USAID
FROM THE AMERICAN PEOPLE

THE UTILITY REGULATOR'S ROLE IN PROMOTING CYBERSECURITY: Resilience, Risk Assessment, and Standards

April 2020
This publication was produced for review by the United States Agency for International Development (USAID). It was prepared by the National Association of Regulatory Utility Commissioners (NARUC).

THE UTILITY REGULATOR'S ROLE IN PROMOTING CYBERSECURITY: Resilience, Risk Assessment, and Standards

Project Title:	Europe and Eurasia Energy Sector Cybersecurity Initiative
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Cooperative Agreement #:	AID-OAA-A-16-00049
Recipient:	National Association of Regulatory Utility Commissioners (NARUC)
Date of Publication:	April 2020

USAID
FROM THE AMERICAN PEOPLE

National Association of Regulatory Utility Commissioners

SANS

IEC®

ACER
Agency for the Cooperation of Energy Regulators

This publication was made possible through support provided by the Energy and Infrastructure Division of the Bureau for Europe and Eurasia under the terms of its Cooperative Agreement with the National Association of Regulatory Utility Commissioners, No. # AID – OAA-A-16-00049. The opinions expressed herein are those of the authors and do not necessarily reflect the views of the US Agency for International Development or the National Association of Regulatory Utility Commissioners.

Acknowledgments

The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards was developed in partnership with the National Association of Regulatory Utility Commissioners (NARUC) and with the generous support of the United States Agency for International Development (USAID).

NARUC would like to express its appreciation to the team of volunteer authors who dedicated their time to preparing this report in order to help energy regulators around the world assess options for improving cybersecurity in the energy sector. It is remarkable to have gathered such a group of technical experts from three organizations on two continents to collaborate in the greater goal of sharing their insights for the consideration of energy regulators.

Lead Authors

- **Stefano Bracco**, Agency for the Cooperation of Energy Regulators (ACER)
  Mr. Stefano Bracco is Knowledge Manager and Security Officer in the Corporate Services at the European Union Agency for the Cooperation of Energy Regulators. He has been working in EU Institutions/Bodies for the past 22 years, focusing on implementation of policies in different areas. He has been a researcher and co-author of papers published in peer-reviewed international journals or presented at international scientific conferences, covering several topics (Energy, Nuclear Energy, Natural Language Processing and Bio-Informatics). He has an extensive knowledge of energy cybersecurity in Europe. He is chairman and co-chairman of Task Forces focusing on cybersecurity for Energy from a Regulatory perspective and a member of the Smart Grid Task Force of the European Commission.

- **Frances Cleveland**, Xanthus Consulting International, on behalf of the International Electrotechnical Commission (IEC) (www.iec.ch) System Committee - Smart Energy - Cyber Security Task Force[1]
  Ms. Cleveland has managed and consulted on Smart Grid information and control system projects in the electric power industry for over 35 years. Her expertise has focused primarily on Smart Grid information interoperability standards, smart inverter functionalities for Distributed Energy Resources (DER), cyber security issues, resilience of the power grid, and integration of systems, including DER, plug-in electric vehicles (PEV), Advanced Metering Infrastructures (AMI), Distribution Automation (DA), substation automation, SCADA systems, and energy market operations. In the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronic Engineers (IEEE), she is:

    - Convenor of IEC TC57 WG15 for IEC 62351 cybersecurity standards for power system operations.
    - Editor for IEC TC57 WG17 for IEC 61850-7-420 information model standard for DER systems, electric vehicles, and distribution automation
    - Lead for Cybersecurity Guidelines TF for the IEC System Committee - Smart Energy (SyC-SE) and Member of WG2, WG3, WG5, and WG6
    - US Technical Advisor to the IEC ACSEC (Cyber Security)
    - Technical Advisor to the IEC TC 57 for WG17 (Distributed Resources), WG14 (CIM for Distribution and AMI Integration), WG 03 (RTU telecontrol), WG07 (ICCP), WG15 (Information Security), WG16 (Market Operations), WG19 (Harmonization of TC57 standards)
    - Secretary for IEEE 1547.3 on cyber security recommendations for DER meeting the IEEE 1547 interconnection requirements

[1] http://xanthus-consulting.com/about_xanthus/staff.html

- **Tim Conway**, SANS Institute
  Mr. Tim Conway is Technical Director of ICS and SCADA programs at SANS. Responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Formerly, the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). He is also responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Prior to his work at SANS he worked as an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He has sat on various boards including the RFC CIPC, NERC CIP Interpretation Drafting Team, the National Electric Sector Cybersecurity Organization Resource (NESCOR) and others.[2]

The authors would like to thank former NARUC staff Gizelle Wray and Crissy Godfrey for their guidance and review during the development of this guide.

The authors also thank the following experts in energy regulation for contributing their time and expertise and offering valuable insights throughout the development of the guide.

Expert Review and Advisory Committee

- Lynn Costantini, Center for Partnerships and Innovation, NARUC
- Mike Assante, SANS Institute
- Konstantinos Moulinos, European Union Agency for Cybersecurity (ENISA)
- Ardian Berisha, Energy Regulators Regional Association (ERRA)

[2] https://www.sans.org/security-awareness-training/tim-conway

Table of Contents

List of Figures

Executive Summary

Since 2016, the United States Agency for International Development (USAID)'s Bureau for Europe and Eurasia has taken a leadership position in promoting regulatory and utility preparedness of cybersecurity in defense of critical infrastructure. Through work in Eastern Europe and Eurasia, USAID and NARUC have provided technical information and trainings to promote the capacity of energy regulators to play a leading role in protecting and advancing the energy sectors of their countries.

This guide was initially developed for regulators in Europe and Eurasia to reinforce their knowledge of practical cybersecurity solutions in the face of ongoing threats within the energy sector. [3] However, the questions of how to evaluate risks, assess mitigation measures, and select standards are relevant for regulators around the world.

NARUC's intention in preparing this guide is to provide a consolidated review of multiple cyber concepts that can serve as a nontechnical and user-friendly guide to energy regulatory staff. Regulators are charged with several core functions, such as ensuring security of supply, evaluating utility investment plans, and setting tariffs. As cyber threats continue to evolve, energy regulators need to increase their technical capacities to be able to serve as leaders within their countries and promote coordination among governmental and non-governmental institutions. This guide provides a useful summary of international cyber standards (with more detailed information included in the annex) so that regulators can have a starting point to more easily evaluate options for their national and/or regional contexts.

This guide addresses:

1. Cybersecurity resilience
2. Security by design
3. The difference between information technology (IT) and operations technology (OT) environments
4. Risk assessments
5. Standards to consider when developing regulations and frameworks

This guide is sequenced to help energy regulators understand core cyber principles so they can develop and implement appropriate, country-specific regulatory structures and mechanisms. The principles are essential building blocks to assist stakeholders to adapt to a constantly changing cyber threat environment and evolving technologies. There are myriad standards already in existence, so regulators and utilities should draw from those, analyze lessons learned, and customize their structures and mechanisms to their own contexts.

While it may seem a daunting task to figure out where to begin, regulators should start with the *What* as a basis. Some standards are focused on high-level organizational security requirements and more detailed recommended controls (*What*), whereas other standards focus on the technologies that can be used to supply these cybersecurity controls (*How*).

The attached annex outlines some key existing cybersecurity standards and best practices organized by type (*What* and *How*) and the processes to take to move towards compliance. NARUC believes that the annex serves as a useful resource tool for regulators and other decision makers to evaluate the myriad of standards that have already been created. These can be considered as starting points and can then be adapted to local contexts.

Regulators should also engage in continuous education and capacity building efforts, sharing information, and drawing upon lessons learned. Just a few of the key recommendations that are addressed in this guide include:

[3] USAID's Europe and Eurasia Bureau began to focus heavily on cybersecurity after the 2015 Ukrainian power grid cyberattack. Through NARUC and the United States Energy Association (USEA), USAID is addressing cyber threats at both the regulatory and utility levels in the region.

- **Non-prescriptive standards**. The standards that outline *what* must be achieved, not *how* to specifically achieve it, will provide entities the flexibility to build and maintain programs that work for them.
- **Drive the development of standards**. Standards created by the industry and for the industry are necessary for complex operational environments like an electric system. However, in certain circumstances, the regulator will need to step in to drive progress through issuance of mandatory standards.
- **High, medium, and low requirement applicability**. This ensures prudent controls based on risk to the electric system.

In conclusion, regulators and utilities must consider **organizational reform** (corporate culture) first and foremost. The *What* standards target the high-level organizational structure and targeted controls, which is at the core of cybersecurity preparedness.

Introduction

What is the regulator's role regarding cybersecurity and cyber resilience? Should utilities be left to establish their own approaches, or should regulators take the lead to establish cybersecurity and resilience recommendations and/or requirements to assure a secure electrical grid? If the latter, what should cybersecurity and resilience regulations look like? Further, should economic regulators intervene in the technical details of the grid without having a clear mandate for this? This guide is a resource to help regulators navigate the decision-making process as it pertains to cybersecurity and direct their priorities accordingly.

At a minimum, energy regulators have clear mandates to ensure the quality of supply of energy. Whether a blackout is short or long, or occurs from a man-made intervention or a natural cause (i.e., weather), the public wants power restored as quickly as possible. Regulators also review and/or approve rate filings from the utilities. They must balance fair and reasonable rates with utilities' needs for investment. As utilities make investments to increase cyber protection and/or manage recovery after a cyber incursion, the regulators must assess the prudency of these investments.[4]

As energy regulators around the world increasingly embrace their roles and the associated challenges of managing cybersecurity, they continue to recognize increasing responsibilities. Regulators should develop their capacities to contribute to the development of necessary frameworks, including cyber standards and consistent implementation of those standards. Regulators can organize the appropriate governance and enforcement structures to ensure that cyber standards are implemented appropriately.[5]

With this in mind, cybersecurity and resilience against cyberattacks are vital requirements for any business, particularly those responsible for critical infrastructure. Power system operators must continue to manage a rapidly evolving electrical grid and ensure reliability and improved quality of service. However, utility operations are becoming increasingly complicated as they also tackle new market structures, rapidly evolving technologies, and government societal goals (such as increased access and affordability).

It is important to note that, when all stakeholders recognize the importance of cybersecurity preparedness, a voluntary approach to standards and risk assessment can be used, which promotes strong cooperation. However, if any of the parties involved in safeguarding critical infrastructure, such as power systems, fail to adhere to the agreed-upon objectives and roles under a voluntary approach, then a mandatory approach may become necessary. There is an additional level of assurance with a mandatory approach because utilities can feel confident that there will be a provision for cost recovery by following set standards. Regulators also may find it easier to audit the utility for adoption and implementation of mandatory standards. The information in this paper is for regulators who are being asked to address the cybersecurity issues of utilities and other businesses to minimize the likelihood of cyberattacks and, in particular, the impacts of "successful" cyberattacks.

These concepts provide the framework for implementing a strong cybersecurity environment and provide the business case for how standards can meet cyber resilience needs.

[4] See also Ragazzi et al., *Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators*.

[5] This is not intended to downplay the critical importance of utilities in the development and implementation of these frameworks. As this guide will show, utilities will want to engage with regulatory commissions during this process to ensure that their interests are protected and understood by the stakeholders involved. Utilities and regulators will need to embark on this important journey together, and to begin an important dialogue that addresses these complex issues.

