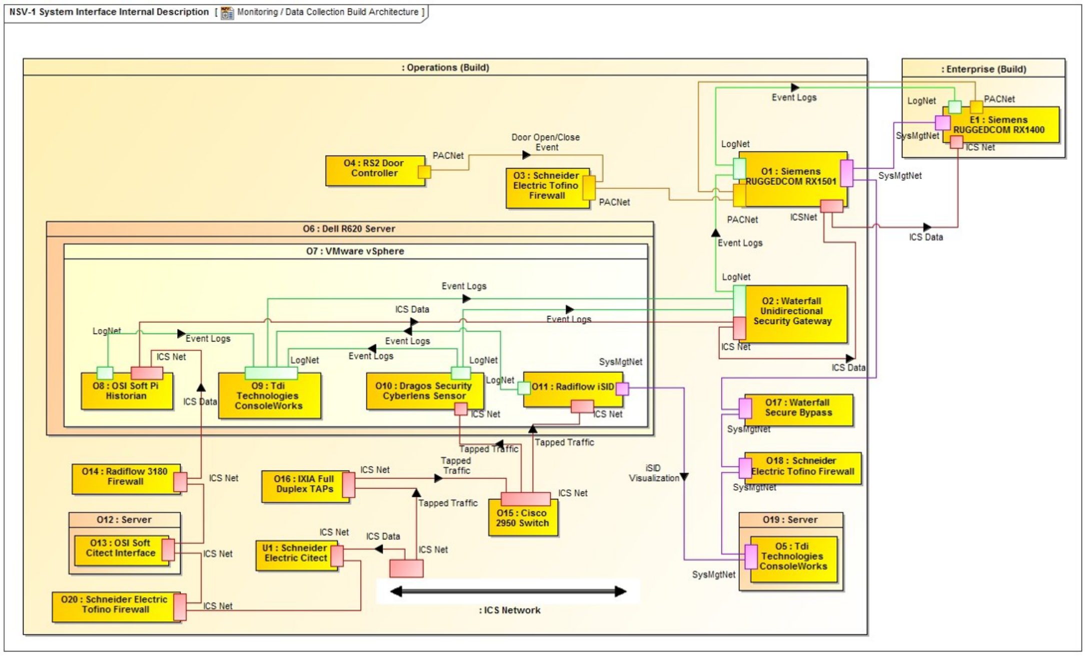
When implementing the example solution, utilities need to consider the type of network connection in place between Operations and Enterprise to determine what protection might be needed for data in transit.

The physical access sensor in the example solution is provided by an RS2 door controller (O4). The controller monitors a door open/close switch and sends events whenever the door at the facility is opened or closed. This information is sent over the build collaborator's enterprise network. To prevent unintended interactions between the collaborator's enterprise network and the NCCoE energy sector lab, a Schneider Electric Tofino firewall (O3) is installed between the collaborator's enterprise network and the VPN.

A Dell R620 server (O6) running VMware (O7) was deployed to the cogeneration facility to host monitoring and data collection software. These are infrastructure components needed for the lab build but not considered part of the example solution.

The Historian in the example solution was implemented by an OSISoft Pi Historian (O8) installed on the Dell server (O6). In this case, the Historian was not an existing component in the facility. This facility uses a Schneider Electric Citect SCADA system to control operations. ICS data for the facility is collected and stored by this Citect SCADA system. To collect this data, the OSIsoft Citect Interface software (O13) is used to pull data from the Citect SCADA system (U1) and store it in an OSIsoft Pi Historian (O8). To ensure that data flow from the Citect SCADA system (U1) to the OSIsoft Pi Historian (O8) is unidirectional, the Citect Interface software (O13) is installed on a dedicated physical server (O12), isolated from the Citect SCADA system by a Schneider Electric Tofino firewall (O20), and isolated from the Pi Historian (O8) by a Radiflow 3180 firewall (O14). The Pi Historian (O8) replicates data to another Pi Historian in the NCCoE energy sector lab.

Figure 4.4 Operations Monitoring and Data Collection Lab Build Architecture



The ICS Asset Management system in the example solution is implemented by Dragos Security CyberLens. CyberLens is deployed in the cogeneration facility as a sensor (O10), which monitors the ICS network, collects relevant information in files, and transfers the files to a CyberLens server in the NCCoE energy sector lab.

The ICS Intrusion Detection component in the example solution is provided by Radiflow iSID (O11). Events detected by iSID (O11) are sent via syslog to the log collector/aggregator implemented by TDi Technologies ConsoleWorks (O9). In addition to log data from iSID (O11), ConsoleWorks (O9) also collects log data via syslog from CyberLens Sensor (O10) and the Pi Historian (O8). ConsoleWorks (O9) augments the syslog records with an additional time stamp and an integrity seal. These records are stored in files which are transferred to another instance of ConsoleWorks in the NCCoE energy sector lab.

Both CyberLens Sensor (O10) and iSID (O11) need ICS network data as input. To get this data without affecting the network traffic used to run the cogeneration facility, IXIA full duplex taps (O16) were installed in the ICS network at appropriate points. These taps are designed to ensure ICS network traffic flow continues even if power to the tap is interrupted. The taps are connected to a Cisco 2950 network switch (O15). The span port of the switch is connected to both CyberLens Sensor (O10) and iSID (O11) to provide the necessary network data. Both the taps (O16) and the span port on the switch (O15) are inherently unidirectional so that ICS network data can only flow out of the ICS network to the data aggregation and analysis tools in the NCCoE Energy Sector lab No data can flow back into the ICS network from the monitoring and data collection components.

Data transferred from the Pi Historian (O8), CyberLens Sensor (O10), and ConsoleWorks (O9) to the NCCoE energy Sector lab is sent using a Waterfall Security Solutions, Ltd. Unidirectional Security Gateway (O2). This gateway ensures that data can only flow out from the cogeneration facility to the NCCoE, and is not physically able to flow back from the NCCoE to the facility.

Radiflow's iSID (O11) has a web interface that is used to both manage the system and provide security analysts access to additional information about events reported via syslog. Access to this web interface is provided via components (O17, O18, O19, and O5) originally intended for remote management of monitoring and data collection components. These components are described in section 4.3.1.

4.2.2 Example Solution Data Aggregation and Analysis Lab Build

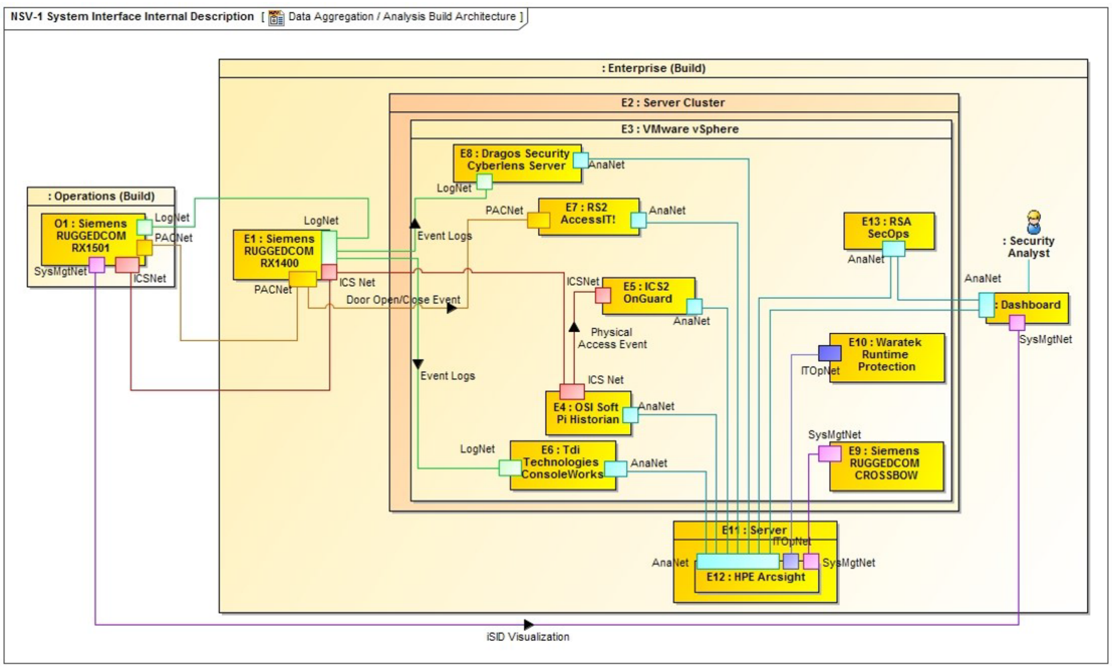
Figure 4.5 shows the products used to build an instance of the data aggregation and analysis portion of the example solution. The instance was constructed in the NCCoE energy sector lab. This lab provides the enterprise environment in the example solution. The VPN between the operations and enterprise in the example solution is provided by a Siemens RUGGEDCOM RX1400 (E1) in the lab and an RX1501 (O1) in the cogeneration facility.

A Dell server cluster (E2) running VMware (E3) is installed in the NCCoE energy sector lab to host monitoring, data aggregation, and analysis software. A separate server in the lab (E11) hosts HPE ArcSight. These are infrastructure components needed for the lab build but not considered part of the example solution.

The SIEM in the example solution is provided by HPE ArcSight (E12). ArcSight is the central repository for all events generated.

Waratek Runtime Application Protection (E10) implements the Application Monitor and Protection component of the example solution. Waratek Runtime Application Protection monitors and protects Java applications to detect potential cross-site scripting attacks. A Java application was written to access data from the enterprise OSISoft Pi Historian (E4) database. This application is monitored by Waratek Runtime Application Protection (E10) and reports and blocks attempted SQLi attacks against the Historian (E4) to ArcSight (E12).

Figure 4.5 Enterprise Data Aggregation and Analysis Lab Build Architecture



The ICS Asset Management System in the operations facilities of the example solution is provided by Dragos Security CyberLens. As implemented, CyberLens is divided into two parts, a Sensor (O10) in operations and a Server (E8) in enterprise. The Sensor (O10) sends data files to the Server (E8) for analysis. When the server detects a change to the assets on the ICS network in operations, it sends an event to ArcSight (E12).

The PACS in the example solution is implemented by RS2 Access It! (E7). Door open/close events from the RS2 door controller (O4) in operations are sent to Access It! (E7) and stored in an internal database. An ArcSight database connector is used to extract these events and send them to ArcSight (E12).

The enterprise Historian is provided by the OSISoft PI Historian (E4). ICS data from the operations Pi Historian (O8) is replicated to the enterprise PI Historian (E4). This data is used by the ICS Behavioral Monitoring component in the example solution, implemented by ICS^2 OnGuard (E5), to detect unusual ICS behavior. OnGuard (E5) reports this unusual behavior to ArcSight (E12).

The enterprise log collector/aggregator component in the example solution is provided by TDi Technologies ConsoleWorks (E6). This instance of ConsoleWorks (E6) receives files from the operations instance (O9). The files contain integrity-sealed syslog records. The enterprise instance of ConsoleWorks (E6) verifies the integrity seal on the records and sends the syslog records to ArcSight (E12).

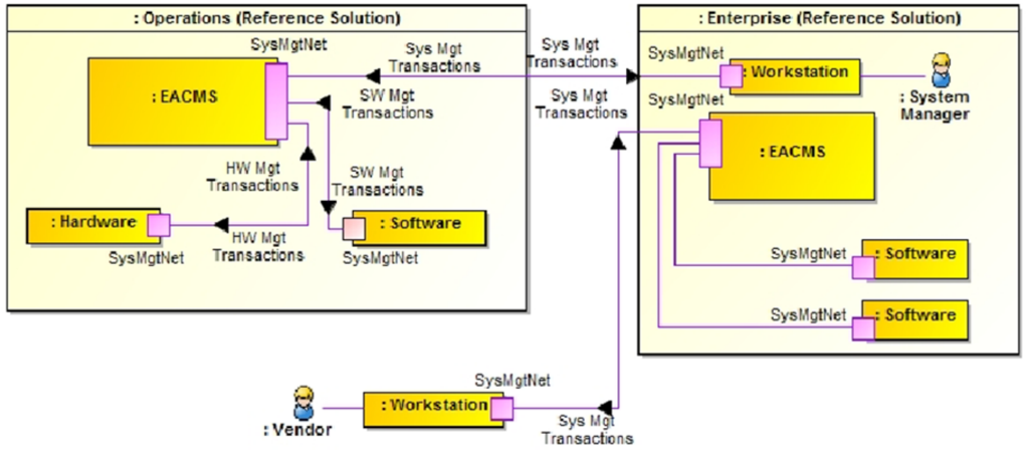
Siemens RUGGEDCOM CROSSBOW (E9), which implements part of the remote management connection described in section 4.3, sends log information about remote management actions to ArcSight (E12).

The analysis workflow engine, analysis tools, and visualization tools in the example solution are implemented by RSA Archer Security Operations Management (E13). This product extracts event data from ArcSight (E12) and performs analyses to identify potential cyber incidents.

