Lecture 6: Interoperability, standards and cyber security

George Konstantinou, University of Cyprus

01/08/2020

Nicosia, Cyprus

Course material developed in collaboration with Technical University of Sofia, University of Western Macedonia, International Hellenic University, University of Cyprus, Public Power Corporation S.A., K3Y Ltd and Software Company EOOD

with support from Erasmus +

Content of the lecture

6.1 Introduction

6.2 Interoperability

6.3 Interoperability today

6.4 Benefits and challenges of interoperability

6.5 Model for Interoperability in the Smart Grid Environment

6.6 Smart Grid Network Interoperability

6.6.1 Interoperability and Control of the Power Grid

6.7 Standards

6.8 Smart Grid cyber security

6.8.1 Cyber security state of the art

6.9 Cyber security risks

6.10 Cyber Security Concerns Associated with AMI

6.11 Mitigation Approach to Cyber Security Risks with AMI

6.12 Cyber security and improving methodology for other users

Summary

References

6.1 Introduction to Chapter

- Implementation of the smart grid components and interoperability requires an important revision of current standards and protocols. In addition, improving the physical and cyber security of the network, which is quite fragile, is a very important task.
- Today's power distribution and monitoring are still in the initial stages of becoming a smart grid, with some substation networks connected by microwave, power lines, and fiber optics.
- Network backbones are very basic, and not intended to securely connect every home, building, and appliance throughout a utility's service territory. It is difficult to add millions of these connections to a distribution system, and utilities find themselves in the position of having to prepare for the future!

6.2 Interoperability

- Interoperability is defined as: ***" the ability of two or more systems to exchange and use information"***
- The issues include the interoperation of system components supposedly conforming to a particular standard as well as the interoperation of components across standards.
- For example, the International Electrotechnical Commission (IEC) identifies the various objects and attributes as mandatory, optional, or conditional. Communications, management, security, and application execution messages must all be well understood by the interoperating equipment.

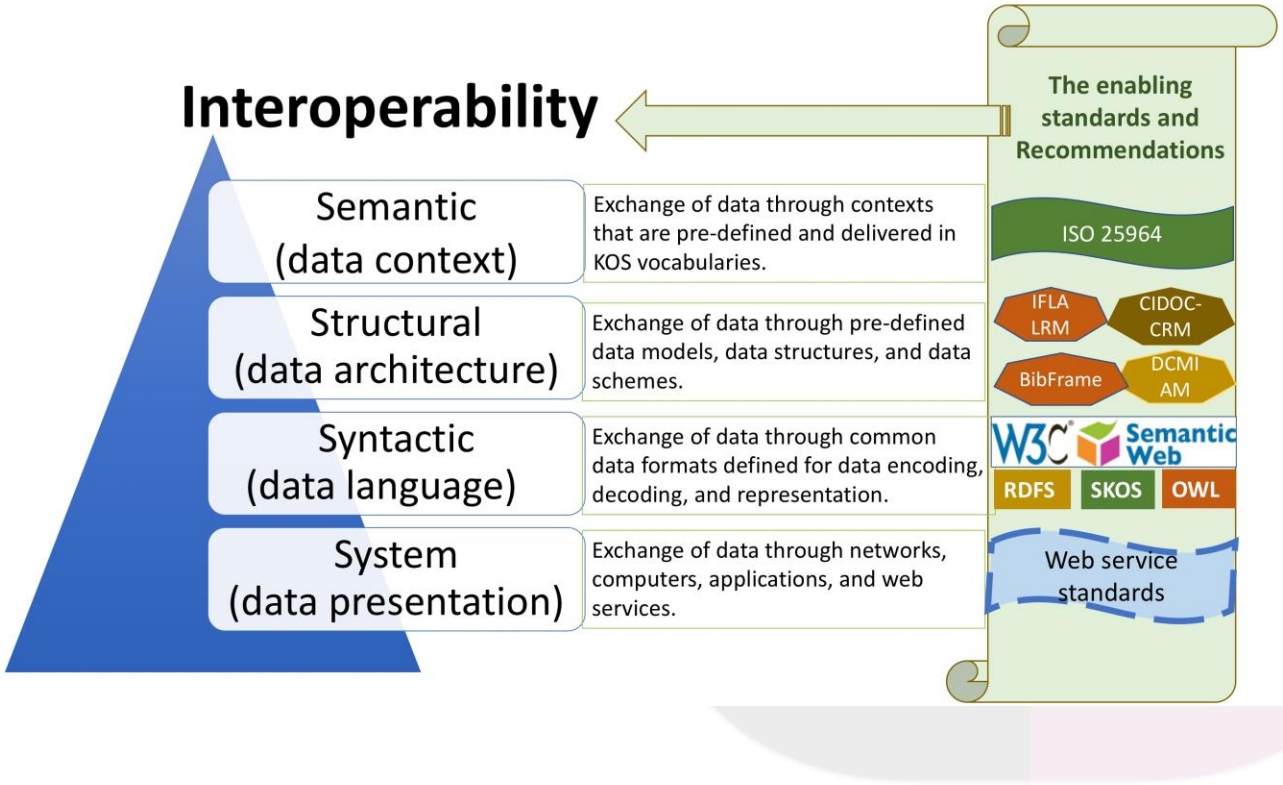
6.2 Interoperability

- A careful approach will include:

1.Reviewing the activities of governing bodies: The outcome will determine the activities to be undertaken by smart grid users

2.Reviewing components before deployment: Ensure compatibility with functional requirements

3.Developing internal project standards: Address continuing issues and the governing body efforts.

