National Electrical Manufacturers Association

Representing Electrical and Medical
Imaging Equipment Manufacturers
www.nema.org

November 15, 2016

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Communications and Technology
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

The Honorable Michael Burgess
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Janice Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden, Chairman Burgess, Ranking Member Eshoo, and Ranking Member Schakowsky:

On behalf of the National Electrical Manufacturers Association (NEMA)—the trade association representing nearly 400 electrical and medical imaging manufacturers, 400,000 American jobs, and more than 7,000 facilities across the United States—I am writing to thank you for holding a hearing on the security of connected devices, "Understanding the Role of Connected Devices in Recent Cyber Attacks."

As the manufacturers of the equipment used in ten of the sixteen Critical Infrastructure Sectors designated by Presidential Policy Directive 21—Chemical Sector, Commercial Facilities Sector, Critical Manufacturing Sector, Energy Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, and the Water and Wastewater Systems Sector—the electrical and medical imaging industries are committed to protecting the cyber and physical security of the United States and its citizens.

In order to improve the supply chain security of NEMA members' products, NEMA members collaborated to produce and publish a set of industry best practices for electrical and medical imaging manufacturers to implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. *Supply Chain Best Practices* (NEMA CPSP 1-2015, enclosed) covers all aspects of the supply chain security, from manufacturing to delivery to operation to decommissioning.

Cybersecurity is a rapidly evolving threat, and NEMA and our members take the security of electrical and medical imaging products very seriously. We thank you for focusing on this important topic, but caution that government policies and regulations cannot always keep up with the pace of cybersecurity threats. Industry is already taking a proactive approach to cybersecurity, and will continue to do so in the future. Any new security policies or regulations must be flexible enough to allow manufacturers to continue to innovate and provide their customers with cyber-secure products.

1300 North 17th Street, Suite 900 - Rosslyn, VA 22209 - 703.841.3200 - 703.841.5900 fax

If you have any questions, please contact Patrick Hughes, Senior Director of Government Relations and Strategic Initiatives, at 703-841-3205 or patrick.hughes@nema.org.

Sincerely,

Kyle Pitsor
Vice President, Government Relations

CC: The Honorable Fred Upton
The Honorable Frank Pallone, Jr.

Enclosure: NEMA Guideline Document *Supply Chain Best Practices* (NEMA CPSP 1-2015)

NEMA Guideline Document
CPSP 1-2015

Supply Chain 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.

© 2015 National Electrical Manufacturers Association. All rights, including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention for the Protection of Literary and Artistic Works, and the International and Pan American copyright conventions.

EXECUTIVE SUMMARY

PURPOSE

This document identifies a recommended set of supply chain best practices and guidelines that electrical equipment and medical imaging manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. The document addresses United States supply chain integrity through four phases of a product's life cycle:

- An analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's supply chain;
- Tamper-proofing to ensure that the configurations of the manufactured devices have not been altered between the production line and the operating environment;
- Ways that a manufactured device enables asset owners to comply with security requirements and necessities of the regulated environment;
- Decommissioning and revocation processes to prevent compromised or obsolete devices from being used as a means to penetrate active security networks.

This document is not meant to be all-inclusive but rather a representation of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain. Each type of manufactured product will have some tolerance to the risks identified in this document. Understanding and documenting the acceptable risk level is critical to establishing the correct processes to deal with those risks.

DOCUMENT STRUCTURE

For each phase of the product life cycle, the following information is provided:

- Identification of threats and their relevance (including appropriate informative reference standards or other documents that might apply);
- Analysis to determine implications;
- Recommendations that electrical equipment and medical imaging manufacturers should incorporate.

© 2015 National Electrical Manufacturers Association

Contents

EXECUTIVE SUMMARY 2

ACKNOWLEDGEMENTS 4

INTRODUCTION 5

DOCUMENT SCOPE 5

DEFINITIONS 5

RISK TOLERANCE 5

SUPPLY CHAIN COMMUNICATION 5

BEST PRACTICES 6

MANUFACTURING AND ASSEMBLY 6

- Identification of Threats 6
- Analysis and Recommendations 7

TAMPER-PROOFING 10

- Identification of Threats 10
- Analysis and Recommendations 11

SECURITY DEVELOPMENT LIFE CYCLE 13

- Identification of Threats 13
- Analysis and Recommendations 14

DECOMMISSIONING/REVOCATION 17

- Identification of Threats 17
- Analysis and Recommendations 18

Appendix A REFERENCE DOCUMENTS 20

Appendix B REFERENCE ARCHITECTURES 23

Figures

Figure 1 SGAM Framework 23

Figure 2 Interoperability Layered Categories Defined by GWAC 26

Tables

Table 1 SGAM Domains 24

Table 2 SGAM Zones 25

© 2015 National Electrical Manufacturers Association

Acknowledgements

This white paper guideline document was developed by the cybersecurity working group of the National Electrical Manufacturers Association (NEMA). The group includes representation across the following divisions within NEMA: Industrial Automation, Electronics, Building Systems, Power Equipment, Lighting, Wire & Cable, and the Medical Imaging and Technology Alliance (MITA). At the time this white paper was published, the cybersecurity working group was composed of the following member companies:

ABB, Inc.—Raleigh, NC
Acuity Brands, Inc.-—Conyers, GA
Eaton—Cleveland, OH
Encore Wire Corporation—McKinney, TX
GE Healthcare—Waukesha, WI
GE Industrial Solutions—Plainville, CT
Honeywell Automation & Control Solutions—Golden Valley, MN
Landauer, Inc.—Glenwood, IL
Panasonic Corporation of North America—Secaucus, NJ
Panduit Corporation—Tinley Park, IL
Phillips Healthcare—Andover, MA
Rockwell Automation—Milwaukee, WI
S&C Electric—Chicago, IL
Schneider Electric—Andover, MA

© 2015 National Electrical Manufacturers Association

INTRODUCTION

This document will identify a recommended set of supply chain best practices and guidelines that NEMA and MITA manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. Successful implementation of the practices described in this document will also address a known area for development, alignment, and collaboration (supply chain risk management) identified in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was developed as a response to Presidential Executive Order 13636—Improving Critical Infrastructure Cybersecurity.

