The Growing Need for Cyber Security in Smart Grid Networks

Stan Pietrowicz, Tom Mazzone

**Telcordia Technologies, Inc.
331 Newman Springs Road/NVC 2Z319
Red Bank, NJ 07701**

spietrow@telcordia.com

Keywords: Cyber Security, Field Area Network, Distribution Automation, FAN Network Analyzer, FAN Intrusion Detection System, FAN Visualization

Abstract

With the proliferation of new distributed intelligence, communication networks, and automation controls, particularly in Field Area Networks, utilities must address growing Smart Grid security needs with new approaches and tools. Smart Grid security needs to be built in and layered upfront in the planning stages rather than added during or after-deployment. Smart Grid security requires a top-down planning approach that begins with the update or definition of new Smart Grid security policies and systematically proceeds through the iterative steps of security architecture and system design, followed by threat, risk, and resiliency analysis, and finally security testing before system deployment. Telcordia advocates introducing a structured Smart Grid Technology Introduction Process to ensure that critical requirements for business, power operations, security, IT/OT, procurement, and other needs are addressed in a consistent manner for each Smart Grid project.

FAN situational awareness is a growing need and concern. Telcordia has been helping its Smart Grid clients to fill gaps in FAN security through research, developing FAN Protocol Analysis tools, extending Intrusion Detection Systems into FAN environments and developing FAN Visualization solutions to meet their engineering, operations, and security needs.

1. INTRODUCTION

Largely due to the urgency to spend stimulus funds, many utilities have deployed Smart Grid technologies without taking the time to update their security policies, define a Smart Grid security architecture that supports their Smart Grid vision, or properly plan new security capabilities to mitigate the growing cyber risk inherent in an intelligent and networked Smart Grid. Utilities are being asked to emerge from a “culture of compliance” to a new “culture of cyber responsibility.” Compliance with NERC-CIP does not mean your network is secure – it is a bare minimum requirement for many utilities. The proliferation of networked distributed intelligence, particularly in Field Area Networks (FANs), and a more interconnected Smart Grid introduces the potential for many new security vulnerabilities and business risks that need to be managed. Utilities must address their growing Smart Grid security needs with new approaches and tools.

2. A SMART GRID SECURITY MODEL – BUILDING IN SMART GRID SECURITY

Smart Grid security should be built in and layered upfront in the planning stages rather than added during or after-deployment. Utilities are committing considerable resources to deploy large amounts of Smart Grid technologies, which include field equipment and their supporting operations and IT systems. Of greater consequence, Smart Grid is triggering dramatic changes to utility operations, processes, and support approaches. At a time when a utility’s core business processes are being redefined, there is an opportunity to plan and introduce a new top-down security approach to secure new Smart Grid capabilities and make enhancements to existing programs.

Telcordia recommends using a structured approach to planning Smart Grid Security as illustrated below in Figure 1.

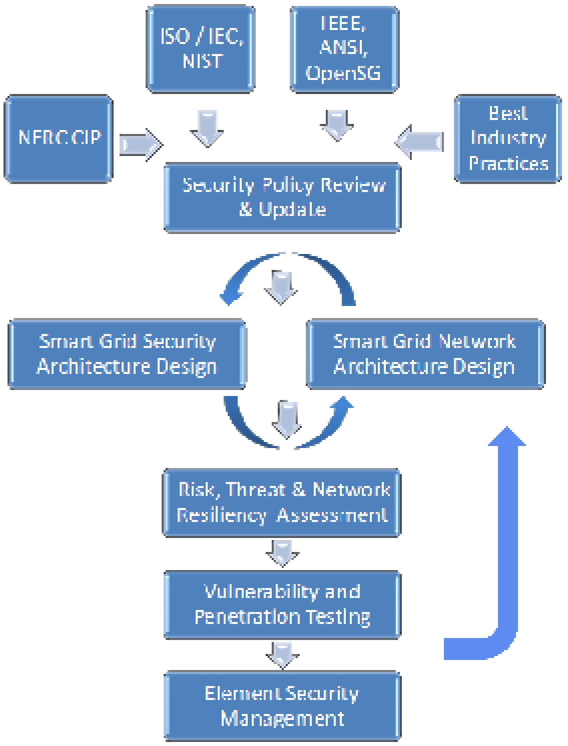
ISO / IEC, NIST
IEEE, ANSI, OpenSG
NERC CIP
Best Industry Practices
Security Policy Review & Update
Smart Grid Security Architecture Design
Smart Grid Network Architecture Design
Risk, Threat & Network Resiliency Assessment
Vulnerability and Penetration Testing
Element Security Management

