Compatibility with NIST's emerging smart grid framework for standards and protocols

Progress Energy continues to be an active participant in all relevant industry groups (e.g. EEI, NIST and GridWise) and standards development organizations (e.g. NERC, IEEE). This conscious business decision aims to ensure awareness and positive influence of the standards and requirements. Standards are a significant concern for Progress Energy because of our strong commitment to providing reliable bulk electric power. Our proactive involvement has provided early warning of changes that need to be accounted for in relevant solutions. For example, the NERC CIP project team performed an analysis of FERC Order 706 in Jan 2008 and immediately worked to address the direction of the forthcoming NERC CIP standards in advance of CIP Draft 3. Also, Progress Energy began leveraging drafts of the DHS Procurement Language document and ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems Standard as they were being developed.

Progress Energy has demonstrated a strong commitment to the development of the NIST Interim Roadmap for the Smart Grid by participating in all of the formal workshops, reviewing and providing input on the development of roadmap articles, and participation in the Cyber Security Coordination Task Group. Our direct involvement has translated into Distribution System Demand Response project architecture updates through regular engagement of project team architects and directly based on the material from the NIST Roadmap initiative. The information and standards from the NIST Roadmap initiative are already being used in design, planning and requirements development for upcoming Smart Grid initiatives like commercial and targeted AMI. Progress Energy requires compatibility with NERC CIP 002-009, ANSI C12.19 DNP3, IEC 61850 and IEC 61968 for all new devices, systems and tools.

1.5.2 Cyber Security

Progress Energy's fundamental approach to cyber security leverages a
including the principles Cyber security threats continue to increase in number, complexity and level of impact. At the same time, business needs are driving requirements for increasing access and interoperability across enterprise applications, process computing environments, enterprise networks, and the Internet.

Progress Energy's corporate strategy embraces and integrates cyber security risk management methodologies and philosophy in our processes, ways of doing business, initiatives and in maintaining regulatory compliance.

Cyber security risks

Rather than attempting to make a defined architecture secure, Progress Energy chooses to architect cyber security into the solution beginning at the concept stage. This ensures that major architectural decisions are influenced by the requirement to be secure and resilient. As part of the plan, ongoing cyber security evaluations are to be performed during the design and procurement, installation and commissioning, and the ongoing maintenance and support phases of the project. The strategies used at each project phase include these security-related activities:

-
-
-
-

An important consideration in developing a cyber security strategy is to continually update and maintain the security framework as technology and standards evolve. Specific areas include:

- Network Intrusion Detection/Prevention and Monitoring –affects the confidentiality, integrity and availability of information and control components for the grid.
- Vulnerability Management – identification and verification of risk remediation is integrated into business processes and procedures.
- Key Management and Cryptography – procedures and solutions enabling cryptographic mechanisms employed for security, accountability, non-repudiation and data integrity.
- Cyber Security Incident Response – provide emergency incident response procedures for any newly discovered or derived attack scenarios.
- Customer Privacy – ability to secure data and components that may not be under the full control of the utility.
- Operational Security – scalable and tightly integrated with business and utility operations.
- Natural Disasters – tactics to manage security risks after natural disasters such as fire, flood or hurricanes.
- Application Vulnerabilities – minimize the risk to the confidentiality, availability and integrity of the Smart Grid data through the Software Development Lifecycle Methodology (SDLM).

Cyber Security Criteria used for vendor and device selection

Vendor and device selection is a critical part of the process to ensure secure, reliable solutions. During the Request for Information and Request for Proposal (RFI/RFP) processes we evaluate respondents using a comprehensive assessment process to produce consistent results. This process was amended in 2007 to include new requirements for the selection of all new equipment and systems.

There are multiple industry standards that serve as inputs for the deployment lifecycle such as DHS Cyber Security Procurement Language, the NERC CIP Cyber Security Standards, as well as international standards, such as IEC. Other inputs include legislative and regulatory requirements as well as corporate policies and standards. These requirements are then turned into component functional models and specifications which form a basis of the criteria for making specific product and device selections. Based upon cyber security risk assessments, the selection criteria are prioritized and weighted to provide the best technology and product/device selection. Other non-technical requirements include vendor stability, vendor support, adherence to industry and global standards, and lastly vendor knowledge of legislative/regulatory requirements and controls. In addition to our own training, expertise and experience, we utilize the following sources:

- DHS – Cyber Security Procurement Language for Control Systems
- NERC CIP 002-009
- ISO/IEC 27002 – Information technology — Security techniques — Code of practice for information security management.

- IEEE-1686 – IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

Progress Energy requires all potential RFI respondents to produce executive summaries of any third party testing. Progress Energy plans and conducts technical security assessments using numerous vulnerability assessment tools during proof of concept initiatives and at multiple phases during the design and implementation of solutions.