Historically, commissions and utilities in some partnering countries in the region have remained siloed due to the political environment. It is, however, imperative that this tradition begin to evolve as the issues become more complex in this dynamic environment. The advancement of technology, the integration of supply, and the threat of cyber attacks means that both parties will need to combine their expertise to appropriately strategize and communicate best practices. Regulators will need to ensure that an environment of collaboration exists with utilities and that each party is met with mutual respect and understanding of their shared goals.

Critical Concepts on Cybersecurity and Resilience for Regulators

As a start, it is vital that regulators, as well as utilities, understand the five critical cybersecurity and resilience concepts discussed in-depth in the following sections:

Five Critical Concepts on Cybersecurity and Resilience
Concept #1: Resilience is the strategy for ensuring business continuity
Concept #2: Security by design is the most cost-effective approach to security
Concept #3: IT and OT are similar but different
Concept #4: Risk assessment, risk mitigation, and continuous updates of processes and incident notification are fundamental to improving security
Concept #5: Cybersecurity standards and best practice guidelines for OT environments should be used to establish security programs and policies

2.1 Cyber Resilience as the Overall Strategy for Ensuring Security of Supply

Cybersecurity is far more than preventing attacks by malicious hackers. The modern perspective on cybersecurity also entails improving the resilience of the power system by mitigating threats from security incidents that affect cyber assets and could disrupt operations.[6] Specifically, the concept of cyber resilience calls for plans for ensuring safety and reliability before incidents (identify and prevent), during incidents (detect and respond), and after incidents (recover).[7]

The mitigation of threats to resilience combines cybersecurity techniques (such as access control, detection of anomalous behavior, and incident logging) with organizational and engineering strategies, which allow the organization to prepare for and adapt to changing conditions and to withstand, and recover rapidly from, disruptions. These engineering strategies include traditional power system reliability measures, such as redundant equipment, contingency analysis, and backup systems. They should be augmented to address cyber asset vulnerabilities, such as planning for the loss of multiple assets, utilizing isolation capabilities to limit cascading effects or attacks, and even training personnel in manual operation procedures for emergency situations when an automated system is down or needs to be disabled.

Since human errors and misconfigurations are the most common cybersecurity events, checks on data entry or control commands should be included in resilience support. Because persons with detailed knowledge of power system operations are the most dangerous attackers, additional engineering strategies may need to be deployed to mitigate threats from this type of attacker, such as two-factor authentication and continuous monitoring of networks for anomalous traffic. In addition, storms can affect not only the power system, but its cyber assets. Therefore, backup generators, communication networks, and spare cyber equipment should be located in secure sites, yet easily accessible when needed.

Regulators have an additional consideration when guiding utilities on cybersecurity, and they can take advantage of existing standards and lessons learned. For example, the use of a cybersecurity framework (e.g., the NIST Cybersecurity Framework) may be a valid option. A cybersecurity framework can provide a template for

[6] A cyber asset is any equipment with computer processing capability, including controllers of hardware assets, but not the hardware assets themselves (e.g., an electromechanical breaker). Cyber assets can be affected by physical actions (cutting a wire, damaging a transformer), as well as cyber actions (introducing malware, inadvertently entering incorrect data).

[7] Note that the US National Institute of Science and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) is one of many internationally recognized frameworks and serves as an example that has proven successful for many regulators and energy stakeholders. See NIST, *Framework*.

establishing organized security policies for preventing cyberattacks as well as provide guidelines for planning preparedness efforts following the inevitable successful cyberattack or security incident that affects assets. Regulators could suggest that utilities use one such cybersecurity framework to organize their approaches to developing their cybersecurity plans. For example, a summary of key concepts from the National Institute of Standards and Technology (NIST) includes the following:

- Identify assets, threats, vulnerabilities, and potential impacts from a security incident.
- Protect information assets through configuration design, access control, personnel procedures, personnel security training, and appropriate technologies.
- Detect security incidents through continuous monitoring and event detection, as well as assess the severity of security incidents.
- Respond to security incidents, in collaboration with national computer security incident response teams (CSIRTs), to mitigate the impacts of incidents through prior planning and the application of mitigation procedures and technologies.
- Recover from security incidents by planning, improving, and reassessing threats and vulnerabilities.

2.2 Security by Design as the Most Cost-Effective Approach

The cost of cybercrime continues to increase each year. In a single day there are about 780,000 data records that are lost due to security breaches, 33,000 new phishing messages, and 4,000 ransomware attacks globally.[8] Analysts estimate the total 2019 cost of cybercrime at $2 trillion, which is a fourfold increase from 2015.[9]

With this in mind, designing security into cyber systems from the beginning is the most cost-effective approach to cybersecurity, since it minimizes risk and financial expenditures. Security by design permits more consistency across all systems with well-defined configurations of networks and information flows. Users will have consistent procedures to follow, rather than ad hoc security approaches.

Effective security cannot just be patched on to existing power system operational processes, but should be an intrinsic part of system designs and configurations, operational procedures, and information technologies. Inserting security procedures and technologies after initial system design is also costly because such insertions are often ad hoc and require major modifications to system configurations as well as significant retraining of personnel. If designed from the beginning, security becomes a normal part of the life cycles of power system cyber assets and operational procedures.

The term security by design covers many aspects,[10] such as system configurations, network configurations, planning procedures, and data management. Many of the benefits of security by design can be realized even if systems are just being upgraded or slowly replaced, since having a well-thought-out plan is effective for including security at each upgrade or replacement step.

[8] Lewis, *Economic Impact.*

[9] Morgan, "Cyber Crime."

[10] Security by design is a concept created to address how to protect the core pillars of information security, confidentiality, integrity, and availability. The Open Web Application Security Project (OWASP) created a comprehensive list of security by design principles that cyber professionals should adhere to. Following OWASP's principles can assist utilities in securing and drastically reducing the risk of successful cyberattacks. See OWASP Foundation, "Security by Design."

Examples of the security by design principles include: (1) minimize attack surface area, (2) establish secure defaults, (3) apply the principle of least privilege, (4) fail securely, (5) do not trust services, (6) apply separation of duties, (7) avoid security by obscurity, (8) keep security simple, (9) fix security issues correctly, and (10) apply defense-in-depth principles.

These principles are considerations that require their own detailed analysis, but for the purposes of this paper are listed for informational purposes only.

Some of the aspects of security by design involve becoming aware of potential threats and vulnerabilities before finalizing system and network configurations. For example, if the most critical systems can be located within a well-defined electronic security zone, also known as an electronic security perimeter, access to these critical systems can be designed to be limited, protected, and carefully monitored (see Figure 1). Such a design reduces "attack surfaces" that could be exploited by malicious entities or simply misused by accident.

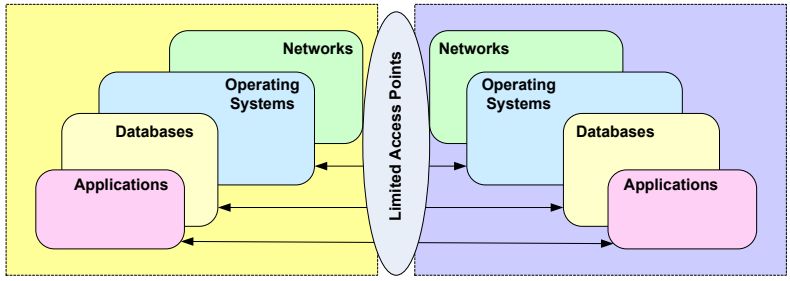

Figure 1: Security by Design: Electronic Security Perimeters
Source: Xanthus Consulting International

Security by design can improve possible security mitigation actions, since planning for the inevitable successful security breaches (failure scenarios) leads to training and contingency actions and the development of strategies to mitigate these potential breaches. Further, in security by design scenarios, access control can be implemented down to the data levels, not just to the system levels, which allows true end-to-end security between users and their access to data, thus limiting very precisely who can monitor and/or control what data. The same access control can also be applied to the data flows between software applications.

Flows of valid information to the right places within the right times are the most critical requirements for operational environments. Security by design can ensure that this level of assurance is provided by secure protocols natively supported by systems as part of the core capabilities of the systems. For example, validating information can help mitigate the threat of persons who have the knowledge to disrupt power system operations by ensuring that data verification is engineered within each system. At the same time, access to data may be constrained due to security policy requirements.

Security policies established during the design of systems can mandate procedures for purchasing and updating systems. With such security policies, the configurations of communication networks can be carefully designed, and the security of the supply chain can be better known and managed.

Nonetheless, it is well recognized that security cannot be designed quickly for existing systems, particularly since power system components may have vastly different life cycles. Therefore, it is crucial that, even for existing systems, security should be designed into operational procedures and should provide a well-defined methodology for system upgrades.

Regulators can communicate with utilities to develop a security by design approach to cybersecurity, including the transitions of legacy equipment to more secure equipment. Regulators could recommend that utilities identify security by design principles they are or will be implementing. For instance, regulators can request information on:

- Utility security policy for operations, covering overall security organization and procedures.
- Roles that personnel will be assigned (e.g., system operator, maintenance personnel, protection engineer, security engineer) and their responsibilities, privileges, and constraints (least privilege and separation of duties).
- Techniques for ensuring that role-based access control strictly enforces those privileges and constraints.
- Personnel security vetting and training procedures.
- Operational system configurations, including electronic security perimeters, access points, and technologies for security flows of information across perimeters.
- Plans for logging, assessing, and reporting different levels of security incidents.
- Plans for operating the power system after different types of incidents (e.g., equipment failures, personnel mistakes, natural disasters, and cyberattacks).

- Plans for recovering from security incidents.

Depending on the situation in each country, this security by design may include voluntary standards or may need a stronger framework to add clarity and confidence by enacting mandatory standards.

2.3 IT vs. OT: Differing Security Requirements in the Information Technology and Operational Technology Environments

In traditional business environments, the IT department is considered the expert in all matters related to cybersecurity. For most corporate cyber assets, the IT department is well placed to understand and address threats and to design methods to minimize vulnerabilities and respond to attacks. In general, since corporate cyber assets are mostly vulnerable to breaches of the confidentiality of the information contained within computer systems, most IT security focuses on preventing access to sensitive data.

However, in OT environments such as power systems, deliberate cybersecurity incidents or inadvertent errors and failures of cyber assets can also have physical repercussions because power systems are cyber-physical systems. The aspect with the greatest consequences is safety; the deliberate or inadvertent mis-operation of a cyber asset could cause equipment damage, personal harm, or even death. The second most important aspect is the reliability of the power system. Although power systems have always been built with the reliability of their physical assets (e.g., breakers, transformers, power lines) as the most critical design requirement, the reliability of the supporting cyber assets must nowadays also be designed to the same degree.

Therefore, for OT, as illustrated in Figure 2, availability and data integrity are the most critical requirements (where sometimes availability is the most important, while at other times data integrity is paramount).[11] With their experience in reliability, it is often the experts in power system operations who best understand what responses to cyber asset incidents may or may not be appropriate and, combined with IT cyber expertise, how best to utilize engineering strategies and operation of the physical electrical system to minimize the impacts of such cyber asset incidents.