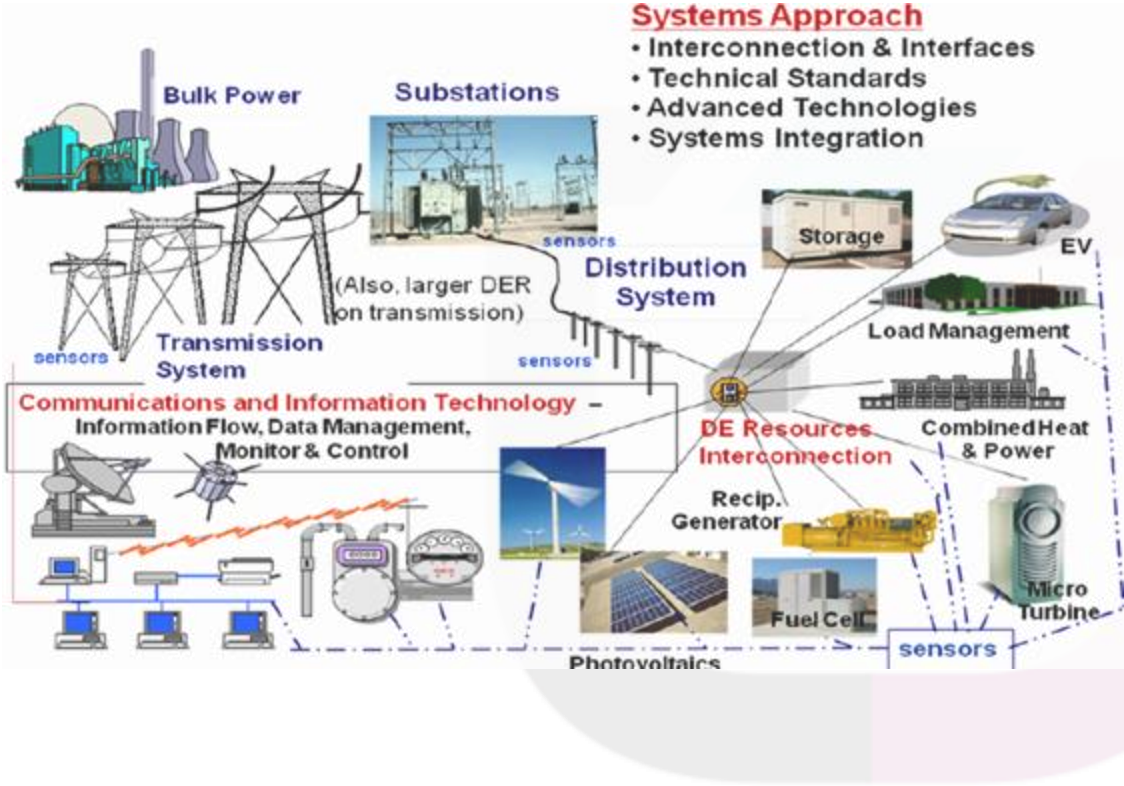


6.3 Interoperability today

- Interoperability is a key term in the development of smart metering to facilitate the competitive energy retail market [4].
- There are two elements to interoperability: technical and commercial.
- ***Technical interoperability*** is mainly about defining the functionality for gas and electricity metering interfaces that provide smart metering (format and data content) service requirements. The definition of technical interoperability will depend on the market model the use of smart metering. WAN and LAN communications interfaces will be explored. Consumer engagement important to delivering consumer benefits will be identified in a cost-benefit analysis.
- Use of case studies will have to be future-looking to ensure that opportunities such as DSM and smart grids are not precluded by any solution.

6.4 Benefits and challenges of interoperability

- *Interoperability* allows a network to *autonomously* integrate all components and systems of electric power supply, monitoring and measurement devices, distribution and substation equipment, and management and communication equipment. An important outcome is the minimization of human intervention.
- The challenges include the need for technical advancement of the network, the adaptation of existing technologies, and the development and implementation of comprehensive standards. Procedures to estimate vandalism, hacking, and other malicious attacks will accelerate the development of security protocols for authentication and validation before access to the system.



6.5 Model for Interoperability in the Smart Grid Environment

- Several features in the interoperable environment of a network have to be taken into account (relatively to each other) but also independently. The following example illustrates a conceptual model of the smart grid developed by the GridWise Architecture Council (GWAC).
- An eight - layer stack, termed the GWAC stack, provides a context for determining smart grid interoperability requirements and defining exchanges of information.
- The layers represent the chronological processes that enable various interactions and transactions within the smart grid. Each layer depends upon the layer beneath it and so each layer must function properly for the entire stack to be effective. As more complex functions are required by the network, more layers will be required to achieve interoperability.

6.5 Model for Interoperability in the Smart Grid Environment

According to GWAC, each category/driver subdivided by layers has a special purpose, as follows:

1. **Technical:** Emphasizes the syntax (or format) of the information, focusing on how the information is represented on the communication medium
2. **Informational:** Emphasizes the semantic aspects of interoperation, paying attention to what information is exchanged and its meaning
3. **Operational:** Emphasizes the realistic (business and policy) aspects of interoperation, especially those dealing with the management of electricity.

6.6 Smart Grid Network Interoperability

- Machines require specific input data and guidance in order to complete their tasks. The challenge here is to design proper language and protocols to ensure the communication between machines that run on the same or different protocols.
- The goal is to achieve quick, efficient, and speedy transfer of data among and across devices. Interoperability is not limited to a physical aspect of the network, because design engineers must also consider that when two devices try to exchange data, the messages must now “speak the language” of network navigation and must be properly “addressed” to reach the destination device.
- This creates the need for implementing networking standards so that machines that need to be connected can communicate without interruption or disruption. However, this is not a simple task to undertake.

