NEMA Industrial Automation Control Products and Systems Section

Statement of Cybersecurity Principles

January 2014

The National Electrical Manufacturers Association (NEMA) coordinates the development of shared technical standards and joint policy positions by more than 400 manufacturers of electrical equipment in the United States.

NEMA’s Industrial Automation Control Products and Systems Section represents manufacturers of mechanical, electromechanical, and solid-state devices, components, and controls used in the industrial sector. The Section speaks with one voice on cybersecurity policy matters.

Background

Industrial Control System (ICS) products are computer-based systems that make use of specialized software and embedded devices that control and automate processes and machines. They are essential components of critical infrastructure, including but not limited to critical manufacturing facilities, oil refineries, chemical facilities, power plants, electrical grids, pipelines, rail networks, and water treatment systems.

Ever since ICS products entered widespread use forty years ago, customers have demanded that they be safe, reliable, long-lasting, low-maintenance, and affordable.

Over the last twenty years, developments in open-standard IP-based communication protocols, supplier interoperability, off-the-shelf computer-based products, and connecting control systems to the Internet have heightened the risk of malicious actors accessing ICS products and manipulating the equipment they control.

Governments recently began responding to the threat of malicious cyberattack with policies and guidelines directed at owners and operators of critical infrastructure. Owners, operators, systems integrators, and equipment suppliers are focusing considerable attention on the security-related attributes of ICS products, systems integration, asset management, and enterprise connectivity. The community of stakeholders is investing in the development of relevant cybersecurity standards applicable to ICS products, systems integration, and the operation of automation environments.
Statement

In the competitive market of ICS products, vendors are acting on the increased customer need for product attributes that enhance security. Still, the ways that users configure and manage their facilities impact security at least as much as the attributes of the embedded ICS products do. Managing the risk of malicious access to ICS products is the shared responsibility of end-users, systems integrators, and ICS product vendors.

It is reasonable to expect ICS product vendors to do the following things to help ensure that the free market will deliver continuing improvements in the security of ICS products.

a. Use reasonable efforts to investigate, confirm, resolve, and disclose security vulnerabilities in a vendor’s ICS products once the security vulnerability is brought to the attention of the vendor.

b. Where a security vulnerability can reasonably be addressed with a software/firmware update, or other remediation, make the update/information easily available to customers.

c. When disclosing a security vulnerability, provide practical and operational advice to help owners and operators reduce the risk of harm.

d. Provide clear documentation of the security-relevant attributes of the vendor’s ICS products.

e. Provide clear documentation regarding the international security standard(s), certification(s), or approval(s) to which the vendor’s ICS products conform, as well as the methods used to assess the conformity. The leading security standards that ICS product vendors are using to guide development of their product families include ISA/IEC 62443.

Given the shared responsibility of multiple parties, security-related expectations directed at ICS product vendors should recognize the following realities.

a. ICS products that were designed, sold, and installed many years ago remain in use in countless infrastructure and manufacturing processes both nationally and internationally.

b. Many old ICS products that are still in use today cannot easily support security-related software/firmware updates.

c. The ICS product vendor does not always perform the installation or the system integration and usually does not own/operate the facility. The product vendor may have the capability but not the authority to influence the security posture of the owner’s/operator’s automation environment.

d. ICS product vendors are not necessarily apprised of all of the places where their products are in use today or of their current state.

e. Effective control system cybersecurity involves more than just secure product attributes. It must also include secure installation, secure operation (including management,
training, policies, and procedures), and secure maintenance of the ICS products and the environments in which they are used.

f. Many ICS systems are connected to a business enterprise system, a remote network, or both, thereby increasing the risk to the automation environment and business systems.

For more information, please visit [www.nema.org/1is](http://www.nema.org/1is).

Contact: Jim Creevy, jim.creevy@nema.org or 703.841.3265.