4.3 Example Solution Remote Management Connection

Because elements of the example solution are separated from the system managers who install, configure and manage them, a remote management connection is needed from the enterprise to operations. Additionally, while not part of the example solution, the vendors who collaborated with NCCoE to construct the lab build of the example solution need remote access to the NCCoE energy sector lab to install, configure, and integrate their products. Figure 4.6 depicts the example solution for both remote management connections. Example implementation of remote management is depicted in Figure 4.7 and Figure 4.8.

Figure 4.6 Remote Management Example Solution



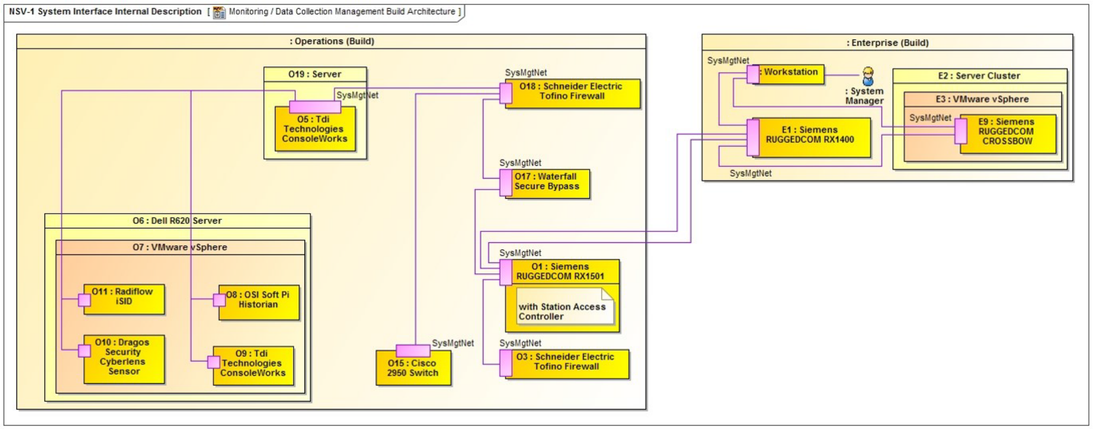
A workstation in the enterprise facility connects to the Operations EACMS. The system manager authenticates to the EACMS and controls the system manager's access to hardware or software within operations, as a privileged user, to perform system management functions. A VPN is used to protect data in transit between Operations and Enterprise. In the lab build, the connection between Operations and Enterprise uses the public Internet. Hence, protection for data transiting the Internet is needed. When implementing the example solution, utilities need to consider the type of network connection in place between Operations and Enterprise to determine what protection might be needed for data in transit.

To install and manage their software in enterprise, vendors connect via VPN to an EACMS in Enterprise. The vendors authenticate to the EACMS and are granted access to the software they provided.

4.3.1 Example Solution Operations Remote Management Lab Build

The lab build of operations remote management, depicted in Figure 4.7, provides two distinct implementations of the EACMS. One implementation that provides remote management for software running on the Dell R620 server (O6) uses the Siemens RUGGEDCOM RX1501 (O1), the Waterfall Secure Bypass switch (O17), a Schneider Electric Tofino firewall (O18), a Linux server (O19), and an instance of TDi Technologies ConsoleWorks (O5). The second implementation which provides remote management for hardware in operations uses Siemens RUGGEDCOM CROSSBOW (E9) and the Station Access Controller capability in the Siemens RUGGEDCOM RX1501 (O1). While the build used each implementation for a specific set of resources, either hardware or software, each implementation is capable of managing both hardware and software.

Figure 4.7 Operations Remote Management Lab Build Architecture



The EACMS implementation for remote management of software in operations has the system manager connect to operations from enterprise over the VPN created using the Siemens RUGGEDCOM RX1400 (E1) and RX1501 (O1). The system manager needs to connect to the operations management instance of ConsoleWorks (O5). However, a Waterfall Secure Bypass (O17) is installed in the network path from the RX1501 to the ConsoleWorks (O5). The Secure Bypass (O17) is a normally-open physical switch. To perform remote management, a person in the operations facility must turn a key on the Secure Bypass (O17) to close the switch[2]. Once the switch is closed, a timer is activated that automatically opens the switch after a preset time period. Remote management can only be performed if the personnel at the operations facility agree to allow access.

A Schneider Electric Tofino firewall (O18) restricts the protocols that can be used to connect to the operations management instance of ConsoleWorks (O5). Once connected to (O5), the system manager authenticates and is allowed to connect to virtual machines on the Dell server (O6).

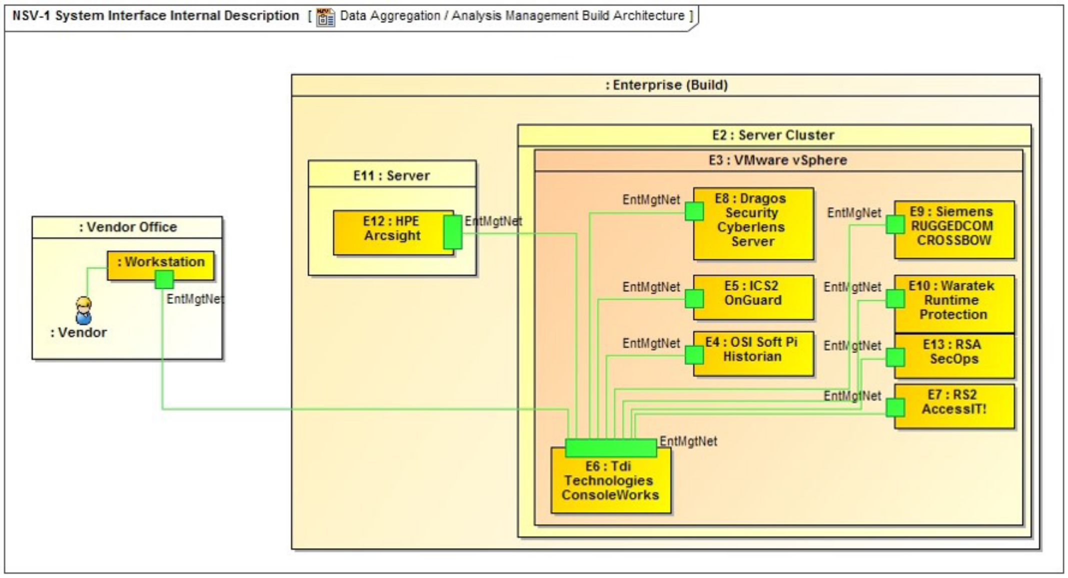
To remotely manage hardware in operations, the system manager authenticates to Siemens RUGGEDCOM CROSSBOW (E9) in enterprise. CROSSBOW (E9) determines the resources the system manager is allowed to access and then makes a connection over the VPN to the resource using the Station Access Controller integrated in the RX1501 (O1). In the lab build, the Tofino firewall (O3) isolating the door controller is connected directly to the network switch in the RX1501 (O1), and no operations personnel action is needed to manage the firewall. To manage the Cisco 2950 network switch that connects ICS network taps (O15) to CyberLens Sensor (O10) and iSID (O11), operations personnel must close the switch on the Secure Bypass (O17).

4.3.2 Example Solution Enterprise Remote Management Lab Build

Figure 4.8 depicts the implementation of remote access to the NCCoE energy sector lab for vendors.

2.In the case of this lab build, the collaborator's cogeneration facility representing operations is a staffed facility so an operator is available to close the switch on the secure bypass (O17).

Figure 4.8 Enterprise Remote Management Lab Build Architecture



The VPN providing vendor connectivity to the enterprise in the example solution is provided as core lab infrastructure by the NCCoE, and is outside the scope of the lab build. Use of this VPN requires two-factor authentication.

The EACMS for vendor access in the example solution is implemented by TDi Technologies ConsoleWorks (E6). Vendors authenticate to ConsoleWorks and are allowed to connect to the virtual machines or physical server hosting their product(s). Additionally, ConsoleWorks records all the actions performed over a connection. This provides an audit trail that documents vendor activity, which can be used for accountability as well as constructing the how-to portion, volume C, of this practice guide.

5 Security Characteristics Analysis

We organized the security analysis of the SA reference design into two parts. Section 5.1, Analysis of the Reference Design's Support for CSF Subcategories, analyzes the SA reference design in terms of the specific subcategories of the CSF[1] that it supports. It identifies the security benefits provided by each of the reference design components and how the reference design supports specific cybersecurity activities, as specified in terms of CSF subcategories.

Section 5.2, Reference Design Security Analysis, discusses potential new vulnerabilities and attack vectors that the reference design, or the infrastructure needed to manage the reference design, might introduce, as well as ways to mitigate those vulnerabilities. Overall, the purpose of the analysis is to identify the security benefits provided by the reference design and how they map to CSF subcategories, as well as to understand the mitigating steps to secure the reference design against potential new vulnerabilities.

5.1 Analysis of the Reference Design's Support for CSF Subcategories

Table 5.1, SA Reference Design Components and the CSF Subcategories they Support, lists numerous reference design components, their functions, and the CSF subcategories that they support. Although the particular products that were used to instantiate each component in the build are also listed, the focus of the security analysis is the CSF subcategories supported by these products. This analysis does not concern itself with specific products or their capabilities. In theory, any number of commercially available products could be substituted to provide the security capabilities of a given reference design component. Figure 5.1 and Figure 5.2 depict the monitoring/data collection and data aggregation/analysis sub-architectures of the reference design using the generic names of each component.

Figure 5.1 Monitoring/Data Collection Sub-architecture Depicted Using Generic Component Names

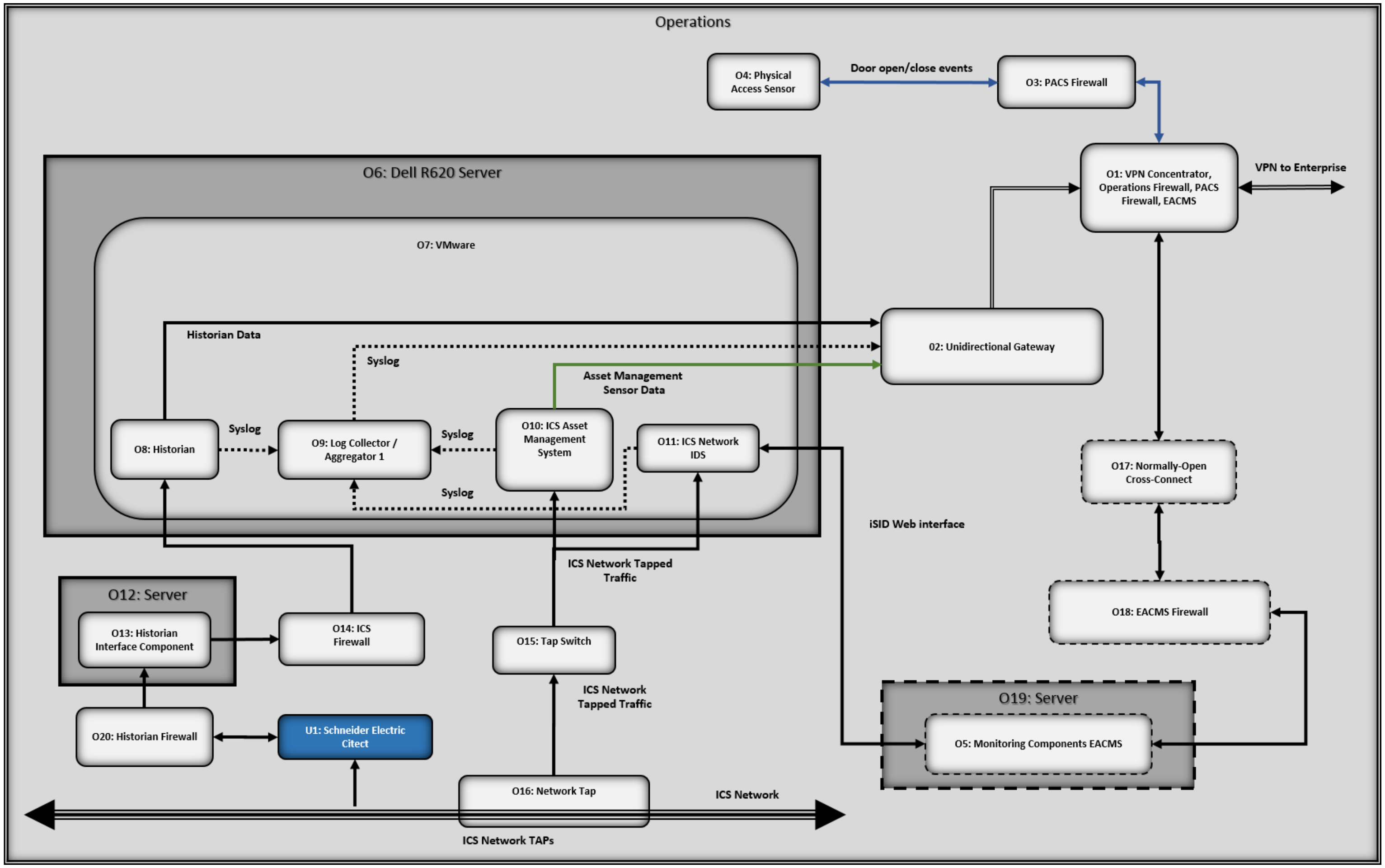


Figure 5.2 Data Aggregation/Analysis Sub-architecture using Generic Component Names