6.6 Smart Grid Network Interoperability

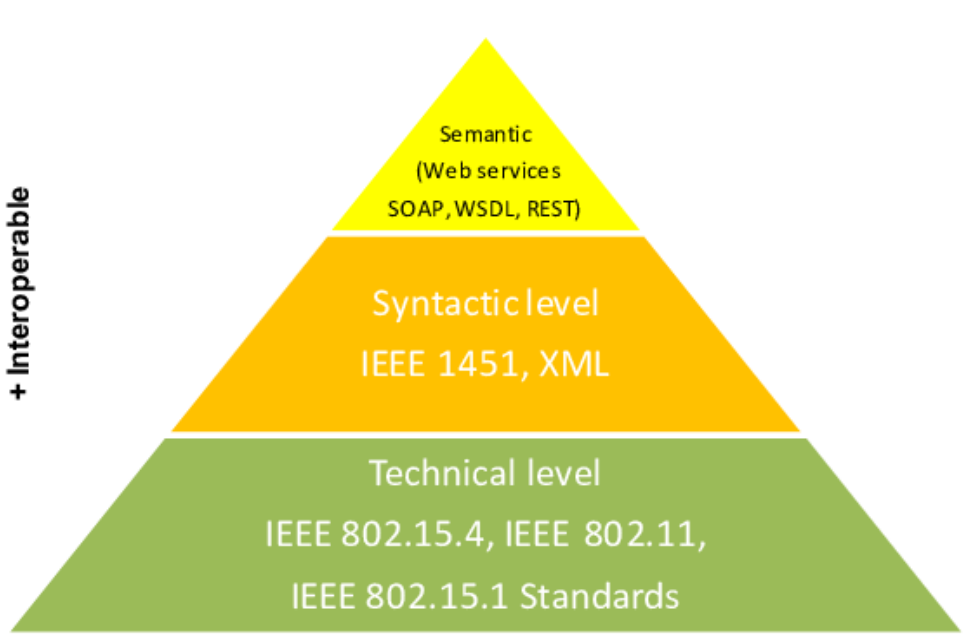
- For example, some machines may use a particular language protocol that requires another machine - attempting to communicate - to complete specific system requirements, that may lie outside its scope, before transmission can be completed.
- A network control is a major issue for utilities. To upgrade to a smart system, the network should be matched with equipment that detect problems, report back to the utility, receive control or restorative commands, and execute them.
- Full control means that all machines communicate, interpret, and perform tasks that most machines today cannot do so.

6.6.1 Interoperability and Control of the Power Grid

- The use of SCADA (Supervisory Control and Data Acquisition) and EMS (Energy Management System) have nowadays become ineffective. Control centers need to communicate with other control centers as well as regulatory agencies, energy markets, independent power producers, large customers and suppliers, to keep up with the evolving market environment.
- Control centers must be able to connect to machines that have smart technology to facilitate effective performance with little or no interruptions.
- In the best case scenario, the user/customer should have some degree of autonomy over consumption with a faster, more effective response to supply problems.

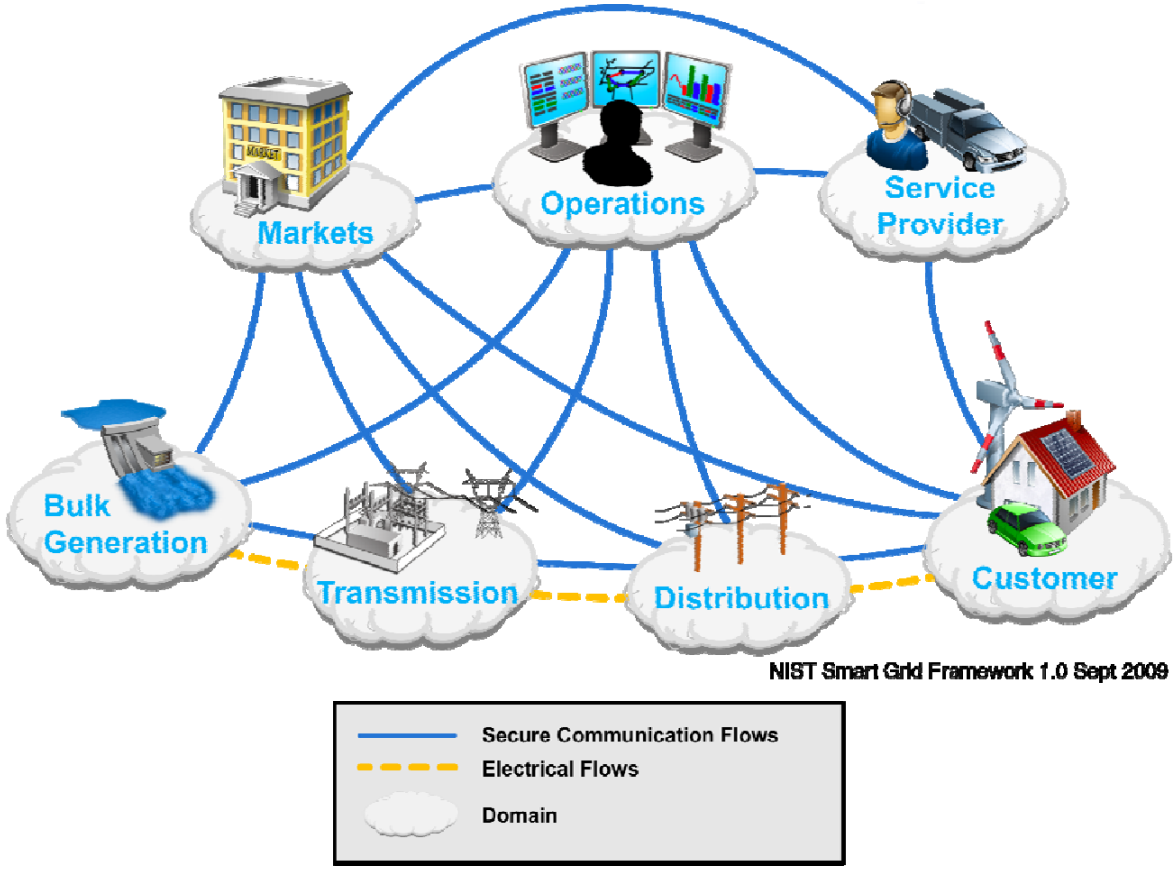
6.7 Standards

- Standards are the specifications that establish the relevance of a product for a particular use or that define the function and performance of a device or system.
- Many standards bodies, including the National Institute of Standards and Technology (NIST), International Electrotechnical Commission (IEC), Institute of Electrical and Electronic Engineers (IEEE), Internet Engineering Task Force (IETF), American National Standards Institute (ANSI), North American Reliability Corporation (NERC), and the World Wide Web Consortium (W3C) are currently addressing interoperability issues for a broad range of industries, including the power industry.



