A NEMA White Paper CPSP 2-2018

Cyber Hygiene Best Practices

Published by

National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

www.nema.org

The requirements or guidelines presented in this NEMA white paper are considered technically sound at the time they are approved for publication. They are not a substitute for a product seller's or user's own judgment with respect to the particular product discussed, and NEMA does not undertake to guarantee the performance of any individual manufacturer's products by virtue of this document or guide. Thus, NEMA expressly disclaims any responsibility for damages arising from the use, application, or reliance by others on the information contained in this white paper.

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller’s products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEMA has no power, nor does it undertake to police or enforce compliance with the contents of this document. NEMA does not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety-related information in this document shall not be attributable to NEMA and is solely the responsibility of the certifier or maker of the statement.

Executive Summary

Purpose

Cyber Hygiene Best Practices identifies a set of industry best practices and guidelines that electrical equipment and medical imaging manufacturers can implement to raise their level of cybersecurity sophistication in their manufacturing facility and engineering processes. The document provides guidelines for proactive and reactive security with a focus on people, processes, and products.

The guideline document addresses raising a manufacturer's level of cybersecurity sophistication by following seven fundamental principles:

a. Segmenting networks
b. Understanding data types and flows
c. Monitoring devices and systems
d. User management
e. Hardening devices
f. Updating devices
g. Providing a recovery plan/escalation process

This document is not meant to be all-inclusive but rather a representative set of best practices that vendors can implement both in their manufacturing facility and engineering processes. This document is also not intended to describe security best practices for the manufactured devices.

Document Structure

For each fundamental principle, the following information is provided:

a. Identification of threats and an analysis of their implications;
b. Additional reference documents and;
c. Recommendations that electrical equipment and medical imaging manufacturers should incorporate.

CONTENTS

Figures

Acknowledgements

This white paper guideline document was developed by a task force of the IoT Cybersecurity Council group of the National Electrical Manufacturers Association (NEMA). The following individuals were members of the task force.

Canon Medical Systems USA, Inc.	Royal Chen, Scott Nitsche
Eaton	Leon Newsome
Lutron Electronics Company, Inc.	Doug Kuhlman, Walt Zaharchuk
OSRAM SYLVANIA Inc.	Roy Harvey
Philips	Joe Burgoyne, Ben Kokx
S&C Electric Company	Steve Upp
Siemens Healthineers	Henri “Rik” Primo
Siemens Industry	Harry Brian, Sergey Chibizov, Frank Garrabrant

NEMA also extends its thanks to Jim Gilsinn, Principal Engineer from Kenexis for his contributions in the development of this document.

NEMA’s IoT Cybersecurity Council approval of this document does not necessarily imply that all council members voted for its approval or participated in its development. At the time this white paper was published, the IoT Cybersecurity Council was composed of the following member companies:

ABB, Inc., Raleigh, NC
Acuity Brands, Inc., Conyers, GA
Canon Medical Systems USA, Inc., Tustin, CA
Eaton, Cleveland, OH
Eberle Design, Inc., Phoenix, AZ
Encore Wire Corporation, McKinney, TX
GE Healthcare, Waukesha, WI
GE Lighting, Cleveland, OH
Honeywell International, Inc., Morris Plains, NJ
Hypertherm Inc., Hanover, NH
Lutron Electronics Company, Inc., Coopersburg, PA
Nidec Motor Corporation, St. Louis, MO
OSRAM SYLVANIA Inc., Wilmington, MA
Panasonic Corporation of North America, Secaucus, NJ
Panduit Corporation, Tinley Park, IL
Phillips, Andover, MA
Philips Lighting, Somerset, NJ
Rockwell Automation, Milwaukee, WI
S&C Electric, Chicago, IL
Schneider Electric, Andover, MA
Siemens Healthineers, Malvern, PA
Siemens Industry, Inc., Norcross, GA
Southwire Company, Carrollton, GA
Universal Lighting Technologies, Nashville, TN
VERTIV, Columbus, OH

Introduction

This cyber hygiene document identifies a set of industry best practices and guidelines for electrical equipment and medical imaging manufacturers to raise their level of cybersecurity sophistication in their manufacturing facility and engineering processes. The document provides guidelines for proactive and reactive security with a focus on people, processes, and products.