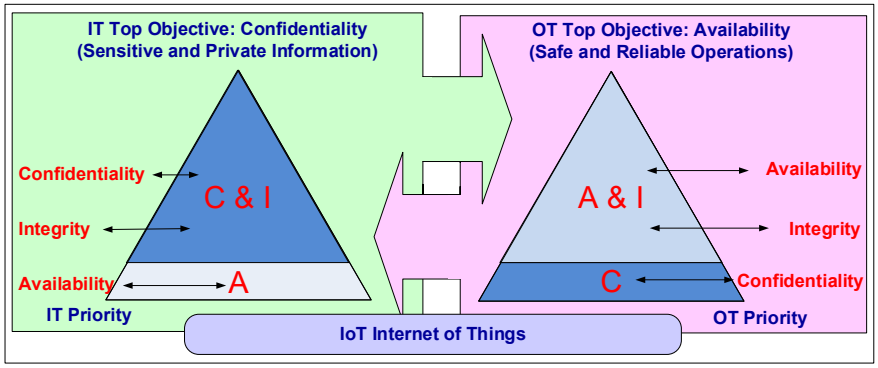

Figure 2: IT and OT Objectives are Similar but Different
Source: Xanthus Consulting International, derived from [1]

When securing operational environments, some very specific security challenges arise. For instance, the need for high availability of both physical and cyber assets requires engineering designs with a focus on redundancy, high-reliability, and high-performance requirements of these assets. These security requirements may necessitate changes in network configurations and information flows, such as the use of security perimeters, demilitarized zones, and firewalls. In addition, very high-speed real-time processes involving peer-to-peer interactions, autonomous actions, time sensitivity, and other characteristics, require different security solutions from those typically used in IT.

At the same time, operational constraints must be taken into account in these designs. For instance, constraints on equipment resources (e.g., timing, bandwidth, network access) can impact the cybersecurity procedures and

[11] Availability and data integrity and have been subject to a battle over whether availability supersedes integrity. Certainly no one would continue to make a process 100 percent available to an adversary. However, in a situation where the data integrity of a process cannot be ensured, the likely course of action includes moving off-line safely until it is possible to gain ensure integrity and validate that the process was not being mis-operated. In reality, these two priorities must be quickly balanced and considered. This is noted in Figure 2.

technologies that could be used. In particular, heavy encryption techniques or online access to certificate authorities are generally not possible for operational assets. In addition, the timing for system maintenance and equipment updates or upgrades is constrained by power system operational requirements, such as only having short windows during the spring or fall for taking equipment out of service.

Another constraining element for applying cybersecurity reflects the large amount of legacy equipment with long life cycles that cannot be easily upgraded to include cybersecurity techniques. In addition, given the criticality of power system operations, security should not prevent operational actions. In particular, emergency actions and "break the glass" scenarios must be built into security procedures.

Another major difference in securing an operational environment as opposed to a traditional business environment is the need to utilize Internet-of-Things (IoT) networks and technologies, in particular to interact with customer sites for monitoring and managing distributed energy resources (DER) and communicating with smart meters. This use of IoT implies that utilities can no longer rely on only their own proprietary communication networks, but they must nonetheless still apply cybersecurity techniques to their interactions across public networks using well-known communication technologies.

Regulators can suggest that utilities encourage their IT and OT groups to work closely together to develop an optimal and coordinated approach to cybersecurity and resilience and to discuss any security requirements. In particular, as such a project evolves, these experts could jointly perform threat, vulnerability, and impact assessments to determine different types of risks and how best to utilize both cyber and power engineering methods and operations to minimize the impacts of incidents. Such assessments would use the resilience and security-by-design approaches previously described, but would be sure to use the expertise of both IT and power system experts.

Other considerations include holistic approaches that will allow utilities to cultivate and promote cross-functional knowledge of IT and OT security. This includes promoting a cyber culture through safety-culture and safety-hygiene courses; tailor-made trainings, security; and safety education through trainings, exchanges, and exercises. Regulators should consider these practices when assessing the compliance culture of utilities in addition to risk assessments.

2.4 Risk Assessment, Risk Mitigation,[12] and Life Cycle Processes and Incident Notification

Risk assessment, risk mitigation, and life cycle continuous update of processes and incident notification are fundamental to improving security. Using business requirements (financial, brand, operation, societal), derived from methodologies defined in international standards for OT environments, organizations can determine security risk exposure.

The strategy for risk mitigation must take into account operational constraints and integrate those of the OT networks. The constraints of OT networks often include the protection of physical assets and personal safety, as well as constraints related to the performance and architecture of the networks. It is important to consider that, in the context of electric utilities, it is the energy processes that provide service to the end customer.

Some assets can cost several million dollars and require more than a year to be replaced, so security measures to mitigate damage to these assets are very important. For the best risk mitigation solutions, integrating the professionals of these environments not as consultants, but directly as part of the team in charge of cybersecurity, is key. This recommendation is valid for all departments or teams of a business such as telecommunications and OT engineers, since the vulnerability to an attack and the possible responses to an attack will need to mobilize all skills to restore the system. The implementation of continuous improvements of security policies, procedures, and technologies becomes vitally important during the continuous life cycle process. By conducting periodic

[12] "Risk" can be defined as a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event. Risk assessments are used to identify, estimate, and prioritize risk resulting from the operation and use of informational systems to organizational operations, organizational assets, individuals, other organizations, and countries at a national level.

Risk mitigation refers to actions aimed at systematic reduction of exposure to a risk (i.e., targets, impact, severity).

security reviews or test scenarios, utilities can better ensure that systems will be kept updated and new mitigation processes will be put in place.

Figure 3 illustrates the general risk management process. The challenge is how to apply these concepts to develop a cybersecurity plan for the operational environment. No single process can meet all requirements, but some general rules are useful on how, when, and for what purpose to apply these cybersecurity standards and guidelines to improve resilience and security of the OT environment.

Regulators can encourage utilities to perform risk assessments to understand the threats and vulnerabilities more clearly and to determine their possible risk mitigation options. These risk assessments can start by covering most operational processes, but then take a more focused look at specific areas of threats and vulnerabilities over time.

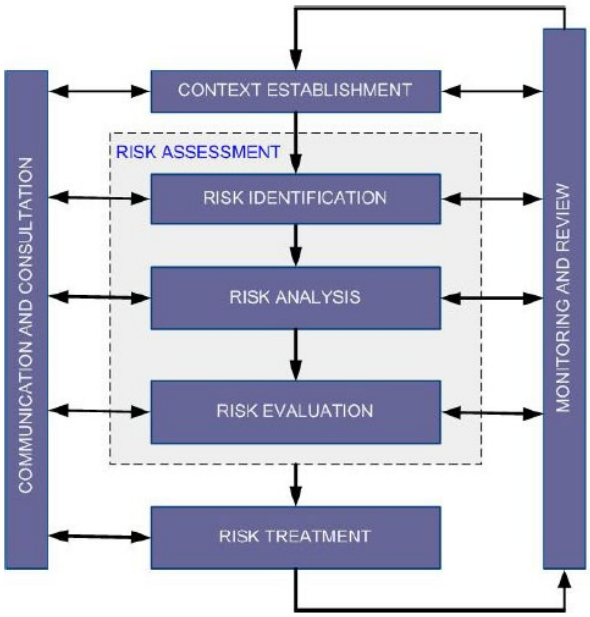

Figure 3: Risk Management Process
Source: ISO/IEC 27005 (2018) [7]

The following list details the key risk assessment steps:

- Collect the high-level business and regulatory requirements that apply to the OT environment, and identify the impacts (safety, economics, operational) if the requirements are not met.
- Choose a risk assessment method, based on organizational requirements and constraints.
- Choose the scope of the risk assessment to be performed, based on the boundaries of the targeted systems, including not only the systems internal to the boundaries, but also the interfaces with other OT and non-OT systems.
- Understand that threats can be associated with physical equipment, information, processes, interactions, configurations, and other assets.
- Balance the risk against the mitigation costs of reducing that risk to an acceptable level. Internal security policies must determine the acceptable risks.[13] Risk mitigation may involve an update to the risk assessment to ensure that the risks are indeed acceptable, particularly if many changes have been made as part of risk mitigation.
- Apply security controls to mitigate the risks that were identified.
- Select and implement risk mitigation solutions across systems after completing the risk assessment.
- Determine what actual control implementations (i.e., which specific procedures and/or technologies and/or commercial products) should be applied for each type of security control.
- Monitor all control solutions over time to ensure continued effectiveness and to determine if possible attacks have potentially overcome the control solutions.

[13] The determination of risk tolerance is at the core of the challenge that utilities and regulators face. There are various risk assessment tools and maturity models that can be employed to help utilities quantify their risk tolerances and allow regulators sufficient information to provide verification.

2.5 Cybersecurity Standards and Best Practices for the Energy Industry

Given the complexity of business processes and the wide variety of cyber assets used in the energy environment, no single cybersecurity standard can address all security requirements, security controls, resilience strategies, and technologies. Some standards and guidelines are focused on high-level organizational security requirements and more detailed recommended controls (*What*), whereas other standards focus on the technologies that can be used to supply these cybersecurity controls (*How*).

Although many additional documents are available from national or international organizations such as NIST, the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), and the North American Electric Reliability Corporation (NERC), Figure 4 outlines cybersecurity standards and best practices organized by type (*What* and *How*) and the processes needed to come into compliance.

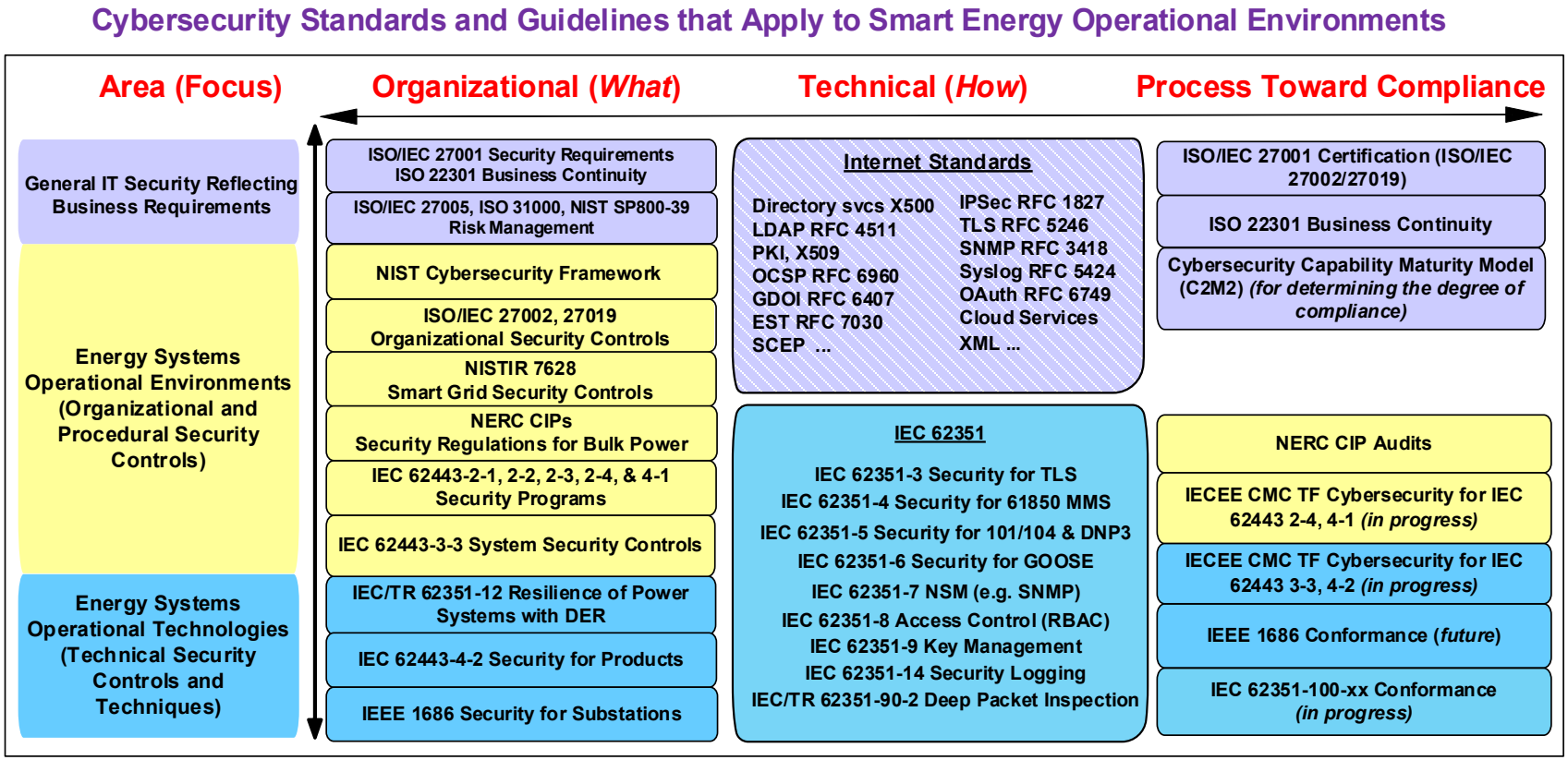

Figure 4: Key International Organization for Standardization (ISO)/IEC Cybersecurity Standards and Guidelines
Source: Xanthus Consulting International.