DOCUMENT SCOPE

This guideline document addresses United States supply chain integrity through four phases of the product life cycle: manufacturing and assembly, tamper-proofing, security development life cycle, and decommissioning/revocation. This document is not meant to be all-inclusive but rather a representation of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain.

DEFINITIONS

Key terms used throughout this document:

Manufacturer: an organization or entity that makes a device through a process that includes raw materials, components, or assemblies

Embedded component: a component with a dedicated function within a larger electrical or mechanical device

Tamper-proofing: a methodology used to hinder, deter, or detect unauthorized access to a device

Operational compliance: a state of being in accordance with established guidelines, specifications, or requirements

Revocation: the act of recall or annulment

Decommissioning: a formal process for removing a device from active status

Upstream suppliers: those who supply components to a manufacturer, including chip manufacturers and software driver developers

RISK TOLERANCE

Each type of manufactured product will have some tolerance to the risks identified in this document. Understanding and documenting the acceptable risk level is critical to establishing the correct processes to deal with those risks.

Understanding the level of acceptable risk is also required for establishing correct upstream and downstream supply chain relationships. It is typically difficult, if not impossible, to have a greater level of security (i.e., lower level of risk) than the upstream supply chain can provide.

SUPPLY CHAIN COMMUNICATION

An often unspoken risk is lack of communication across the supply chain. Depending on the expected lifetime of a product, the requirement for communication can be a major source of overhead. The

© 2015 National Electrical Manufacturers Association

requirement for communication extends upstream to all embedded component providers and downstream to all manufacturers and customers.

BEST PRACTICES

Each of the following sections contains 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.

MANUFACTURING AND ASSEMBLY

This section focuses on an analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's supply chain. Embedded components could be hardware-related, such as a microprocessor chip or an Ethernet chip on a motherboard, or software-related, such as an embedded operating system (O/S) or firmware/code stored in a non-volatile memory device, such as ROM or flash memory. The analysis done in this section needs to take into account security considerations of upstream suppliers in the supply chain to determine their levels of malware protection and detection.

Identification of Threats

1. Maliciously Tainted Components

   A maliciously tainted component is one that has been procured through a manufacturers' authorized channel but has been tampered with or altered in a way that is not compatible with its design specification. When describing software components, the term "malware" is sometimes used. Components that have been corrupted might not perform as intended and could enable a specific attack on an entity or organization using the particular product that includes the installed components. Failure, degraded performance, rogue functionality, and weakened security mechanisms are all possible outcomes of maliciously tainted components.

2. Counterfeit Components

   A counterfeit component is one that is supplied to a manufacturer directly or indirectly by other than an authorized channel and is presented as being legitimate even though it is not. Counterfeiting poses a risk because the component's integrity cannot be validated, the performance might be substandard, and specific technical support services are not available.

3. Practices of Upstream Suppliers

   Components could be supplied to a manufacturer via a normal distribution channel or a gray-market source. A normal distribution channel refers to the established chain of business(es) through which a component passes before it reaches the manufacturer. A gray market is the trade of a component through a distribution channel that while legal, is unofficial, unauthorized, or unintended. Manufacturers need to understand how procured components are moving through their distribution channels in order to verify legitimacy. Whenever components are purchased outside normal distribution channels, there is additional risk of maliciously tainted or counterfeit components being entered into the product.

© 2015 National Electrical Manufacturers Association

4. Lack of Formal Design Processes

   A formal design process is a multi-step process that includes research, conceptualization, feasibility study, establishment of design requirements, preliminary design, detailed design, production planning and tool design and, finally, production of a specific product. Ideally, this process should be documentable and repeatable. In addition, manufacturers need to understand how security considerations would be integrated into every step of the process, beginning with its initiation.

   There are two sources of risk with design processes. First, the design processes of upstream suppliers place limits on the risk of the integrating manufacturer. Second, the design processes of a manufacturer will have obvious impact on the components and products provided downstream to other manufacturers or consumers.

5. Software Executables

   A software executable or executable code is software in a form that can be run on a computer. It usually refers to machine language, the set of native instructions the computer carries out in hardware. Executable code may also refer to programs written in interpreted languages that require additional software to execute. There might be unnecessary capabilities or features of these executables that would affect the product's overall security. The challenge is to identify and then either disable or lock down these particular aspects without affecting the overall intended functionality of the software.

Analysis and Recommendations

1. Maliciously Tainted Components

   Several published standards speak to the need for malware detection and protection. Manufacturers can choose to follow any or all of the techniques described in the documents identified below:

   a) The *Open Trusted Technology Provider™ Standard* (section 4.2.1.12). Malware detection tools should be deployed as part of the code acceptance and development process. These techniques should also be used before final packaging and delivery.

   b) The SAFECode *Software Integrity Controls* document. Malware scanning at exchange points between parties, using the most recent malware signature files and more than one scanning engine.

   c) NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.6) speaks to the need to apply static analysis tools to search for virus/malware signatures.

   d) IEC 62443-1-1, *Industrial Communication Networks—Network and System Security* (section 5.6.6) calls out scanning for malicious software as an effective threat countermeasure.

   Recommendations: Manufacturers should work with upstream component suppliers to identify component versions and should thoroughly evaluate each new version of a component. This evaluation should include a malware analysis. In addition, each component supplier should

© 2015 National Electrical Manufacturers Association

identify the methods used to ensure that the component is not altered between manufacture and receipt.

Where technically feasible, code signing is one method of ensuring deliverables have not been altered. It also provides methods to ensure the authenticity of the deliverable and supplier. Code signing is the process of digitally signing executables and scripts by use of a cryptographic hash to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. Almost every code-signing mechanism will provide some sort of digital signature mechanism that answers the questions of authentication (who signed the code?) and integrity (has the code been tampered with since it was signed?).

The code signing white paper developed by Certificate Authority Security Council (https://casecurity.org/wp-content/uploads/2013/10/CASC-Code-Signing.pdf) includes a number of best practices that can be used to address the biggest issue with code signing: the protection of the private signing key associated with the code-signing certificate.