Document Scope

The guideline document addresses raising a manufacturer's level of cybersecurity sophistication by following seven fundamental principles:

a. Segmenting networks
b. Understanding data types and flows
c. Monitoring devices and systems
d. User management
e. Hardening devices
f. Updating devices
g. Providing a recovery plan/escalation process

This document is not meant to be all-inclusive but rather a representative set of best practices that vendors can implement both in their manufacturing facility and engineering processes. This document is also not intended to describe security best practices for the manufactured devices.

Definitions

Active Directory: Microsoft's trademarked directory service, which is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

Bill of Materials (BOM): A list of the raw materials, sub-assemblies, intermediate assemblies, sub-components, parts and the quantities of each needed to manufacture an end product.

Botnet: A number of internet-connected devices, each of which is running one or more software applications with automated tasks over the internet.

Computer Security Incident Response Team (CSIRT): A concrete organizational entity that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.

Cookie: A tiny file that is stored on your computer that contains past browsing information.

Demilitarized Zone (DMZ): A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet

Distributed Denial of Service (DDoS): An attack that makes an on-line service unavailable by overwhelming it with traffic from multiple sources.

Hardening: The process of securing a system by reducing its surface of vulnerability.

Industrial Control System (ICS): A general term that encompasses several types of control systems and associated instrumentation used for industrial process control.

International Electrotechnical Commission (IEC): An international standards organization that prepares and publishes international standards for all electrical, electronic and related technologies

Internet Engineering Task Force (IETF): The body that develops and promotes voluntary internet standards, in particular, the standards that comprise the internet protocol suite.

Information Technology (IT): The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

Internet of Things (IoT): The IoT refers to the ever-growing network of physical objects that have internet connectivity, and the communication that occurs between these objects and other internet-enabled devices and systems.

Intrusion Detection System / Intrusion Prevention System (IDS/IPS): IDS/IPS refers to technical means used to identify unexpected or malicious activity within a network. IDS will typically notify a security management application (e.g., SIEM) of a potential intrusion, whereas IPS will automatically block an intrusion once detected.

Joint Test Action Group (JTAG): The common name for the IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture. It is a method for testing interconnects on printed circuit boards or sub blocks inside an integrated circuit.

Lightweight Directory Access Protocol (LDAP): An application protocol for querying and modifying items in directory service providers like Active Directory.

Management Information Base (MIB): A formal description of a set of network objects that can be managed thru SNMP.

National Institute of Standards & Technology (NIST): A measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce

Operational Technology (OT): The hardware and software designated to detect or cause changes in the physical state of a system.

Patch: A piece of software that’s used to correct a problem with an operating system or software program.

Print Spooler: A system service in the Microsoft Windows operating system that is responsible for the management of the jobs that have been sent to the printer or the print server of a network.

Remote Access: Any access to a control system from another location

Remote Desktop: A separate program or feature found on most operating systems that allows a user to access and interact with an operating computer system’s desktop. The access occurs via the Internet or through another network in a different geographical location.

Simple Network Management Protocol (SNMP): An internet standard protocol for collecting and organizing information about managed devices on IP networks.

Security Information and Event Management (SIEM): A security management approach to provide a holistic view of the security related information that is collected, correlated and analyzed.

Supervisory Control and Data Acquisition (SCADA): A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers to interface to the process plant or machinery.

Transmission Control Protocol / Internet Protocol (TCP/IP): A suite of communication protocols used to interconnect network devices on the internet.

Transport Layer Security (TLS): A cryptographic protocol that provides communications security over a computer network.

