INTEROPERABILITY, STANDARDS, AND CYBER SECURITY

CHAPTER 8

CONTENTS

INTRODUCTION

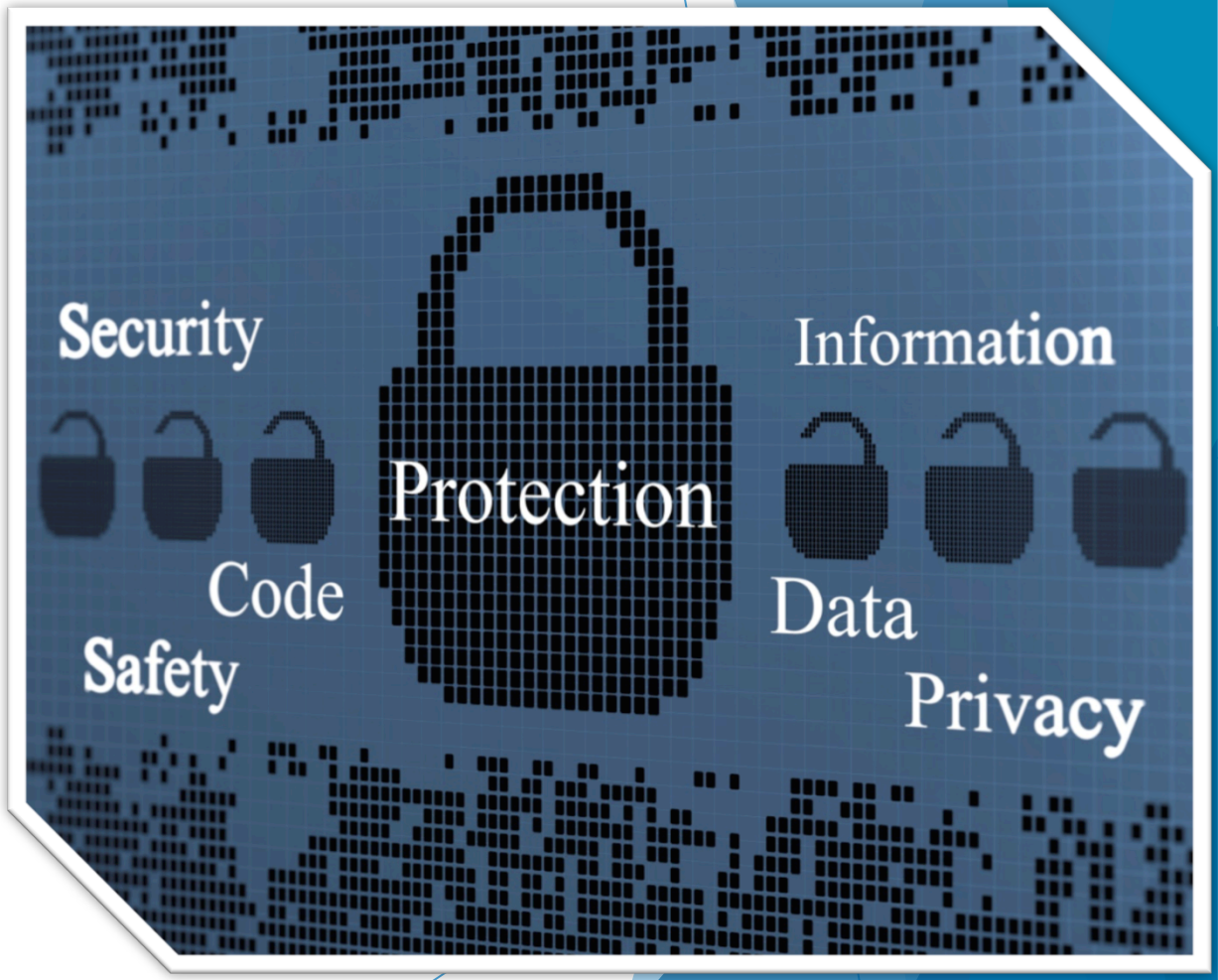
- Deployment of the smart grid ' s components and interoperability requires a substantial overhaul of today ' s standards and protocols.

- Improving the physical and cyber security of the network, which is notoriously vulnerable, is a top priority for the new architectural framework.

INTRODUCTION

- In fact, adding millions connections to a distribution system is no easy task, and power companies are in the precarious position of having to prepare for the future.

- The following discussion outlines the challenges for planners and designers and the role of policy - makers in attaining reliability and secure operations.