2. Counterfeit Components

Some suggested procedures and techniques that manufacturers can use to address fraudulent/ counterfeit components are identified in the standards documents listed below:

a) SAE International SA AS5553, *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*, was created in response to a significant and increasing volume of fraudulent/counterfeit electronic parts entering the aerospace supply chain. The document was expanded to address fraudulent/counterfeit risk mitigation on a global scale across multi-sector electronic supply chain industries and to provide uniform requirements, practices, and methods to mitigate the risks of receiving and installing fraudulent/counterfeit electronic parts. Section 4 describes a control plan that documents processes used for risk mitigation, disposition, and reporting of suspect or confirmed fraudulent/counterfeit parts and/or assemblies containing such parts.

b) ISO/IEC 27036-1: 2014 (parts 1, 2, and 3) is an introductory part of ISO/IEC 27036, *IT Security—Security techniques—Information security for supplier relationships.* It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships.

c) The *Open Trusted Technology Provider™ Standard* (section 4.2.1.11) lists counterfeit mitigation techniques, such as security labeling and scrap management.

d) NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 3) describes a supply chain risk-management plan that addresses an organization's internal and external practices and controls employed to minimize the risk posed by counterfeits.

Recommendations: It is suggested that manufacturers follow a documented purchasing process that gives preference to procuring components from only the original component manufacturers or their authorized suppliers. Manufacturers should also have in place some type of industry-recognized incoming inspection technique in order to discover counterfeit components before they become physically integrated into a product.

© 2015 National Electrical Manufacturers Association

Tracking disposition of components might also be necessary if counterfeit detection occurs after a device has been shipped, in order to facilitate a recall.

3. Practices of Upstream Suppliers

As previously recommended, manufacturers should follow a documented purchasing process that gives preference to procuring components from only original component manufacturers or their authorized suppliers. Manufacturers can further mitigate the risks associated with upstream suppliers by adopting any of the following:

- Inclusion of terms and conditions related to security requirements in procurement contracts;
- Additional component acceptance procedures;
- Independent, third-party validation of supplier conformance;
- A practice for sampling incoming components (per lot/unit). This could be done at the upstream supplier before shipment or at the manufacturer's facilities upon arrival.

4. Lack of Formal Design Processes

The following identified standards address the need for a formal design process that includes software, firmware, hardware, and security aspects. Manufacturers can choose to follow any or all of the methods described.

- The *Open Trusted Technology Provider™ Standard* (section 4.1) describes the need to include documented requirements that are traceable, a well-defined engineering method, configuration management, quality and test management, and product sustainment capabilities. Additional levels of security are obtained by following a secure development engineering method.
- NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems,* states that a prerequisite for successful supply chain risk management begins with the fundamental performance of good system design that includes security requirements at inception.
- Both NIST IR 7622 (section 4.6) and IEC 62443-1-1, *Industrial Communication Networks—Network and System Security* (section 5.4) mention defensive design techniques, the practice of anticipating all possible ways an end user might misuse a product, and then designing to make such use impossible or minimize its negative consequences.

Recommendations: Manufacturers should have in place a documented design process. This process should be repeatable and measurable and should effectively identify and address potential vulnerabilities. Ideally it should be auditable via some type of organizational quality assurance procedure. This process should be documented in a way that can be shared with downstream manufacturers. Manufacturers should request process documentation from upstream suppliers as part of the contract agreement.

© 2015 National Electrical Manufacturers Association

5. Software Executables

   Suggested manufacturing techniques to address the unnecessary capabilities of software executables that could pose additional security risk are mentioned in the standards below.

   - The SAFECode *Software Integrity Controls* document addresses examining “out of the box” defaults on the source code and configuring it to be secure by default.

   - IEC/TR 80002-1, *Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software,* is a report aimed at risk management practitioners who perform risk management when software is included in a medical device/system. It details a management process that analyzes risk identifying known or foreseeable hazards that software failures could contribute to, evaluates the risk to determine if reduction is required, and suggests various risk controls that can be implemented in the software itself.

   - NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.9) mentions the possibility of software service/maintenance agreements for critical software elements.

   Recommendations: Manufacturers should have well-defined processes to identify and remediate vulnerabilities of software/firmware associated with a particular device throughout its life cycle. Several industry-recognized software vulnerability mitigation techniques (e.g., stack buffer overrun protection) are available for manufacturers to use as they work to develop software for a particular product.

TAMPER-PROOFING

This section focuses on tamper-proofing, which ensures that the configurations of the manufactured devices have not been altered between the production line and the operating environment. Another term often used in the same context is tamper-resistance. Tamper-proofing ranges from simple features like screws with special heads, to more complex elements, such as devices that render themselves inoperable or encrypt all data transmissions between individual chips, or the use of materials requiring special tools and knowledge. Effective tamper-proofing of a manufactured device ensures its integrity. If tamper-proofing measures can’t be provided, procedures to detect tampering should be made available to the receiver.

Identification of Threats

The system aspects listed below would require some form of tamper-proofing:

1. Hardware (embedded components)

   Embedded hardware components could include a microprocessor or an Ethernet chip on a motherboard. Tamper-resistant microprocessors are used to store and process private or sensitive information. Examples of tamper-resistant chips include a secure crypto processor and chips used in smartcards or integrated circuit cards.

© 2015 National Electrical Manufacturers Association

2. Software Components

   Software components include an operating system and any additional applications. Software tamper-proofing refers to protecting it against reverse engineering and modification.

   Tamper-proofing is not a single measure but rather a collection of different transformations that individually protect each other, as well as the software to be protected. Consideration should be given to possible impact on software performance as a result of any tamper-proofing mechanisms.

3. Data Storage Devices

   Storage could be either volatile or non-volatile. The main difference between the two is what happens when power is turned off. Volatile storage, such as memory, requires constant power in order to retain the data. With non-volatile storage, such as a hard disk drive, once the data is written it will remain for a considerable amount of time. However, there are also several types of non-volatile memory, such as read-only memory (ROM) or flash memory. The move to more non-volatile memory types in systems introduces new vulnerabilities as sensitive data (such as passwords) might still reside in main memory after a system is powered off or rebooted. Tamper-proofing storage devices would ensure that the data present on those devices has not been compromised.