The most relevant high-level "*What*" cybersecurity standards include:

- ISO/IEC 27001 Security audit (general at information-system level)
- ISO/IEC 27002 Further specifies controls defined in ISO/IEC 27001
- ISO/IEC 27019 Focused specifically for industrial control systems (ICS)/supervisory control and data acquisition (SCADA) (OT)
- NIST Cybersecurity Framework
- NIST Interagency Report (NISTIR) 7628 Smart Grid Security Guidelines
- NERC Critical Infrastructure Protection (CIPs)
- IEC 62443-2-1, 2-2, 2-3, 2-4, and 4-1 Security programs
- IEC 62443-3-3 System security requirements
- IEC 62443-4-2 Security for products
- IEC 62351-12 Resilience of the power system with DER
- IEEE 1686 Security for substations

The technical-level standards provide standardized methods and technologies on "*How*" these cyber assets could be made more secure and resilient. These standards include many internet standards, as well as the specific IEC 62351 security standards for different communication protocols, role-based access control, network and system monitoring, key management, logging, and deep packet inspection.

Most of these standards have (or are planned to have) conformance testing and certification standards associated with them. These cybersecurity standards and guidelines are described in more detail in the Annex.

Regulators could suggest that utilities select the security standards and guidelines that are the most pertinent for each of the levels of security assessments, security procedures, and security technologies.

In particular, regulators could encourage a rigorous approach to using high-level cybersecurity standards to better ensure that security requirements are well understood and that security controls are applied appropriately across all areas. Regulators could also suggest that utilities review the technical-level standards to best determine which are appropriate to meet specific security requirements.

Alternatively, it is beneficial for regulators to explore initiatives and guidelines that map security standards from many different sources to provide a complete point of reference, thus ensuring all necessary security controls are considered.

Cybersecurity Procedures That Regulators Can Recommend To Secure Utility Operations

Below are preliminary steps, while the Annex highlights specific internationally recognized standards that can be considered for future regulatory implementation.

3.1 Preliminary Steps

Regulators can suggest some very preliminary steps to be taken by utilities even while they develop a more formal cybersecurity process. These include:

- Become familiar with cybersecurity standards, including both international standards and any regional or national standards.
- Develop an inventory of all cyber assets, including systems, networks, databases, intelligent electronic devices, gateways, and any device with "intelligence."
- Determine what OT and IT areas/departments have already implemented some type of cybersecurity measures, and which have not addressed cybersecurity at all. This includes the management of user accounts, control center systems, substation systems and equipment, and other areas.
- Start monitoring the status of key cyber assets with notifications or alarms. Even without a full risk assessment, just having visibility into the status of cyber assets can be very important.
- Isolate the operations networks from the corporate networks, and certainly from the Internet: use physical separation where possible, firewalls for all access points, and security perimeters around substations and control centers with access only through firewalls.

Regulators may very well be at this stage as they implement cybersecurity processes. It is important to note that these preliminary steps will involve strategic relationship building. It is encouraged that regulators develop the necessary relationships with stakeholders. These stakeholders include both external bodies (e.g., ministry staff, utility CEOs) and internal commission staff to provide support during this extensive process. The importance of cybersecurity and the large effort that will need to be made by regulators and utilities will require long-term support and a vision of maintaining secure systems. Once regulators and utilities can build and maintain a relationship to support implementation of cybersecurity standards, their efforts will have long-lasting effects.

3.2 Risk Assessment Procedures

Utilities have the important task of making power systems safe through risk assessments. Performing risk assessments can result in a number of outcomes, such as: (1) power system designs that include monitoring of these power system assets; (2) redundancy of certain equipment, including security fences around substations and other dangerous sites to isolate equipment from unauthorized access; and (3) clear operating rules for normal and emergency situations. The same type of risk assessment can be undertaken for cyber assets. While the energy regulator would not be privy to all details from a utility's risk assessment due to confidentiality issues, the regulator should be briefed in such a way as to allow it to assess the preparedness of the utility and consider rate-recovery with respect to investment expenses.[14]

Once some of the preliminary steps have been taken, a risk assessment process should ensue. This risk assessment process consists of the following key steps:

- Collect the high-level business and regulatory requirements that apply to the OT environment, and identify the impacts (safety, economic, operational) if the requirements are not met. These high-level requirements establish the most important conditions that both power systems and their supporting cyber assets must meet.

[14] The *Cybersecurity Evaluative Framework for Black Sea Regulators*, published in 2017, was developed as part of a USAID/NARUC project as an easy-to-use tool for regulators to evaluate utilities' cybersecurity preparedness. The framework was designed to provide a structured way for regulators to assess what level of cybersecurity preparedness utilities have reached and identify areas for improvement. See NARUC, *Evaluative Framework*.

The evaluative framework recommends that regulators take five initial steps and provides 107 sample questions drawn directly from cybersecurity interrogatories conducted by US regulators. The questions focus on 12 core cybersecurity subject areas, and they are designed to elicit responses from utilities that will give regulators enough information to gauge their overall levels of cybersecurity preparedness.

  - Establish internal security policies by determining what risks are acceptable and identifying the procedures and the catalog of controls to address unacceptable risks.

- Establish the risk assessment process based on best practices and well-established standards, using cyber frameworks (such as the ISO/IEC 27000 series) to ensure all types of risks are identified.
  - Conceptually, risk assessments identify the financial and other impacts for mitigating the risk, and then assess the balancing of that risk (impact versus likelihood of event) against the mitigation costs for diminishing that risk.
  - However, practically, there are a number of methods for assessing risks that have been described in different standards or guidelines. Some methods are more quantitative than others, but most still rely on the experience of power system and cybersecurity experts to identify the vulnerabilities, likely threats, possible impacts, and potential mitigating configurations, procedures, and/or technologies relevant to their systems.
- Perform risk assessments on the areas of interest (e.g., for a particular project) using methods identified in risk assessment guidelines and based on the impacts from the business and regulatory requirements. The risk assessments must take into account the scope of specific projects and also the project's interfaces with other OT and non-OT systems.
  - Risk assessments can be done at different levels (e.g., for a whole substation or some devices in a substation, or for one small site or a large generating plant).
  - Some risks, such as threats to the safety of personnel, may not have a great financial impact, but would necessarily be rated as highly important.
  - Some other types of risk may not be important enough to apply any specific mitigations.
  - Most types of risks should be evaluated to balance their potential impact and likelihood against the cost of mitigations. Often, one mitigation can minimize the impacts of many risks, such as isolating control networks from corporate networks.
- Determine what actual control solutions (i.e., which specific procedures and/or technologies or even products) could or should be applied for each type of risk:
  - For different environments, the control solutions could be different and could be based on different standards.
  - Some mitigations may be engineering strategies (e.g., redundant systems, data validity checking, physical isolation, or monitoring), whereas others may be cybersecurity methods (e.g., access control, firewalls, certificates, or encryption).
  - Constraints on these potential control solutions should be identified, given the different issues associated with different OT environments, such as different constraints in a substation environment (long times between opportunities to patch systems) or a DER environment (unavailable knowledge of on-site security).
- Start the process of applying the selected mitigation solutions that were determined during the risk assessment process:
  - It may not be possible to apply some typical or selected control solutions to systems in specific projects as initially defined, particularly for legacy systems. For instance, legacy systems may not be capable of supporting specific control solutions, such as antivirus applications or secure patching procedures.
  - Therefore, alternate methods may need to be redefined to take into account the differences in system and device capabilities for particular environments and projects (These alternate methods may be offered by vendors or in-house groups that have experience with these different environments).

  - These alternate methods could be obtainable because a vendor proposes to meet a particular risk level, not just provide a specified control solution.
  - Vendors may also be asked to integrate their systems with the utility-standard control solutions.
- Validate results after risk mitigation solutions have been implemented:
  - Verify, as the project progresses, that the applied mitigation solutions have been applied correctly and provide the expected mitigations.
  - Explain how these mitigation solutions should be applied, as this is crucial to understanding how they are expected to work and how to evaluate the solutions for effectiveness.
  - Perform simulations to assess how well any mitigation solution may work.
  - Determine if the mitigation solutions have actually mitigated the risk adequately and perform another risk assessment, if necessary.
  - Include an assurance process, such as an audit, possibly by a different group.
- Monitor, over time, all security procedures and technologies in the completed project to ensure that the mitigation solutions remain effective and determine whether possible future technologies or attack vectors could potentially overcome the original mitigation solutions.
  - In all cases, possible security events identified by such monitoring should be sent to a central computer emergency response team (CERT) or CSIRT site.
- Ensure that the central site is capable of filtering and assessing the importance of security events or sequences of security events.

3.3 Eventual Move toward Security Procedures and Standard Security Technologies

This risk assessment process actually involves determining mitigation procedures and technologies. Ideally, these should ultimately be consistent with each other, but because legacy equipment cannot always accommodate new technologies and because standardized solutions are not yet available, such mitigation solutions often start as ad hoc or temporary measures. Over time, there should be movement toward consistent security procedures and standard security technologies.

Conclusions

Regulators will increasingly need to support the requirements of cybersecurity and resilience for energy businesses. In particular, regulators will need to encourage or require (depending on whether there are voluntary or mandatory standards) the top management of utilities to design comprehensive security policies, processes, procedures, and technologies that cover resilience, security by design, operational requirements, risk management, and the use of cybersecurity standards and guidelines. Such security can only be effective if it is seen as critical by top management and is promulgated down to all levels. This security culture must permeate the entire organization, and may increasingly need to be driven by regulatory requirements and laws.

Cybersecurity procedures should not be reinvented. Regulators can (and should) rely on existing cybersecurity standards and guidelines. When considering investments (and cost-recovery), utilities (and thus regulators) should focus on ensuring that a system is secure and resilient. Standards must be known and understood prior to being adopted and imposed and they should address organizational/governance aspects, including the financial impact of implementation of said standards.

