National Electrical Manufacturers Association

Position Statement on Cyber Security

Introduction

The National Electrical Manufacturers Association (NEMA) is a trade association through which the electro-industry develops and promotes positions on standards and government regulations, and members acquire information on industry and market economics. In supporting the NEMA mission as it relates to Cyber Security, our objective in this position statement is to promote the competitiveness of the U.S. electrical product industry through the development of standards and advocacy of policy in federal and state legislatures and executive and regulatory agencies.

NEMA's interest in Cyber Security is driven in part by the seven major findings described by the Department of Energy in their *Metrics for Measuring Progress Toward the Implementation of the Smart Grid* publication:

- Enable active participation by consumers
- Accommodate all generation and storage options
- Enable new products, services, and markets
- Provide power quality for the range of needs in a digital economy
- Optimize asset utilization and operating efficiency
- Anticipate and responds to system disturbances in a self-healing manner
- Operate resiliently against physical and cyber attack and natural disasters

In applying these findings, the objectives for electrical manufacturers for Cyber Security in Smart Grid are twofold: the risk to business operations from security breaches; and the risk to product development and marketing as the federal government adopts preventive measures.

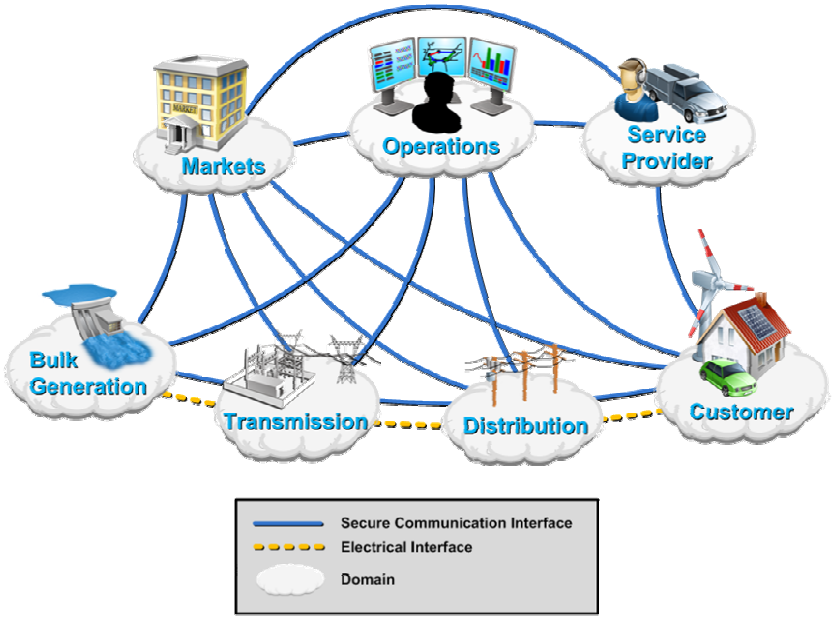
A breach in Cyber Security would have a couple of immediate effects: first, utility service interruptions (including their potential disruptions to business, commerce, and other activities); and second, the unavoidable scramble to patch the breach. This could involve countless hours of research and development staff time, contractors and consultants, etc. which would be a considerable financial burden on the utilities and manufacturers alike. The implementation of those patches would involve potential changes to the manufacturing process, deployment of patches to the installed base, product recalls, rebates and many other expensive options, not to mention the potential for lawsuits, both valid and frivolous, based on the potential outages described above.

An additional interest of the manufacturers is standardizing on common approaches to cyber security across utility areas of control as well as state boundaries. It is critical to invest the time and resources upfront to select the optimal architecture, minimize risks, and attain a reasonable balance between costs and security. Additionally, there exists a need for states to work together in order to provide utilities with a uniform security implementation approach. If public utility commissions do not lead with a common approach, then it will be very difficult for utility companies, manufacturers, the National Institute of Standards and Technology (NIST), and Standards Development Organizations (SDOs) to coordinate their security standards development efforts increasing the level of difficulty for manufacturers to provide interoperable solutions. The corresponding drop in interoperability could also lead to a lower quality of service to electricity customers.

Definitions

In order to foster an understanding of this Cyber Security discussion, the following terms will be used in the context as described:

Domain – A domain is an area of operational responsibility within the Smart Grid architecture. For the purpose of this document, the domain considerations will follow those of the Conceptual Model of the Smart Grid as crafted by NIST, where each of the "clouds" in the diagram represents a grid *domain*:



Layer – A layer is the application of a security measure in the Cyber Security architecture. For example, the first layer of security is the physical connection to a device in the Smart Grid. Another layer could be a log-in server to authenticate any user that is trying to issue commands to Smart Grid devices. Encryption is yet another layer, and so on. Having a *layered security architecture* implies that multiple security measures could be applied to any connection to the Smart Grid.