6.7 Standards

- The urgent need for the development of standards has led NIST to develop a plan to accelerate the identification and establishment of standards "while establishing a robust framework for the longer-term evolution of the standards and establishment of testing and certification procedures."
- Based on the first phase of this work, NIST published the NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 4.0 in February 2021
- In this publication, nearly 169 existing standards are identified. doi.org/10.6028/NIST.SP.1108r4



6.7 Standards

Standard Body	Description of Roles	Key Standards applicable to the Smart Grid Environment	
The International Electrotechnical Commission (IEC)	Leading global organization which publishes standards for electrical electronic and related technologies for the electric power industry.	IEC 61850	• Substation automation, distributed generation (photovoltaics, wind power, fuel cells, etc.), SCADA communications, and distribution automation. Work is commencing on Plug—in Hybrid Electric Vehicles (PHEV).
	Applicable standards have been developed in the area of communication for the power industry.	IEC 61968	• Distribution management and AMI back office interfaces
		IEC 61850	• Substation automation, distributed generation (photovoltaics, wind power, fuel cells, etc.), SCADA communications, and distribution automation. Work is commencing on Plug—in Hybrid Electric Vehicles (PHEV)
		IEC 61968	• distribution management and AMI back office interfaces
		IEC TC 13 and 57	• Metering and communications for metering, specifically for AMI.
Institute of Electrical and Electronic Engineers (IEEE)	Standards in all areas of electrical, electronic and related technologies. Standards developed in the area of communications and interoperability.	IEEE 802.3	• Ethernet
		IEEE 802.11	• WiFi
		IEEE 802.15.1	• Bluetooth
		IEEE 802.15.4	• Zigbee
		IEEE 802.16	• WiMax
Internet Engineering Task Force (IETF)	Responsible for Internet standards, dissemination of request for comment (RFC) documents for finalization of standards	RFC 791	• Internet Protocol (IP)
		RFC 793	• Transport Control Protocol (TCP)
		RFC 1945	• HyperText Transfer Protocol (HTTP)
		RFC 2571	• Simple Network Management Protocol (SNMP)
		RFC 3820	• Internet X.509 Public Key Infrastructure (PKI) for security

Summary of Relevant Standards for Smart Grid Developed by Key Standards Bodies

6.7 Standards

American National Standards Institute (ANSI)	Developed relevant standards for interoperability of AMI systems	ANSI C12.19 ANSI C12.22	• Metering "tables" internal to the meter • Communications for metering tables)
National Institute of Standards and Technology (NIST)	Publications which provide guidelines toward secured interoperability.	NIST SP-800.53 NIST SP-800.82	• Recommended Security Controls for Federal Information Systems. • Guide to Industrial Control Systems (ICS) Security.
North American Electric Reliability Corporation (NERC)	Security standards for the bulk power system which may be extended to the distribution and AMI systems.	NERC CIP 002-009	• Bulk Power Standards with regards to Critical Cyber Asset Identification, Security Management Controls, Personnel and Training, Electronic Security Perimeter(s), Physical Security of Critical Cyber Assets, Systems Security Management, Incident Reporting and Response Planning, and Recovery Plans for Critical Cyber Assets
World Wide Web Consortium (W3C)	Interoperable technologies (specifications, guidelines, software, and tools) for the world wide web	HTML XML SOAP	• Web page design • Structuring documents and other object models • Web services for application-to-application communications for transmitting data

Summary of Relevant Standards for Smart Grid Developed by Key Standards Bodies

6.7.1 Approach to Smart Grid Interoperability Standards

- The roadmap for interoperability by NIST includes the following applications:

1. Demand Response and Consumer Energy Efficiency
2. Wide Area Situational Awareness
3. Electric Storage
4. Electric Transportation
5. Advanced Metering Management
6. Distribution Grid Management
7. Cyber Security
8. Network Communications

6.8 Smart Grid cyber security

- Cyber security is a concept that has become quite important with the recent advances in smart grid technologies with the increased use of digital information and controls technology to improve reliability, security, efficiency of the electric grid and the deployment of smart technologies (real - time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.
- The interaction of the power, communication, and information networks are critical to facilitating resiliency and sustainability of the infrastructures which further enhance the provision of adequate power and support economic and social growth of the nation.
- Technologies and protocols are developed for the maintenance of system, network, data, and SCADA security while conducting vulnerability assessment, incident recognition, recording, reporting, and recovery. Protection of network data as well as web - based or stored data is conducted.

6.8.1 Cyber Security State of the Art

- Cyber security is a high priority of smart grid technologies. Cyber security ensures the integrity, confidentiality, and availability of the electronic communication systems necessary for the management and protection of the smart grid's energy, information technology, and telecommunications. This contains information and communications systems and services as well as information contained in these systems and services.
- Information and communications systems and services are comprised of the hardware and software that process, store, and communicate information. Processing includes paper, magnetic, electronic, and all other media types.