Figure 1 - Smart Grid Security Model

2.1. Security Policy Review and Update

The first step in planning Smart Grid security should begin with a review and update of the utility's information and network security policies. Information security policies define the guiding principles by which security controls are applied to protect systems, data, and processes. In many cases, the information and network security policies used by utilities are out of date and inadequate. Often written from an Information Technology perspective with many exceptions and carve outs for Operations Technology, the security policies of most utilities did not anticipate the rich controls being made available in Smart Grid field equipment. They did not anticipate the need to securely manage hundreds of thousands or millions of intelligent devices, many of which cannot be physically protected behind a six-sided protective enclosure. They did not anticipate the requirement to better protect the confidentiality and integrity of information in transit. They did not anticipate the compelling business need for information to cross the Operations Technology-Enterprise barrier. They did not anticipate the level of system interconnection within the utility, the new hosting and outsourcing arrangements, and the electronic communications with new external entities that have emerged in the energy value chain. They did not anticipate the new customer web portals and communications infrastructure that each utility will need to interact with its customers. They did not anticipate the difficult and worrisome problem of supply chain cyber threats.

Based on Telcordia's experience, some of the key areas in utility information security policies that require update or new addition are:

- Embedded Hardware Security Policies
- Wireless System Security Policies
- PKI and Crypto Key Management
- Critical Operations Policies
- Security Monitoring and Event Reporting
- Software Release/Patch Policies
- Network Segmentation Policies
- Availability & Network Resiliency
- Risk Assessment Compliance
- Supply Chain Risk Management
- Supplier Access Policies
- Equipment Lifecycle Management

To update and formulate new security policies, utilities should leverage various industry activities and best practices from other related industries. While NERC CIP is often the first cited document for utility security, many of the changes brought about by Smart Grid will probably fall outside its scope. This does not mean that a utility is therefore exempt from securing those assets. Instead, it places the burden on the utility to assume cyber responsibility to understand that threats and risks to its assets and plan a layered defense.

Various Smart Grid security standards and recommendations are currently under development. Some of the more prominent standards development organizations are the International Organization for Standardization (ISO); International Electrotechnical Commission (IEC), National Institute for Standards and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), EnergySec – National Electric Sector Cybersecurity Organization (NESCO) Internet Engineering Task Force (IETF) and the Open Smart Grid Users Group (OpenSG). Utilities can also look across to the Communications Industry, which has been managing complex large scale networks for decades, for best security practices.

While utilities should look to standards to understand their direction and framework, they should not expect to find a "one size fits all," or "drop in place" security recipe. Utilities need to individually assess whether standards and recommendations are applicable to their individual needs, goals and Smart Grid vision.

Security is both a science and art. There are techniques and controls, especially in the area of cryptography that are based on brilliant math. However, the creation of a layered security architecture that balances business needs and risks remains an art. It is often said that each utility's vision of Smart Grid is a little different because of its environment and circumstances. Thereto, its approach to Smart Grid security will need to follow.

One of the most underestimated resources for security planning in utilities is enlightened engineers within the utility itself. Rather than exclusively looking outward for a security solution, whether it be to equipment vendors or standards, utilities need to turn inward and supplement their knowledge with carefully chosen best practices in security. Telcordia has found that with some expert guidance, direction and technical support, utilities can formulate a security architecture that best serves their needs. This is essential; otherwise the result of a poorly executed security planning process is a set of policies that conflict with operational needs or policies that cannot be implemented. Ultimately, security is about mitigating risk to acceptable level that can be afforded by the business.