Telnet: A protocol used on the internet or local networks to provide a bi-directional interactive text-oriented communication facility using a virtual terminal connection.

Universal Serial Bus (USB): An industry standard that defines cables, connectors and communications protocols for connection, communication, and power supply between computers and devices.

Whitelisting: An access control approach based on a list of acceptable entities that are allowed access to a system or network blocking out everything else**.**

Wireless Local Area Network (WLAN): A wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building.

Risk Tolerance

Risk tolerance refers to the amount of risk a manufacturer is willing to accept in order to meet their strategic objectives. Note: organizations will have different risk tolerances depending on their particular sectors and management. Understanding and documenting the acceptable risk level is critical to establishing the correct processes to deal with those risks.

Fundamental Principles

For each of the following fundamental principles, the document sections contain an identification of threats, their relevance (including appropriate informative reference standards or other documents that might apply), an analysis to determine implications, and recommendations that NEMA and MITA manufacturers should incorporate. The best practices that are described in this document are applicable to most manufacturing environments.

1. Segmenting Networks

This principle focuses on the design of data networks that logically/physically separate manufacturing systems data flows from business or public networks. It also provides the capability to segment critical manufacturing sub-networks from other manufacturing sub-networks with differing security requirements. Network segmentation involves dividing the network into smaller networks (called zones.) Compartmentalizing devices into zones does not necessarily mean isolating them. Conduits connect the security zones and facilitate the transport of necessary communications between the segmented security zones. Figure 1A and Figure 2A depict a typical segmented manufacturing network as well as a typical segmented multi-institution manufacturing network.