6.8.1 Cyber Security State of the Art

- Cyber security is defined as security from threats a computer or computer terminals meet and the protection of other physical assets from modification or damage from accidental or malicious misuse of computer - based control facilities [1].
- Smart grid security protocols contain elements of deterrence, prevention, detection, response, and mitigation; a mature smart grid must be capable of thwarting multiple, coordinated attacks over a span of time.
- Advanced security will reduce the impact of abnormal or hostile events on grid stability and integrity, ensuring the safety of society and the economy.

6.8.1 Cyber Security State of the Art

- Tasks include identifying used case studies with cyber security considerations, performing risk assessment such as vulnerabilities, threats and impacts as well as developing security architecture [2]. The underlying concept is that security should be built - in, not added - on.
- **This strategy includes:**

1. Review of the system functionality and data flows with particular attention to their similarities and differences with identified smart grid use cases (as documented in the NIST Roadmap).
2. Identification of relevant threats and the consequences/impacts if the confidentiality, integrity, availability, or accountability of the system data flows are compromised.

6.8.1 Cyber Security State of the Art

- Security requires many different solutions and ***is not relegated to encryption and password protection***.
- Facets of the cyber security include:

1. Security assessment and hardening of the existing systems
2. Vulnerability assessment
3. Disaster recovery
4. Intrusion detection incident response
5. Event logging, aggregation, and correlation

6.8.1 Cyber Security State of the Art

- Another critical understanding of the issue of security for the purpose of development is the realization of the inevitability of the occurrence of breaches. This leads to the development of contingency and recovery plans.
- Critical objectives for the development of cyber security for the smart grid environment are ensuring the confidentiality, integrity, and availability of device and system data and communications channels, and securing logging, monitoring, alarming, and notification.
- Data protection will require confidentiality of communicated and stored data for the power system facilitated by authentication methods and the use of cryptography which includes encrypted authentication, to make it difficult for hackers. A combination of detective, corrective, and preventive controls will formally address cyber security risks.

6.8.1 Cyber Security State of the Art

	Traditional Threats faced by Legacy System	Threats faced by the New System
Impact	Direct damage to physical utility	Indirect damage to physical assets through damage to software systems
Location of origination of threat	Local	Local or remote
Target	Individuals	Individuals, competitors, and organizations
Point of Attack	Single site	Multiple point simultaneously
Duration of Damage	Immediate damage causing obvious damage	Attack may be undetected or lie dormant and then be triggered later
Occurrence	Single episode	Continued damage associated with attack
Restoration	Restoration after attack	Attacker may have continued impact preventing restoration

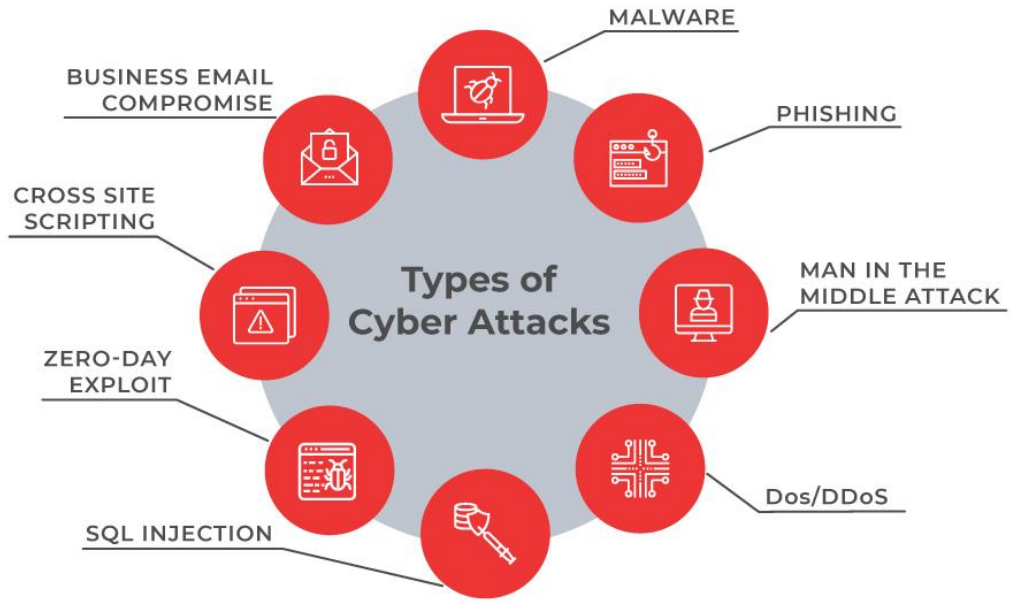
Threats Facing the Electric Power System

6.8.1 Cyber Security State of the Art

- All known cyber threats are monitored with a form of detective control. These include technologies such as host - based intrusion detection systems (HIDS) to monitor unauthorized changes to servers and deployed systems, network - based intrusion detection systems (NIDS) to detect network - based attacks, and platform - specific controls like virus detection and malware detection.
- These detective controls provide important data to design and testing staff about the real attacks and threats that the system faces / might face. Detective controls often provide forensic- quality evidence that can be used to reconstruct attacks and potentially identify and/or prosecute attackers.
- Additionally, data from detective controls also assist in the selection of corrective and preventive controls.

6.8.1 Cyber Security State of the Art

- Corrective controls seek to restore normal operations in the event of a successful cyber attack.
- Such controls are both manual, for example, a standardized procedure for switching to a backup system, and automatic, for example, failover designs that automatically disable compromised systems and replace them with known good systems.
- Corrections often seek to isolate and preserve successful attacks so that forensic analysis can proceed and permanent corrections, for example, in design, construction, or deployment, can be established.