2.2. Security Architecture Design

Once a firm set of security policies have been adopted across the utility by both IT and OT segments, the next phase in the process is to transform those security policies into a practical and implementable security architecture. The development of a security architecture is best done concurrently or in cooperation with Smart Grid planning and design. Due to the complexity and interaction among networks, systems, and applications, the practice of "bolting" on security after design is completely inadequate, and in some cases, not possible. The business risk of not incorporating security requirements during the planning process is the deployment of a system that in some cases will cost hundreds of millions of dollars and may expose a utility to significant security risks and the threat of exploitation for the next decade, if not result in the premature replacement of the system.

Best industry practices to address difficult security concerns, such as supply chain threat, necessitate not only new practices and procedures, but specific system and design approaches. System and network equipment that was once considered unquestionably trusted may now need to be treated as a potential security risk. A series of checks and balances need to be carefully inserted into the design to ensure that no system or equipment is beyond scrutiny.

Some of the challenges that Telcordia can help utilities address in developing a security architecture include:

- New intelligent devices with disparate security capabilities that vary across product and vendor,
- Multiple security domains with different policies, level of trust, and using different LAN and transport technologies, some of which may be proprietary,
- Policies, implementation, and procedures to actively mitigate supply chain threats,
- Securing distribution and energy management system from external attack and insider threats,
- Securing embedded systems and controllers,
- Selecting a security monitoring approach,
- Securing a geographically dispersed network that is exposed to a wide range of physical security threats,
- Designing a scalable, wide-area security solution that accommodates both security policy and operations objectives.

2.3. Threat and Risk Assessment

Threat and risk assessment is an essential part of the security planning process. Utilities need to understand their potential adversaries, i.e., the threat agents, their motives and capabilities. They need to understand the forms of attack they may undertake, including not just cyber assaults, but also combinations of cyber and kinetic attacks. They need to understand the potential impact and harm such attacks could inflict to the integrity of their systems, reliability of their power, safety of their employees and customers, and their corporate reputation. These risks need to be prioritized using a methodology that satisfies the business philosophy of the utility, being careful not to discount the troublesome category of threats with low probability, but high impact.

While a high-level threat and risk assessment should be conducted early to help formulate security policies, an in-depth threat and risk assessment should be performed against the system security architecture using an independent team of security professionals. The purpose of this assessment is to validate that the security architecture accomplished the spirit of the security policies and to evaluate the unique security threats and risks associated the system design and its integration with other utility systems. A key part of this assessment is a resiliency analysis to assess the system's ability to recover and for the utility to maintain control in the event that any part or combination of facilities becomes unavailable due to natural or man-made events. This analysis should provide an independent verification that the security architecture design has achieved the utility's security objectives. Any gaps or unmitigated threats identified by the threat and risk assessment should be addressed in a revision to the security architecture.

2.4. Security Vulnerability and Penetration Testing

Prior to deployment, all Smart Grid systems, equipment, and applications should be subject to security testing. Security testing has a two-fold purpose. First, security testing is required to validate that security controls claimed by the vendors and incorporated into the system security architecture have indeed been implemented in the equipment to be deployed. A security architecture that exists solely on paper or in a vendor's roadmap does not provide much benefit. The starting point of every security testing effort should be to validate the existence and operation of claimed security controls. Once validated, vulnerability and penetration testing then attempts to find weaknesses that have crept into the network because of implementation flaws, unforeseen interactions among system capabilities, and shortcomings in security policies.

There is a direct linkage between the quality of vulnerability and penetration testing results in embedded systems and the time and resources allocated to the task. Security testing on embedded system Smart Grid devices is different than traditional IT penetration testing. It requires the application of different security techniques and, in some cases, custom-made tools. As a pioneer in conducting in-depth security assessments on Smart Grid systems, Telcordia has developed its own Smart Grid assessment methodology. Shown in Figure 2, this methodology covers four quadrants: Network, Hardware, Software and Firmware, and Wireless/Radio.