4. Communications

   System communications can occur via wired network, wireless network, cellular, or Bluetooth, for example. Data transmitted through these various channels should be secured in order to prevent unauthorized access and misuse. It is widely known and accepted by the industry that some open-standard industry protocols in use today cannot be secured.

Analysis and Recommendations

1. Hardware (embedded components)

   Several published standards mention procedures for tamper-proofing hardware-embedded components: The *Supply Chain Security Assurance* document suggests that hardware products might mitigate the threat of tampering by using one or more of these techniques: tamper-resistant labeling, smart tags, or delivery via a trusted courier.

   - NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.9) recommends incoming inspections and acceptance testing of incoming items to detect evidence of tampering. It also stresses the importance of a configuration baseline.

   - Federal Information Processing Standard (FIPS) PUB 140-3 (section 4) lists security requirements for hardware cryptographic modules used within a security system protecting sensitive information in computer and telecommunications systems. It identifies four security levels; as the levels increase, so do the corresponding security and tamper-proofing requirements.

   Recommendations: At minimum, manufacturers should be required to use some type of tamper-resistant coating or seal for all hardware components.

© 2015 National Electrical Manufacturers Association

2. Software Components

Some suggested procedures and techniques that manufacturers might use to address tamper-proofing software are listed in the following standards documents:

- The *Supply Chain Security Assurance* document suggests that cryptographic checksums or a digital signature can be implemented to mitigate the tampering threat.

- FIPS PUB 140-3 (section 4) lists security requirements for software and firmware cryptographic modules used within a security system protecting sensitive information in computer and telecommunications systems. It identifies four security levels; as the levels increase, so do the corresponding security and tamper-proofing requirements.

Recommendations: At the Operating System (O/S) layer, manufacturers should consider using an O/S with minimal kernel features and reduced application sets. With the advent of Software Development Kits (SDKs), malicious individuals can manipulate commercial O/S kernels. Making the kernel harder to manipulate increases the integrity of the O/S component. Development-specific features should be disabled prior to shipping, and code should be stripped of debugging features and symbols. Joint Test Action Group (JTAG) is one such feature. JTAG is 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.

Manufacturers should use tamper-resistant techniques to produce software that is more difficult for an attacker to modify. Code signing, as mentioned earlier, should also be used.

3. Data Storage Devices

Tamper-resistant storage techniques provide a level of assurance for data integrity. Some processes that manufacturers should consider: increasing the level of authentication required for updating, modifying, or deleting data; encrypting data to ensure limited data access; hashing or assigning a digital signature to data; or creating immutable storage that can never be changed.

Recommendations: Manufacturers should consider the operational threat landscape that data will exist and implement appropriate data integrity controls. There are several publications that can assist manufacturers in selecting appropriate controls, including:

- NIST SP 800-111, *Guide to Storage Encryption Technologies for End Use Devices* (sections 3 and 4) provides guidance for organizations in understanding storage encryption technologies for devices and planning, implementing, and maintaining storage encryption technologies.

- IEEE STD 1619, *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices,* specifies cryptographic transform and key archival methods for protection of data in sector-level storage devices.

4. Communications

Tamper-resistant communication starts with a focus on ensuring that data cannot be manipulated maliciously. As an example, to assess the opportunity for malicious individuals to intercept,

© 2015 National Electrical Manufacturers Association

modify, and then send data to the intended recipient or device, manufacturers should consider the logical path by which the data will travel. This is called a “man-in-the-middle” attack. There are several ways to provide a level of tamper-proofing to communications. Secure-by-default protocols, such as SFTP, HTTPS, FTPS, and SSH, add levels of authentication to data streams and are relevant and industry-accepted.

Recommendations: Manufacturers should tamper-proof communications by permanently disabling historically unsecure communications services (e.g., TFTP, FTP, and Telnet) and should opt for secure-by-default protocols for their communication services. Manufacturers that use secure communications should understand the requirements of the protocols they use and configure them correctly. If PKI is used, for example, then the manufacturer should understand the necessary certificate and cipher requirements to ensure security. At minimum, a manufacturer should request external validation of security code if there is no in-house knowledge.

Suggested standards that address secure communications protocols in more detail include:

- IEC 62351 is a series of standards developed for information exchange for power systems and related systems, including energy management, supervisory control and data acquisition (SCADA), and distribution automation. However, not all industrial protocols are addressed in IEC 62351.

- ISO/IEC 27033 (parts 1-5) is a series of standards that provide detailed guidance on security aspects of the management, operation, and use of information-system networks and their inter-connections.

SECURITY DEVELOPMENT LIFE CYCLE

This section addresses ways the manufactured device enables asset owners to comply with the security requirements and necessities of the regulated environment. Depending on the environment where the device is installed, this could range from demonstrating auditable configuration management procedures to conformance with additional standards.

Identification of Threats

1. Configuration Management Practices

   Configuration Management is a systems engineering process for establishing and maintaining consistency of a product’s performance, functional, and physical attributes with its requirements, and design and operational information throughout its projected life cycle. This type of process facilitates orderly management of system information, as well as system changes.

2. In-house and Third-party Quality Assurance Audits

   Quality Assurance (QA) is a method of preventing mistakes or defects in manufactured products and avoiding problems when delivering the items. QA is applied to physical products in pre-production to verify that what will be made meets specifications and requirements, and during manufacturing production runs by validating that unit/lot samples meet quality controls. QA is also applied to software to verify that features and functions meet objectives and that the code is immune to known bugs prior to shipping or release of new software products or versions.

© 2015 National Electrical Manufacturers Association

A QA audit is conducted by an internal (in-house) or external (third-party) auditor that helps to ensure an organization's processes and systems are in place and being followed. The objective of the audit is to draw attention to necessary improvements and ensure that requirements are being followed in order to deliver consistent products.

3. Risk Management

It is important for manufacturers to understand the regulatory, contractual, physical, and operational environment in which a device will be installed. Understanding this environment allows the manufacturer to characterize the threats and vulnerabilities to which the device will be subjected.

Once this characterization has been completed, manufacturers should develop a risk response by analyzing the identified threats and vulnerabilities with their impact and likelihood. Additional operating or design controls might need to be developed, or specialized warnings and instructions to the asset owner might be necessary to address risk. As manufacturers change, update, or create new devices, this same risk management approach should be applied.