6.8.1 Cyber Security State of the Art

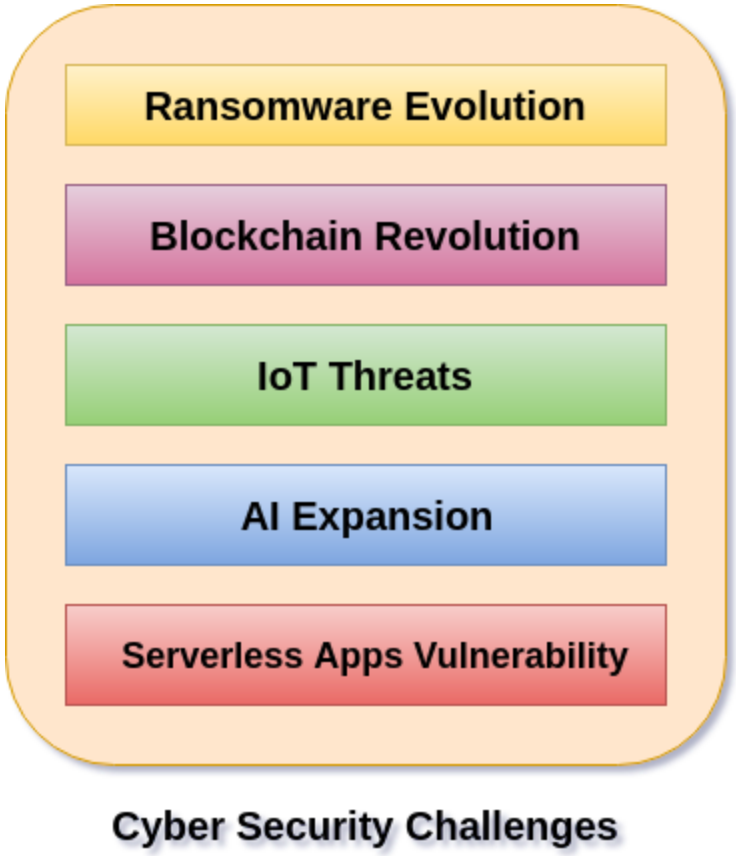
- For example, the secure development approach seeks to address risk throughout the life - cycle and throughout the engineering process, but preventive controls are a logical, efficient, and effective complement to secure implementation.
- Some attacks, for example, denial-of-service, can only be mitigated with a combination of secure engineering and preventive controls. Other attacks can be partially mitigated with a protective control, for example, network rules or role-based access controls, until a more comprehensive change to the system can be developed, tested, and deployed.
- As required, GridPoint deploys preventive controls to satisfy regulations, adhere to best practices, or to mitigate cyber security risks, including network-level filtering and rules, operating system-level mechanisms, and hardware-level mechanisms.

6.9 Cyber Security Risks

- Cyber security risks appear in each phase of the project life - cycle and include risks to managerial, operational, and technical processes.
- These risks may impact equipment and systems, network management and integration, communications, control and operations, and system availability.
- The primary components that may be vulnerable to security risks include IT applications, communications network, and endpoints (for example, meters, in - home displays, and thermostats). There are substantial risks to the integrity of data and control commands due to the exchange of information through publicly accessible equipment, for example, smart meters using over-the-air communications technologies, for example, wireless or radio frequency, which may be intercepted and altered if not secured.

6.9 Cyber Security Risks

- A number of system constraints need to be considered to satisfy security requirements.
- The requirements described do not prescribe which solution, for example, the use of narrow- or wide- band communications technologies, is most appropriate in a given setting.
- Such a decision is typically based on making prudent trade - offs among a collection of competing concerns.



Cyber Security Challenges

6.9 Cyber Security Risks

- The following trade - off must include the considering cyber security risk:

1. Other business or non - functional requirements
2. Performance (for example, response time)
3. Usability (for example, complexity of interactions for users)
4. Upgradability (for example, ease of component replacement)
5. Adaptability (for example, ease of reconfiguration for use in other applications)
6. Effectiveness (for example, information relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent, and usable manner)

6.9 Cyber Security Risks

7. Efficiency (for example, the provision of information through the most productive and economical use of resources)
8. Confidentiality (for example, protection of sensitive information from unauthorized disclosure)
9. Integrity (for example, accuracy, completeness, and validity of information in accordance with business values and expectations)
10. Availability (for example, information being available when required by the business process)
11. Compliance (for example, complying with the laws, regulations, and contractual arrangements)
12. Reliability (for example, the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities)

6.9 Cyber Security Risks

It is important to consider system **constraints** when developing applying security requirements, which include: Constraints

1. Computational (for example, available computing power in remote devices)
2. Networking (for example, bandwidth, throughput, or latency)
3. Storage (for example, required capacity for firmware or audit logs)
4. Power (for example, available power in remote devices)
5. Personnel (for example, impact on time spent on average maintenance)
6. Financial (for example, cost of bulk devices)
7. Temporal (for example, rate case limitations)

