PROJECT DESCRIPTION

ENERGY SECTOR ASSET MANAGEMENT

For Electric Utilities, Oil & Gas Industry

Jim McCarthy, Principal Investigator
Michael Powell
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Titilayo Ogunyale
John Wiltberger
Devin Wynne
The MITRE Corporation

March 2018

Energy_nccoe@nist.gov

This revision incorporates comments from the public.

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

This document describes a challenge that is relevant across the Energy Sector. NCCoE cybersecurity experts will address this challenge through collaboration with members within the energy industry and with cybersecurity technology providers. The resulting example solution will detail an approach that can be used by the Energy Sector.

ABSTRACT

Industrial control systems (ICS) comprise a core part of our nation's critical infrastructure. Energy sector companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine, and transport oil and natural gas. There are a wide variety of ICS assets, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs), and intelligent electronic devices (IEDs), that provide command and control information and functions on operational technology (OT) networks. These assets are primary targets of cyber attacks. Vulnerabilities within these systems and devices present opportunities for malicious actors to cause disruptions to the power grid and to oil and gas assets and processes.

Energy Sector companies must monitor and manage ICS assets at all times to reduce the risk of such attacks. The NCCoE, in collaboration with members of the energy community and with cybersecurity technology providers, is planning a project to create an example solution to address this complex asset management challenge. This project will result in a freely available NIST Cybersecurity Practice Guide that includes an example solution for electric utilities and for oil and gas companies to effectively track and manage their assets.

KEYWORDS

Energy Sector Asset Management (ESAM); industrial control systems (ICS); malicious actor; monitoring; operational technology (OT); supervisory control and data acquisition (SCADA)

DISCLAIMER

TABLE OF CONTENTS

1 Executive Summary

Purpose

The National Cybersecurity Center of Excellence (NCCoE) is responding to the Energy Sector's request for an operational technology (OT) asset management solution. To remain fully operational, Energy Sector entities should be able to effectively identify, control, and monitor all of their OT assets. This project will provide guidance on how to enhance OT asset management practices by leveraging capabilities that may already exist in an operating environment or by implementing new capabilities.

The publication of this project description initiates the process to identify project collaborators, as well as standards-based, commercially available, and/or open-source technologies. These products will be implemented in a laboratory environment to build a standards-based, modular, end-to-end example solution that will address the security challenges of OT asset management. The approach will include architectural definition, physical and logical design, a comprehensive security analysis, security control mapping, and future build considerations. The output of the process will be the publication of a multi-volume National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide that organizations can use to enhance their ability to improve Energy Sector asset management.

Scope

This project will seek to address the following characteristics of asset management:

- **Asset Discovery**: establishment of a full baseline of physical and logical locations of assets
- **Asset Identification**: capture of asset attributes, such as manufacturer, model, operating system (OS), Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, protocols, patch-level information, and firmware versions
- **Asset Visibility**: continuous identification of newly connected or disconnected devices, and IP (routable and non-routable) and serial connections to other devices
- **Asset Disposition**: the level of criticality (high, medium, or low) of a particular asset, its relation to other assets within the OT network, and its communication (to include serial) with other devices
- **Alerting Capabilities**: detection of a deviation from the expected operation of assets

Assumptions

This project identifies security benefits, including the automated identification of OT assets to enable quick security alerts and increased cybersecurity resilience.

This project makes the following assumptions:

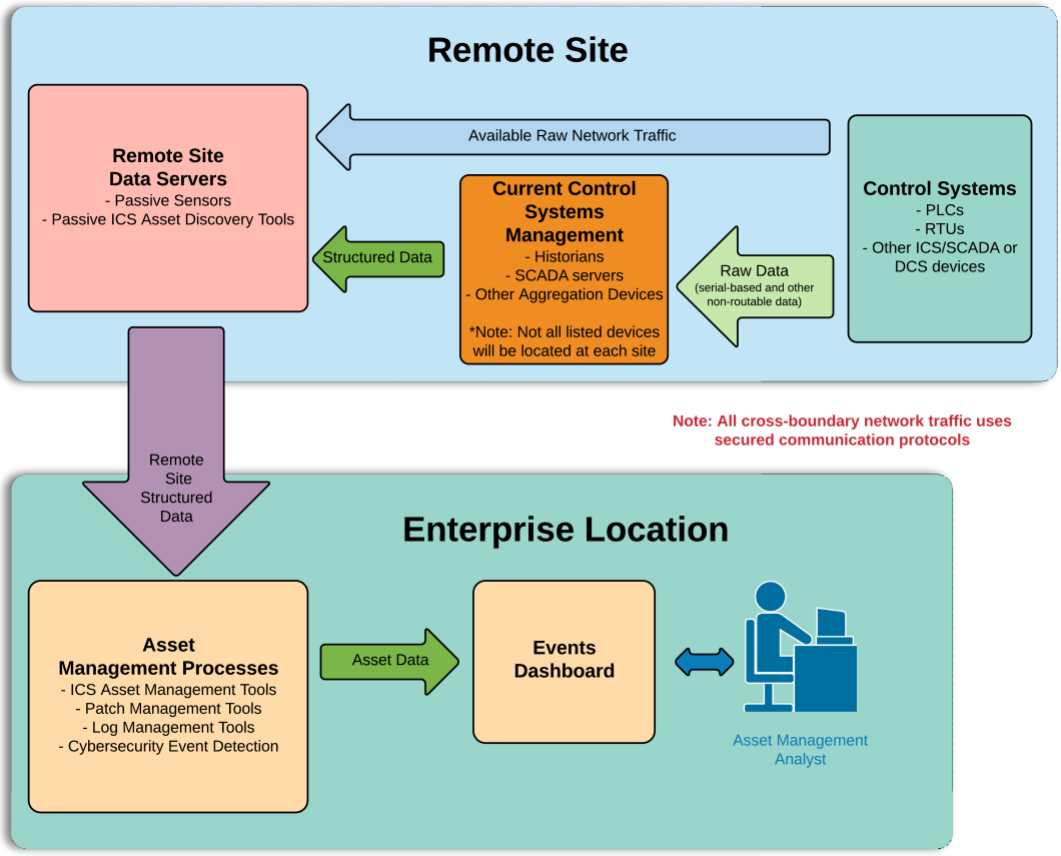
- Some level of an asset management capability already exists within an organization.
- All OT assets within an organization's infrastructure, especially those that are considered critical, need to be identified, tracked, and managed.
- OT networks are comprised of numerous ICS devices, such as programmable PLCs and IEDs, in addition to other vital components, such as engineering workstations, historians, and human-machine interfaces (HMIs), which are typically installed on a Windows and/or Linux OS.

Background

The NCCoE, in collaboration with organizations in the Energy Sector, identified the need to strengthen their asset management capabilities, especially for assets that are geographically dispersed. Vulnerabilities in OT assets present opportunities for malicious actors to cause disruptions to both electrical grid and oil and natural gas infrastructure. Such disruptions can result in economic loss and the interruption of critical services to millions of people. To properly assess cybersecurity risk within the OT network, energy companies must be able to identify all of their assets, especially those that are most critical. This project will describe a reference architecture and an example solution for managing, monitoring, and baselining assets, and will also include information to help identify threats to these OT assets. An OT asset management solution may also serve as a key component of an organization's comprehensive asset inventory, including enterprise assets as well.

2 High-Level Architecture

The figure below depicts the proposed high-level environment and architecture to help improve asset management within an energy organization.



Component List

Collaborating partners (participating vendors) will need to provide components to develop an example solution, including, but not limited to, the following components:

- OT/ICS-specific asset discovery and management tools
- Reliable/secure/encrypted communication devices

- Cybersecurity event/attack detection capability
- Log management/security information and event management (alerting)

Desired Capabilities

The security capabilities of the example solution are as follows:

- OT/ICS asset inventory (to include devices using serial connections)
- High-speed communication mechanisms for remote asset management
- Reliable/secure/encrypted communications
- Continuous asset monitoring
- Log analysis and correlation
- Cybersecurity event/attack detection
- Patch level information

3 Relevant Standards and Guidance

- American National Standards Institute (ANSI)/International Society of Automation (ISA)-TR62443-2-3-2015, *Security for industrial automation and control systems Part 2-3: Patch management in the IACS environment*, 2015. https://www.isa.org/store/isa-tr62443-2-3-2015,-security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-iacs-environment/40228386
- American National Standards Institute (ANSI)/International Society of Automation (ISA)-62443-3-3 (99.03.03)-2013, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*, 2013. https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785
- American National Standards Institute (ANSI)/International Society of Automation (ISA)-62443-2-1-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731
- The Center For Information Security (CIS) Critical Security Controls V6.0 https://www.cisecurity.org/controls/
- Control Objectives for Information and Related Technology (COBIT) 5, Information Systems Audit and Control Association (ISACA). https://www.isaca.org/cobit/pages/default.aspx
- Cryptographic Standards and Guidelines, National Institute of Standards and Technology (NIST). https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1, February 2014. https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