INTEROPERABILITY

- *Interoperability* is *" the ability of two or more systems or components to exchange information and to use the information that has been exchanged. "*

- A careful approach will include:
- ✓ Reviewing the activities of governing bodies
- ✓ Reviewing components before deployment
- ✓ Developing internal project standards

INTEROPERABILITY
State -of-the-Art-Interoperability

- There are two elements to interoperability:

  technical and commercial.

- *Technical interoperability* is largely about defining the functionality for gas and electricity metering interfaces providing smart metering (format and data content) service requirements.
- The definition of technical interoperability will depend on the market model the use of smart metering.

INTEROPERABILITY
State -of-the-Art-Interoperability

- *In commercial side*, consumer engagement essential to delivering consumer benefits will be identified in a cost benefit analysis.
- *Demand-Side Menagement (DSM)* refers to all investments and activities that effect customers' load shapes and usage.

INTEROPERABILITY
Benefits and Challenges of Interoperability

- Interoperability allows a network to seamlessly and autonomously integrate all components and the minimization of human intervention in this process is an important benefit of this functionality.

INTEROPERABILITY
Benefits and Challenges of Interoperability

- The challenges include the need for technical enhancement of the network, adoption and adaptation of existing technologies, and development and implementation of comprehensive standards.
- Procedures to address vandalism, hacking, and malicious attacks will require the development of security protocols for authentication and validation before access is granted.

INTEROPERABILITY
Model for Interoperability in the Smart Grid Environment

- The following illustrates a conceptual model of the smart grid developed by the Grid Wise Architecture Council (GWAC).

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

INTEROPERABILITY
Model for Interoperability in the Smart Grid Environment

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

INTEROPERABILITY
Interoperability and Control of the Power Grid

- To upgrade to a smart system, the network should be outfitted with equipment that can detect problems, report back to the utility, receive control or restorative commands, and execute them.
- Control centers must be able to connect to machines that have smart technology to facilitate effective performance with little or no interruptions.
- Ultimately, the user/customer should have some degree of autonomy over consumption with a faster, more effective response to supply disruptions.

STANDARDS

Many standards bodies:

- 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),
- The World Wide Web Consortium (W3C)

are addressing interoperability issues for a broad range of industries, including the power industry.

TABLE 8.1. Summary of Relevant Standards for Smart Grid Developed by Key Standards Bodies [4]

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.	IEEE 802.3	• Ethernet
	Standards developed in the area of communications and interoperability.	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

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

STANDARDS
Approach to Smart Grid Interoperability Standards

The roadmap for interoperability by NIST includes the following applications:

- Demand Response and Consumer Energy Efficiency
- Wide Area Situational Awareness
- Electric Storage
- Electric Transportation
- Advanced Metering Management
- Distribution Grid Management
- Cyber Security
- Network Communications

TABLE 8.2. Standards for the Various Electric Grid Levels

Level	Standard	Description	Application
Transmission /Distribution Level	IEEE Standards for Synchrophasors for Power Systems (IEEE C37.118-2005)	This standard defines synchronized phasor measurements used in power system applications. It provides a method to quantify the measurement, tests to be sure the measurement conforms to the definition, and error limits for the test. It also defines a data communication protocol including message formats for communicating this data in a real-time system.	Phasor measurement units communication
Transmission /Distribution Level	IEEE Standard for Interconnecting Distributed Resources with the Electric Power System (IEEE 1547-2003)	Itemizes criteria and requirements for the interconnection of distributed generation resources into the power grid.	Physical and electrical interconnections between utilized and distributed generation.
Transmission /Distribution Level	Common Information Model (CIM) for Power Systems (IEC 61968/61970)	Describes the components of a power system and power system software data exchange such as asset tracking, work scheduling and customer billing at an electrical level and the relationships between each component.	Application level energy management system interfaces.
Distribution	Communication networks and systems in substations (IEC 61850, Ed. 1 - 2009) IEC 61850	Standard for the design of electrical substations which addresses issues of interoperability, integration, intuitive device and data modeling and naming, fast and convenient communication. It includes abstract definitions of services, data and common data class, independent of underlying protocols.	Telecontrol /Telemetering Substation automation
Distribution /End User	Advanced Metering Infrastructure (AMI) System Security Requirements—AMI-SEC (June 2009)	Provides the utility industry and vendors with a set of security requirements for Advanced Metering Infrastructure (AMI) to be used in the procurement process, and represent a superset of requirements gathered from current cross-industry accepted security standards and best practice guidance documents.	Advanced metering infrastructure and SG end to end security
Distribution /End User	American National Standard For Utility Industry End Device Data Tables (ANSI C12.19-2008)	Defines a table structure for utility application data to be passed between an end device and a computer. Does not define device design criteria nor specify the language or protocol used to transport that data. The purpose of the tables is to define structures for transporting data to and from end devices.	Revenue metering information model

SMART GRID CYBER SECURITY

- Cyber security is a concept that has become increasingly prevalent with the development of the smart grid technology 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.

