

SERA as a complex approach to provide architecture of cyber-security based on international security standards into critical energy systems

ANDREAS BERTHOLD-VAN DER MOLEN,
Industry Lead EMEA, Power & Utility Industries Microsoft EMEA, USA,
KUKANOV ALEKSEY
Industry Market Development Manager for Power&
Utilities Industries Microsoft RUS
Russia
abvandm@microsoft.com

KEYWORDS

Smart Grid, Standards, Cyber Security, Reference Architecture, SERA, стандарт, информационная безопасность, архитектура.

1 INTRODUCTION

In April 2013 Microsoft has published its next version of strategy initiative named Smart Energy Reference Architecture.

This Smart Energy Reference Architecture (SERA), now in this second iteration, reflects those attributes as well as the hard won lessons of the industry over the last two years. It adds to the first version with new technologies, new concepts, and new protocols. It examines the state of the industry to date, and which paths might make the most sense to pursue to go forward. And it continues to offer the much needed guidance our partners and customers need to think about their smart energy ecosystems, no matter what stage of development they are in.

Just as standards have been the enablers to the development of the smart energy ecosystem, Microsoft views as equally important the establishment of an architectural philosophy with a vision and strong foundation for migrating to the new infrastructure, as well as outlining the services necessary to monitor, control, and report on the assets of this new power system.

The one of the main topics of the SERA is a complex approach to provide the cyber security of all energy assets and whole energy ecosystem based on specific standards and technologies

Security considerations are of utmost concern for the transformation of the current utility network to a smart energy ecosystem because of the mission critical nature of the grid and generation infrastructure.

Regulatory authorities and the industries themselves have intensified their focus on security due to the increased complexity of computing environments and the growing sophistication of attacks that seem to occur almost daily. Concerns have been heightened due to several high profile events demonstrating system breach and, in some cases, improper and unauthorized operation of control systems.

As might be expected due to the importance of utilities to functioning economies and even the very social fabric enabling human life, national governments consider their country's energy assets as critical infrastructure that must be guarded like their very lands and resources. As such, they are taking bold, significant steps to ensure that utilities amplify their attention to security. National regulatory initiatives require concerted attention to the following three types of security:

Physical Security

Physical security includes controlling access to all critical infrastructure, assets IEDs and networks. Utilities are expanding their surveillance programs to monitor and ensure the physical security of the power system

Operational security

Operational security consists of ensuring assets are operated within their designed limits for safety and performance. Proper training, qualification and operation should be included in the utility operational security program and the architecture must enable execution and reporting on these programs.

As utilities run assets closer and closer to design limits, accurate and timely update of operational limits must be maintained. As example:

- Dynamic Feeder Ratings offer a good example of a set of operational limits that must be maintained dynamically and consistently. Running with limits set on a cold winter wind free day could be a real problem if left unchanged for hot, windy summer days.

Cybersecurity

The greatest concern to utilities and regulators has been the relatively porous, inconsistent, and inadequate application of cybersecurity.

This has occurred because the software vendors' selling point solutions over the last two decades have not had to consider their role in a supply chain of an overall security approach. The point solutions unwittingly opened the door to potential attackers who have preyed upon single vulnerabilities to access entire systems. This has been compounded by lack of an integrated and holistic architectural approach to the overall system design to help mitigate risk.

Exacerbating the matter, an even greater threat has presented itself with the advent of the two-way devices that enable the smart energy ecosystem.

In the past, the utility's control of field equipment was channeled through closed, proprietary communication infrastructures. While secure, the closed system may have served to shut out innovative opportunities that would improve operating efficiencies.

The smart grid movement could be described as working to change that. Now, utilities are using open and standards-based infrastructures to control their devices. While openness and interconnection offer great benefit to businesses and users alike, they also enable those who would seek to disrupt their operation, for whatever reason, with even greater opportunity to access networks and devices. Open systems enable a greater data-driven understanding of an energy infrastructure operation. Some new innovations have come with bolt-on, add-on types of security measures. It's like building a house of glass – the views are great from the inside but everyone on the outside might also endeavor to take a look.