- *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0, National Institute of Standards and Technology (NIST), February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 4254, *The Secure Shell (SSH) Connection Protocol*, January 2006. https://www.ietf.org/rfc/rfc4254.txt
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008. https://tools.ietf.org/html/rfc5246
- International Organization for Standardization (ISO) 55000:2014, *Asset Management — Overview, principles and terminology*, January 2014. https://www.iso.org/standard/55088.html
- International Organization for Standardization (ISO) 55001:2014, *Asset Management — Management systems — Requirements*, January 2014. https://www.iso.org/standard/55089.html
- International Organization for Standardization (ISO) 55002:2014, *Asset Management — Management systems — Guidelines for the application of ISO 55001*, January 2014. https://www.iso.org/standard/55090.html
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19770-1:2017, *Information technology — IT asset management — Part 1: IT asset management systems — Requirements,* December 2017. https://www.iso.org/standard/68531.html
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19770-5:2015, *Information technology — IT asset management — Part 5: Overview and vocabulary,* August 2015. https://www.iso.org/standard/68291.html
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*, August 2013. https://www.iso.org/standard/54534.html
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27019:2017, *Information technology — Security techniques — Information security controls for the energy utility industry,* October 2017. https://www.iso.org/standard/68091.html
- National Institute of Standards and Technology (NIST) Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, July 2013. https://doi.org/10.6028/NIST.SP.800-40r3
- National Institute of Standards and Technology (NIST) Special Publication 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, April 2014. https://doi.org/10.6028/NIST.SP.800-52r1
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4
- National Institute of Standards and Technology (NIST) Special Publication 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security,* May 2015. https://doi.org/10.6028/NIST.SP.800-82r2

- National Institute of Standards and Technology (NIST) Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016. https://doi.org/10.6028/NIST.SP.800-160
- National Institute of Standards and Technology (NIST) Special Publication 1800-5 (DRAFT), *IT Asset Management*, 2014. https://nccoe.nist.gov/library/it-asset-management-nist-sp-1800-5-practice-guide
- National Institute of Standards and Technology (NIST) Special Publication 1800-7 (DRAFT), *Situational Awareness for Electric Utilities*, 2017. https://nccoe.nist.gov/library/situational-awareness-electric-utilities-nist-sp-1800-7-practice-guide
- *Reliability Standards for the Bulk Electric Systems of North America,* North American Electric Reliability Corporation (NERC), last updated February 15, 2018. http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

4 Security Control Map

			Informative References						
Function	**Category**	**Subcategory**	**CIS CSC 2016**	**COBIT5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**NERC CIP Standards**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	1	BA109.01, BA109.02	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8	CIP-002-5 R1, CIP-002-5 R2
		ID.AM-2: Software platforms and applications within the organization are inventoried.	2	BA109.01, BA109.02, BA109.05	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8	CIP-010-2 R1
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-2:** Threat and vulnerability information is received from information-sharing forums and sources.	4		4.2.3, 4.2.3.9, 4.2.3.12		A.6.1.4	PM-15, PM-16, SI-5	

			Informative References						
Function	Category	Subcategory	CIS CSC 2016	COBIT5	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected.	13, 14, 17	APO01.06, DSS06.06		SR 3.1, SR 3.8, SR 4.1, SR 4.2	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8	CIP-011-2 R1
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	2			SR 3.1, SR 3.3, SR 3.4, SR 3.8	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3	SI-7	
	Maintenance (PR.MA): Maintenance and repair of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools.		BAI09.03	4.3.3.3.7		A.11.1.2, A.11.2.4, A.11.2.5	MA-2, MA-3, MA-5	CIP-10-2 R4
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	5, 12	DSS05.04	4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8		A.11.2.4, A.15.1.1, A.15.2.1	MA-4	CIP-005-5 R2

			Informative References						
Function	Category	Subcategory	CIS CSC 2016	COBIT5	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-4:** Communications and control networks are protected.	7, 11	DSS05.02, APO13.01		SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	A.13.1.1, A.13.2.1	AC-4, AC-17, AC-18, CP-8, SC-7	CIP-005-5 R1
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	9, 12	DSS03.01	4.4.3.3			AC-4, CA-3, CM-2, SI-4	
		DE.AE-3: Event data is aggregated and correlated from multiple sources and sensors.	6			SR 6.1		AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	

APPENDIX A REFERENCES

NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, *Revision 2*, May 2015. https://doi.org/10.6028/NIST.SP.800-82r2

APPENDIX B ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
CCS CSC	Council on Cybersecurity Top 20 Critical Security Controls
CIP	Critical Infrastructure Protection
COBIT	Control Objectives for Information and Related Technology
DCS	Distributed Control System
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ESAM	Energy Sector Asset Management
HMI	Human-Machine Interface
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
NCCoE	National Cybersecurity Center of Excellence
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controller
RFC	Request for Comments
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication
SSH	Secure Shell
TLS	Transport Layer Security