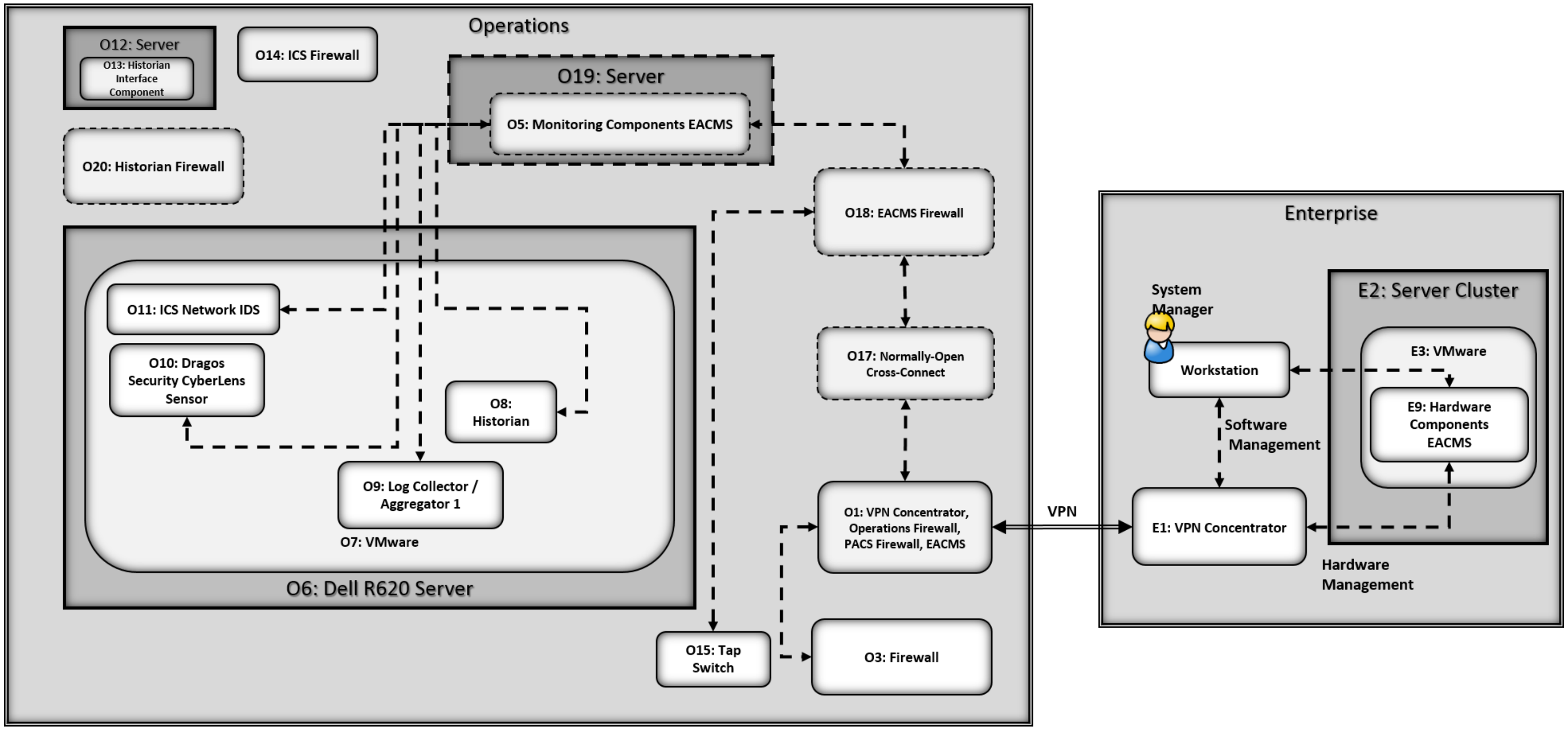


Table 5.1 SA Reference Design Components and the CSF Subcategories they Support

Component	ID	Specific Product	Function	CSF Subcategories
Security Information and Event Management (SIEM)	E12	HPE ArcSight	■ aggregates all IT, windows, OT (ICS) and physical access monitoring, event, and log data collected by the reference design ■ acts as a data normalization and correlation point and enables queries to be developed and executed to detect potential security incidents ■ serves as the central location at which the analyst can access all data collected.	DE.AE-3, DE.AE-5 Related Subcategories: PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-7
Network Tap	O16	IXIA Full Duplex Tap	■ collects data from specific locations on the ICS network and sends it to the monitoring server via the ICS firewall ■ the taps are passive, so if they lose power or otherwise fail, they will not adversely affect the ICS network ■ they also collect data via monitor ports that are inherently unidirectional (and so do not pose any threat of information leaking from the tap onto the ICS network)	DE.CM-1
Log Collector/ aggregator[a]	O9 E6	TDi Technologies Console Works (Operations)	■ log collection and aggregation ■ adds a time stamp and integrity seals the log entries ■ log collection in the operations facility protects against potential data loss in the event that the communications channel between the operations and enterprise facilities fails ■ aggregating the log entries of all monitoring components at the operations log collector/aggregator ensures that this log data gets buffered in the operations facility and can be transferred later in the event that network connectivity to the enterprise network is lost	PR.DS-6, PR.PT-1, DE.AE-3
ICS Asset Management System	O10	Dragos Security CyberLens Sensor	■ monitors ICS traffic and maintains a database of all ICS assets of which it is aware ■ this enables it to detect new ICS devices, ICS devices that disappear, and changes to known ICS devices	ID.AM-1

Table 5.1 SA Reference Design Components and the CSF Subcategories they Support

Component	ID	Specific Product	Function	CSF Subcategories
Network Visualization Tool	E8	Dragos Security CyberLens Server	▪ displays a depiction of network devices, connectivity, and traffic flows	Does not directly support a CSF subcategory. Related Subcategory: ID.AM-3
Physical Access Control System	E7	RS2 Access It!	▪ controls user access to doors ▪ detects and reports door open/close events and user identity	PR.AC-2
Physical Access Sensor	O4	RS2 Door Controller	▪ senses door close/open events ▪ generates alerts when door open and close events occur	DE.CM-2
ICS Network Intrusion Detection System (IDS)	O11	Radiflow iSID	▪ identifies, monitors, and reports anomalous ICS traffic that may indicate a potential intrusion	DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-7
Historian[b]	O8	OSIsoft Pi Historian	▪ serves as a data repository that essentially replicates the database of collected ICS values on the ICS network's Historian ▪ can be configured to generate alerts when changes to certain ICS process values occur	Does not directly support a CSF subcategory. Provides data to be monitored by the ICS behavior monitor. Related Subcategories: DE.AE-5, DE.CM-1
ICS Behavior Monitor	E5	ICS^2 OnGuard	▪ monitors ICS process variable values in the Historian to assess application behavior, detect process anomalies, and generate alerts	DE.AE-5, DE.CM-1
Application Monitor & Protection	E10	Waratek Runtime Application Protection	▪ monitors & protects a running application, analyzes the data it collects, and detects and reports unusual application behavior ▪ e.g., it might generate an alert if it detects a potential SQL injection attack against the SIEM	DE.AE-2, DE.AE-4, DE.AE-5, DE.CM-4
Analysis Workflow Engine	E13	RSA Archer Security Operations Management	▪ automates workflow associated with review and analysis of data that has been collected at the SIEM ▪ enables orchestration of various analytic engines	DE.AE-2

Table 5.1 SA Reference Design Components and the CSF Subcategories they Support

Component	ID	Specific Product	Function	CSF Subcategories
Unidirectional Gateway	O2	Waterfal Unidirectional Security Gateway	■ allows data to flow in only one direction	PR.AC-5, PR.PT-4
Visualization Tool	E13	RSA Archer Security Operations Management	■ provides data reduction and a dashboard capability for the data in the SIEM, as well as risk analysis	Does not directly support a CSF subcategory. Related Subcategory: ID.AM-3
Electronic Access Control and Monitoring System (EACMS)	05	TDi Technologies ConsoleWorks	■ authenticates system managers ■ provides role-based access control of system management functions ■ implements a “protocol break” between the system manager and the managed assets ■ records all system management actions	PR.AC-3, PR.AC-4, PR.PT-1, PR.PT-3, PR.MA-2, DE.CM-3
	E9	Siemens RUGGEDCOM CROSSBOW	■ authenticates system managers ■ provides role-based access control of system management functions ■ implements a “protocol break” between the system manager and the managed assets ■ records all system management actions	PR.AC-3, PR.AC-4, PR.PT-1, PR.PT-3, PR.MA-2, DE.CM-3
	O17	Waterfall Secure Bypass	■ provides time-limited network connectivity to perform system management functions	PR.AC-5, PR.PT-4
	O18	Schneider Electric Tofino Firewall	■ controls network connectivity for performing system management functions	PR.AC-5, PR.PT-4

a. Note that two instances of the log collector component are present in the reference design: one in the reference design's monitoring/data collection sub-architecture and another in its data aggregation/analysis sub-architecture. Integrity seals that are applied by a log collector can only be verified at that log collector. Therefore, the log collector that is in the operations facility does not apply an integrity seal to its entries because these integrity seals cannot be verified in the enterprise.

b. Two instances of the Historian component are present in the reference design: one in the monitoring/data collection sub-architecture and another in the data aggregation/analysis sub-architecture.

The last column of Table 5.1 lists the CSF subcategories that each component of the reference design supports. In Section 3.4.2, Security Characteristics and Controls Mapping, the CSF subcategories are mapped to specific sections of informative references that are comprised of existing standards, guidelines, and best practices for that CSF subcategory. In conjunction with these references, the CSF subcategories are able to provide structure to the assessment of the security support provided by the SA reference design. The references provide use case validation points in that they list specific security traits that a solution that supports the desired CSF subcategories would be expected to exhibit. Using the CSF subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports specific security activities and provides additional confidence that the reference design addresses the SA use case security objectives. The remainder of this subsection discusses how the reference design supports each of the identified CSF subcategories.

5.1.1 Supported CSF Subcategories

The reference design's primary focus is the “Detect” function area of the CSF as well as a few subcategories within the “Identify” and “Protect” function areas. Specifically, the reference design supports:

- all five subcategories of the Anomalies and Events (DE.AE) Category of the Detect Function area
- five of the eight subcategories of the Security Continuous Monitoring (DE.CM) Category of the Detect Function area
- one activity in the CSF Identify function area, which is in the Asset Management category (ID.AM)
- nine activities from various categories of the CSF Protect Function area (PR.AC-2, 3, 4, and 5, PR.DS-2 and 6, and PR.PT-1, 3, and 4)

We discuss these CSF subcategories in the following subsections.

5.1.1.1 DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

This CSF subcategory is supported by the ICS Network Intrusion Detection System (IDS) component of the reference design. This component is a tool for identifying, monitoring, and reporting anomalous ICS traffic that might indicate a potential intrusion. This component, located in the monitoring server, sends syslog events regarding anomalous behavior that it detects to the log collector/aggregator in the monitoring server, which forwards them to the SIEM on the enterprise network, where they can be viewed by a security analyst. In addition to having the ability to send syslog events, the ICS Network IDS component also has its own graphical user interface that can be accessed only by a web interface.

5.1.1.2 DE.AE-2: Detected events are analyzed to understand attack targets and methods

This CSF subcategory is supported by both the Application Monitor and the Analysis Workflow Engine components, both of which are located in the Data Aggregation/Analysis Sub-Architecture. The Application Monitor monitors a running application, analyzes the data it collects, and detects and reports unusual application behavior. In the build, the Application Monitor is configured to generate an alert if it detects a potential SQL injection attack against the SIEM. The Analysis Workflow Engine, located downstream from the SIEM, automates workflows associated with the review and analysis of data that has been collected at the SIEM. It consists of various analytic engines that can be orchestrated. This component enables the automated execution of well-defined courses of action that can be associated with an observable sequences of events.

In some cases, the individual monitoring components in the reference design will be able to single-handedly detect events. In other cases, the aggregation and correlation of event data from multiple sources and sensors might be needed to identify anomalies and thereby enable such detection.

Although ensuring that security analysts actually study, analyze, and understand attack targets and methods is outside the scope of the reference design, the objective of the reference design is to support and facilitate the ability of the analyst to perform these functions. When possible, analysis and anomaly detection procedures might be automated within various components. For events that are not detected automatically, the aggregation of all SA information at the single, centralized SIEM enables analysts to more easily correlate and visualize multiple facets of SA, facilitating their ability to analyze and understand attack targets and methods.