6.9 Cyber Security Risks

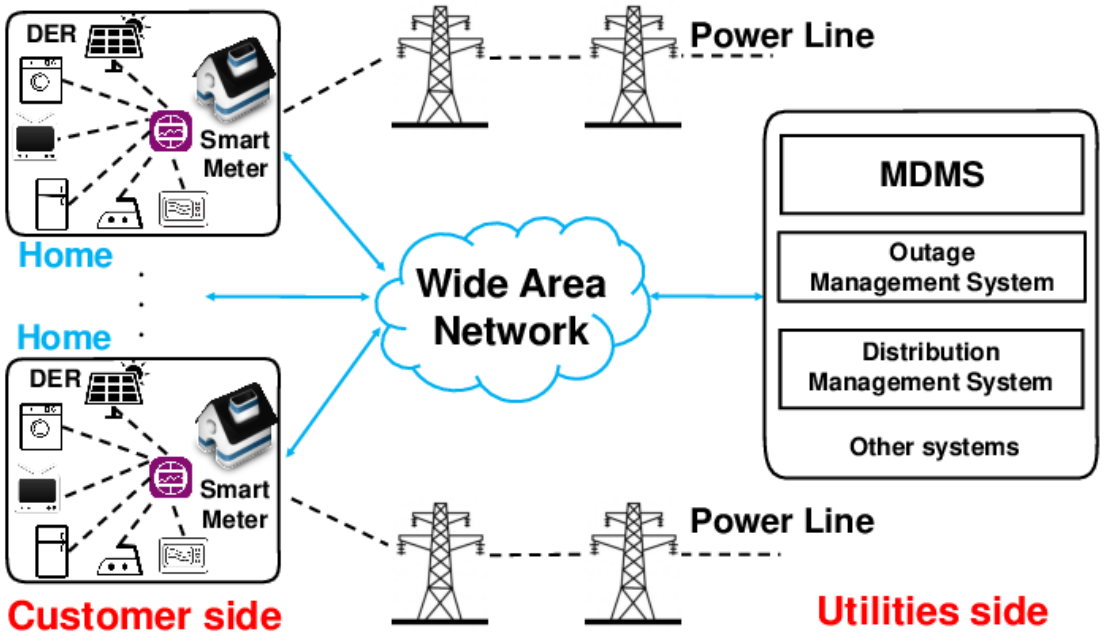
9. Technology
10. Availability
11. Maturity
12. Integration/Interoperability (for example, legacy grid)
13. Life - cycle
14. Interconnectedness of infrastructure
15. Applications (for example, automated user systems and manual procedures that process the information)
16. Information (for example, data, input, processed and output by the information systems in whatever form is used by the business)

6.9 Cyber Security Risks

17. Infrastructure (for example, technology and facilities, that is, hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them, that enable processing the applications)
18. People (e.g., the personnel required to plan, organize, acquire, implement, deliver, support, monitor, and evaluate the information systems and services. They may be internal, outsourced or contracted as required) will consider: time, financial, technical, operational, cultural, ethical, environmental, legal, ease of use, regulatory requirements, scope/sphere of influence.

6.10 Cyber Security Concerns Associated with AMI

- AMI is the convergence of the power grid, the communications infrastructure, and the supporting information infrastructure [3] .
- This system of systems is constituted by a collection of software, hardware, operators, and information and has applications to billing, customer service and support, and electrical distribution. These applications each have associated cyber security concerns as summarized in the next Table.