The only option is to mount blinds, a superficial barrier detracting from the original design and deflecting only glancing attacks. Defenses need to be built into the system everywhere at the architectural level, e.g., like the use of special glass, strong frames, and other measures that work together to secure the entire structure.

In our view, the threats to vulnerabilities are often related to the age of deployed assets. Outdated systems on outdated hardware, operating systems designed to address security threats common 15 years ago, and dated applications cannot be expected to thwart sophisticated, modern threats. Legacy, custom, and even poorly designed COTS (Commercial Off-The-Shelf) applications can represent significant risks. Anti-malware and anti-virus software that is misconfigured, unused, or containing outdated virus definition files may offer a false sense of security, or as little protection as none at all.

The industry's core perception of "security" therefore must change.

2 MAIN

The implementation of security measures must not be viewed as the implementation of single-point chokeholds, like passwords; they must instead be considered holistically across the entire system, all contributors of the supply chain to the system, and throughout that system's entire lifecycle, from inception through adaptation/implementation and even to disablement.

Baking security into the design and development process itself is the only answer, to build a fortress beginning with the first stone. The real key here is to assume that you will have vulnerabilities that you may not even understand right now and how you would make exploitation of those vulnerabilities difficult for an attacker.

SERA First Principles for Cybersecurity

SERA recommendations are based on tried and proven principles that can be applied regardless of implementation technology or application scenario.

Effective Security and the Microsoft Secure Development Lifecycle

Keeping those principles in mind, the Smart Energy Reference Architecture sets as its goal “effective security,” an integrated program that consistently limits the possibility of a security breach and, should a breach occur, helps minimize the impacts on an organization's operations, assets, and people.

It is possible for vendors to implement effective, holistic security with the Microsoft Secure Development Lifecycle (SDL), a process that the industry now broadly recognizes as a best practice, and an approach that has received continuous revision and upgrade over the last eight years as the nature of the threat landscape and sophistication of attacks evolve.

Core security principles

Principle	Concepts
Compartmentalize	Reduce the surface area of attack. Ask yourself how you will contain a problem. If an attacker takes over your application, what resources can he or she access? Can an attacker access network resources? Can you stop an escalation of privilege? How are you restricting potential damage? Firewalls, least privileged accounts, and least privileged code are examples of compartmentalizing.
Use least privilege	By running processes using accounts with minimal privileges and access rights, you significantly reduce the capabilities of an attacker if they manage to compromise security and run code. The identification of privileges prevents an attacker from impacting the entire system or critical operations.
Apply defense in depth	Use multiple gatekeepers to keep attackers at bay. Defense in depth means you do not rely on a single layer of security, or you consider that one of your layers may be bypassed or compromised.
Do not trust user input	Your application's user input is the attacker's primary weapon when targeting your application. Assume all input is malicious until proven otherwise, and apply a defense in depth strategy to input validation, taking particular precautions to make sure that input is validated whenever a trust boundary in your application is crossed.
Check at the gate	Authenticate and authorize callers early — at the first gate. This extends also to applications. Applications white-listing is a powerful tool allowing only known applications to execute.
Fail securely	If failure occurs, ensure other systems are not brought down (prevent cascading outages). If an application fails, do not leave sensitive data accessible. Return friendly errors to end users that do not expose internal system details. Do not include details that may help an attacker exploit vulnerabilities in your application.
Secure the weakest link	Is there vulnerability at the network layer that an attacker can exploit? What about the host? Is your application secure? Any weak link in the chain is an opportunity for breached security.
Create secure defaults	Is the default account set up with least privilege? Is the default account disabled by default and then explicitly enabled when required? Does the configuration use a password in plaintext? When an error occurs, does sensitive information leak back to the client to be used potentially against the system?
Reduce your attack surface	If you do not use it, remove it or disable it. Reduce the surface area of attack by disabling or removing unused services, protocols, and functionality. Does your server need all those services and ports? Does your application need all those features?
Assume violations will occur	Ensure the ability to determine extent and source of the violation. Ensure ability to mitigate the violation, both in real-time and in remediation.