5.1.1.3 DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

This CSF subcategory is supported by the SIEM, which aggregates all IT, OT (ICS), and PACS data that is collected by the reference design. This includes monitoring, event, and log data. The SIEM acts as a data normalization and correlation point. It is a location at which queries can be developed and executed for the purpose of detecting potential security incidents. The SIEM also serves as the central location at which the analyst can access all data collected.

Before log data is sent to the SIEM for aggregation, it is aggregated at two sub-collection points, both of which also support CSF subcategory DE.AE-3. Log data is collected and aggregated at both the log collector/aggregator component in the monitoring/data collection sub-architecture and at the log collector/aggregator component in the data aggregation/analysis sub-architecture. These log collectors/aggregators add time stamps to the collected log entries. The log collector/aggregator in the aggregation/analysis sub-architecture also applies an integrity seal to the log entries.

Support for this subcategory is a main goal of the SA reference design. Aggregation and correlation of SA data from multiple sources and sensors at various analysis and anomaly detection components into a single, centralized SIEM component enables a security analyst to more easily understand attack targets and methods. All physical security, ICS network assets, network security, IT system information, reports, alerts, and other information is consolidated in a single, centralized SIEM component. In some cases, the information sent to the analysis and anomaly detection components and the SIEM might include notifications of potential events that have already been detected. In other cases, the analysis and anomaly detection components or the analyst accessing the SIEM might be able to detect events that were not indicated by any single monitoring component. Only by combining and correlating information from a variety of sources was the event identified.

The SIEM is the normalization point for all SA data. It is a location at which queries can be developed and run for the purpose of looking for anomalies. The security analyst has direct access to the data collected at the SIEM. Analysis components downstream from the SIEM enable the data that has been collected at the SIEM to be analyzed. They also enable automation of the workflow that is associated with the analysis activities, enabling analytic engines to be orchestrated.

5.1.1.4 DE.AE-4: Impact of events is determined

This CSF subcategory is supported by the Application Monitor component, which monitors a running application, analyzes the data it collects, and detects and reports unusual application behavior (e.g., a potential SQL injection attack).

5.1.1.5 DE.AE-5: Incident alert thresholds are established

Although determining incident alert threshold values is outside the scope of the reference design, various reference design components support the ability to establish such thresholds and act upon them when they are exceeded. CSF subcategory DE.AE-5 is supported by four components in the reference design: SIEM, ICS Network IDS, ICS Behavior Monitor, and Application Monitor, each of which generates alerts to report some form of unusual behavior once the detected behavior exceeds established thresholds. The incident alert thresholds in the SIEM might refer to anomalies that are detected as a result of IT, OT, and PACS information correlation. The thresholds in the ICS Network IDS might refer to levels of anomalous ICS traffic. ICS Behavior Monitor component thresholds might refer to ICS process variable anomaly levels. Application Monitor component thresholds are designed to detect and alert to unusual IT application behavior.

Although the Historian component of the reference design does not support this CSF subcategory directly, it provides data to the ICS behavior monitor and thereby supports this subcategory indirectly. The ICS network contains a component that acts as a Historian, recording important information regarding events and variable values for various ICS components. All process values stored in this ICS Historian are conveyed to the Historian component of the reference design via a Historian interface component. As a result, the reference design's Historian component essentially replicates the ICS Historian's database of values that have been collected and monitored. The Historian component's database is not a typical SQL database. It has the capability to issue an “on change” request, meaning that it can be configured to send notices when changes to certain ICS process values occur. This capability enables the reference design to avoid constant polling of Historian component values and constitutes a first line of monitoring defense against potential cybersecurity events on the ICS network that might be detected when the alert thresholds are exceeded for specific ICS variable values.

5.1.1.6 DE.CM-1: The network is monitored to detect potential cybersecurity events

This CSF subcategory is supported by three components:

- Network Tap: collects data from specific locations on the ICS network and sends it to the monitoring server
- ICS Network IDS: monitors ICS traffic and reports anomalous ICS traffic that may indicate a potential intrusion
- ICS Behavior Monitor: monitors ICS process variable values in the Historian to assess application behavior, detect process anomalies, and generate alerts

Although the Historian component does not support this CSF subcategory directly, it can be configured to generate alerts when ICS process variable values change. This CSF subcategory is also listed as being related to the SIEM due to the SIEM's role as the aggregation point for all collected information, which enables it to support network monitoring to detect potential cybersecurity events.

5.1.1.7 DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

This CSF subcategory is supported by the Physical Access Sensor component, which senses door close/open events and generates alerts when door open and close events occur. The Physical Access Sensor component serves as sort of a placeholder for multiple potential PACS monitoring devices that could and should be included in an operational deployment. In an operational deployment, organizations would likely include additional PACS monitoring devices, such as badge readers, to increase the amount and quality of PACS information provided as part of SA. In a real deployment, information coming out of the PACS would include not only door open/close events, but also access decisions based on the identity and permissions of the individuals trying to access the doors. All such monitored PACS (and IT and OT) information is aggregated in the SIEM, which is why CSF subcategory DE.CM-2 is listed as being related to the SIEM. As the aggregation point for all collected PACS data, the SIEM can therefore support the monitoring of the physical environment to detect potential cybersecurity events.

5.1.1.8 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

This CSF subcategory is supported by the EACMS for system managers. All system manager actions are captured by the EACMS and can be provided to the SIEM for review and correlation with other system activity.

5.1.1.9 DE.CM-4: Malicious code is detected

This CSF subcategory is supported by the Application Monitor & Protection component, which monitors a running application, analyzes the data it collects, and detects and reports unusual application behavior (e.g., a potential SQL injection attack). Because the reference design focuses mostly on collecting and integrating OT information, and assumes that the collection and integration of IT information into the SIEM is a solved problem, the Application Monitor component serves as sort of a placeholder for multiple potential IT monitoring devices that could and should be included in an operational deployment. In an operational deployment, organizations would likely include additional IT monitoring capabilities such as anti-virus software to increase the amount and quality of IT information provided as part of SA.

5.1.1.10 DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

This CSF subcategory is supported by the ICS Network IDS component, which identifies, monitors, and reports anomalous ICS traffic that might indicate a potential intrusion on the OT network. This CSF subcategory is also listed as related to the SIEM. The SIEM serves as the aggregation point for all collected information, and can therefore support monitoring for unauthorized personnel, connections, devices, and software.

5.1.1.11 ID.AM-1: Physical devices and systems within the organization are inventoried

This CSF subcategory is supported by the ICS Asset Management System component, which monitors ICS traffic to sense, track, and record ICS assets, and maintains a database of all ICS assets of which it becomes aware. Such monitoring enables this component to detect and identify new devices on the ICS network, devices that disappear from the ICS network, and changes to known ICS devices. This enables it to perform data analytics and anomaly detection as well as management of the inventory of ICS assets that it senses and collects. The ICS Asset Management System sends logs of asset inventory events to the Log Collector/Aggregator and feeds the ICS asset information it collects into the SIEM component.

5.1.1.12 PR.AC-2: Physical access to assets is managed and protected

This CSF subcategory is supported by the reference design's PACS, which controls user access to doors and detects and reports door open/close events. As was stated earlier, the reference design's physical access sensor and control system components serve as placeholders for multiple potential PACS monitoring devices that could and should be included in a reference design deployment to manage and protect physical access to assets. For example, organizations would likely want to include badge readers to support access decisions based on the identity and permissions of the individuals trying to access the doors. The reference design provides the vehicle for integrating information from additional PACS devices into the SIEM.

5.1.1.13 PR.AC-3: Remote access is managed

This CSF subcategory is supported by the functions that comprise the EACMS. Together, these functions allow carefully controlled and monitored remote access to manage monitoring systems deployed to operations.

5.1.1.14 PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

This CSF subcategory is supported by the functions that comprise the EACMS. These functions allow the definition and enforcement of role-based access permissions that incorporate least privilege and separation of duties.

5.1.1.15 PR.AC-5: Network integrity is protected, incorporating network segmentation where appropriate

This CSF subcategory is supported by the use of firewalls, a unidirectional gateway, and a normally-open cross-connect. All of these functions segment the network to preserve integrity.

5.1.1.16 PR.DS-2: Data-in-transit is protected

This CSF subcategory is supported by the use of a Virtual Private Network (VPN), which uses encryption to protect the confidentiality and integrity of all information while it is in transit between the monitoring/data collection sub-architecture and the data aggregation/analysis sub-architecture. The reference design does not, however, protect the confidentiality or integrity of monitored data while it is in transit within either the monitoring/data collection sub-architecture or the aggregation/analysis sub-architecture.

5.1.1.17 PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

This CSF subcategory is supported by the log collector/aggregator that is in the aggregation/analysis sub-architecture of the reference design insofar as the log collector/aggregator integrity seals the log data that it collects. Ideally, the log collector/aggregator in the monitoring/data collection sub-architecture would also apply an integrity seal to each log entry so that this seal could be verified by the log collector/aggregator in the data aggregation/analysis sub-architecture to ensure that no log entries were modified before reaching the data aggregation/analysis sub-architecture log collector/aggregator. This integrity checking of monitoring/data collection log entries, however, is not currently provided in the build because there is currently no mechanism to enable any component other than the log collector/aggregator that applies the integrity seals to verify those seals. In an ideal world, all information sent from components in the monitoring/data collection sub-architecture to the aggregation/analysis sub-architecture would be integrity-protected both while at rest and in transit.

5.1.1.18 PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

This CSF subcategory is supported by the EACMS in Operations and in Enterprise. In Operations, remote maintenance of software requires an operator to manually enable remote access using the normally-open cross connect. Beyond this, the EACMS firewall controls the devices that are accessible, restricting access to the monitoring components EACMS and the network IDS interface. To perform remote maintenance, system managers must authenticate to monitoring components EACMS, which then controls access to the software and maintenance functions the system manager is allowed to perform.

Remote maintenance of Operations hardware is controlled by the hardware components EACMS in Enterprise. System managers must authenticate to the hardware components EACMS, which then controls access to the hardware and maintenance functions the system manager is allowed to perform.

Both the hardware components EACMS and the monitoring components EACMS keep a record of all system management functions performed.

5.1.1.19 PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

This CSF subcategory is provided by both of the log collector/aggregators in the reference design, which aggregate logs from various devices and put timestamps on the log data. Although the SIEM does not directly support this CSF subcategory, PR.PT-1 is also listed as a related subcategory for the SIEM because the SIEM can be used to review audit/log records.

Ideally, all of the monitoring/data collection components in the reference design will be capable of generating log data that contains the relevant event information and sending this log data to the log collector/aggregator component. (In the build, neither the PACS nor the Physical Access Sensor send log data that contains the events to the log collector/aggregator; instead, the SIEM obtains PACS event information via a PACS MySQL database.) The Log Collector/Aggregator component's role is to aggregate all log data that it collects. In addition, when each log entry is received at the log collector/aggregator, it already contains a time stamp added by the sending device. Upon receipt of the log entry, the log collector/aggregator component puts its own timestamp on the entry to indicate the time that it was received. Discrepancies in the sent and received timestamps for a given entry can be monitored to detect suspicious activity. The Log Collector/Aggregator in the monitoring and data collection sub-architecture then sends all logs to the log collector/aggregator in the data aggregation/analysis sub-architecture, which puts its own timestamps on the entries that it receives. It also applies an integrity seal to the entry that can be checked at a later time to ensure that the entry has not been deliberately or inadvertently modified. This log collector/aggregator then sends its log entries to the SIEM. The SIEM consolidates these log entries along with all other SA information.

The collection of SA information in a single location (at the SIEM) enables audit and log records to easily be reviewed in accordance with policy. Furthermore, the analysis tool components into which the SIEM data feeds might facilitate the automation of the review of audit and log records. Whether or not the organization performs these audit and log reviews according to policy is outside the scope of the SA reference design.

5.1.1.20 PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

This CSF subcategory is supported by the functions that comprise the EACMS and by network firewalls. The EACMS controls system manager access to systems in operations. Network firewalls control connectivity to and interaction among network assets.

5.1.1.21 PR.PT-4: Communications and controls networks are protected

This CSF subcategory is supported by a VPN, firewall, a unidirectional gateway, and a normally-open cross-connect. The VPN provides confidentiality protection for data in transit between the operations facilities and enterprise. Firewalls are placed throughout the system to control the network connections that are allowed among function within operations. A unidirectional gateway ensures communication between operations and enterprise is one-way out of operations. The normally-open cross-connect allows a two-way communications path between operations and enterprise, but only when physically closed at the operations side.