As with all aspects of cybersecurity, risk assessments, standards, and other mitigation measures need to continuously adapt. Those who engage in cyberattacks are able to evolve their methods much more quickly than regulations can evolve, so there needs to be some flexibility within standards to address that issue. These standards are not static, and regulators and utilities must constantly reassess their situations and undertake new approaches to address security challenges.

Regardless of which standards are used and whether they are voluntary or mandatory, security and resilience by design will become a highly important focus for regulators to ensure that utilities provide affordable services with the level of quality that consumers deserve and expect. Strategies, policies, and systems need to be based on known best practices and open to future improvements reflecting evolving standards and technologies.

The following Annex provides regulators with additional information on several internationally recognized cybersecurity standards. Regulators can evaluate existing options rather than reinvent new ones, and contextualize them to their own country-specific situations (e.g., voluntary vs mandatory).

Annex: Cybersecurity Standards and Best Practices

This annex outlines several key existing cybersecurity standards and best practices organized by type (*What and How*) and the processes to take to move towards compliance. As regulators increase their knowledge and engage with utilities and other governmental institutions in coordination efforts to promote effective cybersecurity measures, they can build upon lessons learned and standards already in use. Rather than trying to develop completely new standards, it makes more sense for regulators to champion customization of existing standards that have already proven to be useful and implementable.

It is important that regulators understand the core principles behind why standards may be necessary, the consideration of voluntary vs. mandatory in their context, and the steps that utilities in their countries are (or are not) taking. When regulators, utilities, and other key institutions develop collaborative working relationships, they can improve cybersecurity measures in their energy sectors, thus bolstering the security and resilience of the grid.

This annex provides a summary of key aspects of the following frameworks:

- Section A.1 NIST Cybersecurity Framework
- Section A.2 ISO/EC 27000 Series
- Section A.3 NERC Critical Infrastructure Protection Standards
- Section A.4 NISTIR 7628 Guidelines for Smart Grid Cybersecurity
- Section A.5 IEC 62443 Series for Industrial Automation[15]
- Section A.6 IEC 62351 Cybersecurity Series for the Smart Grid[16]

Just as there is no single "best" model for how to effectively regulate the energy sector, the cyber frameworks featured below should be considered in the context of individual country goals and realities. The authors of the guide have prepared summaries of cybersecurity standards that they have in-depth experience with in the hopes of conveying information to help regulators take the next step in leading cybersecurity efforts in their countries.

A.1 NIST Cybersecurity Framework[17]

Using the NIST Cybersecurity Framework is an important first step for cyber professionals when assessing and improving their cyber environments. The framework is used internationally and provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes. A wide range of businesses and organizations can use this methodology to be proactive about risk management and cybersecurity.

[15] IEC. "Search results for '62443.'"

[16] IEC. "IEC 62351:2020 SER Series."

[17] NIST, *Framework*.

As shown in Figure 5, the NIST framework includes high-level functions to identify, protect, detect, respond, and recover. The five functions are applicable to cybersecurity risk management and also to risk management writ large. The detailed categories address all of the specific cybersecurity goals of an organization, such as cyber, physical, personnel, with a focus on business outcomes.

The subcategories provide an in-depth understanding of the Framework Core (Core). There are 108 subcategories, which are outcome-driven statements that provide considerations for creating or improving a cybersecurity program. Since the subcategories are not prescriptive on how to achieve those outcomes, it allows for risk-based implementation that is customized to an organization's needs.

Figure 5: NIST Framework for Improving Critical Infrastructure Cybersecurity

Source: NIST, "Cybersecurity Framework," [16]

As seen in Figure 6, the Core is designed to be intuitive and to act as a translation layer to enable communication between multidisciplinary teams by using simplistic and nontechnical language. There are three key parts: functions, categories, and subcategories.

The NIST framework allows for an organization to have a common language and systematic methodology for managing cybersecurity risk. The Core includes activities to be incorporated in a cybersecurity program that can be tailored to meet any organization's needs. The framework is designed to complement, not replace, an organization's cybersecurity program and risk management processes. The framework helps guide key decision points about risk management activities through the various levels of an organization, from senior executives to the business and process level, as well as implementation and operations.

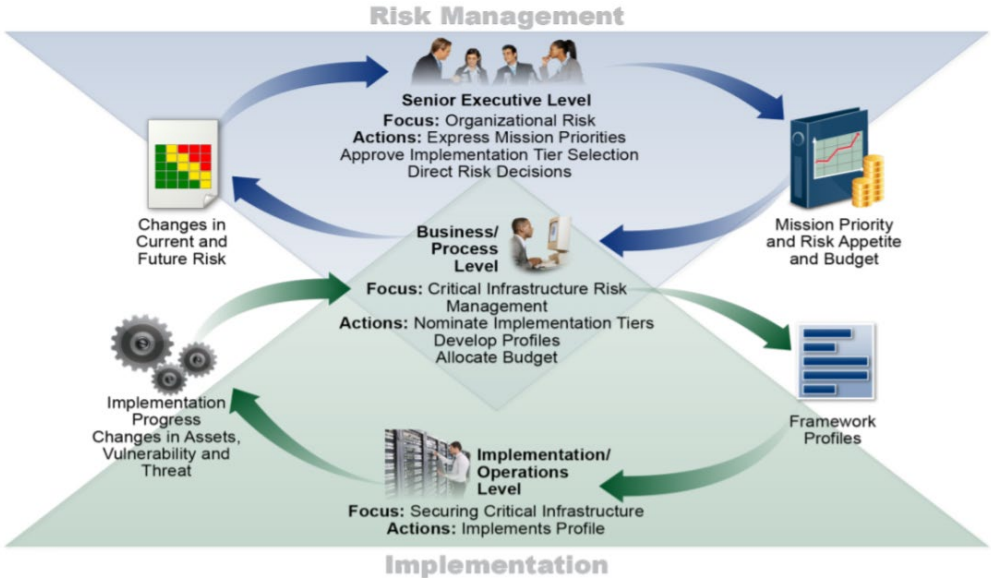

Figure 6: NIST Framework Diagram Illustrating the Risk Management Process Across an Organization

Source: NIST, *Framework*, [15].

A.2 ISO/IEC 27000 Series[18]

The ISO/IEC 27000 series covers a wide range of cybersecurity requirements (see Figure 7). These cybersecurity standards are focused on what cybersecurity policies and procedures should be put in place at the enterprise level.

For the smart grid, the most relevant are ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27019. These standards identify the high-level organizational and procedural requirements for cybersecurity, including risk assessment requirements, personnel security processes, and information security. ISO/IEC 27001 is general for all types of organizations, whereas ISO/IEC 27002 covers industrial organizations. Additional requirements for energy organizations are included in ISO/IEC 27019.

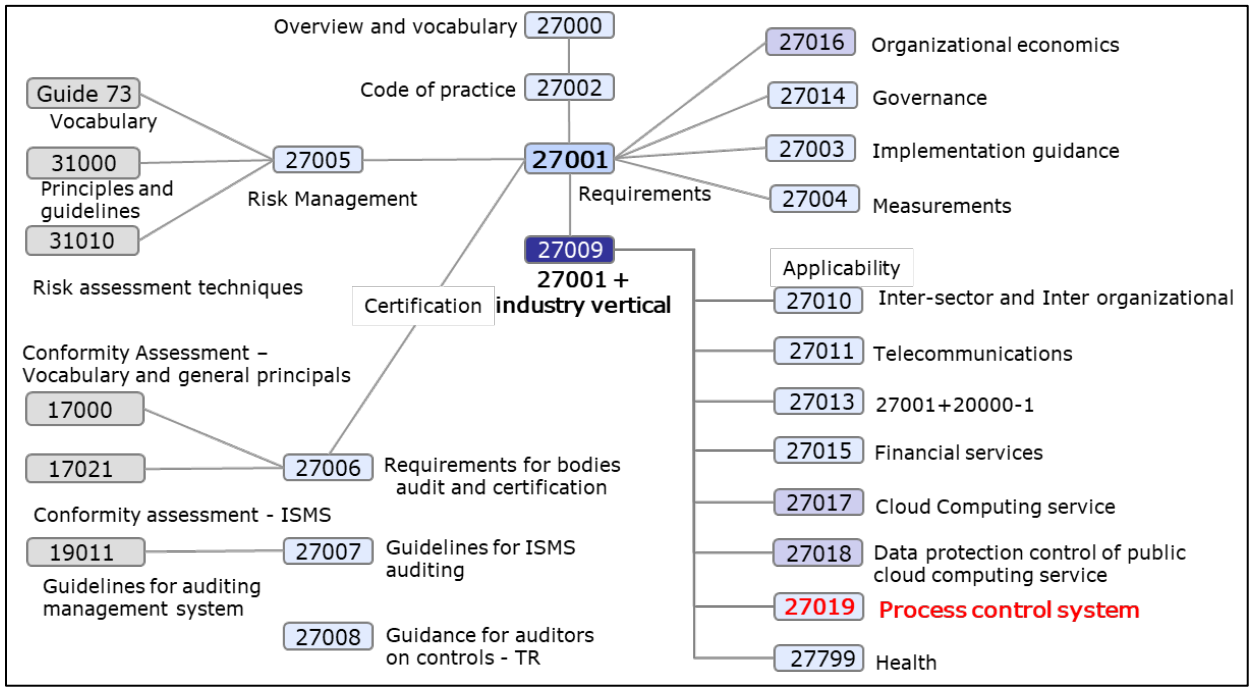

Figure 7: ISO/IEC 27000 Series, Identifying 27019 Specifically for Process Control Systems

Source: ISO/IEC 27000 series, [8]

A.2.1 ISO/IEC 27001 family of standards

ISO/IEC 27001 is a globally recognized standard providing requirements for the establishment of an information security management system (ISMS). The ISO describes an ISMS as "a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process."[19] The standard describes how an organization must set its security objectives and determine the risks that threaten these objectives. The organization can respond to the identified risks with a risk treatment plan. An important part of this plan is choosing appropriate controls from ISO/IEC 27002 and all ISO/IEC 27002 sector-specific standards.

The ISO/IEC 27001 family of standards has grown quickly over the past years, and now includes around 40 standards. Figure 8 gives an overview of the most relevant of the ISO/IEC 27001 standards.

[18] *Information technology - Security techniques - Information security management systems*

[19] https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27001, with other standards in the 27001 family, also provides the framework for third-party audits and certification of an organization's ISMS. Organizations can have their ISMS certified against ISO/IEC 27001 by independent certification bodies, which have to be accredited by a national accreditation body.

The ISMS family of standards consists of interrelated standards, already published or under development, and contains a number of significant structural components. These components are focused on:

- Standards describing ISMS requirements (ISO/IEC 27001).
- Certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001.
- An additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009).

Other documents provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance.