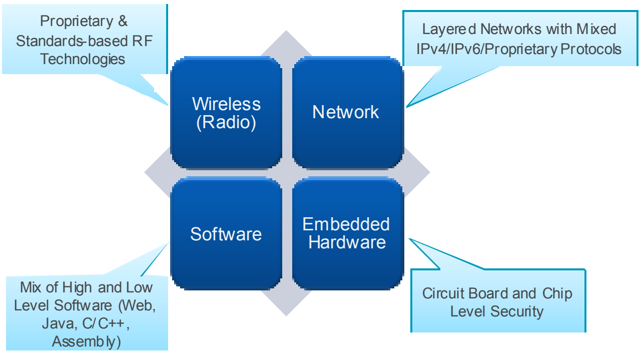
Proprietary & Standards-based RF Technologies
Layered Networks with Mixed IPv4/IPv6/Proprietary Protocols
Wireless (Radio)
Network
Software
Embedded Hardware
Mix of High and Low Level Software (Web, Java, C/C++, Assembly)
Circuit Board and Chip Level Security

Figure 2 – Telcordia Smart Grid Assessment Methodology

While the industry average for an IT security assessment is on the order of a week or two of testing, OT security assessments can take up to 5 times longer to obtain a solid understanding of their security risks. Do not skimp on Smart Grid security testing. Remember, security testing is a process that tries to replicate in a few short weeks what attackers may have years to try to accomplish. Undertaking a more in-depth security assessment is well worth the expense in the long run.

3. A HOLISTIC APPROACH

Telcordia suggests utilities take a holistic approach to their security program, addressing all major business domains in every lifecycle stage and not just focus on the technology aspect. The business domains include:

People: Understanding the stakeholders involved in the process and addressing their needs, expertise and capabilities are critical to successful security policy development and compliance.

Process: A well-proven process will minimize work-arounds and produce results that are less likely to circumvent security policy.

Systems: Automated systems are a necessity for handling complex activities and large volumes of both operations and security related tasks. System security should be considered all the way from planning through retirement and it should take into account how systems interconnect with each other.

Data: Data are what people, processes and systems use to perform tasks. Information security policies and processes must accommodate both efficient business processes while securing data and ensuring its accuracy and integrity.

Technology: Smart Grid technology is introducing new functionality and with it, complexity and vulnerabilities. Security requirements should be defined and included in the solicitation process and carried through into acceptance testing and deployment.

Telcordia also advocates developing an end-to-end Technology Introduction Process (TIP). The TIP will establish a consistent process by which a utility introduces Smart Grid technology into its operating environment. The TIP should describe a series of gates through which each Smart Grid process needs to pass, where each gate specifies the requirements for each of the key stakeholders. Security would naturally be part of several gates, but other business functions such as system operations, IT, and procurement would also be involved. The TIP should be enforced on a corporate-wide basis to eliminate inequities and discrepancies created when individual business units define their own processes.

4. SECURING THE ADVANCED DISTRIBUTION SYSTEM

Deployment of distributed intelligence and communications to enable remote monitoring, control and automation in the distribution network is fundamental to Smart Grid. Examples of intelligent devices being deployed in the distribution infrastructure include substation computers, SCADA bridges and converters, automated reclosers, switched cap banks, sectionalizers and switches, automatic restoration equipment, faulted circuit indicators, feeder meters, smart transformers, smart regulators, sensors and feeder meters. Closer to the customer, Smart Meters and their supporting access nodes, direct load control devices, Home Area Networks, controls for community energy storage devices, vehicle charging stations, and residential solar and wind controls are also being deployed. Most of these devices use wireless communications. Together, they make up a large, complex, heterogeneous network called the Field Area Network (FAN).

Distribution Automation (DA) and the advanced distribution network enables utilities to quickly locate, isolate and recover from faults and create "self healing networks." It enables advanced Volt/VAR control, load balancing of three phase feeders and locating of power leakages. It allows for improved management of more resilient mesh-based distribution networks, rather than the traditional radial topology. It enables the replacement of Run-to-Failure asset management with proactive Condition-Based maintenance techniques. DA also enables the management of distributed energy resources and loads, such as solar assets, battery storage, wind and electric vehicles.

However, these benefits do come with challenges. Some of the operating issues that have already been observed include significant voltage level variations on feeders and increased tap changer operations caused by solar systems and other intermittent power generation. Reverse power flow/back-feeding has been observed on feeder circuits. Complex conditions have created the need for micro-Distribution Management Systems (DMS) to manage local situations. Greater monitoring, data overload and limited communications make it difficult to backhaul all information to a centralized DMS center. Supply and demand imbalances are starting to occur in some markets. Some utilities have already experienced the monetary value of wind-generated power going negative. That is, they now need to build load through demand response because they cannot throttle down or shutdown a plant.