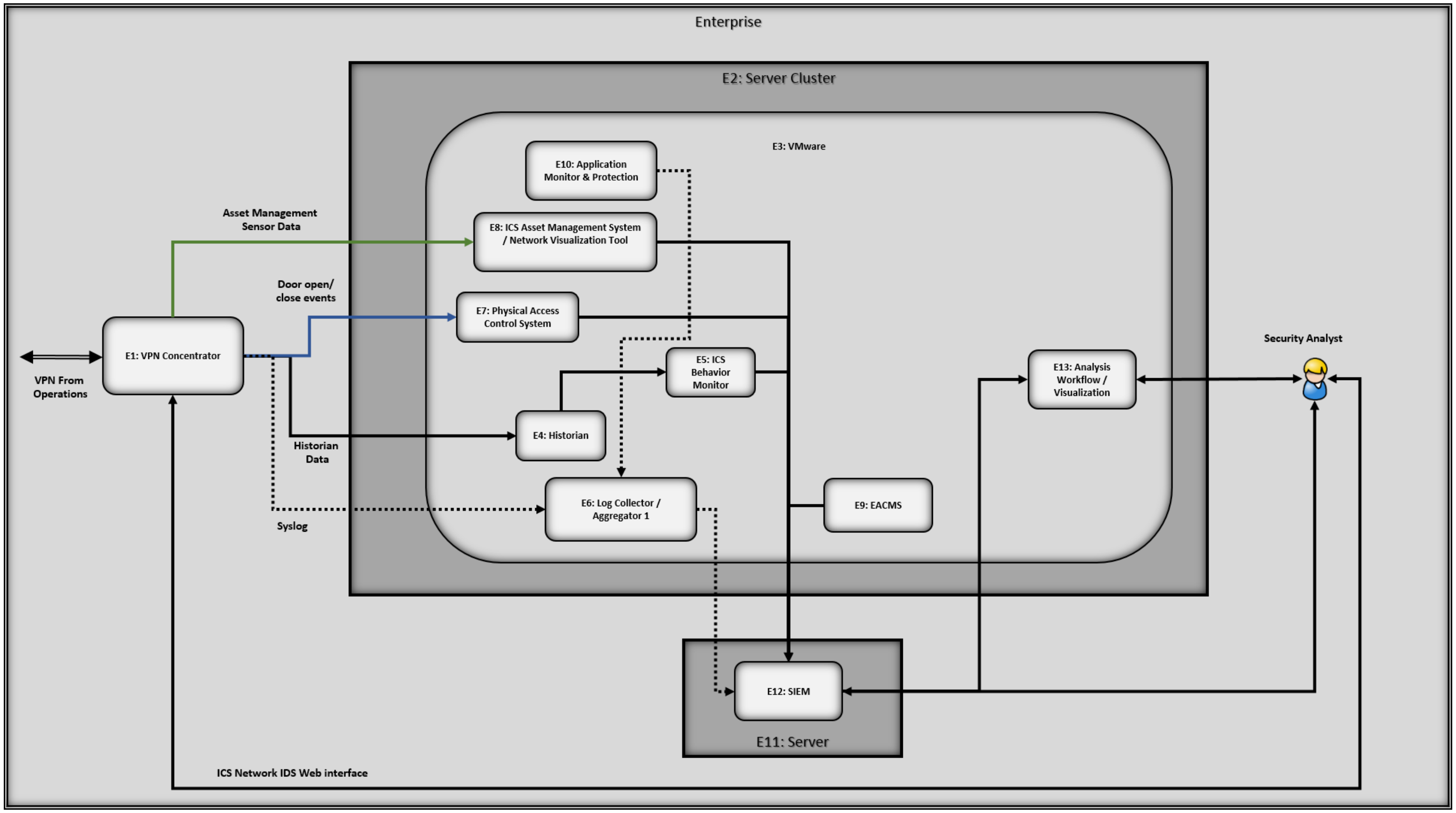
5.2 Reference Design Security Analysis

The list of reference design components included in Table 5.1 focuses only on the components of the reference design that are needed to enable it to meet its SA objective of collecting information from the ICS network, aggregating it at a centralized location, and providing analysis capability in a manner that supports the intended CSF subcategories. Table 5.1 does not include components that are needed to manage or secure the reference design. However, the reference design itself must be managed and secured. To this end, this second part of the security analysis focuses on the security of both the reference design itself and its management infrastructure.

Table 5.2, Components for Managing and Securing the SA Reference Design and Protecting the ICS Network, lists components that are needed to manage the reference design, secure both the reference design and the data it collects, and protect the ICS network. Table 5.2 also describes the security protections provided by each of the management and security components. As with Part 1 of the security analysis, although the products that were used to instantiate each component in the build are also listed, the security protections provided by these products are the focus of this security analysis.

Figure 5.3 depicts the monitoring/data collection management architecture of the reference design using the generic names of each component.

Figure 5.3 Monitoring/Data Collection Management Architecture Depicted using Generic Component Names



Note that because the NCCoE build involved using products from many different vendors, the NCCoE provided those vendors with access to the NCCoE lab for the purpose of product installation, configuration, and maintenance. Therefore, the architecture that was actually instantiated included components for securing this vendor access path. However, this vendor access path is an artifact specific to the NCCoE build. It is not anticipated that organizations that adopt the SA architecture would enable such a vendor access path in their implementations. Therefore, this vendor access path is not included within the scope of the security analysis.

Table 5.2 Components for Managing and Securing the ES-SA Reference Design and Protecting the ICS Network

Component	ID	Specific Product	Security Protection Provided
Electronic Access Control and Monitoring System (EACMS)	O1 O5 O18 O17	Siemens RUGGEDCOM RX1501 TDi Technologies Console Works (Operations Management) Schneider Electric Tofino Firewall Waterfall Secure Bypass	One EACMS component (Siemens RUGGEDCOM RX1501) enables remote configuration of privileged user access to the PACS Firewall. This EACMS component is referred to as the PACS Firewall EACMS. A second EACMS component (TDi Technologies Console Works) enables remote configuration of privileged user access to the consoles of the four components on the monitoring server (Log Collector/Aggregator, ICS Asset Management System, ICS Network IDS, and Historian). This EACMS component is referred to as the Monitoring Components' EACMS. The third EACMS component (Schneider Electric Tofino Firewall) operates as the network port and protocol level to control remote management traffic exchanged between the enterprise network and the Monitoring Components' EACMS. It also serves as the EACMS for the taps switch. This EACMS component is referred to as the EACMS Firewall. The fourth EACMS component (Waterfall Secure Bypass) is hardware that might be manually configured to enable data to be sent into the operations facility to support EACMS activities for a limited period of time. All EACMS components except for the Waterfall Secure Bypass, which is a physical cross-connect, also create an audit trail of all privileged user access to the components that they protect. They send log entries documenting this audit trail to the SIEM. None of the four components that comprise the EACMS are able to be remotely managed. Each EACMS component except for the Waterfall Secure Bypass includes the three policy sub-components listed in the next three rows of this table.
EACMS Policy Administration Point (PAP)	O1 O5 O18	Siemens RUGGEDCOM RX1501 TDi Technologies Console Works (Operations Management) Schneider Electric Tofino Firewall	The point that manages access authorization policies; it is the source of policies for the EACMS and the location at which policies may be created and edited.
EACMS Policy Decision Point (PDP)	O1 O5 O18	Siemens RUGGEDCOM RX1501 TDi Technologies Console Works (Operations Management) Schneider Electric Tofino Firewall	The point that evaluates access requests against authorization policies for the EACMS before issuing access decisions.

Table 5.2 Components for Managing and Securing the ES-SA Reference Design and Protecting the ICS Network

Component	ID	Specific Product	Security Protection Provided
EACMS Policy Enforcement Point (PEP)	O1 O5 O18	Siemens RUGGEDCOM RX1501 Station Access Controller TDi Technologies Console Works (Operations Management) Schneider Electric Tofino Firewall	The point that intercepts user's access request to a resource, makes a decision request to the EACMS's PDP to obtain the access decision (i.e. access to the resource is approved or rejected), and acts on the received decision. In the build, the Siemens CROSSBOW EACMS Station Access Controller is integrated into the Siemens RUGGEDCOM RX1501 component.
PACS Firewall EACMS	O1	Siemens RUGGEDCOM RX1501	Enables configuration of privileged user access to the PAC firewall to be controlled remotely in a manner similar to that in which the Monitoring Components' EACMS enables configuration of privileged user access to the consoles on the monitoring server components to be controlled.
Monitoring Components' EACMS	O5	TDi Technologies Console Works (Operations Management)	Enables configuration of privileged user access to the consoles on the monitoring server components to be controlled remotely in a manner similar to that in which the PACS Firewall EACMS enables privileged user access to the PACS firewall to be controlled.
EACMS Firewall	O18	Schneider Electric Tofino Firewall	Firewall that operates as the network port and protocol level to monitor all traffic received at the monitoring components' EACMS from external sources when the normally-open cross connect is closed. In addition to monitoring traffic, the firewall also restricts traffic flow according to its configured rules. This firewall's purpose is to ensure that the only permitted components to which traffic can flow to and from the normally-open cross-connect are the server for the Monitoring Component's EACMS (O19) and the Taps switch (O15). It is configured to permit only three types of traffic: (1) remote management traffic exchanged between the enterprise network and the Monitoring Components' EACMS, which is used to control privileged user access to the consoles of the four components on the monitoring server and access to the web interface of the ICS Network IDS, (2) remote management traffic exchanged between the enterprise network and the taps switch, and (3) traffic exchanged between the enterprise network and the ICS Network IDS component to support the web interface that enables security analysts that are located on the enterprise network to view SA information using the ICS Network IDS component's graphical user interface. (Note that support for this last type of traffic is one way in which the reference design differs from the build, because the reference design requires that the ICS Network IDS component report potential IDS events by sending syslog events; it does not require support for a graphic user interface to the ICS Network IDS component.

Table 5.2 Components for Managing and Securing the ES-SA Reference Design and Protecting the ICS Network

Component	ID	Specific Product	Security Protection Provided
PACS Firewall	O3	Schneider Electric Tofino Firewall	Monitors traffic sent between the VPN concentrator/PACS Firewall EACMS component and the Physical Access Sensor component. Configured to ensure that the only messages that are permitted to be received from the Physical Access Sensor are door open/close and other valid PACS events are forwarded to the VPN concentrator. The Physical Access Sensor sits on an operational IT network that is connected to the internet. Therefore, this PACS firewall is exposed to the operational IT network and, via that network, to the internet. So configuring the PACS Firewall to accept only PACS sensor messages prevents the PACS devices and the operational network on which they sit from being used as an attack vector to compromise the reference architecture. In particular, the PACS Firewall prevents traffic (other than door controller traffic) from being sent from the internet to the enterprise network via the VPN.
VPN Concentrator	O1	Siemens RUGGEDCOM RX1501	The VPN concentrator supports four types of VPN traffic between the operations facility and the enterprise network: monitoring data sent from the operations facility to the enterprise network; remote management traffic used to support privileged access to the consoles of the four components on the monitoring server, remote management traffic used to support privileged user access to the console of the PACS firewall, and web interface traffic exchanged between the ICS Network IDS component and a remote security analyst located on the enterprise network. The traffic exchanged on this web interface might be either traffic needed to support remote management of the ICS Network IDS component by a security analyst or traffic needed to support the ICS Network IDS component's graphical user interface. (This graphical user interface is not part of the reference design, but it is supported in the build.)
Operations Firewall	O1	Siemens RUGGEDCOM RX1501	Firewall monitoring all traffic sent between the operations facility and external sources and restricting traffic flow according to its configured rules. This firewall is the one device on the operations facility network that is exposed to the Internet at all times. Regarding traffic arriving at the operations facility from external sources, it is configured to permit (1) remote management traffic exchanged between the enterprise network and the Monitoring Components' EACMS, which will be further scrutinized by the EACMS Firewall, (2) remote management traffic exchanged between the enterprise network and the PACS Firewall EACMS, and (3) remote management traffic exchanged between the enterprise network and the taps switch.

Table 5.2 Components for Managing and Securing the ES-SA Reference Design and Protecting the ICS Network

Component	ID	Specific Product	Security Protection Provided
Unidirectional Gateway	O2	Waterfall Unidirectional Security Gateway Hardware	Enforces one-way transfer between a transmitter and receiver within hardware, ensuring that data may be sent from the monitoring server to the enterprise, but not in the reverse direction. The gateway also replicates industrial servers and emulates industrial devices to IT users and applications.
Normally-open cross-connect	O17	Waterfall Secure Bypass	Enables the data unidirectional gateway component to be bypassed so that data can be sent into the operations facility for specific management and monitoring purposes. Must be closed manually and stays closed only for a limited period of time.
ICS Firewall	O14	Radiflow 3180 Firewall	Firewall monitoring all traffic that flows from the Historian Interface component to the monitoring server. This firewall is configured to prevent traffic from flowing in the reverse direction, i.e., to prevent traffic from flowing from the monitoring server to the ICS network. Also, it cannot be managed remotely.
Historian Firewall	O20	Schneider Electric Tofino Firewall	Firewall monitoring all traffic that flows between the ICS Historian and the Historian Interface component. This firewall is configured to prevent traffic from flowing from the Historian Interface component to the ICS network. It cannot be managed remotely.
Historian Interface component	O13	OSIsoft Citect Interface	This component interfaces with the ICS Historian that is on the ICS network. It receives data from the ICS Historian and provides this to the Historian component in the monitoring server of the SA reference architecture, but it does not permit data to travel in the other direction, from the monitoring server to the ICS Historian.
Taps Switch	O15	Cisco 2950 (Aggregator)	This switch aggregates data received from all ICS taps and forwards this data to the monitoring server. It is configured to permit only one-way data flow from the tap interfaces toward the monitoring server interface. No data is permitted to travel out the tap interfaces toward the taps.