Figure 1 summarizes the major security principles described throughout this reference architecture.

Industry Guidance for Security

A number of organizations offer their views on security standards and approaches. The following examples provide several that the utility should consider in developing its own approach, but this is not an exhaustive list for every geographic region. Utilities should consider these among the options they have available to them for establishing their own security framework.

- **The Microsoft Secure Development Lifecycle**

The Microsoft Secure Development Lifecycle (SDL), which will be discussed in detail in the following sections of this document, is also closely connected to utility industry standards governing bodies. In fact, worldwide, a number of organizations have released new guidelines and standards demonstrate how key governmental agencies, trade associations, and utilities are approaching security and security best practices using SDL.

Many of the following guidelines from other industry groups integrate Microsoft SDL concepts into their structures.

- **NIST IR 7628**

The SDL's Security Engineering Principles have been integrated into NIST IR 7628, a three-volume document created by the Cybersecurity Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP) as a guideline for organizations to develop smart grid security strategies.

NIST IR 7628 is the NIST guideline for addressing security throughout all NIST SGIP chartered smart grid standards, regardless of which standards body eventually authors and formalizes the standards. The comprehensive nature of the document has resulted in other geographies and regulatory organizations leveraging the document for their own smart ecosystem security requirements.

- **IEC 62443**

IEC 62443 complements NIST IR 7628 by defining the elements necessary to establish a cybersecurity management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements.

- **IEC/ISO 27034: Application Security**

ISO/IEC 27034 is a six-part standard providing frameworks and process to help organizations integrate security throughout the lifecycle of their applications.

ISO says that the aim of ISO 27034 is to ensure that computer applications deliver the desired/necessary level of security in support of the organization's information security management system.

ISO/IEC 27034 offers guidance on information security to those specifying, designing/programming or procuring, implementing and using application systems, in other words business and IT managers, developers and auditors, and ultimately the end-users of application systems.

- o Part one of ISO 27034 Information technology – Security techniques – Application Security was published in November 2011. Annex A of ISO/IEC 27034-1 is a case study showing how a generalized development process based on the Microsoft SDL aligns to ISO 27034.
- o The part of 27034 that was published in late 2012 serves as a framework for developing secure software applications. The appendix to the standard uses Microsoft SDL as a case study to illustrate points made in the guideline.

- **EC M/490**

The European Commission Directorate General for Energy issued the M/490 Smart Grid Mandate directing the CEN, CENELEC and ETSI organizations to create similar standards including a

reference architecture, security and sustainable processes for the EU. The Working Group includes EU TSOs like ENTSO-E, DSOs, and energy and telecom companies and is focused on rationalizing coverage of IEC 27001/IEC27002, NISTR 7628, IEC 62351-7 and -8. EC M/490 aligns well with the stated program approach for SERA security. A very good treatment of Electric utility Threats is included in the M/490 Working Group Smart Grid Information Security Report on SGIS requirement standards and should be a reference for anyone beginning an undertaking to define and model utility threats.

To demonstrate the point made in the introduction to this section, that the standards are very interconnected across geographies, EC M/490 references NISTR 7628, a standard which incorporates Microsoft Secure Development Engineering Principles.

Industry Guidance for Risk Management

Effective security also requires good risk management. And good risk management is a mindset that accepts the tenant that constant diligence is required to stay one step ahead of continuous threats. Risks must be understood in order to prioritize resources.

Good risk management also accepts the notion that security solutions need to be built in to every possible type of software and process across the IT and OT solution supply chain. Utilities are now requiring that providers build security into their solutions, to address various risks. Utilities should realize that their responsibility for security does not lessen once they make these requirements of vendors – they will still need to have their own security risk management strategy in place while the vendors bring their products up to specification, including mitigating legacy solutions until new vendor software is available.