Relationships between the ISMS family of standards are illustrated in Figure 8:

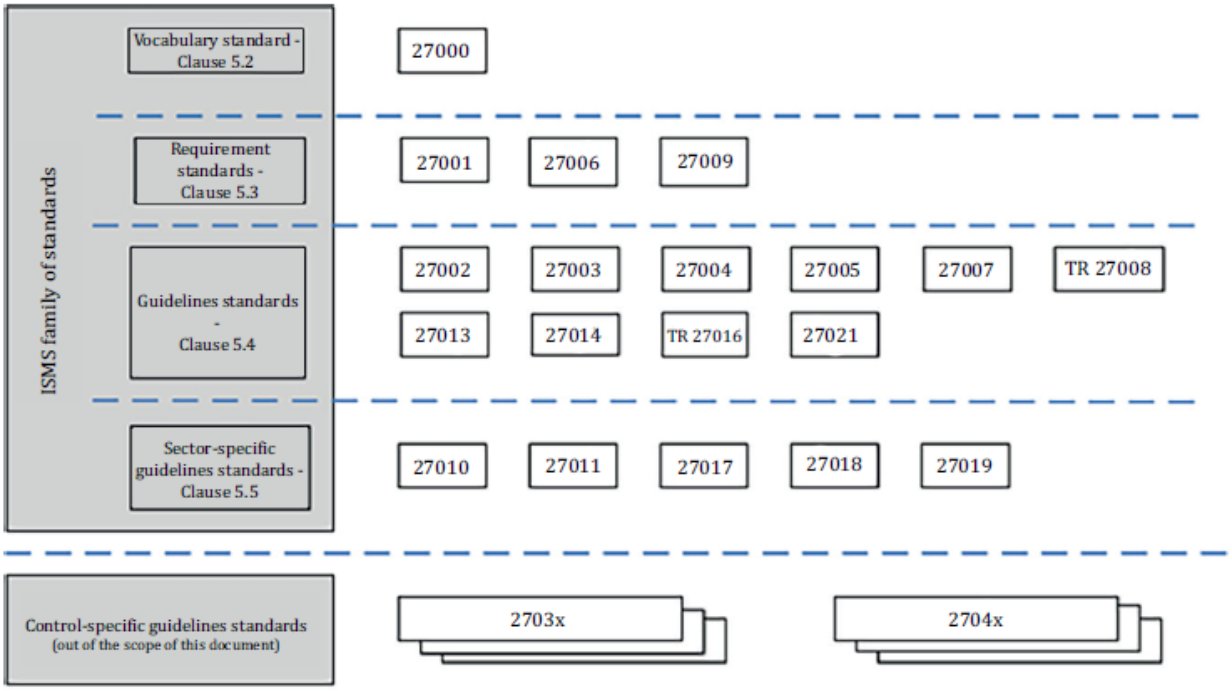

Figure 8: ISMS Family of Standards Relationships
Source: (ISO/IEC 27000:2018), [9]

A.2.2 ISO/IEC 27002:2013[20]

ISO/IEC 27002 is a code of practice—a generic set of controls addressing information security control objectives to mitigate security risks impacting, for example, the confidentiality, integrity, and availability of information.

ISO/IEC 27002 security controls are organized within the following main clauses:

- Organization of information security
- Human resource security
- Asset management

[20] ISO, *Code of Practice*.

- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Compliance

A.2.3 ISO/IEC 27019:2017[21]

ISO/IEC 27019 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. The aim of ISO/IEC 27019 is to extend the ISO/IEC 27000 set of standards to the domain of process control systems and automation technology. This allows the energy utility industry to implement a standardized ISMS in accordance with ISO/IEC 27001 that extends from the business level to the process-control level.

The scope of ISO/IEC 27019 covers process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage, and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes, in particular, the following systems, applications, and components:

- The overall IT-supported central and distributed process control and monitoring and automation technology, as well as IT systems used for their operation, such as programming and parameterization devices.
- Digital controllers and automation components, such as control and field devices or programmable logic controllers (PLCs), including digital sensor and actuator elements.
- All further supporting IT systems used in the process control domain (e.g., for supplementary data visualization tasks and for controlling, monitoring, data archiving, and documentation purposes).
- The overall communications technology used in the process control domain (e.g., networks, telemetry, tele-control applications, and remote control technology).
- Digital metering and measurement devices (e.g., for measuring energy consumption, generation or emission values).
- Digital protection and safety systems (e.g., protection relays or safety PLCs).
- Distributed components of future smart grid environments.
- All software, firmware, and applications installed on systems mentioned previously.

[21] ISO, *Energy Utility Industry*.

A.3 NERC Critical Infrastructure Protection Standards[22]

A.3.1 Background

In the early days of NERC, participation in North America was voluntary and electric utilities that were operating assets within the larger complex bulk electric system were operationally incentivized to manage and maintain their assets in a way that contributed to overall system reliability. Under this voluntary model, common operating practices, guidelines, and standards were created to ensure that various utilities performing reliability tasks could ensure that they were being performed at a level of acceptable utility practice. As electric system reliability events occurred, and new threats to critical infrastructure reliability continued to rise, there was an effort to establish a regulatory structure in the form of the Energy Policy Act 2005, which declared the need for an Electric Reliability Organization (ERO) with the responsibility and authority to develop and enforce standards to ensure the reliability of the bulk power system.

The ERO for North America is NERC, and it has been responsible for working with the NERC Regional Entities to ensure the reliability standards have been implemented and enforced. Although the NERC CIP standards have existed for a decade and half, we will consider the versions of NERC CIP that are in effect currently (a combination of versions 5 and 6), see Figure 9.

Version 5 - 6	Standard Name
CIP-002-5.1*	BES Cyber System Categorization
CIP-003-6	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-5*	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5*	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-2	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection

Figure 9: NERC CIP Standards in effect: a combination of versions 5 and 6.
Source: NERC [14]

To provide background and for the purposes of identifying some of the strengths of the NERC CIP standards, we will discuss some key items for consideration when examining this standards group.

[22] NERC, "CIP Standards."

A.3.2 Standards Developed by the Industry for the Industry

As with all NERC standards, the CIP standards were driven by the electric industry directly. In 2003, a number of asset owners and operators identified cybersecurity—or the lack of cybersecurity—as a considerable risk to the reliability of the electric sector. It was a risk that was only going to increase, as the adoption of cyber assets within industrial control system environments continued to rise in parallel with two other trends—increasing interconnectedness and accessibility of OT systems, and an ever-increasing adversary interest in industrial control system sectors. For this reason, the electric utilities began the process of creating a cybersecurity standard for the industry.

Although the process of creating a standard can be complicated and time-consuming, the important elements to note when considering undertaking such a process include: that the standards be written by a drafting team with representation from electric sector stakeholders, that the drafting process be open and transparent to the public, that there can be numerous industry comment periods to consider modifications to the proposed standard, and, most importantly, the use of industry ballots to approve or reject the standards in development. In this way, the individual organizations that will need to ultimately satisfy the requirements have a voice throughout the entire development process to ensure their concerns are heard or addressed.

A.3.3 Focus on Cyber and Physical Threats to Grid Reliability

In 2009, a jointly commissioned report was released by the US Department of Energy that identified key threats to the electric sector. This report focused on high-impact, low-frequency (HILF) events that have a low frequency of occurrence (meaning possibly never) but that, were they to occur, would be so high-impact that the industry needed to take action to manage the impact. One of the HILF scenarios identified was a coordinated cyber and physical attack against the electric system. Many looked to the CIP Standards to be implemented in a manner that would reduce the immediate and long-term impact of this type of attack. Many individuals with some exposure to the CIP standards are aware that the standards' requirements address cybersecurity needs. However, it should also be made clear that CIP-006 addresses physical security controls for bulk electric system cyber assets within the scope of CIP and CIP-014 addresses physical security protections of critical transmission facilities.

A.3.4 Requirements Applicable to Both Traditional IT Assets and OT Assets

As mentioned in the previous section, the NERC CIP standards are multifaceted, in that the requirements address cyber and physical threats. It also needs to be pointed out that the CIP standards are neither limited in scope to traditional IT assets nor to interconnection sharing devices. Rather, the requirements provide a fairly detailed list of tasks that must be performed on IT and OT assets that could impact the reliability of the entire grid. The requirements ultimately shape what an electric utility must do, but they are not prescriptive as to how the requirements must be met. In this way, the utilities have flexibility in how they will comply and what approaches and technologies they will pursue to satisfy the standards.

A.3.5 Lessons Learned

The CIP standards have been undergoing a continual process of improvement since they were adopted and any country or state considering the CIP standards should take advantage of the many years of implementation-driven improvements that have occurred. The following list describes the strong points of the current versions of CIP:

- **Asset owners drive the development of standards**. Standards created by the industry and for the industry are necessary for complex operational environments like an electric system.

- **Financial enforcement capability**. There needs to be an incentive for entities to take action.
- **Criteria-based facility determination for in-scope assets**. A standard approach that attempts to implement all controls across all things will fail. Identifying the right facilities and the right cyber assets is essential for a successful program.
- **Systematic approach to asset grouping and requirement applicability**. Applying a control to a single device will not always be possible. However, achieving a control on a system when required is an effective implementation approach.
- **High, medium, and low requirement applicability**. This ensures prudent controls based on risk to the electric system.
- **Non-prescriptive standards**. The standards that outline "*What*" must be achieved, not "*How*" to specifically achieve it, will provide entities the flexibility to build and maintain a program that works for them.

Guidance to those choosing NERC CIP – For those regulators considering adoption or modification of the CIP standards to fit their particular needs, the following recommendations will help ensure successful implementation:

- Identify who will be the national authority (like the ERO described above). There will need to be a governance structure in place that will manage the utility reviews and possible auditing of the standards.
- Modify CIP-002-5.1a - Attachment 1 based on the specifics of your electric system to ensure the appropriate level of in-scope assets at the appropriate level of protection (high, medium, or low).[23]
- Review/modify the NERC-defined terms used throughout the CIP Standards to ensure they are understood by and effective for both regulators and utilities.
- Focus on a staggered implementation approach that addresses those control center assets with a wide area impact first. Develop a standards implementation plan that addresses highest-risk facilities first and has later adoption dates for lower-risk environments.
- Pursue peer evaluations from utility to utility during standards-adoption safe-harbor periods. Allow peer utilities to evaluate each other's programs in a manner that supports learning and improvement, prior to conducting a formal audit.
- Educate auditors/evaluators that the stronger an organization's internal controls program is, the more possible violations it will self-identify. This should not be considered a problem in itself and therefore the regulators should ensure appropriate incentives are in place to encourage positive behavior.
- CIP is a baseline set of requirements that are encouraged to be exceeded. Consider the requirements as the cost of doing business and encourage entities to exceed the requirements.
- Err on the side of reliability and security, not document-driven compliance. A program built on policies and plans only, without any actual cybersecurity elements, will not allow an entity to satisfy compliance requirements and will have no effect on cybersecurity.

[23] NERC, *CIP-002-5.1a*.

A.3.6 Core Four Questions

The NERC CIP model provides four key guiding principles for national regulators to follow in order to have effective standards in place.

1) **Define which critical infrastructure assets are in scope.** Asset types are defined in CIP-002 Requirement 1 and specific impact rating criteria are defined in Attachment 1. Attachment 1 criteria thresholds will need to be modified based on the electric system specifics of a particular country or region.
2) **Identify what the appropriate requirements will be.** CIP-003 through CIP-014 provide the requirements for asset owners to implement and manage a controls program. As shown over the years of CIP implementations that occurred at thousands of sites throughout North America, there are a large number of organizations and consultancies capable of designing solid CIP programs, along with full personnel-training and credentialing programs to ensure capable staff to maintain CIP programs.
3) **Establish how assessments of sufficient adherence will be performed.** Throughout the many years of voluntary readiness evaluations, peer assessments, and formal Regional Entity audits there arose a common body of knowledge and formal training that can be leveraged, as well as a large consultancy workforce that is skilled in performing CIP audit work.
4) **Identify who will enforce the regulation and through what methods.** This is the main component that is specific to each country or state and must be defined in a manner that will ensure successful implementation and appropriate levels of enforcement authority to incentivize adoption.