SMART GRID CYBER SECURITY
Cyber Security State of the Art

- The underlying concept is that security should be built - in, not added - on. This strategy includes:

- 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).
- Identification of relevant threats and the consequences/impacts if the confidentiality, integrity, availability, or accountability of the system data flows are compromised.

SMART GRID CYBER SECURITY
Cyber Security State of the Art

- Facets of the cyber security include:

- Security assessment and hardening of the existing systems
- Vulnerability(Güvenlik açığı) assessment
- Disaster recovery
- Intrusion (İhlal) detection incident response
- Event logging, aggregation, and correlation

  (Olay günlüğü, toplama ve korelasyon)

TABLE 8.3. Threats Facing the Electric Power System

	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

SMART GRID CYBER SECURITY
Cyber Security Risks

- Cyber security risks appear in each phase of the project life - cycle and include risks to managerial, operational, and technical processes.
- The following trade - off must include the considering cyber security risk:

- *Other business or non - functional requirements*
- *Performance* (for example, response time)
- *Usability* (for example, complexity of interactions for users)
- *Upgradability* (for example, ease of component replacement)
- *Adaptability* (for example, ease of reconfiguration for use in other applications)

SMART GRID CYBER SECURITY
Cyber Security Risks

- *Effectiveness* (for example, information relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent, and usable manner)
- *Efficiency* (for example, the provision of information through the most productive and economical use of resources)
- *Confidentiality* (for example, protection of sensitive information from unauthorized disclosure)
- *Integrity* (for example, accuracy, completeness, and validity of information in accordance with business values and expectations)

SMART GRID CYBER SECURITY
Cyber Security Risks

- *Availability* (for example, information being available when required by the business process)
- *Compliance* (for example, complying with the laws, regulations, and contractual arrangements)
- *Reliability* (for example, the provision of appropriate information for managementto operate the entity and exercise its fi duciary and governance responsibilities)

SMART GRID CYBER SECURITY
Cyber Security Risks

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

- *Constraints*
- *Computational* (for example, available computing power in remote devices)
- *Networking* (for example, bandwidth, throughput, or latency)
- *Storage* (for example, required capacity for firmware or audit logs)
- *Power* (for example, available power in remote devices)

SMART GRID CYBER SECURITY
Cyber Security Risks

- *Personnel* (for example, impact on time spent on average maintenance)
- *Financial* (for example, cost of bulk devices)
- *Temporal* (for example, rate case limitations)
- *Technology*
- *Availability*
- Maturity
- Integration/Interoperability (for example, legacy grid)
- *Life – cycle*
- *Interconnectedness of infrastructure*

SMART GRID CYBER SECURITY
Cyber Security Risks

- *Applications* (for example, automated user systems and manual procedures that process the information)
- *Information* (for example, data, input, processed and output by the information systems in whatever form is used by the business)
- *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)

SMART GRID CYBER SECURITY

Cyber Security Concerns Associated with AMI

- *Advanced metering infrastructure (AMI) is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers.*
- Each utility ’ s AMI implementation will vary based on the specific technologies selected, the policies of the utility, and the deployment environment.

TABLE 8.4. 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

TABLE 8.5. AMI Security Domain Descriptions

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)

SMART GRID CYBER SECURITY

Mitigation Approach to Cyber Security Risks

- This process of mitigation of errors or sources of insecurity includes the following:
- Identifying and classifying the information that needs to be protected
- Defining detailed security requirements
- Reviewing the proposed security architecture that is designed to meet the requirements
- Procuring a system that is designed to meet the specified security requirements and includes the capability to be upgraded to meet evolving security standards

SMART GRID CYBER SECURITY

Mitigation Approach to Cyber Security Risks

- Testing the security controls during the test and installation phase
- Obtaining an independent assessment of the security posture before deployment
- Developing a remediation plan to mitigate the risks for identifi ed vulnerabilities
- Installing a system with built - in management, operational, and security controls
- Monitoring and periodically assessing the effectiveness of security controls
- Migrating to appropriate security upgrades as security standards and products mature

SMART GRID CYBER SECURITY

Mitigation Approach to Cyber Security Risks

- Monitoring of communication channels
- Monitoring spike in usage (meter reading) to detect possible failures or tampering with the devices
- Making sure devices synchronize with the network within a given time frame to detect tampering, potential problems, and device failures.
- 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.

SUMMARY

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

1. Computational techniques
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.

- 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.


Any
Questions

Thanks for your listening…