5.2.1 Protecting the ICS Network

A main security requirement of the SA use case is to ensure that the ICS network is not impacted by the monitoring to which it is subjected. In particular, it is crucial to ensure that, although data can flow from the ICS network to the reference design, a minimal amount of very strictly restricted data is allowed to flow from the reference design onto the ICS network. There are two paths on which data flows from the ICS network to the monitoring server: from the ICS network taps, and from the ICS Historian.

These taps are inherently unidirectional. By design, they permit data to flow only from the ICS network to the monitoring server. They are not able to allow data to flow from the monitoring server to the ICS network. These taps are also passive, meaning that if they were to lose power or otherwise fail, they would not disrupt the flow of data on the ICS network.

This unidirectional transmission path is enforced by the Historian Firewall (O20) (i.e., a Schneider Electric Tofino Firewall in the build), the Historian Interface component (O13), the server on which it resides, and the ICS Firewall (O14) (i.e., the Radiflow 3180 firewall in the build), all of which sit between the ICS Historian (i.e., Schneider Electric Citect in the build) and the monitoring server. These components are critical for ensuring that only a small amount of strictly restricted data is permitted to travel into the ICS network from the monitoring server.

In the build, the Historian Interface component (O13) pulls data from the ICS Historian (Schneider Electric Citect, U1) and pushes this information to Historian component in the monitoring server (O8). This means that the Historian interface component (O13) needs to send a message to the ICS Historian (U1) that sits on the ICS to cause it to send the Historian data to the Historian Interface component. Therefore, the Historian Firewall (O20) between the Historian Interface component and the ICS Historian has to be configured to permit requests for data to flow from the Historian Interface component to the ICS Historian. It also has to be configured to allow Historian data to flow in the opposite direction, i.e. from the ICS Historian to the Historian Interface component.

The fact that requests for data pulled from the ICS Historian must be permitted to be sent from the operations network to the ICS network is not ideal. To protect the ICS network, it would be preferable prevent all data flow from the operations network to the ICS network. To ensure that requests for Historian data are the only type of data that is permitted to be sent from the operations network to the ICS network, it is essential that the Historian Firewall (O20) that sits between these two components be configured to limit the data that is sent to the ICS network to the necessary requests for Historian data and nothing more. It is also essential that this Historian Firewall (O20) cannot be configured remotely. This ensures that only an insider who has physical access to this firewall (O20) would be able to modify its rules to permit additional traffic to enter the ICS network from the operations network.

Once it has the Historian data, the Historian Interface component pushes this data to the Historian component (O8) on the monitoring server. This means that the firewall (O14) that sits between the Historian Interface component and the Historian component can (and must) be configured not to permit any data to flow in the direction from the monitoring server to the Historian Interface component. It is also essential not to allow this firewall (O14) to be configured remotely.

In short, the reference design balances two competing goals:

- protecting the ICS network as fully as possible from the receipt of potentially harmful data from the reference design itself, and
- enabling the ICS Historian to receive requests for data from the reference design.

It achieves these goals by isolating the Historian interface component on both sides by firewalls, ensuring that these firewalls are configured correctly, and ensuring that neither these firewalls, the Historian Interface Component, nor the server that the Historian Interface Component sits on are remotely configurable. It should also be noted that the Historian Interface component is running on a server that is distinct from the monitoring server. This separation ensures that the reference design does not depend solely on VMWare's ability to separate applications running on it to ensure that no data is permitted to travel from the monitoring server to the Historian Interface component. As discussed, none of the components located between the ICS Historian and the monitoring server may be managed remotely. Creating additional means to configure these components from outside of the operations facility is considered a greater risk than being unable to monitor changes to these firewalls from outside of the facility; therefore, only technicians physically on site at the operations facility may change the configuration of these components.

5.2.2 Protecting the Reference Design from Outside Attack

Measures implemented to protect the monitoring and data collection sub-architecture itself from outside attack include:

- The PACS Firewall situated between the Physical Access sensors and the VPN concentrator/PACS Firewall EACMS is configured to permit only door open/close events and other valid notifications to be sent from the Physical Access sensors to the monitoring and data collection sub-architecture. The Physical Access sensors sit on the facility's operational network, which exposes them to the internet. The PACS firewall plays a crucial role in preventing external attacks to the monitoring network. It prevents the PACS devices and the operational network on which they sit from being used as an attack vector to compromise the monitoring and data collection sub-architecture.
- Data should only be allowed to flow from the enterprise network into the monitoring server under carefully controlled circumstances and with very limited restrictions. The architecture's unidirectional gateway component (i.e. the Waterfall Unidirectional Security Gateway Hardware component in the build) that sits between the monitoring server and the VPN concentrator component (i.e., the Siemens RUGGEDCOM RX1501) is designed to enforce this unidirectionality. This unidirectional gateway is a combination of hardware and software. The hardware physically permits only one-way transfer across an optical connection between a hardware transmitter and a hardware receiver. The hardware ensures that monitored data may be sent from the monitoring server to the enterprise, but no data may be sent in the reverse direction on this connection into the monitoring server. Unidirectional gateway software replicates industrial servers and emulates industrial devices from the protected operations network to the enterprise network.

5.2.3 Protecting the Remote Management Paths

In the example solution presented, for the purpose of monitoring, the SA architecture design assumed that the data aggregation/analysis activity would be performed at a physically separate location from the data monitoring/collection activity. This scenario was used to reflect real-world operations; its risk is greater than the scenario in which the monitoring/data collection sub-architecture and the data aggregation/analysis sub-architecture are physically co-located in the same secure facility. Therefore, mechanisms for protecting the data and management path between the two parts of the architecture that support these activities are integral to the reference design.

For the purpose of monitoring, data should flow unidirectionally from the operations facility to the enterprise network. For management purposes, however, there is a need for traffic to be able to flow into the operations facility from the enterprise network. In particular, incoming traffic is required to enable remote management of the following components:

- the PACS Firewall (one of the Schneider Electric Tofino Firewalls in the build), which sits between the VPN concentrator and the Physical Access Sensor
- the four data collection components in the monitoring server at the operations facility
- the taps switch, which sits between the ICS taps and the monitoring server
- the PACS Firewall EACMS/Operations Firewall

Remote management traffic destined for the monitoring server or the taps switch must instead bypass the unidirectional gateway to reach its destination. This remote management traffic can be used to monitor and configure the PACS firewall.

Remote management traffic destined for the monitoring server or the taps switch must instead bypass the data diode to reach its destination. To enable this bypass, we used the normally-open cross-connect component (the Waterfall Secure Bypass component in the build). Closing this normally-open cross-connect enables traffic to flow back and forth between the enterprise network and the monitoring server for limited time periods.

These remote management access paths contain numerous components and features designed to secure them. These components are as follows:

- VPN concentrator - is directly exposed to the Internet. This component is situated on its own network in the operations facility.
- Operations Firewall - monitors all traffic sent between the operations facility and external sources and restricts traffic flow according to its configured rules. It is exposed to the internet at all times.

  This component contains a Policy Enforcement Point (PEP) for the PACS firewall (the Schneider Electric Tofino firewall between the RS2 Door Controller and the RUGGEDCOM RX1501 in the build) This PEP is the “Station Access Controller” shown within the RUGGEDCOM RX1501 build diagram. It enables administrative access to the console of the PACS firewall to be managed and monitored remotely.
- Normally-open Cross-connect - enables the unidirectional gateway to be bypassed, enabling traffic to flow into the operations facility monitoring architecture. As mentioned earlier, the unidirectional gateway sits on a path between the monitoring server and the Operations Firewall/VPN concentrator (RUGGEDCOM RX1500) to ensure that information can flow only unidirectionally from the monitoring server to the enterprise network.

  This component is a physical switch that is normally open, ensuring that no data can be transmitted across it. This switch must be closed manually with a physical key by an operator who is located on site at the operations facility to enable remote traffic to enter the monitoring/data collection portion of the architecture from the enterprise. Once closed, it will remain closed for a limited, configurable amount of time (e.g., 30 minutes), and then it will automatically open (unless explicitly opened before this time period expires). The connection cannot be enabled remotely.
- The EACMS Firewall - this component is instantiated using the Schneider Electric Tofino firewall in the build. After passing through the VPN concentrator, the operations firewall, and the Normally-open Cross-connect, traffic received from the enterprise flows to the

EACMS Firewall. Because of its placement behind the VPN concentrator, the Operations Firewall, and the Normally-open Cross-connect, this component is not by default exposed to any traffic from outside of the operations facility except for those periods of time when the Normally-open Cross-connect has been explicitly closed and traffic sent to the facility on a VPN meets the requirements for entry that are enforced by the Operations Firewall.

When such a connection into the operations facility from outside is established, the EACMS Firewall is needed to monitor traffic being exchanged between the operations facility and the outside. This firewall operates at the network port and protocol level to monitor and control remote management traffic exchanged between the enterprise network and both the taps switch and the Monitoring Components' EACMS. Three types of traffic are permitted by the EACMS Firewall:

  - remote management traffic exchanged between the Enterprise network and the Monitoring Components' EACMS (TDi Console Works), which is used to manage privileged access to each of the components on the monitoring server
  - web interface traffic exchanged between the ICS Network IDS component on the monitoring server and a remote security analyst located on the enterprise network. The traffic exchanged on this web interface might be needed either to support remote management of the ICS Network IDS component or to enable the security analyst to view SA data via the ICS Network IDS component's graphical user interface
  - remote management traffic exchanged between the Hardware Component EACMS (Siemens RUGGEDCOM CROSSBOW) on the Enterprise network and the taps switch, which is used to administer the taps switch

- Monitoring Components' EACMS - this component is instantiated using TDi ConsoleWorks in the build. Remote management traffic coming through the EACMS firewall to the operations facility that is destined for one of the four monitoring server components may only reach those components via the Monitoring Components' EACMS. This is a component that administrators must use to configure user privileges or to access the consoles of the four components on the monitoring server. This component is connected to the consoles of each of the four applications running on the monitoring server so it can control access to these consoles and permit only those users with administrator privileges to access each console. It also records all activities that are performed on these consoles. The Monitoring Components' EACMS enables the monitoring server components to be configured remotely, but the tool itself cannot be configured remotely. Web interface traffic that his sent between the ICS Network IDS component (O11) and a security analyst on the enterprise network must also be sent through the Monitoring Component's EACMS. This web interface traffic includes both SA monitoring data accessed via the ICS Network IDS graphical user interface and traffic needed to remotely manage the ICS Network IDS.

  The Monitoring Components' EACMS runs on a server that is separate and distinct from the monitoring server. This separation is necessary to ensure that the architecture does not depend solely on VMWare's ability to separate applications running on it, which would be the case if the Monitoring Components' EACMS were on the same VMWare server as the monitoring server and its components. The server on which the Monitoring Components' EACMS server is running cannot be remotely managed.

- PACS Firewall EACMS (O1)- this component is instantiated in the build using the Siemens RUGGEDCOM RX1501 component that sits on the enterprise network. It enables monitoring and configuration of user privileges on the PACS firewall (O3) in a manner similar to the Monitoring Components' EACMS (O19). The PACS Firewall EACMS is used to remotely configure and manage the PACS Firewall, i.e., the firewall that sits between the VPN Concentrator (O1) and the Physical Access Sensors (O4).

To further protect the remote management path, the reference design does not permit any components that are in the remote management path to be remotely configurable. The only way that components and software that are in the remote management path can be administered and configured is in person.

5.2.4 Protecting the Remote Path to the IDS Web Interface

As mentioned earlier, the ICS Network IDS component has a web interface through that facilitates remote management and access to its graphical user interface. Because a security analyst using the web interface to view SA data is expected to be located on the enterprise network rather than at the operations center, SA traffic will flow between the ICS Network IDS and the enterprise network via this web interface. Security mechanisms are needed to monitor and restrict this traffic flowing into the operations center. The web interface traffic uses the same path as traffic managing the monitoring server components remotely; it relies on the same security mechanisms as those that protect the remote management path, namely the operations firewall (O1), the normally-open cross-connect (O17), the EACMS firewall (O18), and the Monitoring Components' EACMS (O19).