4. In-house/Third-party Testing

Testing a particular product within the confines of a manufacturer's facility serves to provide an internal level of confidence that the product is performing as intended. This testing could include specifying additional conditions for the environment in which the product will be installed.

Third-party certification testing refers to testing of a particular device or product (such as an accredited testing lab) to the specified requirements of the operational environment. Third-party labs typically generate an official results document upon successful test completion.

5. Incident (or Event) Management Plan

"Incident, or event, management" describes the activities of an organization to identify, analyze, and correct hazards or threats in an effort to prevent future occurrences. The absence of effective incident management can rapidly disrupt business operations, information security, IT systems, employees, customers, upstream suppliers, and other vital functions.

Analysis and Recommendations

1. Configuration Management Practices

Several standards mention the need for a formal configuration management practice. Manufacturers can follow any of the methods described in the documents below:

- The *Supply Chain Security Assurance* document lists suggested configuration management practices for the provider and the evaluator.

- NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.3) includes configuration management in its list of 21 practices that an organization should consider when creating the list of measures it will employ as part of its information security strategy.

© 2015 National Electrical Manufacturers Association

- FIPS PUB 140-3 (section 4.10) includes configuration management in the life cycle assurance (design, development, and operation) of a cryptographic module. Depending on the security level of the module, it might require additional life cycle assurances, such as automated configuration management.

Recommendation: At minimum, manufacturers should have a formal, documented configuration management process in place that includes the following five distinct disciplines:

- A formal document and plan to guide the configuration management program as part of the security development process;
- Configuration identification that consists of setting and maintaining baselines that define the system or subsystem architecture, components, and any developments at any point in time;
- Configuration control, which includes evaluation of change requests and change proposals and their subsequent approval or disapproval;
- Configuration status accounting, which includes the process of recording and reporting configuration item description and all departures from the baseline during design and production;
- Configuration verification and audit, which is an independent review of hardware and software for the purpose of assessing compliance with established performance requirements, appropriate standards, and product baselines.

2. In-house and Third-party Quality Assurance Audits

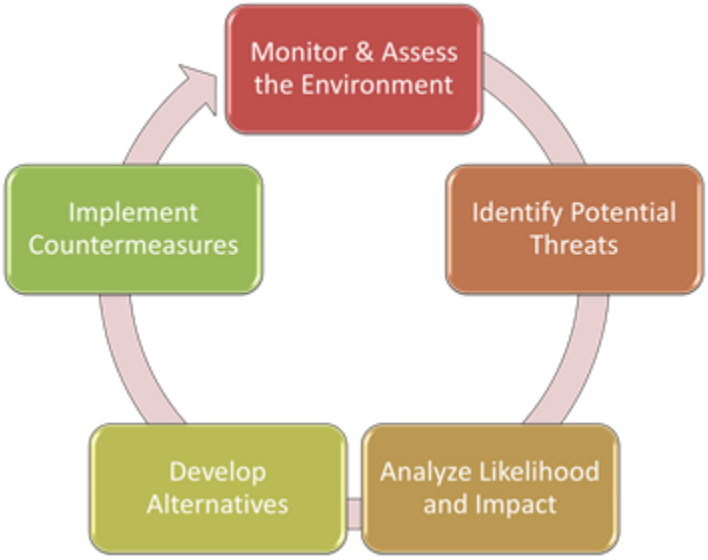
Many security standards, such as NIST SP 800-53 Rev. 4, IEC 62443, ISO/IEC 15408, and the ISO 27000 series, are available to add further levels of assurance and rigor into the product development, production, and IT environments. Some manufacturers might consider third-party testing as an additional level of assurance.

Recommendations: The standards described above specify management systems that are intended to bring information security under explicit management control. Manufacturers should adopt a methodology and engage a third party to audit that methodology at agreed-upon periodic intervals.

3. Risk Management

According to the *US Department of Homeland Security (DHS) Risk Lexicon,* 2010 Edition, “risk management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.” The implication of this definition for manufacturers is that they have a method in place to deal with ongoing threats to their devices. This leads to the standard wheel diagram for risk management:

© 2015 National Electrical Manufacturers Association



This diagram is not intended to illustrate the definitive method for designing a company's risk management system but to label the kind of considerations it should take into account. Additional considerations include:

- Internal versus external risks
- Communicating about risks and impacts to:
    - Upstream providers
    - Downstream asset owners

Many standards mention risk management approaches. Manufacturers might choose to follow (or evaluate for operational risk that would impact their security development life cycle and supply chain implications) the techniques described in any of the documents listed below.

- NIST SP 800-30 Rev.1 is a risk management guide for Information Technology Systems.
- ISO 31000 is a family of standards that provides principles and generic guidelines on risk management.
- The NIST Cybersecurity Framework provides a common language for understanding, managing, and expressing cybersecurity risk, both internally and externally.

4. In-house and Third-party Testing

There are several published standards that speak to the need for testing as a means to evaluate a particular system's compliance with its specified security requirements. Manufacturers might choose to implement the testing procedures described in these documents:

- NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.6) describes multiple types of testing (manual review,

© 2015 National Electrical Manufacturers Association

fuzz testing, static and dynamic analysis, penetration) that should be done throughout the system development life cycle.

- FIPS PUB 140-3 (section 4.9) specifies the testing requirements of the security functionality implemented in the cryptographic module.

Recommendations: At minimum, manufacturers should test their products or devices in order to validate compliance with the security requirements and necessities of the regulated environment. Depending on the environment, third-party testing might be required.

5. Incident, or Event, Management Plan

Recommendations: Manufacturers should develop a plan to manage incidents or 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 maintain tight communication channels with consumers/customers and upstream suppliers in order to keep abreast of any vulnerability issues and steps to mitigate the issues.

By extension, manufacturers should practice responsible disclosure. ISO/IEC 30111, *Information technology—Security techniques—Vulnerability handling processes* (sections 6-8) and ISO/IEC 29147, *Information technology—Security techniques—Vulnerability disclosure* (sections 6-9) are two standards that a manufacturer might choose to follow.