5. FAN SECURITY

One of the greatest challenges in the advanced distribution network that continues to elude many utilities is how to monitor and secure FANs. FANs are exposed to a variety of threats. For example, an attacker may attempt to disable power in a local area or at a specific address. Metering data transiting FANs may be forged, altered or subject to eavesdropping, which could result in improper billing and loss of customer privacy. Power quality may be maliciously degraded by making unauthorized changes to distribution circuits and regulators. Large power loads, such as vehicle chargers, could be maliciously cycled to create significant fluctuations and instability in the power system. Sensor data could be altered to maliciously influence power operations. Denial of Service attacks may render automatic field systems ineffective or unresponsive because they cannot communicate. Utilities may lose partial or complete control of field components. Unauthorized actions may result in permanent damage to expensive infrastructure. Security compromises in one energy service company may have cascading consequences on others entities in the energy value chain. Attacks on the supply chain of field component hardware and software may result in latent cyber threats that can pervade the system.

FANs are difficult to secure for a number of reasons. First, FANs are composed of embedded systems that have limited security and management capabilities. FAN devices, for instance, may not support strong cryptographic controls, centralized authentication, fine-grain authorization, and detailed security logging. These are security features that are taken for granted in many enterprise networks. Because most FAN equipment is built on proprietary platforms, utility security and network managers do not have the option of enhancing their capabilities by layering on third party software. The use of proprietary network technologies and communications protocols and the lack of a common data model mean that utilities are heavily reliant on whatever capabilities are available in the support system software provided by the equipment vendor. The general immaturity of FAN management software often leaves OT security and network managers without many of the tools commonly available to their IT counterparts. The end result is that utilities have been deploying FANs with little to no visibility in network health and security. Better capabilities are needed to improve situational awareness, not just for power operations, but also for the health of FAN communications and security monitoring of FAN endpoints. Utilities are now expressing need for FAN situational awareness, diagnostic capabilities, network performance and optimization tools, intrusion detection capabilities, and modeling tools.

5.1. Telcordia FAN Analyzer

Telcordia has been undertaking research in a number of areas to improve visibility into FANs for security, network performance monitoring, and diagnostics. A first-of-its-kind tool that Telcordia has been developing is a protocol analyzer for AMI and DA FANs. The Telcordia FAN analyzer is modular, probe-based tool that enables a utility to independently monitor and decode FAN wireless signals. Much like a packet analyzer used in IP networks, the Telcordia FAN analyzer passively intercepts FAN traffic and decomposes captured packets into individual information elements. Using custom-built extensions to the industry-standard Wireshark® protocol analyzer, the Telcordia FAN supports proprietary FAN protocols and inherently supports IPv6, IPv4 and a rich set of protocols available in the open source tool. The probe portion of the Telcordia analyzer is a custom network access adaptor that incorporates the non-standard radio technology needed to capture and demodulate AMI and DA wireless signals. Although Telcordia's efforts have focused on the 900 MHz ISM band, an interchangeable probe architecture enables it to support different radio technologies.

The Telcordia FAN analyzer can be used as a standalone tool for network analysis to support utility engineering, operations, and security functions with real-time access to network traffic. Designed to support captures from multiple probes, the Telcordia FAN analyzer can simultaneously capture traffic on multiple frequency channels and different segments of the FAN. One or more probes can be deployed in the field to capture and backhaul traffic to a central repository for analysis. Utilities obtain direct visibility into network behavior and can monitor the interaction among nodes and backend systems. Insights can be gained into network performance and routing. Multiple triggering techniques allow users to focus in on traffic of interest. The Telcordia FAN analyzer can also be used as a portable diagnostic tool for field technicians and as a laboratory test solution for pre-release testing of FAN product enhancements. Future capabilities include the ability to insert traffic into FANs for diagnostic and test purposes.

5.2. Telcordia FAN Intrusion Detection System

Telcordia is also researching and developing a first-of-its kind Intrusion Detection System (IDS) for AMI and DA FANs. The Telcordia FAN IDS is a scalable, probe-based system with distributed intrusion detection intelligence and centralized storage. The FAN IDS builds upon the Telcordia FAN analyzer by creating a system of intelligent probes with the capability to detect anomalies and security events as shown in Figure 3.