A.4 NISTIR 7628 Guidelines for Smart Grid Cybersecurity

A.4.1 NISTIR 7628 Cybersecurity Controls

The NISTIR 7628 consists of guidelines intended primarily for addressing cybersecurity of smart grid systems and the constituent subsystems of hardware and software components. The NISTIR 7628 guidelines are very similar in scope to the ISO/IEC 27019 standard, except these guidelines focus exclusively on the smart grid sector. They define approximately 300 high-level security controls, based on similar security controls in other NIST documents, including the NIST framework (see Figure 10).

Ref.	
SG.AC	Access Control
SG.AT	Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid Information System Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid Information System and Services Acquisition
SG.SC	Smart Grid Information System and Communication Protection
SG.SI	Smart Grid Information System and Information Integrity

Figure 10: NISTIR 7628 Smart Grid Security Requirements Families,
Source: Xanthus Consulting International, derived from [17]

A.4.2 NISTIR 7628 Cybersecurity Logical Reference Model

The NISTIR 7628 guidelines also extend these cybersecurity controls beyond the general requirements. They describe a high-level logical interface reference model that defines 22 logical interface categories. These logical interface categories are characterized by the communication requirements and constraints between systems within and across smart grid domains and cover: operations, market operations, back-office systems, substations, customer sites, DER, and other field equipment. For each of these logical interface categories, the appropriate high-level security requirements are also identified and annotated. Figure 11 shows the Logical Reference Model (sometimes referred to as the Spaghetti Diagram) that illustrates the types of communication requirements and constraints associated with the smart grid.

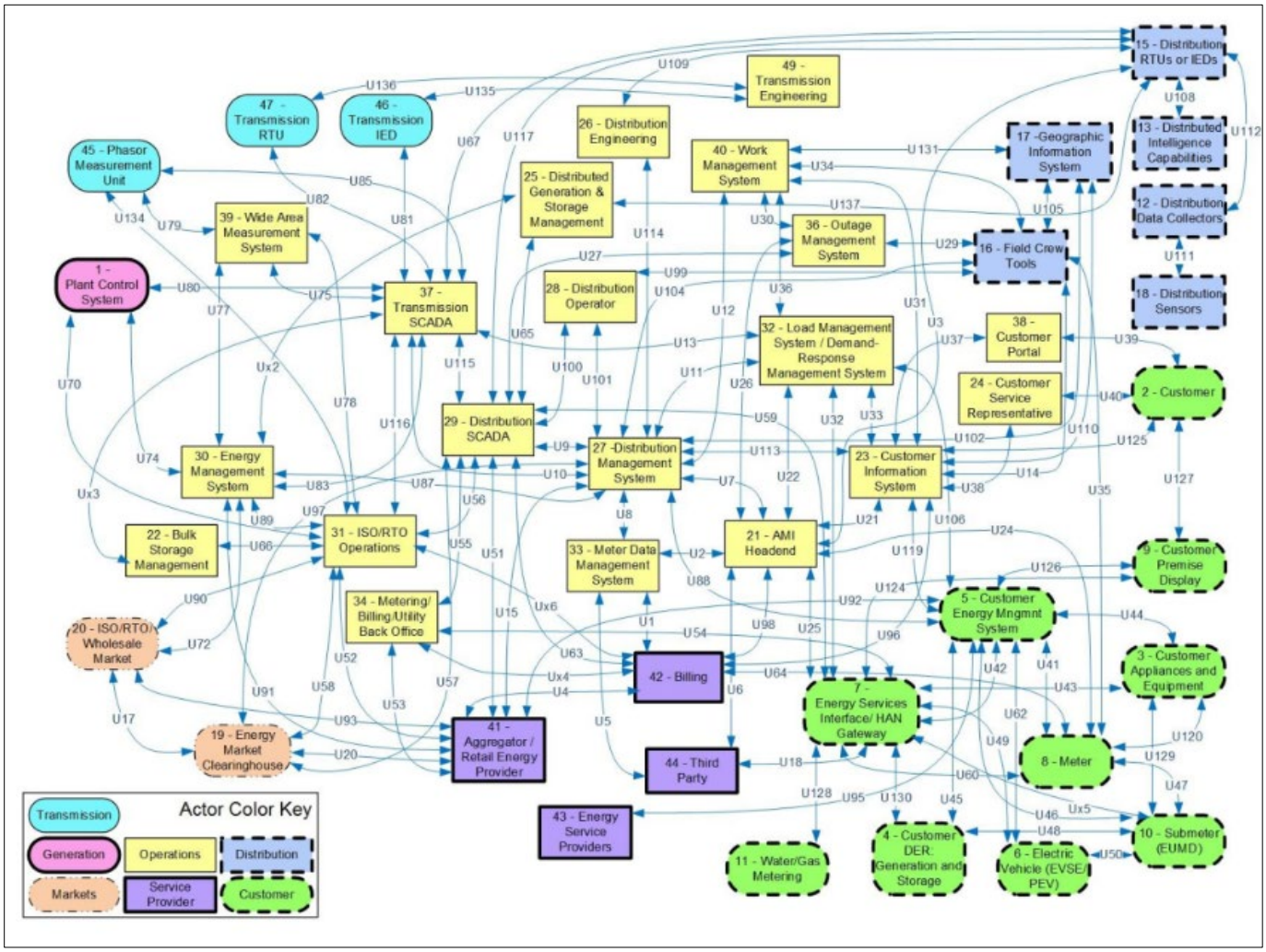

Figure 11: NISTIR 7628 Spaghetti Diagram High-Level Logical Reference Model
Source: NISTIR 7628, [17]

A.5 IEC 62443 Series for Industrial Automation[24]

A.5.1 IEC 62443 Background

The international industrial security standard IEC 62443 is a security requirements framework defined as a joint activity between the IEC and the ISA99 committee. The standard specifies security for industrial automation and control systems (IACS) and covers both organizational and technical aspects of security. Although focused on industrial automation in general, most of the cybersecurity requirements also apply to the energy sector and include more details on specific operational and field equipment requirements for cyber-physical systems than the ISO/IEC 27000 series alone. For instance, it details requirements for patch management and poses specific security requirements for systems or components to cope with a specific security level. Of particular pertinence to the smart grid are the organizational requirements, IEC 62443-2-2, 2-3, 2-4, and 4-1, and the more technical requirements covered in IEC 62443-3-3 and 4-2. Requirements for asset owners of industrial control systems are defined in IEC

[24] IEC. "Search results for '62443.'"

62443-2-1 to enhance ISO 27001-mandated efforts with domain-specific security controls. For smart grid-related enhancements of the information security management framework, ISO 27019 already exists.

As stated, technical security requirements are specified by distinguishing different security levels for industrial automation and control systems. In the set of corresponding documents, security requirements are defined not only to target the solution operator and the integrator, but also the product manufacturer.

A.5.2 IEC 62443 Organization

As shown in Figure 12, different parts of the standard are grouped into four clusters, covering:

- Common definitions and metrics.
- Requirements on setup of a security organization (ISMS related, comparable to ISO 27001, as well as solution-supplier and service-provider processes).
- Technical requirements and methodology for security on a system-wide level.
- Requirements on the secure development life cycle of system components, and security requirements to such components at a technical level.

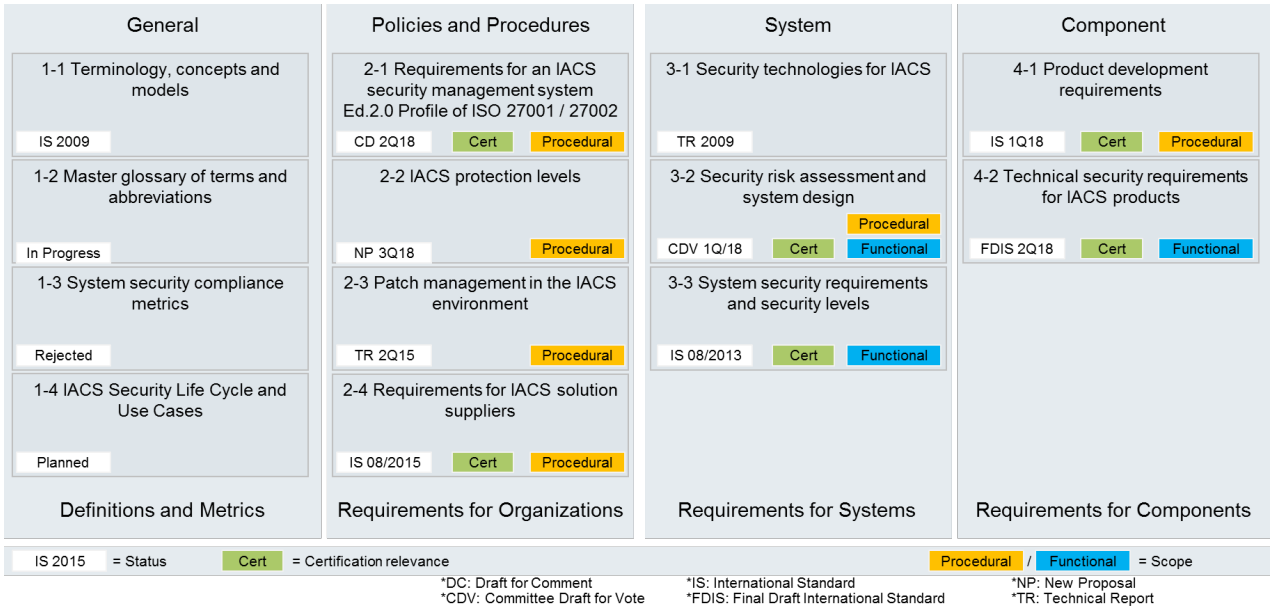

Figure 12. IEC 62443 Series of Industrial Security Standard – Overview
Source: ISA99.org, [5] Xanthus Consulting International personal communication

Figure 13 gives an overview on which parts of IEC 62443 are relevant for the different roles. The operator of an automation system operates the automation and control system that have been integrated by the system integrator, using components of product suppliers.