5.2.5 Protecting the SIEM

The SIEM component enables information collected at the reference design's disparate sensors and monitoring components to be combined, correlated, and analyzed in a way that would not be possible when using the data from a single SA component in isolation. Aggregation of SA information in the SIEM provides enormous potential in terms of anomaly detection and increased SA. Ironically, the main strength of the reference design might serve as its vulnerability, unless properly protected. If an adversary can penetrate the SIEM to modify or delete information, if he can alter the processes used to analyze or visualize asset information, or if he can alter information while in transit to the SIEM, then the very system that was designed to increase SA and make a wide variety of asset information centrally available to security analysts could be used as an attack vector. It is imperative that access to the SIEM be strictly limited to a small number of authorized users. Ideally, the integrity of the monitored information will also be protected from the points at which it is collected until it reaches the SIEM component. Ensuring the integrity and completeness of all data sent to and stored in the SIEM is essential to securing the reference design solution. If the components used to implement the reference design do not inherently provide data integrity for monitored information that is sent to the SIEM, then security will rely on enforcement of strict physical access control to ensure that attackers are not given the opportunity to access and modify/delete data that is in the SIEM or in transit to the SIEM.

It is worth noting that the absence of an SIEM does not mean that an energy organization does not have this SA information stored on its networks. Access to the SA information resides instead at disparate locations on the network. Energy services organizations still have the need to safeguard this SA information in the various locations where it is generated, stored, and while in transit.

5.2.5.1 Controlling Access to the SIEM

Only highly privileged users should be permitted to log into the SIEM. No users should be permitted to modify SA data that is being stored on this component. Monitoring, logging, and auditing of all console activity performed on this component is essential to ensuring that authorized users are not performing unauthorized activities on this component. Periodic reports should be generated listing all users who logged into the SIEM component and activities performed.

5.2.5.2 SIEM Data Verification

Mechanisms are needed to help ensure that information collected or generated at a collection component is sent to and received by the SIEM, i.e., that the SIEM actually receives all of the monitored information that it is supposed to. If an adversary were to have the ability to disable a sensor without the reference design being alerted, serious harm could result. Mechanisms are needed to ensure that if a monitoring or collection system is disabled or otherwise unable to send information to the SIEM, or if monitored information is deleted before reaching the SIEM, the absence of this information will be detected so that the situation can be remedied. Ideally, liveness checks for each of the devices on the enterprise network that report directly to the SIEM can be built into the SIEM, so that if heartbeat messages or other expected updates are not received at the expected intervals, alerts will be generated.

To the extent possible, these checks may be configured and implemented with the reference design components themselves. For example, ArcSight, the SIEM used in the build, can be configured to generate alerts when it does not receive data. However, this mechanism is not foolproof. Configuration of the SIEM requires that ArcSight alerts be tuned using a baseline of received data. Accuracy of the alerts depends on the extent to which the data that is sent mimics the baseline used to tune the SIEM. There is no guarantee that every item of information that is dropped would be detected. If monitoring devices are generating heartbeat messages, the SIEM could be equipped with a script to enable it to detect missing messages and thereby infer that either a monitoring device or its communications channel to the SIEM is not operational.

The SIEM cannot be expected to be able to detect the failure of monitoring devices that do not report directly to it. If a sensor reports to an intermediate system rather than directly to the SIEM itself, the intermediate system must be involved in detecting the potential failure of the sensor. There needs to be a way for the SIEM and all intermediate components in the reference design to know if the sensors that report to them are alive and well. Having sensors send heartbeats is one example of how such a liveness detection mechanism could be implemented. Mechanisms should be designed for each sensor type so that the sensor's liveness can be validated and an alert can be generated when the sensor fails. For example, if the ICS Access Management System on the enterprise network does not receive an update from the ICS Access Management System on the operations network, it should generate an alert. Similarly, if the log collector/aggregator in the monitoring server detects that it has not received a log message that was sent to it by one of the monitoring components, it should be configured to generate an alert.

The ability to detect sensor failure is complicated by the unidirectional nature of the data transfer from the operations network to the enterprise network. This one-way transfer of information prevents components on the enterprise network from trying to ping sensors on the operational network. Given this constraint, it might make most sense to have a designated application in the operations network that is responsible for tracking the health of all monitoring devices and periodically sending a status report regarding sensor health to the enterprise network. Given that it is already receiving information from all monitoring components on the operational network, the Log Collector/Aggregator component is a good candidate location for implementing such a centralized sensor health tracking service in the operations network.

5.2.5.3 Information Integrity Protection

If SA information were to be deleted, modified, or falsified, whether in-transit or at-rest, the result could be catastrophic. Access to each reference design component and especially the SIEM must be protected to prevent modification or deletion of collected SA information. Although end-to-end integrity protection for data at rest and for data in transit is desirable, such comprehensive protection is not a component of this reference design. As a compensating mechanism, an adversary must be local to the operations network to compromise the integrity of monitored information that is on the operations network because monitoring data is not permitted to enter the operations network from outside; all data paths for monitoring data are outbound. (Note that the build's support of a web interface for monitoring ICS Network IDS data via a graphical user interface violates this principle.) While this leaves the potential for malicious activity by an adversary who is an authorized user on the operations network, this approach greatly reduces component threat exposure. The reference design's use of a VPN protects data integrity and confidentiality while data is in route between the operations facility and the enterprise facility.

Within the enterprise network, all data in transit to the SIEM can have its integrity protected using ArcSight connectors that have integrity checking (and/or encryption) enabled. Such use of integrity-checking connectors between all components and ArcSight might take care of integrity protection for data in transit within the enterprise network. However, there does not seem to be an equivalent general solution for protecting data in transit within the operations network. If ArcSight connectors were to be used to send syslog, Historian, or other monitored data to the SIEM from the operations network, the integrity of the received data could be validated at the SIEM. However, because of the unidirectional nature of the one-way transfer between the operations network and the enterprise network, there would be no way for the SIEM to become aware that it has lost its connection to the source in the event that the communications network should fail.

In much the same way that mechanisms are needed for each sensor type to ensure that the sensor's liveness can be validated, mechanisms for ensuring the integrity of each type of monitored data are also needed. Each data transfer in the reference design should be protected with integrity mechanisms to ensure that any loss or modification of data that occurs during the transfer will be detected: the integrity of Historian data sent from the Operations Historian component to the enterprise Historian component, the integrity of information sent from the ICS Asset Management System sensor on the operations network to the ICS Asset Management

System server and network visualization tool on the enterprise network, the integrity of door open and close events sent from the Physical Access Sensor on the operations network to the PACS on the enterprise network, and the integrity of syslog data sent from the Log Collector/Aggregator on the operations network to the Log Collector/Aggregator on the enterprise network.

Syslog data can, in theory, be encrypted, to ensure the integrity of the log data, assuming the individual products used to implement the reference design support syslog encryption. However, relying on syslog encryption to protect the integrity of data sent from monitoring devices to the SIEM suffers from the same drawback as would relying on ArcSight encryptors: if the communications network between the operations network and the enterprise network fails, the SIEM would not have any way to be alerted to this failure, and log data that is in-transit between the two networks would be dropped. Instead, the proposed solution for the reference design is for the log collector/aggregator on the operations network to collect all syslog data sent from other monitoring components and apply an integrity seal to this syslog information. The integrity seal is applied not only to the syslog record, but to the entire log file up to that point, so it protects the record's place in the file in addition to protecting the content of the record. The operations network instance of the log collector/aggregator sends syslog records to the enterprise network instance of the log collector/aggregator. The enterprise instance of the log collector/aggregator applies equivalent integrity seals to the received records. Should a question arise about the integrity of syslog records, both the operations and enterprise log collector/aggregators can validate the integrity of the records they hold. Further, a comparison could be made between operations and enterprise records. Because the log records are stored in a log collector/aggregator on the operations network instead of being sent directly to the enterprise network from each of the monitoring devices that generate them, these log records will not be dropped or lost in the event that the communications channel between the operations and enterprise networks fails.

5.3 Securing an Operational Deployment

When deploying the SA reference design in a live, operational environment, it is essential that organizations follow security best practices to address potential vulnerabilities, ensure that all assumptions on which the solution relies upon are valid[1], and minimize any risk to the operational ICS network. The following list of best practices recommendations are designed to reduce this risk, but should not be considered comprehensive. Merely following this list will not guarantee a secure environment.

- Test individual components to ensure that they provide the expected CSF subcategory support and that they do not introduce potential vulnerabilities. For example, the taps deployed should be tested to verify that they are passive, i.e., that when power is turned off to them they do not disrupt the flow of traffic on the network on which they are deployed. They should also be tested to validate that they only permit data to flow in one direction, ensuring that they cannot be used as an entry point for malicious traffic to enter the network that is being monitored by the taps.

1. Note that the laboratory instantiation of the reference architecture builds did not implement every security recommendation.

- Harden all components: all components should be deployed on securely configured operating systems that use long and complex passwords and are configured according to best practices.
- Scan operating systems for vulnerabilities.
- Keep operating systems up-to-date on patching, version control, and monitoring indicators of compromise by performing, for example, virus and malware detection.
- Maintain all components in terms of ensuring that all patches are promptly applied, anti-virus signatures are kept up-to-date, indicators of compromise are monitored, etc. (patches should be tested before they are applied).
- Change the default password when installing software.
- Identify and understand what predefined administrative and other accounts each component comes with by default to eliminate any inadvertent back doors into these components. These accounts must be disabled and, even though they are disabled, their default passwords must also be changed to complex passwords.
- On key devices that protect the ICS network (e.g., the ICS firewall and the Historian firewall) and that are on the remote management path, the number of accounts on these devices should be limited, ideally, to one specific administrator and a backup account. As is the case in the reference design, all components on the remote access path should be configurable only in person.
- Implement mechanisms to monitor the ICS and Historian firewalls.
- Organizations leveraging the reference design solution should conduct their own evaluations of their implementation of the solution.
- All reference design components that are designed to detect anomalies and identify potential areas of concern with the use of analysis tools should be equipped with as complete a set of rules as possible to take full advantage of the analysis and anomaly detection capabilities of each component. The rules that are implemented must be consistent across components and they must enforce the organization's security policies as completely and accurately as possible. The SIEM should be configured with rules indicating the ICS systems, software, applications, connections, device, values and activities, that are authorized to enable it to ensure that only authorized personnel, connections, devices and software are on the ICS network.
- Identity and Access Management (IdAM) and Information Technology Asset Management (ITAM) security infrastructures should be put into place that will protect the reference design solution (namely, control access to each reference design component and especially to the SIEM component) and help ensure that the information fed into the SIEM component is complete and unmodified.
- The access control policies for the SIEM component should be designed to enforce best security practices such as the principle of least privilege and separation of duties, and these policies should be devised so that they can detect anomalous behavior or information that could indicate a security breach. Access to this component should require authentication and use of long and complex passwords. SA data stored in this component should be read-only, with any attempt to modify or delete information generating security alerts and log entries.

- Firewall configurations should be verified to ensure that data transmission is limited to those interactions that are needed to support sending information from various data-gathering components to the SIEM component and to analysis components as explicitly indicated in the reference design flow diagram. In addition, the inter-component connections that are permitted should be restricted to specific IP address and port combinations.
- Physical access to the both the operations and the enterprise networks should be strongly controlled.
- If possible, SA information sent from the monitoring components to the SIEM component should have integrity-checking mechanisms applied to enable tampering detection. Integrity mechanisms should conform to most recent industry best-practices.
- All components of the reference design solution should be installed, configured, and used according to the guidance provided by the component vendor.
- Only a very few users (super-administrators) should be designated to have the ability to control (initiate, modify, or stop) the types of information that each monitoring component collects and sends to the SIEM. Any changes made to the types of information to be monitored by or sent from any given collection component or device should, by policy, require the approval of more than one individual, and these changes must themselves be reported to the SIEM component.
- Whenever a super-administrator logs into or out of a collection component, these events must be reported to and logged at a "monitor of monitors" system as well as to the SIEM component. Upon logging in and logging out, a list of the types of information that the mid-tier device will report to the SIEM component should be sent so that any permanent changes the super-administrator has made to this list can be detected.
- Ideally, it should not be possible for anyone, including super-administrators, to modify the logging policies on any collection component such that a change to the list of information reported to the SIEM component would not itself be reported. However, this might not be how collection components are implemented. Therefore, it is imperative that a configuration management component that is part of a "monitor of monitors" system be configured to frequently validate and enforce such reporting at all collection devices. Furthermore, access to the configuration management component must be strictly controlled to ensure that its configuration is not changed such that it will not enforce reporting of configuration changes at all other mid-tier devices.
- Super-administrator access to the configuration management component should, by policy, require more than two individuals. All changes made during super-administrator access to the configuration management component should be reviewed by more than two individuals.

5.4 Security Analysis Summary

The SA reference design's integration, consolidation, and display of the SA information enables converged, efficient, and quick access to the variety of SA information that is collected, enabling better SA. In addition, consolidation of disparate types of PACS, IT, and OT information in a single location (the SIEM), enables the organization to correlate and analyze different types of monitored information in a way that is not possible when analyzing different categories of information in isolation, enabling security incidents to be detected and responded to in a timely and prioritized fashion. This consolidation, combined with the ability to apply rules-based analysis to the information, makes it possible for the SA system to automatically detect anomalous situations that might be indicative of a security breach that would otherwise have been impossible to detect by any single component of the system working in isolation.