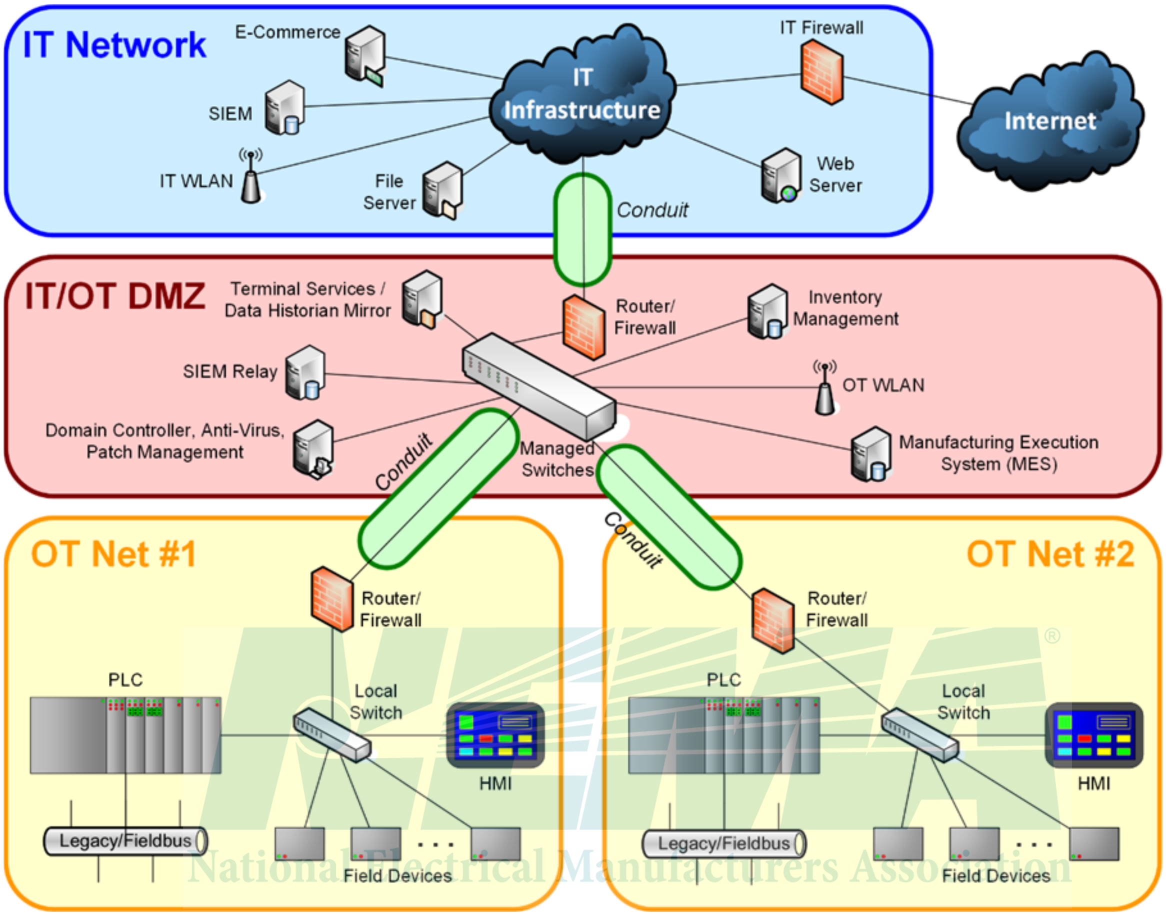

Figure 1 A Typical Segmented Manufacturing Network

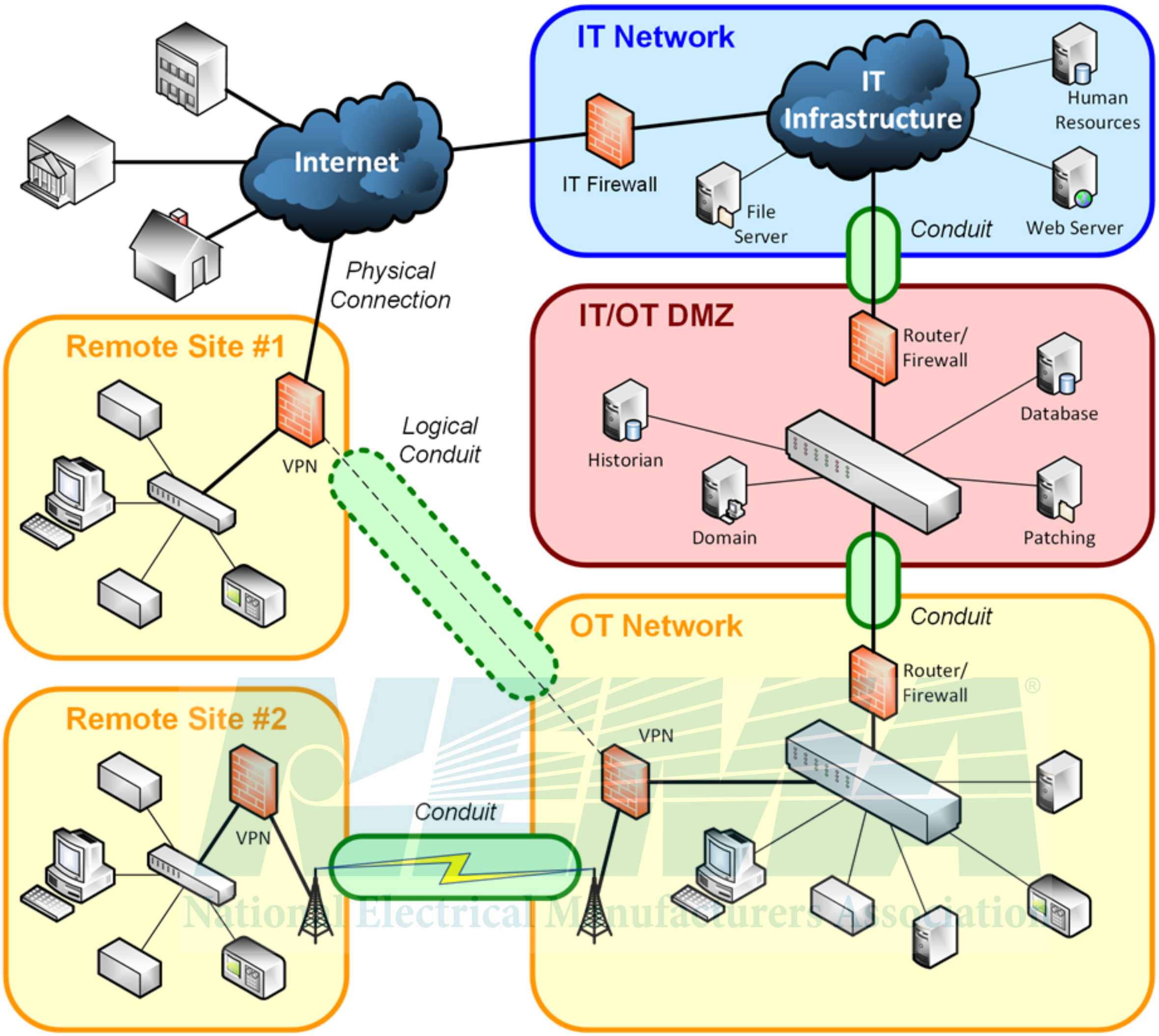

Figure 2 A Typical Segmented Multi-Institution Manufacturing Network

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. One of the goals of the segmentation of networks is preventing non-essential or even malicious network traffic from ingressing the operational technology (OT) network. This type of traffic can disrupt, and in some cases, even modify the OT traffic or OT device functions. Therefore, only valid, authenticated OT network traffic should be permitted to enter the OT network zones.

Another goal of the segmentation of networks is to prevent sensitive data from egressing a security zone. Some of the recent high-profile attacks included a “phone-home” capability, where the attack included an exfiltration agent that was able to send data out of the victim’s network back to a command and control host. Again, only valid, authenticated network traffic should be permitted to exit the security zones.

Reference Documents

a. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

   1. A.3.3.4 Network segmentation

b. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels

   1. SR 5.1 Network segmentation

c. NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)

   1. AC-4 Information Flow Enforcement
   2. SC-7 Boundary Protection

d. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

Manufacturers Recommendations

Networks are segmented through the use of a barrier device that can control what passes through the device. On Ethernet-based networks running the transmission control protocol/internet protocol (TCP/IP), the most common barrier devices in use are firewalls, routers, data diodes, and layer 3 switches.