In addition to the above states of vigilance, utilities should consider the following guidelines for risk management as offered by the following organizations and included in the Appendix to this document:

- U.S. Department of Energy Risk Management Process Guideline
- Carnegie Mellon Electricity Subsector Capability maturity Model (ES-C2M2)

REGULATORY GUIDANCE FOR CYBERSECURITY

Understanding the scope and applicability of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIPs) to cybersecurity is a key component of any North American interconnected transmission utility, or any worldwide utility where the regulators follow or directly adopt the standards as applicable.

The CIP standards 2-9 below provide a framework for identification and protection of assets that fall into the category of Critical Cyber Assets supporting reliable operation of the US Bulk Electric System. The version 4 CIPs are in force until FERC ratifies CIPs version 5, which would take effect in 2015. The references herein are to the CIPs version 5 standards. The NERC CIPs website can be used for the version 4 standards.

Relevant NERC CIPs, Version 5	
CIP Reference Number	CIP Title
CIP-002-5	Cyber Security - BES Cyber System Categorization
CIP-003-5	Cyber Security - Security Management Controls
CIP-004-5	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-5	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-5	Cyber Security - Systems Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-5	Cyber Security - Recovery Plans for BES Cyber Systems

Figure 2 - NERC CIPs version 5 are expected to take effect in 2015.

The following section seeks to describe where these resources reside and how ICT systems that operate the equipment are affected. This is not a legal interpretation of the CIPs standards and cannot be a replacement for proper due diligence by individual utilities' for their specific case.

- **NERC CIPS ICT SYSTEMS CONSIDERATIONS**

New versions of NERC CIPs standards for utilities continue to evolve as the nature of new threats become known, as best practices develop, and as utilities gain greater understanding of the regulations. The following sections describe what areas are included under NERC CIPs and discuss the gaps/grey areas as well.

- **NERC CIPS FOR FUNCTIONAL SECURITY ZONES**

For example, utilities are now creating functional security zones (FSZ) with progressively tighter controls and reporting to comply with NERC CIPs.

The following diagram shows three FSZs ranging from corporate IT to the tightest controlled environment of the control center network and applications.

- **NERC CIPS FOR BULK POWER SYSTEMS**

The NERC CIP standards focus directly on operation of the Bulk Power System. As such, these control systems are directly affected:

- **Energy Management Systems (EMS)** at transmission voltage levels
- **Protection and Control Systems** for transmission protective relaying
- **SCADA systems** which supply real-time information to the EMS
- **Reliability Coordination Systems** across major control areas

- **NERC CIPS FOR DISTRIBUTION LEVEL SYSTEMS**

The NERC CIPs currently are only applicable to distribution voltage level systems and equipment if the systems contribute to 300MW of automated load shedding or compromise of the systems would adversely affect operation of the Bulk Electric System. Some systems typically fall outside of the current standards:

- Distribution Management Systems
- Distribution-level Outage Management Systems
- Meter Data Management

- **NERC CIPS FOR DEVICE MANAGEMENT**

The functionality of traditional substation devices coupled with the introduction of NERC CIP-007 is leaving many utilities uncertain about how to effectively approach the problem of total device management. Total device management includes removing the separation between IT and OT equipment as well as understanding the cyber-security practices that are requiring utilities to rethink their approach to remote engineering access, device password management, configuration management, and active device monitoring. This problem is worsened with the vendor-variety of our equipment that is installed within our substations. This presentation makes an argument for why all of these functions cannot be considered separately, and that a unified architecture is required to effectively solve the problem. As well, aspects of integrating legacy device configuration management with modern IEC-61850 practices are also discussed.