6 Functional Evaluation

We conducted a functional evaluation of the SA example solution to verify that several common key provisioning functions of the example solution, as implemented in our laboratory build, worked as expected. The SA workflow capability demonstrated the ability to:

- implement a converged alerting capability to provide a comprehensive view of cyber-related events and activities
- utilize multiple commercially available products to achieve the comprehensive view
- provide a converged and comprehensive platform that can alert utilities to potentially malicious activity

Section 6.1 explains the functional test plan in more detail and lists the procedures used for each of the functional tests.

6.1 SA Functional Test Plan

This test plan includes the test cases necessary to conduct the functional evaluation of the SA use case. The SA implementation is currently in a split deployment set up, with part of the lab being at the NCCoE (Enterprise Side) and the other at University of Maryland (Operations Side). Section 5 describes the test environment. Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 6.1 provides a template of a test case, including a description of each field in the test case.

Table 6.1 Functional Test Plan

Test Case Field	Description
Parent requirement	Identifies the top-level requirement or series of top-level requirements leading to the testable requirement
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated
CSF Categories	Associated subcategories from the NIST SP 800-53 rev 4 Cybersecurity Framework controls addressed by the test case
Description	Describes the objective of the test case
Associated test cases	In some instances, a test case may be based on the outcome of another test case(s). For example, analysis-based test cases produce a result that is verifiable through various means such a s log entries, reports, and alerts
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration or protocol and content
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure
Expected results	The expected results for each variation in the test procedure

Table 6.1 Functional Test Plan

Test Case Field	Description
Actual results	The actual observed results in comparison with the expected results
Overall result	The overall pass/fail result of the test. In some instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified

6.2 SA Use Case Requirements

This section identifies the SA functional evaluation requirements that are addressed using this test plan. Table 6.2 lists those requirements and associated test cases.

Table 6.2 Functional Evaluation Requirements

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Test Case
CR 1	The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk		
CR 1.a		IT	SA-2, SA-3, SA-4, SA-6
CR 1.b		OT	SA-1, SA-3, SA-4, SA-5, SA-6
CR 1.c		PACS	SA-1, SA-3
CR 2	The SA system shall include an SA workflow capability that increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions		
CR 2.a		IT	SA-2
CR 2.b		OT	
CR 2.c		PACS	
CR 3	The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned		
CR 3.a		IT	SA-1, SA-5, SA-6

Table 6.2 Functional Evaluation Requirements

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Test Case
CR 3.b		OT	SA-6
CR 3.c		PACS	SA-1
CR 4	The SA system shall include an SA workflow capability that simplifies regulatory compliance by automating generation and collection of a variety of operational log data		
CR 4.a		IT	SA-5
CR 4.b		OT	
CR 4.c		PACS	

6.3 Test Case: SA-1

Table 6.3 Test Case ID: SA-1

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS (CR 3) The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned. (CR 3.a) IT, (CR 3.c) PACS
Testable Requirement	(CR 1.b) OT, (CR 1.c) PACS, (CR 3.a) IT, (CR 3.c) PACS
Description	▪ Show that the SA solution can monitor for door access and correlate to badge used. ▪ Show that the SA solution recognize OT device going offline and alert IT network to anomalous condition. ▪ Show that the SA solution can correlate timeframe between door access and OT device going offline.
Associated Test Cases	Event Correlation - OT & PACS: Technician accesses sub-station/control-station and OT device goes down. Alert of anomalous condition and subsequently correlate to PACS to see who accessed facility.
CSF Categories	DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-2, PR.AC-2

Table 6.3 Test Case ID: SA-1

Preconditions	▪ SA solution is implemented and operational in both Operations and Enterprise Network ▪ Ensure door controllers are properly installed and configured.
Procedure	1. At the Operations Network, open door leading to lab network to create door open event. 2. Once inside, unplug a connection from one of the network taps to the aggregating switch (this is to simulate an ICS device being disconnected). 3. Monitor SIEM for correlation activity.
Expected Results (pass)	1. CyberLens and system recognizes missing device(s) and notifies SIEM. 2. AccessIt! updates SIEM of door activity. 3. SIEM correlates timing between door activity and device(s) missing. 4. SIEM generates alert accordingly.
Actual Results	1. CyberLens system alerted to a device offline. 2. Access It! alerted to door open event. 3. SIEM shows each individual alert, along with timing between the alert.
Overall Result	PASS

6.4 Test Case: SA-2

Table 6.4 Test Case ID: SA-2

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT (CR 2) The SA system shall include an SA workflow capability that increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions. (CR 2.a) IT
Testable Requirement	(CR 1.a) IT, (CR 2.a) IT
Description	▪ Show that the SA solution can monitor user input for validity. ▪ Show that the SA solution can actively defend against software-based attacks. ▪ Show that the SA solution can alert IT to potential attacks.
Associated Test Cases	Event Correlation - OT & IT: Enterprise (IT) java application communication with OT device (Historian) and used as a vector for SQL injection (SQLi).
CSF Categories	DE.AE-1, DE.AE-2, DE.CM-1, DE-CM-4

Table 6.4 Test Case ID: SA-2

Preconditions	■ Web application running Java is installed. ■ Web application is connected to a database. ■ Web application server is installed and used to run Java-based web application.
Procedure	1. Connect to web application to query database. 2. Attempt a normal query for data. 3. Attempt a malicious query for data exfiltration.
Expected Results (pass)	1. The database should return normal results when a normal query is initiated. 2. The web application should return no results when a malicious query is initiated. 3. SIEM should be alerted by Waratek upon receipt of a malicious query.
Actual Results	1. Normal queries yielded normal results as expected. 2. Malicious queries yielded warnings and no results from web interface. 3. SIEM was alerted of malicious queries by Waratek and displayed malicious queries in dashboard.
Overall Result	PASS

6.5 Test Case: SA-3

Table 6.5 Test Case ID: SA-3

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Testable Requirement	(CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Description	■ Show that the SA solution can monitor network traffic inside of the operations network. ■ Show that the SA solution can alert to IP addresses not in expected ranges. ■ Show that the SA solution can alert on failed logins above a given threshold. ■ Show that the SA solution can correlate aforementioned anomalous behavior and alert analyst accordingly.

Table 6.5 Test Case ID: SA-3

Associated Test Cases	Event Correlation - OT & IT / PACS-OT: Unauthorized access attempts detected and alerts triggered based on connection requests from a device on the SCADA network destined for an IP that is outside of the SCADA IP range. This test case focuses on the possibility of a malicious actor attempting to gain access to an OT device via the Enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.
CSF Categories	DE.AE-1, DE.AE-2, DE-AE-3, DE.AE-5, DE.CM-1, DE.CM-7
Preconditions	▪ Waterfall Unidirectional Security Gateway is configured to allow traffic one-way out of the Operations Network. ▪ ConsoleWorks configured with authorized user access requirements.
Procedure	1. Attempt authorized login to operations device. 2. Attempt unauthorized login to operations device. 3. Connect laptop to Powerconnect 7024 switch and attempt communication on network.
Expected Results (pass)	1. Allows connection to operations device from authorized users. 2. Alerts on threshold of unauthorized logins/failed login attempts to operations device. 3. Alerts to new device found on network. 4. Blocks attempts of communication from new device to other network devices.
Actual Results	1. ConsoleWorks connections allowed from authorized users to OT devices. 2. OT devices alert on failed login attempts. 3. SIEM alerts are shown in dashboard for failed login attempts.
Overall Result	PASS

6.6 Test Case: SA-4

Table 6.6 Test Case ID: SA-4

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Testable Requirement	(CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS

Table 6.6 Test Case ID: SA-4

Description	▪ Show that the SA solution can utilize behavioral patterns to recognize anomalous events inside respective networks. ▪ Show that the SA solution can alert analysts to behavioral anomalies within respective networks.
Associated Test Cases	Data Exfiltration Attempts: examine behavior of systems; configure SIEM to alert on behavior which is outside the normal baseline. Alerts can be created emanating from OT, IT and PACS. This test case seeks alerting based on behavioral anomalies, rather than recognition of IP addresses.
CSF Categories	DE.AE-1, DE-AE-3, DE.AE-5, DE.CM-1, DE.CM-7
Preconditions	▪ Established baselines in Operations network. ▪ Ensure continued monitoring of modeled behavior in Operations network.
Procedure	1. Inject new IP addresses into established baseline sensor for Operations network. 2. Inject anomalous network traffic (previously unreported protocols) into baseline sensor. 3. Manipulate Enterprise Historian to show anomalous data/tags being stored. 4. Replicate network traffic to show higher volume than normal in baseline.
Expected Results (pass)	1. CyberLens acknowledges unknown IP address and/or protocols and reports to SIEM. 2. ICS2 recognizes changes within historian to detect anomalous industrial control behavior and alerts SIEM. 3. ICS2 recognizes uptick in historian activity and alerts SIEM. 4. CyberLens recognizes uptick in network activity and alerts SIEM. 5. SIEM aggregates alerts and notifies analyst.
Actual Results	1. CyberLens alerts to both unknown new IP address as well as new protocols. 2. Unable to manipulate Enterprise Historian with current setup. 3. CyberLens alerted to changes in network traffic. 4. SIEM aggregated alerts and showed alerts on dashboard.
Overall Result	PARTIAL PASS

6.7 Test Case: SA-5

Table 6.7 Test Case ID: SA-5

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk (CR 1.b) OT (CR 3) The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned (CR 3.a) IT, (CR 3.b) OT (CR 4) The SA system shall include an SA workflow capability that simplifies regulatory compliance by automating generation and collection of a variety of operational log data (CR 4.a) IT, (CR 4.b) OT
Testable Requirement	(CR 1.b) OT, (CR 3.a) IT, (CR 3.b) OT, (CR 4.a) IT
Description	▪ Show that the SA solution can detect when anomalous types of network traffic communicate with devices.
Associated Test Cases	Configuration Management: unauthorized (inadvertent or malicious) uploading of an ICS network device configuration. Alert will be created to notify SIEM this has occurred. Detection method will be primarily based on inherent device capability (i.e. log files).
CSF Categories	DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-7, ID.AM-2
Preconditions	▪ Baseline established for Operations network.
Procedure	1. Connect through VPN to Operations monitoring network. 2. Inject file into network traffic to mimic unauthorized/unseen protocols between monitored components.
Expected Results (pass)	1. iSID recognizes anomalous network traffic and alerts SIEM. 2. SIEM aggregates alerts and notifies analyst.
Actual Results	1. iSID shows alert for injected data. 2. SIEM aggregated alerts from iSID and displayed on dashboard.
Overall Result	PASS

6.8 Test Case: SA-6

Table 6.8 Test Case ID: SA-6

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk (CR 1.a) IT, (CR 1.b) OT (CR 3) The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned (CR 3.a) IT, (CR 3.b) OT
Testable Requirement	(CR 1.a) IT, (CR 1.b) OT, (CR 3.a) IT, (CR 3.b) OT
Description	■ Show that the SA solution can detect and notify on the introduction of an unknown device to ICS network. ■ Show that the SA solution can notify analyst of unknown device.
Associated Test Cases	Rogue Device Detection: alerts are triggered by the introduction of any device onto the ICS network that has not been registered with the asset management capability in the build.
CSF Categories	DE.AE-1, DE.AE-3, DE.CM-2, DE.CM-7, ID.AM-1, PR.AC-2
Preconditions	Baseline established for Operations Network
Procedure	1. Connect previously unknown device to network tap aggregation switch. 2. Create IP address on unknown device within known IP address range. 3. Send spoofed traffic to monitor.
Expected Results (pass)	1. CyberLens recognizes anomalous network device and alerts SIEM. 2. SIEM aggregates alerts and notifies analyst.
Actual Results	1. CyberLens recognized new device on network and alerted SIEM 2. SIEM aggregated alerts from CyberLens in dashboard and notified analyst
Overall Result	PASS

Appendix A Acronyms

CA	Certificate Authority
CSF	Cybersecurity Framework
DMZ	Demilitarized Zone
EACMS	Electronic Access Control and Monitoring Systems
ICS	Industrial Control Systems
IdAM	Identity and Access Management
IDS	Intrusion Detection System
IT	Information Technology
ITAM	Information Technology and Asset Management
NCCoE	National Cybersecurity Center of Excellence
OT	Operational Technology
PAC	Physical Access Control
PACS	Physical Access Control Systems
PEP	Policy Enforcement Point
RMF	Risk Management Framework
SA	Situational Awareness
SAC	Station Access Controller
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SQL	Structured Query Language
SQLi	Structured Query Language Injection
UMd	University of Maryland
VPN	Virtual Private Network