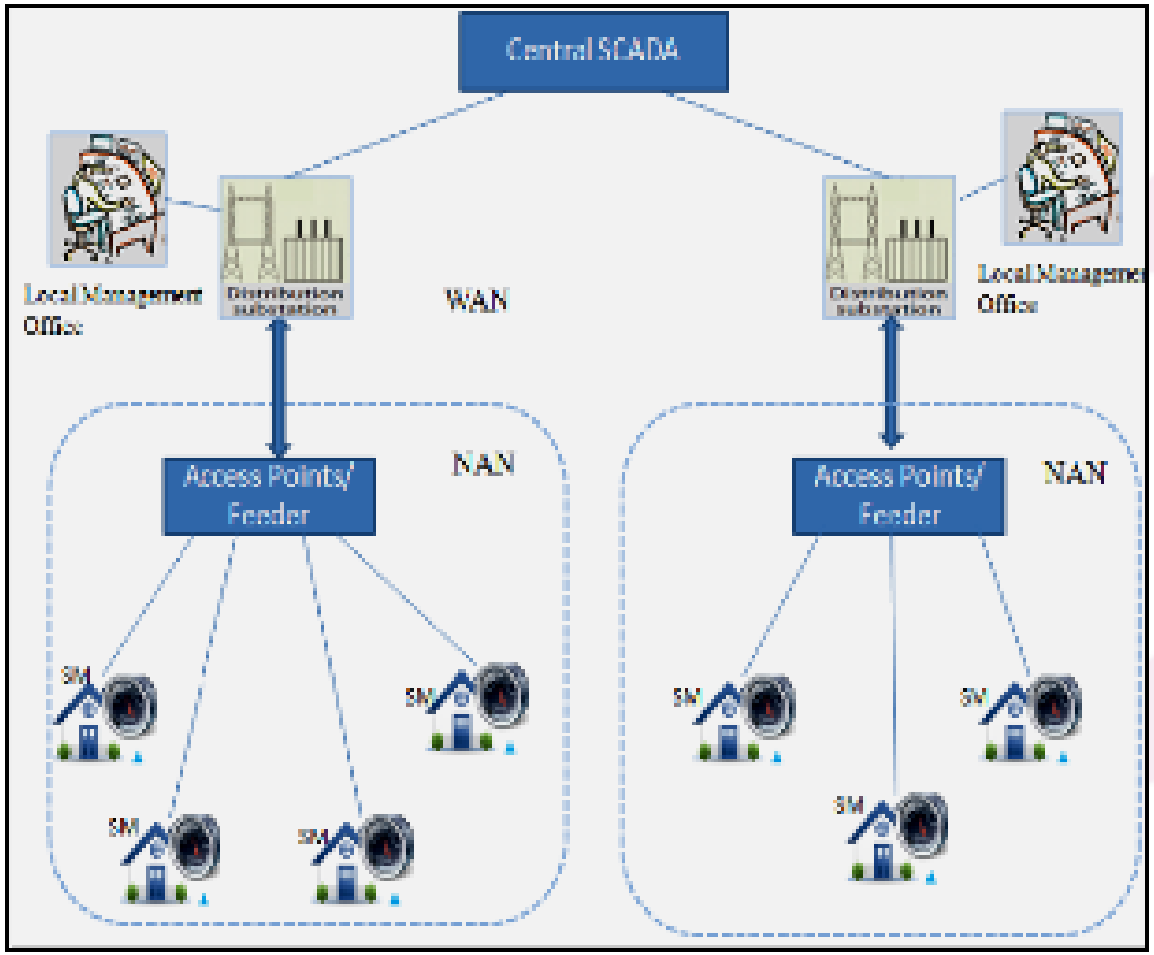
erns Associated with AMI

Cyber Security Concerns Associated with AMI Systems

Application	Cyber-Security Concerns
Market Applications: Billing	• Confidentiality of: ◦ Privacy of customer data, signals and location data • Integrity of: ◦ Meter data ◦ Signals for message and location and tamper indication • Availability of: ◦ Meter data (for remote read), connect/disconnect service
Customer Applications	• Confidentiality of: ◦ Access control for customer equipment via controls, price signals and messages ◦ Privacy of customer data and payments • Integrity of: ◦ Control messaging and message information containing prepayment data, usage data, rate information ◦ Meter data for remote reading ◦ Signals for message and location and tamper indication • Availability of: ◦ Meter data (for remote read), connect/disconnect service, usage data, rate information ◦ Customer payment data and usage balances customer devices
Distribution System Application	• Confidentiality of: ◦ Access control of customer equipment including remote service switch and HAN devices • Integrity of: ◦ Control messaging and message information ◦ System Data • Availability of: ◦ Customer devices ◦ System data

6.10 Cyber Security Concerns Associated with AMI

- The development of the security domain for AMI systems is addressed in Reference 3 and a security domain model was developed to bound the complexity of specifying the security required to implement a robust, secure AMI solution and to guide utilities in applying the security requirements to their AMI implementation.
- The services shown in the next Table are descriptions of each of the six security domains. Each utility's AMI implementation will vary based on the specific technologies selected, the policies of the utility, and the deployment environment.



6.10 Cyber Security Concerns Associated with AMI

Security Domain	Description
Utility Edge Services	All field services applications including monitoring, measurement and control controlled by the utility
Premise Edge Services	All field services applications including monitoring, measurement and control controlled by the customer (the customer has the control to delegate to third party)
Communications Services	Applications that relay, route, and field aggregation, field communication aggregation, field communication management information
Management Services	Attended support services for automated and communication services (includes device management)
Automated Services	Unattended collection, transmission of data and performs the necessary translation, transformation, response, and data staging
Business Services	Core business applications (includes asset management)

AMI Security Domain Descriptions

6.11 Mitigation Approach to Cyber Security Risks with AMI

- This process of mitigation of errors or sources of insecurity includes the following:

1. Identifying and classifying the information that needs to be protected
2. Defining detailed security requirements
3. Reviewing the proposed security architecture that is designed to meet the requirements
4. Procuring a system that is designed to meet the specified security requirements and includes the capability to be upgraded to meet evolving security standards
5. Testing the security controls during the test and installation phase
6. Obtaining an independent assessment of the security posture before deployment
7. Developing a remediation plan to mitigate the risks for identified vulnerabilities

6.11 Mitigation Approach to Cyber Security Risks with AMI

8. Installing a system with built- in management, operational, and security controls
9. Monitoring and periodically assessing the effectiveness of security controls
10. Migrating to appropriate security upgrades as security standards and products mature
11. Monitoring of communication channels
12. Monitoring spike in usage (meter reading) to detect possible failures or tampering with the devices
13. Making sure devices synchronize with the network within a given time frame to detect tampering, potential problems, and device failures.
14. Penetration testing will be performed using the latest hacking techniques, to attempt to break into the systems, identifying possible vulnerabilities, and remotely validating the authenticity of the software running in the meters.

6.12 Cyber security and improving methodology for other users

- Every communication path that supports monitoring and control of the smart grid is a two-way communication path.
- Each path is a potential attack path for a knowledgeable attacker. There are many potential entry points physically unprotected.
- Wireless networks can be easily monitored by attackers and may be susceptible to man - in - the middle (MitM) attacks.
- Security mechanisms in place are intended to prevent unauthorized use of these communication paths, but there are weaknesses in these mechanisms. The history of security in complex networks implies that more vulnerability is yet to be discovered. Thus, the key points include:

6.12 Cyber security and improving methodology for other users

1. Using spot checks on systems to go beyond the current paper chase approach to validating CIP compliance
2. Acknowledging that attackers and malware will find ways around/through current outer - wall – based network defenses, instituting a less - perimeter, defense-oriented approach to security controls with guidance on use of DMZs between internal networks.

Summary

- This chapter has delved into the fundamental tools and techniques essential to the design of the smart grid.
- The tools and techniques were classified into:

(1) computational techniques and

(2) communication, measurement, and monitoring technology.

- Based on the performance measures, that is, controllability, interoperability, reliability, adaptability, sustainability, efficiency, stochasticity, and predictivity, the chapter identified the most suitable applications of the tools.

Summary

- Ongoing work in the critical area of standards development by NIST and IEEE was explained, including consideration of the available standards to be adopted and/or augmented for application.
- The issue of interoperability was presented as it pertains to present grid technologies and the introduction of newer technologies.
- Acknowledging the grid's increasing dependence on communication and information systems is necessary to any discussion of the challenges of developing and deploying adequate cyber security protections.

References

- [1] Appendix B2: “A System’s View of the Modern Grid - Sensing and Measurement”, National Energy Technology Laboratory, 2007
- [2] J.L. Marinho and B. Stott. “Linear Programming for Power System Network Security Applications”, IEEE Transactions on Power Apparatus and Systems 1979 , vol. PAS - 98 , pp. 837 – 848
- [3] A. Englebrecht. Computational Intelligence: An Introduction. John Wiley & Sons, Ltd., 2007
- [4] J.A. Momoh. Electric Power System Application of Optimization, New York: Marcel Dekker, 2001