The generally accepted good practice is to use a barrier device to manage the communication across the conduit that links the OT zone to the information technology (IT) zone. The barrier device can serve as a good automated tool to enforce that security practices be followed in the OT zone, such as not allowing inbound email or communications to/from the Internet.

For high-risk industrial control systems (ICS), the use of a demilitarized zone (DMZ) in conjunction with an OT zone offers additional risk reduction opportunities between the low-security level IT zone and the high-security level OT zone. The security level for the DMZ is higher than the IT zone but less than the OT zone. The function of this zone is to eliminate or greatly reduce all direct communication between the OT zone and the IT zone. Where wireless local area network (WLAN) access to an OT network is considered necessary by a manufacturer, it is recommended that the OT WLAN network have a distinct SSID. The connectivity from that WLAN should be limited to the smallest OT zone possible.

A further consideration for segmentation is that of remote access. Remote access to the OT zone should only be enabled when necessary and authenticated. Remote user access to the OT zone may require multifactor authentication, depending on the security level requirement.

The risk associated with the ICS may be too great to allow any opportunity for compromise by an external agent. A facility may choose to disconnect all conduits between the OT zone and any other zone. This is a very valid network segmentation strategy for consideration. Facilities choosing to adopt this isolation approach are not automatically eliminating all risk. There may still be much vulnerability that could be exploited locally. Appropriate layers of cyber and physical protection should be employed to address the residual risk remaining after isolation of the OT zone from the IT zone.