Utilities must address:

- The complexities of managing substation device passwords
- Risks incurred when manually managing device passwords
- Factors to consider when integrating automated password management
- Identifying the need to approach this problem in a vendor-agnostic manner

- Describing how configuration management is a natural extension of remote engineering access and password management
 - Integrating legacy device configurations with IEC-61850 SCL
 - Enhancing substation device situational awareness and configuration management with device active monitoring
- **NERC CIPS GREY AREAS**

While the above examples offer clear-cut examples of what is included and excluded, the following systems operate in NERC CIP grey areas:

- **Electricity Markets** – the Reliability Coordination function and the real-time dispatch fall under NERC CIPs - as well as any ICT systems running in the same network environment as these physical market-clearing functions. However, the rest of the electricity markets functionality – like financial market clearing, bidding, monitoring, settlement, reporting – do not need to conform to NERC CIPs, as long as they are not executing on the reliability coordination system LAN.
- **DR, DER, Load Aggregation** – these fall under NERC CIP at certain load levels. For instance:
 - The well-defined limit of 300MW above which these systems fall under the CIP regulations.
 - If a DR system or a Load Aggregator dispatches over 300MW of Load Reduction which might be used for grid stability or under frequency/under-voltage mitigation in the Bulk Power System, they fall under NERC CIPs.
 - If a system is directly controlling the output (or sending pricing signals which control the output) of distributed energy resources used for grid stability or ancillary services, above the 300MW limit, fall under the CIPs regulations.
- **Communication Links to Auxiliary Systems** – At present, NERC CIPs do not cover these communication links, but future releases are expected to incorporate them into the applicable standards.
- **Other Systems on Control Center LAN** – Other systems that are physically implemented on the EMS Control Center LAN do fall under CIPs guidelines, whether or not they have anything to do with dispatch of the Bulk Electric System. The NERC CIPs guidelines provide good guidance for best practices for maintaining and protecting these ICT systems but due to the effort involved in tracking and maintaining records for these non-critical systems, it is clear they should be removed from the control center environment.

Cloud computing datacenters provide great environments for many compute, storage, or communication intensive ICT deployments. The NERC CIPs have implications as to what can and cannot be considered for cloud deployment:

- Those systems described in the previous section as not being covered by NERC CIPs can be considered for cloud deployment.
- Mobility and load aggregator/DR systems that connect to a broad array of devices may be ideal candidates for cloud deployment.

PREPARING WITH A HOLISTIC SECURITY STRATEGY

In smart energy environments for bulk transmission in North America, the NERC CIPs represent non-negotiable minimal compliance practices.

It is incumbent upon those utilities to adjust their security strategies according to awareness that the security landscape is evolving and that NERC CIPs represent a minimum standard. By themselves, they are not adequate for proper security management on a permanent basis. Therefore, the following strategy is appropriate to all North American utilities as well as worldwide utilities in its holistic scope.

- **Setting Priorities for Security Strategy**

Utilities do not have unlimited financial resources to implement full-scale security upgrades. The Center for Strategic and International Studies offers its [20 Critical Security Controls Version 4.0](#) as a consensus audit guideline for effective cyber defense and is well worth taking into account.

- **Applying SDL**

As introduced in section 3.7.3.2, the Microsoft Secure Development Lifecycle serves as core component of many industry guidelines and standards and may be applied in a holistic manner by providing:

- Security Education for all Development and IT Staff
- Threat Modeling
- Risk Prioritization
- Incident Response Planning
- Incident Remediation and Recovery Planning
- Disaster Recovery Plans
- Cross-Industry Incident Notification Services and Programs

- **Independent Solution Vendor Application of SDL**

Pushing the concern about security outside the organization requires third-parties to acknowledge its importance to the utility.

Independent software providers should have as their goal the implementation of repeatable processes that reliably deliver measurably improved security.

As such, software vendors must transition to a more stringent software development process that focuses, to a greater extent, on security by:

- minimizing the number of security vulnerabilities extant in the design, coding, and documentation
- detecting and removing vulnerabilities as early in the development lifecycle as possible.
- mitigating the effect of an exploit of an unknown vulnerability

The need for this process is greatest for the enterprise and consumer software solutions that process inputs received from Internet, to control critical systems likely to be attacked, or to process personally identifiable information.