DECOMMISSIONING/REVOCATION

This section focuses on decommissioning and revocation processes to prevent compromised or obsolete devices from being used to penetrate active security networks. This can be especially important for manufacturers who deal in used or factory-refurbished equipment. When such a device is pulled from an active network, how does the manufacturer or asset owner dispose of it? For refurbished equipment, how is the privacy and security information wiped from the device to the satisfaction of regulators and customers? In some instances, the type of data that passed through the device might require that the device be destroyed or disabled.

Identification of Threats

1. Protection/Disposal of Legacy Data

Legacy data present on any type of storage device should be protected in a secure format or properly deleted or disposed of in order to prevent its extraction or reuse. This data might reside somewhere on an asset owner network or some form of cloud storage in addition to the device. Data remanence should be taken into consideration, as this is the residual representation of digital data that can exist even after attempts have been made to erase it.

2. Physical Disposition/Destruction of Device

With the physical destruction of a storage device, the primary goal is to render the disk physically inoperable or, at minimum, leave the platters severely fragmented.

© 2015 National Electrical Manufacturers Association

3. Communication pathways

   A device pulled from an active network will have used some type of communication pathway (e.g., Ethernet, wireless, Bluetooth, internet). “Pivoting” refers to a method used by penetration testers that uses a compromised or obsolete system (whose media access control or MAC address is known to the network) to attack other systems on the network. Using the compromised system, an attacker has an improved aspect of remaining undetected and can leave less of a fingerprint.

Analysis and Recommendations

1. Protection/Disposal of Legacy Data

   Recommendations: At minimum, manufacturers should use purging/sanitization techniques to remove sensitive data from a system or storage device with the intent that the purged data cannot be reconstructed by any known technique. For those environments with stronger security requirements, manufacturers should consider using some type of self-encrypting hard drive that would render all data on the hard drive unreadable via a cryptographic erase of the data encryption key.

   The following standards address sanitization techniques that manufacturers might choose to follow.

   - NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization* (sections 3-5).
   - Department of Defense 5220.22M, *National Industrial Security Program Operating Manual* (chapter 5, section 7) addresses disposition and retention of classified information and materials.

2. Physical Destruction/Disposition of a Device

   Recommendations: Manufacturers should use any of the following options to physically destroy a hard disk drive: shredding the circuit boards into a size smaller than .5 inches, thereby destroying the flash memory in the process; drilling 6-10 holes with a sheet metal or masonry bit throughout the disk platters; heating the magnetic media to a particular temperature in order to deform the shape so that the data is completely removed.

   Physical destruction/disposition of a device is addressed in the following standards, which manufacturers might choose to follow.

   - NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization* (sections 3-5) is a guideline for media sanitization that includes destruction/disposal procedures.
   - Department of Defense 5220.22M, *National Industrial Security Program Operating Manual* (chapter 5, section 7) addresses the disposition and retention of classified information and materials.

3. Communication Pathways

   Recommendations: Manufacturers should remove/decommission the systems appropriately, rather than leaving them connected to a network. By performing penetration tests, manufacturers

© 2015 National Electrical Manufacturers Association

can actually replicate the types of actions a malicious attacker would take, providing a more accurate representation of a particular system's security posture. Penetration testing is the process of attempting to gain access to resources without knowledge of user-names, passwords, and other normal means of access. The primary factor that separates a penetration tester from an attacker is permission.

The wide variety of tools used in penetration testing consists of two main types: reconnaissance, or vulnerability, testing tools and exploitation tools. Several O/S distribution systems (popular examples include Kali Linux, Pentoo, and WHAX), geared toward penetration testing, are available.

© 2015 National Electrical Manufacturers Association

Appendix A
REFERENCE DOCUMENTS

CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Reference Architecture* (November 2012)

GridWise Interoperability Context-Setting Framework (March 2008)

Open Trusted Technology Provider™ Standard (O-TTPS), version 1.0 (April 2013)

SAFECode *Software Integrity Controls* document (June 2010)

NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (October 2012)

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015)—may replace some NIST IR7622 references in the future

IEC 62443-1-1:2009, *Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models* (July 2009)

ISO 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements* (September 2013)

ISO 27002:2013, *Information technology—Security techniques—Code of practice for information security controls* (September 2013)

SAE International Standards Organization, SA AS553, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition* (January 2013)

NIST SP.800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013)

IEC/TR 80002-1:2009, *Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software* (September 2009)

FIPS PUB 140-3, *Security requirements for cryptographic modules* (Draft, September 2009)

NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments* (September 2012)

NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010)

NIST SP 800-39, *Managing Information Security Risk* (March 2011)

Certificate Authority Security Council Code Signing Whitepaper

Supply Chain Security Assurance document (August 2013)

© 2015 National Electrical Manufacturers Association

ISO 27799:2008, *Health informatics—Information security management in health using ISO/IEC 27002* (July 2008)

ISO/IEC 15408-1:2009, *Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model* (December 2009)

ISO 31000:2009, *Risk management—Principles and guidelines* (December 2009)

ISO 30111:2013, *Information technology—Security techniques—Vulnerability handling processes* (October 2013)

ISO 29147:2014, *Information technology—Security techniques—Vulnerability disclosure* (February 2014)

NIST *Cybersecurity Framework*, version 1.0 (February 2014)

NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* (November 2007)

IEC/TS 62351-1:2007, *Power systems management and associated information exchange—Data and communications security—Part 1: Communication network and system security—Introduction to security issues* (May 2007)

IEC/TS 62351-3:2007, *Power systems management and associated information exchange—Data and communications security—Part 3: Communication network and systems security profiles including TCP/IP* (June 2007)

IEC/TS 62351-4:2007, *Power systems management and associated information exchange—Data and communications security—Part 4: Profiles including MMS* (June 2007)

IEC/TS 62351-5:2013, *Power systems management and associated information exchange—Data and communications security—Part 5: Security for IEC 60870-5 and derivatives* (April 2013)

IEC/TS 62351-6:2007, *Power systems management and associated information exchange—Data and communications security—Part 6: Security for IEC 61850* (June 2007)

IEC/TS 62351-7:2010, *Power systems management and associated information exchange—Data and communications security—Part 7: Network and system management (NSM) data object models* (July 2010)