2. Understanding Data Types and Flows

This principle focuses on the understanding of the applications in which products are being deployed. For manufacturers and end users it is important to know what data should flow through a network, where that data typically goes, and what or who should have access to it.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. Within an internet of things (IoT), ICS, and supervisory control and data acquisition (SCADA) network the amount and types of data that they send and receive are relatively static. The introduction of new communication paths that are outside the norm of typical data flow patterns could represent malicious activities that could either compromise or shut down the respective network.

Reference Documents

a. NIST SP800-53, Rev 5 (Draft): Security and Privacy Controls for Information Systems and Organizations (August 2017)
   1. AC-4 Information Flow Enforcement
   2. CA-9 Internal System Connections

b. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

Manufacturers Recommendation

When new communication paths, and changes to existing communication paths, are introduced into a network, alarms should go off to indicate that something may be wrong. These alerts would feed into the manufacturers monitoring devices and systems.

3. Monitoring Devices and Systems

This principle addresses how manufacturers should provide the ability to monitor the health and security of their devices and systems within their environment. Monitoring capability should be provided through existing well known and standard software mechanisms (i.e., Simple Network Management Protocol [SNMP], Syslog) that do not get into specific process parameters.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. An effective monitoring system will serve to enhance the built-in security of the corresponding device or system.

Reference Documents

a. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels
   1. FR 6 Timely response to events

b. NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)
   1. AU-2 Audit Events
   2. AU-3 Content of Audit Records
   3. AU-7 Audit Reduction and Report Generation
   4. AU-8 Time Stamps
   5. CA-7 Continuous Monitoring
   6. SI-4 System Monitoring

c. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

d. IETF RFC 5424: The Syslog Protocol

Manufacturers Recommendation

Manufacturers should have devices designed to allow centralized monitoring of their performance, network statistics, core functionality, and security features.

SNMP is widely used as it exposes management data in the form of variables on the managed systems organized in a management information base (MIB) that describes the system status and configuration. These variables can then be remotely queried (and in some cases, manipulated) by managing applications. While three significant versions of SNMP have been developed, Version 3 features improvements in performance, flexibility, and security. Therefore Version 3 should be used or supported. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, and printers.

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. A wide variety of devices such as printers and routers use the syslog standard. It can be used for system management and security auditing as well as general information, analysis and debugging. There are also options available within Syslog to use TCP and Transport Layer Security (TLS) if the manufacturer's environment can support it to ensure reliable and secure delivery of security events.

In Windows, Linux or other Operating Systems, an event log can be used as a record of a computers alerts and notifications. Microsoft defines an event as "any significant occurrence in the system or program that requires users to be notified or an entry added to a log."

A manufacturer that implements a Security Information and Event Management (SIEM) solution may use the SIEM to gather information from devices such as servers, routers, switches, Intrusion Detection System / Intrusion Prevention System (IDS/IPS) appliances and firewalls to gather a holistic view of security for their entire network. SIEMs often include event analysis capabilities that can identify active security events by correlating information from multiple sources within the manufacturer's network and presenting them in a more context meaningful presentation format to a manufacturer's IT/OT network security engineering personnel.

4. User Management

End user management capabilities should be provided by the manufacturers that intelligently control access to computer network security. It is typically broken down into the following (4) areas:

a. Administration—Manufacturers should have the capabilities to create, modify, and delete accounts on the system. This could be either centrally or locally managed.
b. Authentication—Manufacturers should have a process to verify the identity of a user. Based on the degree of acceptable risk this could be multi-factor.
c. Authorization—Manufacturers should provide the capability to manage user privileges, for example, role-based access control.
d. Audit—Manufacturers should have a way to monitor the actions taken and resources consumed by a user or process, and to store the data in an audit log.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. Perhaps one of the most common threats is manufacturers not enabling a mandatory default password change on first use. While default passwords are very useful for vendors and end-users in allowing quick configuration of a device from its out-of-box state issues arise when default passwords are not changed by the end-user; vendors do not provide an easy mechanism to change them, or hard-coded passwords are included in the device.