EUROPEAN UNION SECURITY AND SMART ECOSYSTEM STANDARDS

The European Commission has mandated that the European Standards Organization issue standards for the smart grid in Europe. The EC set up the Smart Grids Task Force in 2009 to develop policy and regulatory directions for smart grid deployment under the Third Energy Package, a gas and electricity market liberalization for the European Union. The commission has issued recommendations for the major components of the smart grid/smart energy ecosystem, including:

- Preparations for the roll-out of smart metering systems
- Sets of common functional requirements for smart meters
- Standards for smart grids
- Mandates for electric vehicles

- The adoption of communication standards for smart grids

More details you can read in the special chapter (3.9) of SERA.

BENCHMARKING STUDIES

The last few years have been noteworthy for the number of pilot projects and benchmarking studies that have occurred to prove the ability of technology to accomplish the core reliability mission implicit in any implementation of the smart energy economy.

Here's what we do know from various snapshots of measures:

- An Innovation Observatory report believes that 80 percent of worldwide smart grid investments will concentrate in 10 countries in the run up to 2030. The United States will lead smart grid spend for several years, with a \$60 billion total expenditure, but China's investment will reach \$99 billion by 2030. India, Brazil, France, Germany, Spain, and the United Kingdom will all have leading systems, as will Japan and South Korea.¹
- The European Electricity Grid Initiative, an industrial initiative of the European strategic Energy Technology Plan, aims to enable the distribution of up to 35% of electricity from dispersed and concentrated renewable sources by 2020. The EEGI compiled a list of select national projects, achieve and expected results, and their allocation to functional projects. Over 203 projects from 22 European countries were identified. Many projects are slated to complete in 2012.²

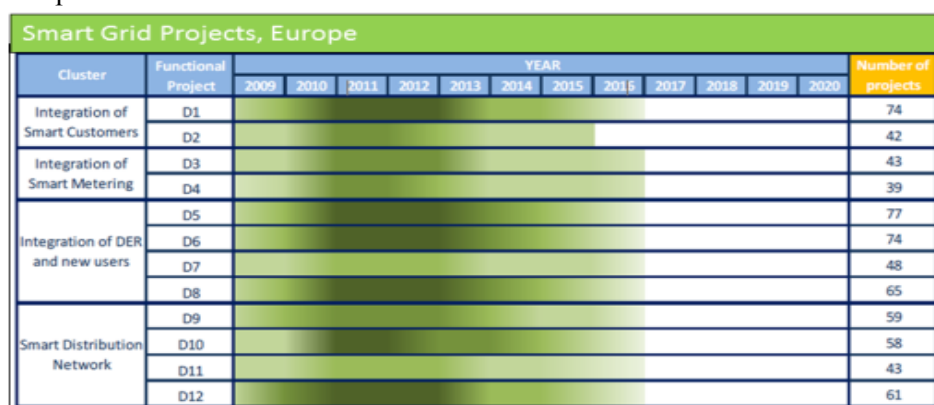


Figure 3: Smart Grids projects in Europe mapped to EEGI functional projects. Darker colors indicate more projects running during that year.

- A survey of 50 initial participants from US and Canadian utilities by the Newton-Evans Research company suggests that power utilities are likely to upgrade, retrofit and buy Energy Management Systems (EMS), supervisory control systems (SCADA), distribution management systems (DMS) and outage management systems (OMS), in the next three years. Plans for procurements of new DMS and (OMS) are significant, with more than one quarter planning to purchase a new or replacement DMS and nearly one-in-five planning OMS procurements. There is interest shown among one-third of these early respondents to combining DMS and OMS on a common platform, but cyber security concerns have been voiced by several operations officials looking into such system combinations.³

¹ "Smart Grid spend to be concentrated in 10 countries." Intelligent Utility, March/April 2012, p. 8.

² "Mapping and Gap Analysis of current European Smart Grids Projects," Report by the EEGI Member States Initiative: A pathway toward functional projects for distribution grids, April 2012, pg. 3.

³ "Preliminary findings point to solid growth for EMS, SCADA, DMS and OMS during 2013-2015 among North American Electric Power utilities."