IEEE Std. 1619-2007, *IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices* (April 2008)

ISO/IEC 27033-1:2009, *Information technology—Security techniques—Network security—Part 1: Overview and concepts* (December 2009)

ISO/IEC 27033-2:2012, *Information technology—Security techniques—Network security—Part 2: Guidelines for the design and implementation of network security* (July 2012)

ISO/IEC 27033-3:2010, *Information technology—Security techniques—Network security—Part 3: Reference networking scenarios—Threats, design techniques and control issues* (Dec 2010)

ISO/IEC 27033-4:2014, *Information technology—Security techniques—Network security—Part 4: Securing communications between networks using security gateways* (February 2014)

© 2015 National Electrical Manufacturers Association

ISO/IEC 27033-5:2013, *Information technology—Security techniques—Network security—Part 5: Securing communications across networks using Virtual Private Networks (VPNs)* (July 2013)

ISO/IEC 27036-1:2014, *Information technology—Security techniques—Information security for supplier relationships—Part 1: Overview and concepts* (March 2014)

ISO/IEC 27036-2:2014, *Information technology—Security techniques—Information security for supplier relationships—Part 2: Requirements* (August 2014)

ISO/IEC 27036-3:2013, *Information technology—Security techniques—Information security for supplier relationships—Part 3: Guidelines for information and communication technology supply chain security* (November 2013)

Energy Sector Control Systems Working Group (ESCSWG) *Cybersecurity Procurement Language for Energy Delivery Systems* (April 2014)

NIST SP 800-88, *Guideline for Media Sanitization Techniques* (September 2006)

Department of Defense (DoD) 5220.22M, *National Industrial Security Program Operating Manual* (February 2006)

Department of Homeland Security (DHS), *DHS Risk Lexicon* (September 2010)

© 2015 National Electrical Manufacturers Association

Appendix B
REFERENCE ARCHITECTURES

Two reference architectures are applicable for the supply chain best practices described in the NEMA guideline document.

The first is the Smart Grid Architecture Model (SGAM) developed by the CEN-CENELEC-ETSI Smart Grid Coordination Group. The SGAM framework and its methodology are intended to present the design of smart grid use cases with an architectural approach allowing for a representation of interoperability viewpoints in a technology neutral manner, both for current implementation of the electrical grid and future implementations of the smart grid.

The SGAM framework consists of five layers representing business objectives and processes, functions, information exchange and models, communication protocols, and components. These layers represent an abstract and condensed version of the interoperability dimensions. Each layer covers the smart grid plane, which is spanned by electrical domains and information management zones. The intention of this model is to represent on which zones of information management interactions between domains take place. It allows presentation of the current state of implementations in the electrical grid, and also depicts the evolution to future smart grid scenarios by supporting the principles of universality, localization, consistency, flexibility, and interoperability.

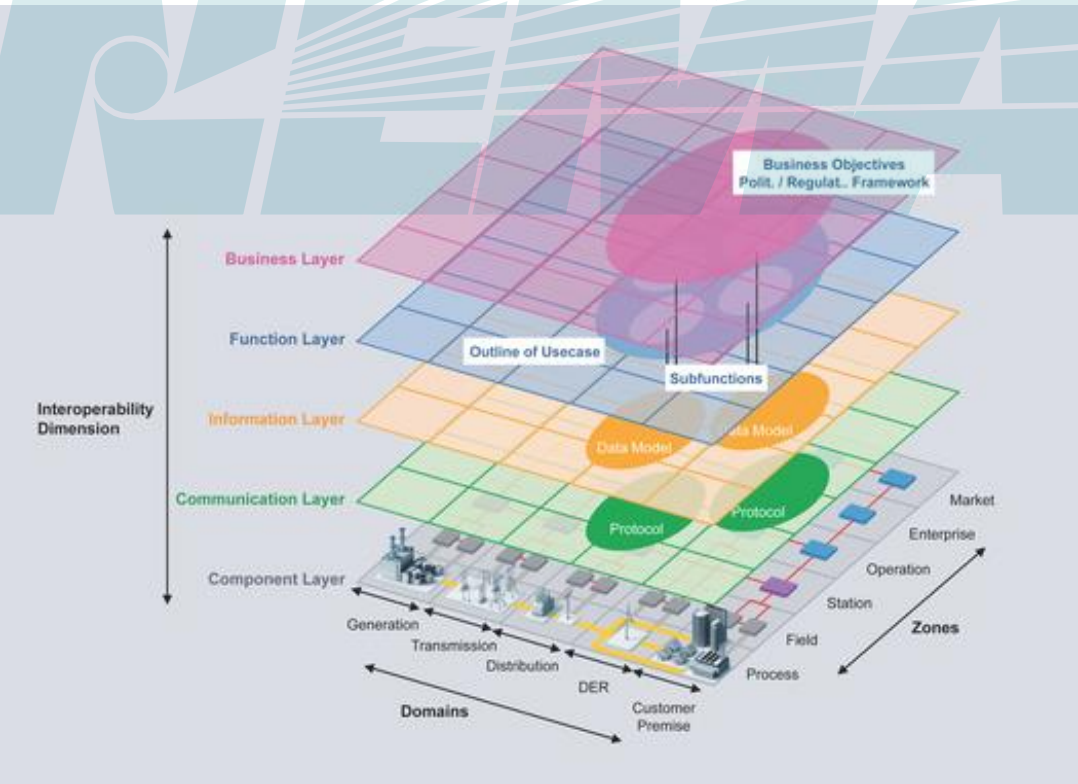


Figure 1
SGAM Framework

© 2015 National Electrical Manufacturers Association

The business layer represents the business view on the information exchange related to smart grids.

The function layer describes functions and services, including their relationships, from an architectural viewpoint. The functions are represented independent from actors and physical implementations in applications, systems, and components. The functions are derived by extracting the use case functionality, which is independent from actors.

The information layer describes the information that is being used and exchanged between functions, services, and components. It contains information objects and the underlying canonical data models. These information objects and canonical data models represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means.

The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service, and related information objects or data models.

The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system actors, applications, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired/wireless communication connections, routers, switches, servers), and any kind of computers.