As an example, recently IoT devices have been used to create large scale botnets that can execute crippling distributed denial of service (DDoS) attacks. The Mirai botnet affected more than 300,000 IoT devices using default or weak passwords to create nearly 600 Mbps of disruptive internet traffic to all the different sites being affected.

Reference Documents

a. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

    1. A.3.3.5 – Element: Access Control: Account Administration
    2. A.3.3.6 – Element: Access Control: Authentication
    3. A.3.3.7 – Element: Access Control: Authorization

b. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels

    1. Support of essential functions
    2. FR 1 Identification and authentication control
    3. FR 2 Use control

c. NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations

    1. AC Access Control Family
    2. AU-14 Session Audit
    3. IA Identification and Authentication Family

d. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

e. KrebsOnSecurity Hit With Record DDoS, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Manufacturer Recommendation

Administration

    a. Ability to add, modify, and delete any user and corresponding credentials within the system.

Authentication

    a. Requirement to change default passwords upon the first login
    b. No fixed /hard coded credentials (credentials which you are unable to change such as usernames and passwords) into devices
    c. Storing account information
        1. Ability to store accounts locally
        2. Ability to access centrally stored account systems, such as Active Directory or Lightweight Directory Access Protocol (LDAP)
    d. Ability to use multifactor authentication
    e. Usage of public key infrastructure, especially for remote login

Authorization

    a. Having role based access
        1. Pre-defined roles

    2. Ability to create user-defined roles

b. Having role based account management
    1. Having different roles for normal users versus administrative roles
    2. Ability to assign arbitrary privileges to roles

c. Ability to map any user account to any role

Audit

a. Ability to record user login/logout along with timestamps.
b. Ability to record files accessed and applications run while logged in
c. Ability to monitor user-created tasks, including scheduled tasks that don't require an active login session.
d. Ability to record failed login attempts along with timestamps.

5. Hardening Devices

This principle addresses techniques manufacturers should use to harden the devices employed to design and manufacture products. The best practices may vary depending on the manufacturer's particular sector.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. As equipment manufacturers use more effective network defenses, attackers identify alternate methods of entry that take them directly inside the shell of the protected and, more importantly, the trusted network environment. Once inside these attacks can exploit vulnerabilities or compromise the environment using multiple vectors such as web, email, and malicious files.

Reference Documents

a. NEMA CPSP 1-2015 Supply Chain Best Practices

b. NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

c. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels
    1. SR 3.5 Input validation
    2. SR 3.6 Deterministic output
    3. SR 3.7 Error handling

d. NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)
    1. SC-27 Platform-Independent Applications
    2. SC-41 Port and I/O Device Access

e. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

Manufacturer Recommendations

There are a number of techniques available to manufacturers for hardening devices. Manufacturers should consider either turning off or disabling a number of device features that are not needed or may have inherent security risks. Examples include Joint Test Action Group (JTAG), Telnet, SNMP Versions 1 and 2, and wireless communication.

Manufacturers may consider removing unnecessary programs such as Word Pad, games, and browser plug-ins such as Java. Manufacturers may also consider removing unnecessary services such as print spooler and remote desktop. Also, manufactures may also consider disabling cookies.

Ethernet and Universal Serial Bus (USB) port blockers can be effective in physically blocking network traffic into a manufactured device.

Error handling and input validation capabilities should also be considered. Examples include sanitizing inputs, static code testing, and software bill of materials (BOM) analysis

Data encryption should be used when the information is confidential and sensitive. Manufacturers need to consider if the data needs to be encrypted at rest within the device, in motion when it is in transmission or a combination of both. Integrity protection should be used when information transfer must be reliable and without error.

