National Electrical Manufacturers Association

NEMA Guideline Document
NEMA CY 70001-2023

Cybersecurity Implementation Guidance for Connected Electrical Infrastructure

Published by:

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

www.nema.org

Executive Summary

This guideline document addresses cybersecurity protection of electrical infrastructure when network connected within the context of a commercial, industrial, or residential building. With an emphasis on safety implications, it describes methods to protect the various systems and products within the infrastructure through best practices, industry standards, or the utilization of compensating controls.

As cybersecurity requirements are appearing in building electrical safety codes, this guide provides a reference point for installers of electrical infrastructure systems and officials and authorities having jurisdiction that inspect for code compliance who are not familiar with cybersecurity compliance aspects.

Contents

Acknowledgments

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

Acuity Brands	Troy Fridley, Tanya Hernandez
Current	Ted Kozenko, Jeremy Yon
Honeywell Building Technologies	Dan Heine
Johnson Controls	Roger Reiswig
Schneider Electric	Mike Pyle, Keith Waters
Siemens Industry	Vincent Baroncini, Adam Chapman, Maria Marks, Joe McCormack
Signify North America Corporation	Tom Stoll

NEMA 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 Cybersecurity Council was composed of the following member companies:

ABB, Inc.—Cary, NC
Acuity Brands, Inc.-—Conyers, GA
Atkore International—Harvey, IL
Canon Medical Systems USA—Tustin, CA
Cerrowire—Hartselle, AL
Current—East Cleveland, OH
Eaton—Cleveland, OH
Encore Wire Corporation—McKinney, TX
GE Healthcare—Waukesha, WI
Hitachi Energy USA Inc.—Raleigh, NC
Honeywell—Northford, CT
Hubbell Inc.—Shelton, CT
Infinitum Electric—Round Rock, TX
Itron Inc—Liberty Lake, WA
Johnson Controls—Westminster, MA
Keltron Corporation—Waltham, MA
Leviton Manufacturing—Melville, NY
Lutron Electronics Company—Coopersburg, PA
Nidec Motor Corporation—St. Louis, MO
Panduit Corporation—Tinley Park, IL
Philips—Cambridge, MA
Phoenix Contact—Middletown, PA
Resideo Technologies—Golden Valley, MN
Rockwell Automation—Milwaukee, WI
S&C Electric—Chicago, IL
Schneider Electric—Boston, MA
Siemens—Alpharetta, GA
Siemens Healthineers—Malvern, PA
Signify North America Corporation—Bridgewater, NJ
Southwire Company—Carrollton, GA
Telecor Inc—Mississauga, ON
Triacta/Quadlogic—Divisions of Metergy Solutions—Carleton Place, ON

1 Scope

This guideline document addresses cybersecurity protection of electrical infrastructure when network connected within the context of a commercial, industrial, or residential building. It does not address cloud-based or other systems outside the scope of the building infrastructure. It describes methods to protect the various systems and products within the infrastructure through best practices, industry standards, or the utilization of compensating controls. An assessment of the network connected system and its components is discussed along with the various solutions to providing cybersecurity across multiple security levels. Emphasis will be placed on network connected electrical infrastructure that has safety implications.

2 Document Audience

The audience for this document is installers of electrical infrastructure systems and officials and authorities having jurisdiction that inspect for code compliance. This guide provides a reference point for those personnel who are not familiar with the cybersecurity compliance aspects.

3 Definitions

Key terms used in the context of this document:

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.

Allow Listing: A process used to identify a list of discrete entities, such as hosts or applications that are allowed to be present or active on a system or network according to a well-defined baseline.

Asymmetric Keys: Generated by a cryptography algorithm that results in a public/private key pair for encryption and decryption.

Authentication: The process of verifying who a user or other entity is.

Authorization: The process of verifying what a user or other entity has access to.

Building Access Control: The process of selectively restricting access to a building or to a specific space within it.

Compensating Controls: A mechanism that is employed to satisfy the requirement to meet a target security level when using products with a lower security level capability in a system (also known as "compensating countermeasures").

Critical Operations Power Systems: Critical operations power systems as defined in Article 708 of NFPA 70 *National Electrical Code*® (NEC) are those systems so classed by municipal, state, federal, or other codes, by any governmental agency having jurisdiction or by facility engineering documentation establishing the necessity for such a system. These systems include but are not limited to power systems, HVAC, fire alarm, security, communications, and signaling for designated critical operations areas.

Cyber Hygiene: A reference to the practices and steps for users of computers and other devices to take to maintain system health and improve online security.

Cybersecurity Security Levels: Technical requirements for systems and products as defined in the IEC 62443 series of standards that indicate the resistance against different classes of attackers.

- **SL1—Security Level 1:** Protection against unintentional or accidental misuse.
- **SL2—Security Level 2:** Protection against intentional misuse by simple means with few resources, general skills, and low motivation.
- **SL3—Security Level 3:** Protection against intentional misuse by sophisticated means with moderate resources.