In general, power system management distinguishes between electrical process and information management viewpoints. These viewpoints can be partitioned into the physical domains of the electrical energy conversion chain and the hierarchical zones (or levels) for the management of the electrical process. Applying this concept allows the foundation of the *Smart Grid Plane* (see Figure 1). The smart grid plane enables the representation on which levels (hierarchical zones) of power system management interactions between domains take place. The domains and their descriptions are listed in Table 1. The zones and their descriptions are listed in Table 2.

Table 1
SGAM Domains

Domains	**Description**
Bulk Generation	Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, offshore wind farms, large-scale solar power plant typically connected to the transmission system
Transmission	Representing the infrastructure and organization that transport electricity over long distances
Distribution	Representing the infrastructure and organization that distribute electricity to customers
DER	Representing distributed electrical resources directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW to 10,000 kW)
Customer Premises	Hosting end users and producers of electricity. The premises include industrial, commercial, and home facilities.

© 2015 National Electrical Manufacturers Association

Table 2
SGAM Zones

Zones	Description
Process	Including the physical, chemical, or spatial transformations of energy (electricity, solar, heat, water, wind) and the physical equipment directly involved (e.g., generators, transformers, circuit breakers, overhead lines, cables, electrical loads—any kind of sensors and actuators that are part or directly connected to the process)
Field	Including equipment to protect, control, and monitor the process of the power system, e.g., protection relays, bay controller—any kind of intelligent electronic devices that acquire and use process data from the power system
Station	Representing the areal aggregation level for field level, e.g., for data concentration, functional aggregation, substation automation, local SCADA systems
Operation	Hosting power system control operation in the respective domain, e.g., distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems
Enterprise	Includes commercial and organizational processes, services, and infrastructures for enterprises (utilities, service providers, energy traders), e.g., asset management, logistics, work force management, staff training, customer relation management, billing and procurement
Market	Reflecting the market operations possible along the energy conversion chain, e.g., energy trading, mass market, retail market

© 2015 National Electrical Manufacturers Association

The second reference architecture is the GridWise Architecture Council (GWAC) Interoperability Framework.

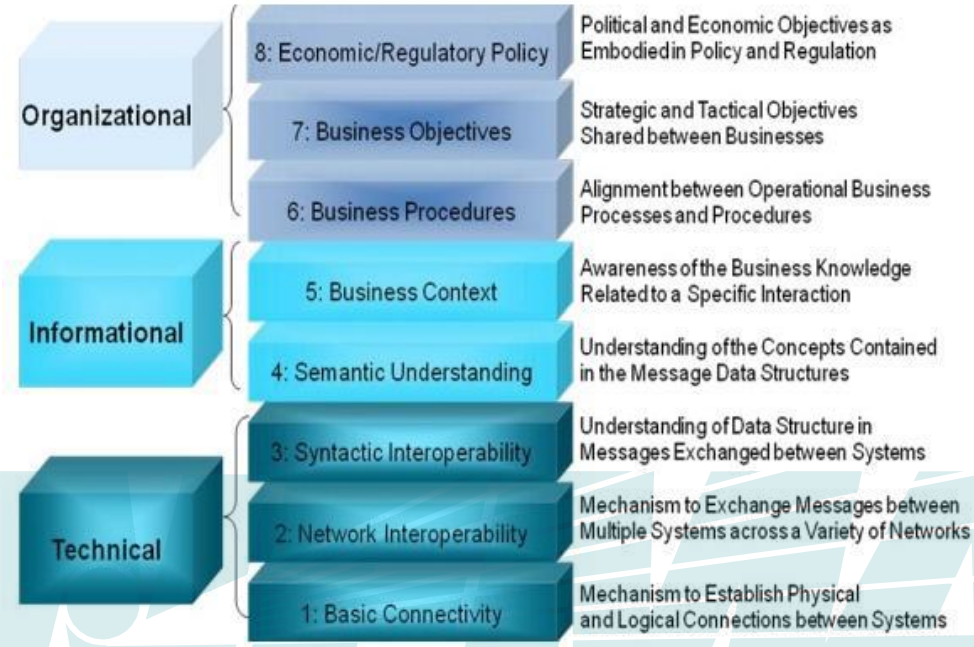


Figure 2
Interoperability Layered Categories Defined by GWAC

The GridWise interoperability context-setting framework identifies eight interoperability categories that are relevant to the mission of systems integration and interoperation in the electrical end-use, generation, transmission, and distribution industries. The major aspects for discussing interoperability fall into the following categories: technical, informational, and organizational. The organizational categories emphasize the pragmatic aspects of interoperation. They represent the policy and business drivers for interactions. The informational categories emphasize the semantic aspects of interoperation. They focus on what information is being exchanged and its meaning. The technical categories emphasize the syntax or format of the information. They focus on how information is represented within a message exchange and on the communications medium.

Basic Connectivity focuses on the digital exchange of data between two systems and the establishment of a reliable communications path. This is achieved by agreeing to conform to specifications describing the data transmission medium, the associated low-level data encoding, and the transmission rules for accessing the medium. Network Interoperability pertains to agreement on how to address the issues arising from transporting information between interacting parties across multiple communication networks. Syntactic Interoperability refers to agreement on the rules governing the format and structure for encoding information exchanged between transacting parties.

© 2015 National Electrical Manufacturers Association

Semantic Understanding refers to rules governing the definition of things, concepts, and their relationship to each other. Together, they make up an informational “model” of how the world works. A model is usually “domain-specific”, e.g., pertaining to one area of expertise. The idea of establishing a business context refers to restricting and refining the aspects of an information model relevant to the specific business process in question.

Effective information interoperability between business organizations requires that the involved organizations have compatible processes and procedures across their interface boundaries. In addition, it’s required that the strategic and tactical objectives of the business organizations be complementary and compatible. Business organizations require that the political and regulatory policies that govern commerce provide the proper environment, incentives, or both, to build business relationships with other organizations, some of which might be considered competitors. This includes national, state, and local governance.

NOTE—No reference architecture exists for embedded systems that include hardware or affected physical systems in a generic fashion.

© 2015 National Electrical Manufacturers Association