Progress Energy actively supports the work identified in the NIST-EPRI Interim Roadmap initiative aimed to implement a Testing and Certification Framework. We see this as a vital step toward industry improvements with the solution providers. The Information System Acquisition, Development and Maintenance section of ISO 27002, A Code of Practice for Information Security Management, will be used to ensure the selection processes include appropriate control points and objectives.

Relevant cyber security standards will continue to evolve as new technologies are introduced

Progress Energy utilizes cyber security standards at the security governance and technology components level. Cyber security standards and best practices, such as those propagated by NERC CIP Cyber Security Standards and AMI-SEC form the basis of Progress Energy's business and cyber security policies. Other widely accepted industry standards such as ISO 27002 and the Sarbanes-Oxley (SOX) Act of 2002, are being used to ensure the inclusion of appropriate control objectives and control points in Progress Energy's security governance policies.

Progress Energy has made significant investments in technologies that are used to enforce and maintain its cyber security policies based on relevant standards and leveraging industry best practices. These technology investments give Progress Energy the ability to manage and evolve the cyber security policies development life-cycle, enforce policies at the technology components level, monitor compliance to policies, and report compliance measurements to management.

Progress Energy implements policy decision points and policy enforcement points in a approach to ensure that only authorized services are consumed. Compliance reporting allows Progress Energy management to review overall compliance posture and provide auditors and security professionals with the ability to drill-down into details surrounding particular security compliance events. Progress Energy's approach provides the flexibility to quickly adapt its cyber security policies to changes in regulations, standards and industry practices. It also supports documentation requests by independent, third-party testers.

Regardless of perspective, the Smart Grid project will account for change on multiple levels, including Methodology, Architecture, Software, and Hardware:

- Methodology – Accounts for and expects emerging security standards to enforce security
- Architecture - with inherent adaptability
- Software and Hardware – Selected for scalability, reuse, and orchestration

Also, in addition to the *Initial Smart Grid Interoperability Standards Framework Release 1.0*, the following list of standards and works are being leveraged to provide interoperability and cyber security requirements for our Smart Grid initiatives. These standards and works are utilized by project teams, operational staff and others to ensure interoperability, reliability and security of Smart Grid Solutions:

- DHS Cyber Security Procurement Language for Control Systems provides information and specific examples of procurement language text to assist the control systems community, both owners and integrators, in establishing sufficient control systems security controls within contract relationships to ensure an acceptable level of risk.
- ISO/IEC 17799/27002 – Information technology — Security techniques — Code of practice for information security management.
- IEEE-1686 – IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- IEEE-1613 – Standard Environmental and Testing Requirements for Communications Devices in Electric Power Substations.

Cyber Security standards and best practices will continue to evolve as new technologies are introduced

Progress Energy employs both internal and third party threat assessments to test and validate the security and communication configurations of Smart Grid hardware and software solutions. Third party assessments are performed annually, while high risk items are scrutinized more frequently utilizing numerous COTS vulnerability assessment tools. Assessment results are documented, including the remediation of findings and reported to the highest levels of the company.

Progress Energy is committed to utilizing the ISO 17799/27002 framework in mapping security controls, determining gaps, defining initiatives and in maintaining regulatory compliance. This official corporate strategy and approach allows Progress Energy to continue to focus on the fundamentals in our cyber security programs and solutions.

In addition, strong, proactive involvement in numerous industry associations, regulatory groups and cyber security organizations is another way Progress Energy remains actively involved and knowledgeable in many specialized areas related to cyber security protection. The following items highlight this commitment within our industry:

- National Institute of Standards and Technology (NIST) - Smart Grid Cyber Security Coordination Task Group (CSCTG) – Progress Energy has actively participated in all of the workshops to date and is committed to continue with this initiative through its completion.
- Edison Electric Institute Security Committee – Cyber Security Subcommittee collaboration on various security topics e.g. NERC CIP, Smart Grid, Physical, CFATS, Aurora follow up, other key topics.
- GridWise Architecture Council Interoperability and Cyber Security Workgroup
- National SCADA Test Bed Advisory Team
- South Eastern Reliability Corporation (SERC) Cyber Advisory Group, Critical Infrastructure Protection Committee (CIPC) & Executive Committee
- Energy Sector Control Systems Working Group (ESCSWG) – responsible for the i.e. Roadmap, the Roadmap to Secure Control Systems in the Electric Sector including outreach and awareness of our peers and vendors.
- Florida Reliability Coordinating Council, Inc.
- North American Electric Reliability Corporation (NERC) CIPC