Defensive techniques to a denial-of-service attack typically involve the use of a combination of attack detection and traffic classification and response tools. They aim to block traffic identified as illegitimate and allow traffic identified as legitimate. While most firewalls and routers do have capabilities to deny incoming traffic from an outside attacker, they can be easily overwhelmed as the attack becomes more and more sophisticated. Other options available include Intrusion Prevention Systems and the use of application front end hardware to analyze data packets as they enter the system and identify them as priority, regular, or malicious.

Finally, manufacturers may wish to consider a secure by default method in which the default configurations are the most secure. A drawback is that these settings may be less backwards compatible and may require more complex initial configuration making it less user friendly.

6. Updating Devices

This principle focuses on procedures that manufacturers should use to update the devices that are currently deployed based on vulnerabilities becoming known as well as the security requirements and necessities of their operating environment. The best practices may vary depending on the manufacturer’s particular sector.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. Updating devices and systems, where possible is an important step in keeping up with recent functionality and security improvements. Unfortunately, this often gets overlooked for a variety of reasons, such as the end users not having a plan for updating when they architect the system or due to the complexity of managing updates in various environments. There are risks that end users could install un-validated patches or updates themselves due to the inherent nature of how they are automatically transmitted.

Reference Documents

a. NEMA CPSP 1-2015 Supply Chain Best Practices

b. NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

c. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

    1. A.3.4.2.5.1 Patching IACS Devices

   2. A.3.4.3 Element: System development and maintenance

d. IEC TR 62443-2-3:2015 Security for industrial automation and control systems—Part 2-3: Patch management in the IACS environment

e. NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)

   1. MA Maintenance Family

f. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

Manufacturers Recommendation

Patches have become increasingly important as a methodology for updating programs or new system security threats which appear regularly, especially in online environments. Manufacturers typically provide some type of patching system for their deployed products and systems. In most instances, the patching system is not automatic as manufacturers have a number of recommended procedures they follow to verify the authenticity of the patch, test the patch, provide guidance if a reboot of the system is required, and to notify the end user of the appropriate time frame for patch validation.

In some instances, manufacturers may decide to recommend mitigating controls (also known as compensating countermeasures), until patches become available and fully tested and validated. Examples include disabling a vulnerable service or disabling ports (which can be done at either the perimeter or device level).

For some environments, manufacturers may provide a recommended anti-virus software package - or implement a whitelisting access control approach for mitigating security threats.

7. Providing a Recovery Plan/Escalation Process

This principle focuses on providing a recovery plan/escalation process that manufacturers should use if a vulnerability is found in the manufactured device. This also includes the possibility of an active exploit against the device.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. The absence of a recovery plan /escalation process can rapidly disrupt business operations, information security, IT systems, employees, customers, upstream suppliers, and other vital functions.

Reference Documents

a. NEMA CPSP 1-2015 Supply Chain Best Practices

b. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

   1. A.3.4.5 Element: Incident planning and response

c. NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)

   1. IR Incident Response Family

d. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

e. ISO/IEC 29147:2014: Information Technology—Security Techniques—Vulnerability Disclosure

f. ISO/IEC 30111:2013: Information Technology—Security Techniques—Vulnerability Handling Processes

Manufacturers Recommendation

Manufacturers should develop a plan to manage incidents and vulnerabilities. Ideally, it should include incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure, monitoring the progress of the incident resolution, and a communication plan to inform affected parties about the status of the resolution.

Manufacturers should also maintain communication channels with end users and upstream suppliers in order to keep abreast of any vulnerability issues and steps to mitigate the issues.

Some software and hardware manufacturers have recently been using what are called “bug bounties” to allow security researchers a way to identify and provide information about a vulnerability to the manufacturer. Before a manufacturer embarks on implementing a “bug bounty” program, it should carefully consider the way in which it reacts to the vulnerability discovery itself, the way in which it reacts to the security researcher, and the way in which it makes the information known to its customers. Companies may want to consider first creating an internal computer security incident response team (CSIRT) where security researchers can report bugs via a responsible disclosure mechanism, and that they have found a way to mitigate those vulnerabilities before considering paying money for those vulnerabilities.