- The growth and transformation of the smart grid is increasing access to critical infrastructure. The number of cyber-attacks on U.S. critical infrastructure increased 52% in 2012, according to a report by the U.S. Department of Homeland Security (DHS). Attacks on gas pipeline companies were successful and “could facilitate remote unauthorized operations.” Energy sector companies suffered 82 attacks, while water sector companies reported 29 attacks.⁴ Therefore, the National Institute of Standards and Technology is focusing on cybersecurity with four primary areas of concern: protecting data and information in a mobile environment in different use cases; continuous monitoring of information security, to enable the exchange of security data and leverage security automation; identity management through standardized work and personal identity verification cards; and completion of a new national standard for a cryptographic hash algorithm for SHA-3.⁵ U.S. President Barack Obama issued an Executive Order directing better cyber security information sharing and creation of a cybersecurity framework, with directions to DHS to encourage development and adoption.⁶
- The International Electrotechnical Commission (IEC) created a comprehensive framework of common technical standards for the smart grid. The body developed five core standards for any smart grid implementation, including:
 - IEC/TR 62357 – Framework of power automation standards and description of the SOA
 - (Service Oriented Architecture) concept
 - IEC 61850 – Substation automation and beyond
 - IEC 61970 – Energy Management System – CIM and GID definitions
 - IEC 61968 – Distribution Management System – CIM and CIS definitions
 - IEC 62351 – Security⁷
- The National Institute of Standards and Technology in early 2012 released the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, laying out a plan for transforming the US electric power system into an interoperable smart grid. The release included a new chapter on the roles of the SGIP; an expanded view of the architecture of the smart grid; a number of developments related to ensuring cybersecurity for the smart grid, including a Risk Management Framework to provide guidance on security practices; a new framework for testing the conformity of devices and systems to be connected to the smart grid—the Interoperability Process Reference Manual; information on efforts to coordinate the smart grid standards effort for the United States with similar efforts in other parts of the world; and an overview of future areas of work, including electromagnetic disturbance and interference, and improvements to SGIP processes. The final framework added 22 standards, specifications, and guidelines to the 75 NIST recommended in January 2010. Of note, the final draft contained a risk management framework offering guidance on security, as well as a framework for testing the conformity of devices and systems to be connected to the smart grid.⁸

More benchmarks you can find out in the SERA document.

⁴ “Hacker hits on U.S. power and nuclear targets spiked in 2012,” by David Goldman, CNN Money, January 9, 2013.

⁵ “Inside NIST’s cybersecurity strategy,” by Nick Wakeman, Regulatory Cyber Security, March 27, 2012.

⁶ “Cyber Security and Getting the President’s Ear,” by Prudence Parks, EnergyBiz, March 27, 2013.

⁷ “IEC Smart Grid Standardization Roadmap,” by SMB Smart Grid Strategic Group, June 2010.

⁸ “NIST releases final smart grid ‘Framework 2.0’ document,” contact Chad Boutin, February 28, 2012.

3 CONCLUSION

The structure, engineering, and objectives of the world's power systems have been undergoing dramatic rethinking and significant change over the last several years due to new, driving forces. Concerns about climate change abatement, the introduction of novel market participants such as plug-in hybrid electric vehicles, and ever increasing worldwide demand for energy are combining to drive development of a smart energy ecosystem that integrates the generating plant with its grid and end users in a holistic and, aspiringly, an automated way.

Many observers believe that the extent to which the transformation to a smart energy ecosystem might change societies is on the same scale as the inception of electricity distribution itself. If true, and there's no reason to doubt it, this dynamic will affect every single part of the power utility industry and how companies operate.

The Microsoft Smart Energy Ecosystem Reference Architecture was designed to maximize agility and enable role-based productivity while ensuring secure IT and operations with the very best ROI for all participants of the smart energy ecosystem. It is intended to ensure this balance now, with existing legacy systems, and in the future, as system requirements expand to address increasing complexities.

REFERENCES

- [1] SERA Advisory Consile (edited by Larry Cochrane), Microsoft, Smart Energy Reference Architecture v.2.0, Aprile 2013