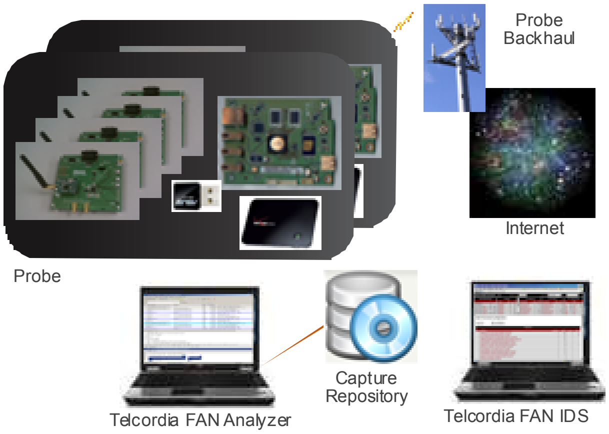

Figure 3 – Telcordia FAN IDS Architecture

Telcordia is currently investigating the feasibility of extending commercially available IDSs, such as Snort®, to support FAN intrusion detection. Telcordia is independently researching security weaknesses at different protocol layers in AMI and DA FANs and defining rules, signatures, and heuristics to detect anomalies and attempts to exploit these weaknesses.

A multiple-layered analysis capability is planned. Probes will run less complex intrusion detection rules in real-time to provide a fast alert capability. More complex, in-depth analysis will be performed offline in the backend, where data from multiple probes can be analyzed for a broader network view.

Since the Telcordia FAN IDS is built as an independent system that does not rely upon a FAN vendor's management components or endpoint security functions, it can be also used to help mitigate supply chain threats. In currently deployed FANs, utilities rely upon the FAN components themselves and vendor support systems to report security events. If the vendor's supply chain was compromised, security events may be disabled or masked, leaving utilities with no indication of a problem. The Telcordia FAN IDS, on the other hand, observes traffic and exchanges between nodes. If the malicious code requires communications between nodes for control or propagation, the Telcordia IDS could potentially detect this anomalous behavior. FAN IDSs are an important new tool that utilities will need to gain situational awareness.

5.3. Telcordia FAN Visualization

Telcordia's FAN research has shed light on the need for capabilities to visualize and better interpret information about the status and health of FANs. Presently, information about FANs is analyzed by utility engineers who collect information from a series of FAN devices and manually attempt to analyze tables of data. Patterns, cause and effect relationships, and a clear understanding of present conditions are often difficult to extract. Little or no capabilities exist today that provide utility operation centers with a real-time view of FAN status and health.

Building upon its expertise in developing network monitoring software for the communications industry, Telcordia has investigated how to gather information from multiple systems, correlate it and present FAN information in a useful manner that supports utility operations centers and its engineering functions. Offered as a custom development service to utilities, Telcordia's FAN Visualization solution improves FAN visibility and situational awareness.

Telcordia's FAN Visualization solution offers multiple network views, each drilling down to a finer level of detail. The high-level view depicts a current view of network connectivity and flags nodes that have posted critical alarms. Connectivity diagrams can be overlaid on geographic maps or RF signal strength maps to show terrain and landmarks. A mid-level view focuses on a smaller portion of the network and provides more detailed statistics about routing, latency, and traffic in a regional area. A low-level view provides detailed information about a particular node. Time sequenced records of the data used to build the network views are maintained so that changes in FAN performance based on time of day, month, season and various environmental conditions can be observed. A baseline FAN performance can be extracted from historical data to define "normal" FAN operation.

There are many use cases for the FAN visualization capability described above:

- Provide a tool for situational awareness in a distribution management center,
- Help diagnose connectivity problems and reasons for failed meter reads in AMI FANs,
- Optimize access node utilization by re-homing FAN nodes,
- Compare as-implemented network topology with the planned network design'
- Observe the changes in network performance as seasons change and environmental factors impact signal propagation,
- Visualize network routing in self-forming mesh networks and understand node latency problems,
- Support troubleshooting of software bugs and issues with new technology,
- Support network traffic planning and scheduling efforts, and understanding network throughput and utilization,
- Visualize the propagation of malicious code or a worm or the pattern of attacks on FAN nodes,
- Monitor FAN performance to enforce Service Level Agreements (SLAs).