Segment – The electric grid is a collection of contiguous, interconnected physical devices from the point where electricity is generated to the point of use. A *segment* of the grid is any set of elements for which the electricity supply can be controlled as a unit. This may be a single building such as an office high-rise, a group of related buildings such as an educational or industrial campus, or a collection of buildings or homes such as a military base or a residential neighborhood.

Manufacturers' Positions

The position of the NEMA member companies on Cyber Security is focused on three major areas of concern: Standards Development, and Legislative and Regulatory Actions.

Standards Development

Hardware. Hardware-based standards for Cyber Security must be designed appropriately for the operating environment including the method of deployment, administration, and any operational considerations (such as weather for outdoor devices). They must also integrate with widely-accepted management systems and practices associated with the electrical industry.
Software. As with hardware-based standards, software solutions in Cyber Security need to be compatible with widely-accepted management systems and practices. Both interoperability and sustainability need to be factored into the features of any standards developed or adopted for software systems.
Transport. Limitations of the communications associated with the electric grid need to be part of the design criteria for Cyber Security standards. Unlike the Internet, the electric grid was not designed as a communications network and therefore cannot support heavy message loads; long-haul distances with limited access to bandwidth will be the norm in many cases.
Operational Sustainability. For the development of any standard in the Cyber Security arena, the concept of how that standard will be supported after deployment needs to be considered. In a distributed operating environment with literally millions of nodes (such as the electric grid), manual maintenance is not a viable option. The application of a security standard as a component of a larger security architecture needs to permit remote administration.

Legislative Actions

Cyber Security Design. The NEMA member companies agree that first and foremost, security must be part of the design consideration for any smart grid component (and its corresponding interactions with other grid elements) from its inception. At the same time, designing and building the entire grid to the highest security standards would simply make it too costly to undertake any form of national modernization project – Cyber Security measures should therefore be deployed judiciously, taking into account segmentation and layering.
Incentives. The fast path to widespread adoption of Cyber Security measures will naturally include incentives. Any legislation dealing with the Smart Grid, Cyber Security, and energy policy in general needs to target incentives for utilities and manufacturers in areas like adoption of best practices and implementation of Cyber Security measures. Given its importance to the process, research and development should be specifically targeted for incentive programs.
Funding Standardization. Building on the success of the NIST programs for standardization in the Smart Grid, legislative actions should continue to provide funding for government agencies, non-government organizations, standards development organizations (SDOs), and individual

companies involved in the development, promulgation, and conformity assessment of standards and technologies for Cyber Security in the Smart Grid.

Legislative Restraint. With the variety of Cyber Security technologies that are now available, it would be easy to become over prescriptive when developing legislation associated with Cyber Security. Laws should be crafted to reflect national priorities and objectives for Cyber Security programs but not constrain innovations by focusing on individual solutions or technologies.

Regulatory Actions

Applying Standards. Combining the intent of the legislative recommendations, regulatory actions should focus on applying the standards that are endorsed by governmental agencies (such as the Department of Homeland Security and the National Institute of Standards and Technology) to achieve the Cyber Security objectives in legislative policy. Rulemaking should be aimed at enabling interoperability through the application of standards and whenever possible, should examine the issues associated with backward compatibility.

Implementation. Regulatory agencies must carefully weigh issues associated with voluntary versus mandatory implementation of a security measure. They should consider the life expectancy of the current installed base of equipment and technology, and consider graduated schedules for adoption when appropriate in order to avoid stranding utility company investments before their useful life has been expended. Rulemaking should be geared to help utilities move faster to replace legacy systems that do not meet emerging Smart Grid standards. Utility companies should be scrutinized for filings that include statements like “where technically or economically feasible” to avoid a business-as-usual posture for the adoption of Smart Grid technologies.

Segmentation. In order to control the cost of deployment, regulators need to consider the overall security architecture in their rulemaking decisions. As with the electric grid itself, the ability to isolate security issues and insulate core grid functionality from their effects is equally important as the strength of the security measure.

Layering. As with segmentation, the aspect of security layering needs to be considered during rulemaking. Individual security measures should not be considered in a vacuum, but rather in the context of how they contribute to the overall security architecture of the system. It would be important to define rules and guidelines for the levels of layered security required as a function of the criticality of a device, its functions, the impact on the surrounding segments of the grid, etc.