6. CONCLUSION

Largely due to the urgency to spend stimulus funds, many utilities have deployed Smart Grid technologies without taking the time to update their security policies, define a Smart Grid security architecture that supports their Smart Grid vision, or properly plan new security capabilities to mitigate the growing cyber risk inherent in an intelligent and networked Smart Grid.

Utilities are being asked to emerge from a "culture of compliance" to a new "culture of cyber responsibility." Compliance with NERC-CIP does not mean your network is secure – it is a bare minimum requirement for many utilities. Smart Grid security needs to be built in and layered upfront in the planning stages rather than added during or after-deployment. Telcordia recommends approaching Smart Grid security with a top-down planning approach that begins with the update or definition of new Smart Grid security policies and systematically proceeds through the iterative step of security architecture and system design, followed by threat, risk, and resiliency analysis, and finally security testing before system deployment. Telcordia advocates introducing a structured Smart Grid Technology Introduction Process to ensure that critical requirements for business, power operations, security, procurement, and other needs are addressed in a consistent manner for each Smart Grid project.

FANs that enable the advanced distribution system present a challenge to secure because of the embedded nature of the components, the use of proprietary radios and communication protocols, and the lack of network monitoring tools. FAN situational awareness is a growing need and concern. Telcordia has undertaken several research efforts to improve visibility into FANs for security and operations. Telcordia's FAN analyzer enables utilities to monitor and decompose FAN traffic as a standalone tool or part of a distributed, probe-based operations system. Telcordia's FAN IDS addresses the need to monitor FANs for anomalies and signs of intrusion, and to mitigate supply chain threats. Telcordia's FAN Visualization solution offers utilities a way to visualize FAN data to support a variety of use cases.

Telcordia has been helping its Smart Grid clients to fill gaps in FAN security through research, developing FAN Analysis tools, extending Intrusion Detection Systems into FAN environments and developing FAN Visualization solutions to meet their engineering, operations, and security needs.

Biography

Stan Pietrowicz is a Senior Principal Security Consultant in the cyber security practice of Telcordia Technologies. With over 20 years of combined experience in the Communications, Smart Energy, and the Intelligent Transportation sectors, Stan is responsible for business development, project management, technical delivery and research. Working for Bellcore and now Telcordia since 1990, Stan's present focus is Smart Grid security and operations where he pioneered the security assessment of Advanced Meter Infrastructures and received the Telcordia's first CEO Award for Innovation in 2011. Stan also manages security research in FAN Security and conducts research in Intelligent Transportation Systems and vehicle communications. Stan received his MSEE from

Rutgers University and BEEE from Stevens Institute of Technology.

Tom Mazzone is a Principle Solution Architect with Telcordia Technologies' Advanced Technologies Solutions responsible for project management, customer solution architecture, process design and reengineering for cyber security, utility smart grid, telecom operations process and software development process quality improvement services. Tom has over 30 years experience in telecommunications network management, provisioning and maintenance systems engineering, operations processes and re-engineering, interconnection regulation and global number portability program development. Tom has 5 years experience with Pacific Bell in various network and operations management positions including switching systems and outside plant equipment maintenance operations control centers. Tom holds a Project Management Professional (PMP) certification from PMI and is ITILv3 Foundation Certified.

Telcordia has over 27 years of experience planning, designing and protecting critical infrastructure and large, complex networks. As a leading global provider of engineering and security services, fixed, mobile, and broadband communications software, and cutting-edge research, Telcordia serves a broad spectrum of communications-intensive markets. Working with a broad range of clients in government, communications, military, finance, energy, automotive, and entertainment, Telcordia has a unique perspective on current and future network needs and best practices. In recognition of Telcordia's role in architecting our nation's communications infrastructure, Telcordia is a member and trusted advisor to the President's National Security Telecommunications Advisory Committee (NSTAC). The NSTAC provides technical and policy advice to assist the President and other stakeholders who are responsible for our nation's critical national security and emergency preparedness services.