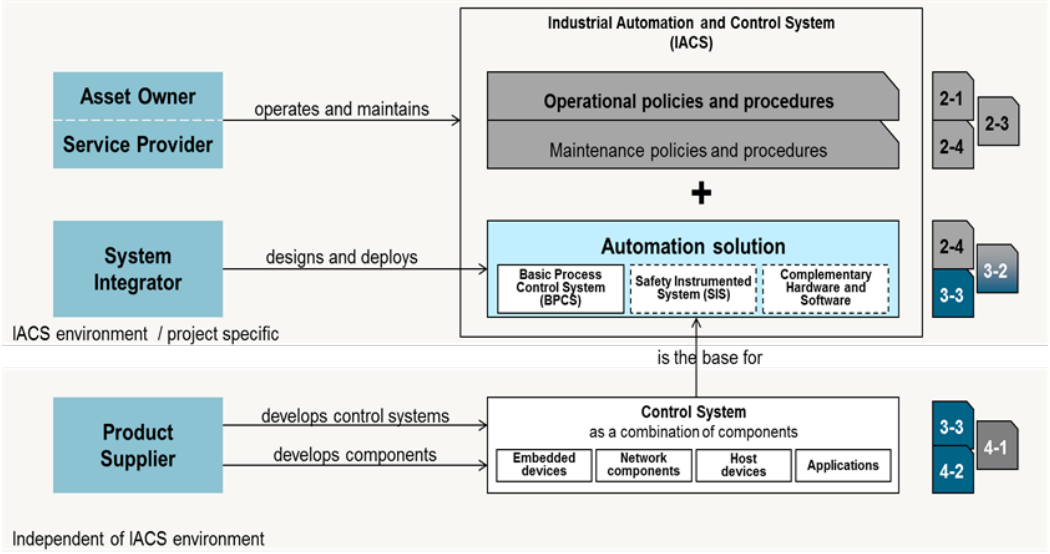

Figure 13. Application of IEC 62443 Parts by Different Roles

Source: Developed by ISA99 to explain IEC 62443-2-4 Ed1.1: 2017, [5] Xanthus Consulting International personal communication

According to the methodology described in IEC 62443-3-2, a complex automation system is structured into zones that are connected by and communicate through so-called "conduits" that map for example to the logical network protocol communication between two zones. Moreover, this document defines security levels (SL) that correlate with the strength of a potential adversary as shown in Figure 14. To reach a dedicated SL, the defined requirements have to be fulfilled. IEC 62443-3-3 defines system security requirements. It does help to focus only on certain facets of security. The security requirements defined by IEC 62443-3-3 help to ensure that all relevant aspects are addressed.

Part 3-3 of IEC 62443 defines seven foundational requirements (FR) of a certain category as: identification and authentication control (FR1), use control (FR2), system integrity (FR3), data confidentiality (FR4), restricted data flow (FR5), timely response to events (FR6), and resource availability (FR7).

For each foundational requirement, there exists several concrete technical security requirements (SR) and requirement enhancements (RE) to address a specific security level. In the context of communication security, these security levels are specifically interesting for the conduits connecting different zones.

A.5.3 IEC 62443 Security Levels

Four Security Levels (SL1, SL2, SL3, and SL4) are defined in IEC 62443-3-2 correlating with the strength of a potential adversary as shown in Figure 14. To reach a dedicated security level, the requirements (SR) and potential enhancements (RE) defined for that security level have to be fulfilled. The standard foresees that a security requirement can be addressed either directly or by a compensating countermeasure. The concept of compensating countermeasures allows to reach a certain security level even if some requirements cannot be implemented directly, e.g., as some components do not support the required technical features. This approach is in particular important for existing industrial automation and control systems, so called "brown-field installations," as existing equipment can be continued to be used.

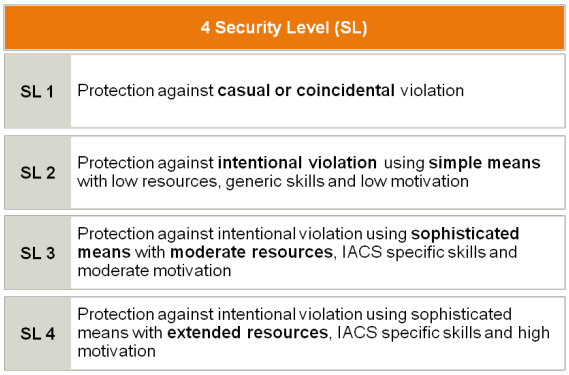

Figure 14. IEC 62443 Defined Security Level

Source: IEC 62443-3-2 [3], Xanthus Consulting International personal communication

The security level of a zone or a conduit (a conduit connects zones) is more precisely a security level vector with seven elements (see also annex A of IEC 62443-3-3). The elements of the vector designate the security level for each foundational requirement. This allows defining the security level specific for each foundational requirement. If, for example, confidentiality is not a security objective within a zone, the security level element corresponding to FR4 "Data confidentiality" can be defined to be SL1 or even none, although SL3 may be required for other foundational requirements (e.g., for FR1, FR2, and FR3). Hence, the resulting security level vector for a zone could be SL= (3, 3, 3, 1, 2, 1, 3) or SL= (2, 2, 2, 0, 1, 1, 0).

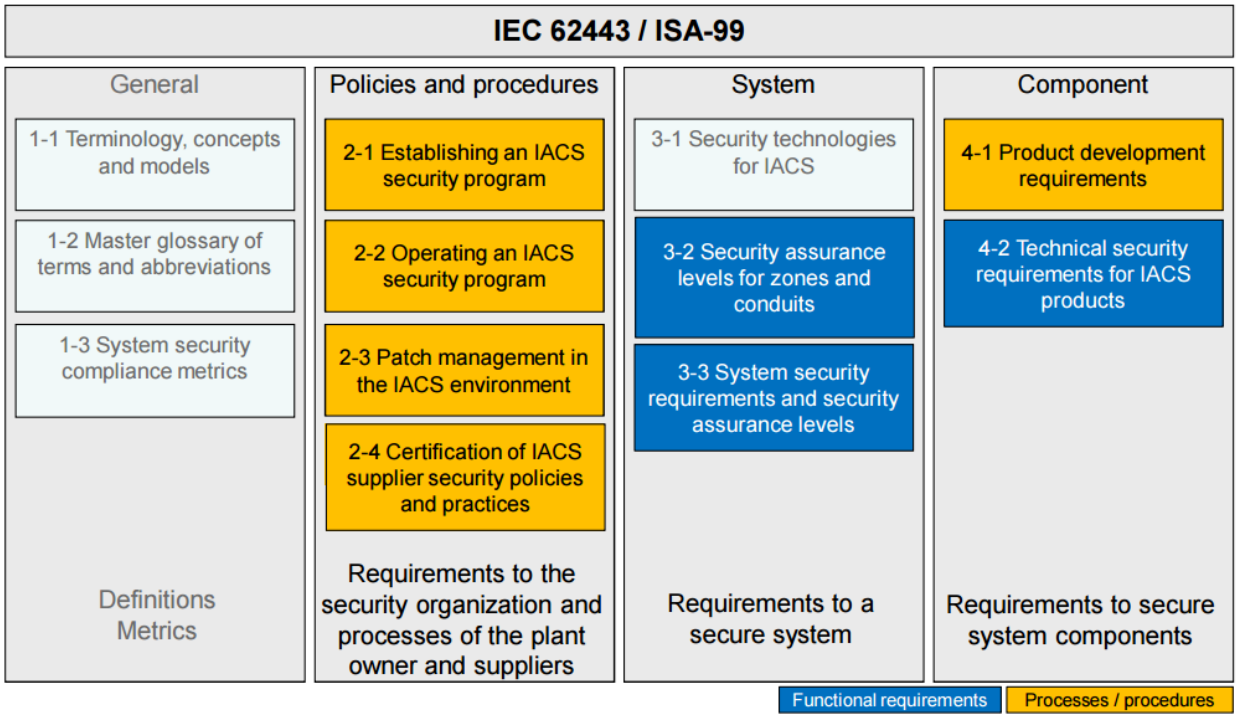

Figure 15: IEC 62443 Series of Cybersecurity Standards Developed by the ISA99 Committee
Source: ISA99.org, [3], Xanthus Consulting International personal communication

A.6 IEC 62351 Cybersecurity Series for the Smart Grid[25]

A.6.1 IEC 62351 Overview

The IEC 62351 series of standards includes cybersecurity technologies for the communication protocols defined by the IEC TC57,[26] specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. As shown in Figure 16, there is not a one-to-one correlation between the IEC TC57 communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers. Conformance testing for these standards is also part of the series as IEC 62351-100-xx.

[25] IEC. "IEC 62351:2020 SER Series."

[26] More detailed information can be found on the IEC TC57's public website: IEC, "WG15 Public Site."

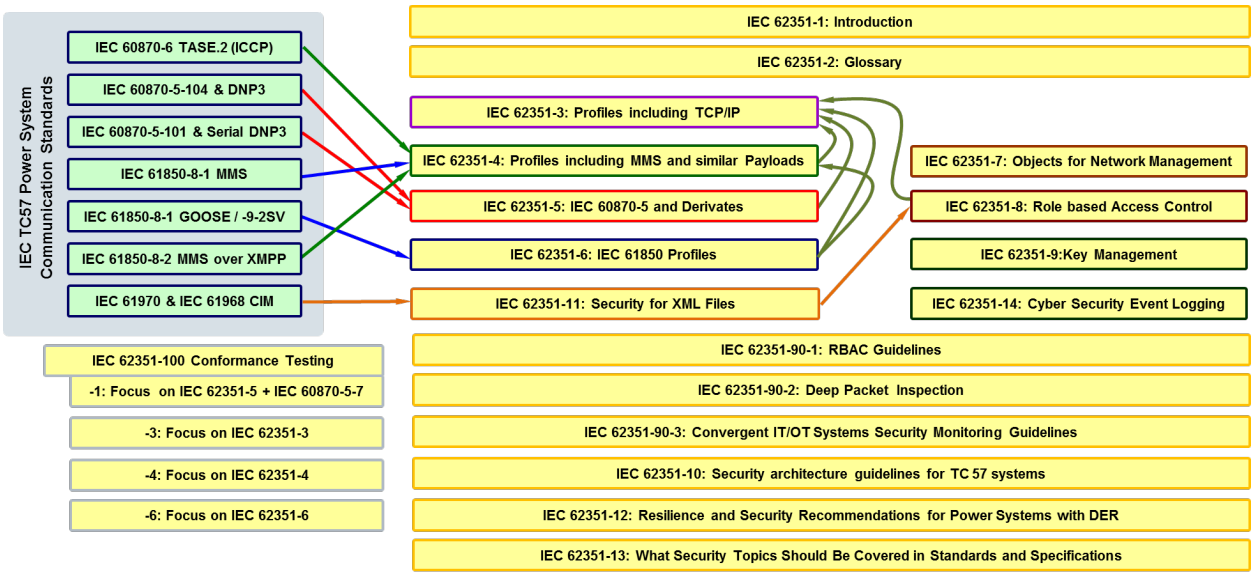

Figure 16: IEC 62351 Series of Cybersecurity Standards

Source: Xanthus Consulting International.

A.6.2 IEC 62351 Cybersecurity Standards for Communication Standards

The IEC 62351 cybersecurity standards consist of the following components for securing communication standards:

- IEC Technical Specification (TS) 62351-1:2007: Introduction – This first part of the standard covers the background on security for power system operations and introductory information on the series of IEC 62351 security standards.
- IEC TS 62351-2:2008: Glossary of Terms – This part includes the definition of terms and acronyms used in the IEC 62351 standards. These definitions are based on existing security and communications industry standard definitions as much as possible, given that security terms are widely used in other industries as well as the power system industry. The terms in this glossary are provided for free access on the IEC website at http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2.
- IEC 62351-3:2014: Data and Communication Security – Profiles Including transmission control protocol/internet protocol (TCP/IP). These security standards cover those profiles used by:
  - IEC 60870-6 (Telecontrol Application Service Element [TASE.2]/Inter-control Center Communications Protocol [ICCP]).
  - IEC 60870-5 Part 104.
  - IEEE 1815 (Distributed Network Protocol 3 [DNP3]) over TCP/IP.
  - IEC 61850 over TCP/IP.
- IEC 62351-4: Data and Communication Security – Profiles Including Manufacturing Message Specification (MMS) and similar payloads. These security standards cover those profiles used by:
  - IEC 60870-6 (TASE.2/ICCP) using the Manufacturing Message Specification (MMS).
  - IEC 61850-8-1 using the MMS profile of data objects.

  - IEC 61850-8-2 using Extensible Markup Language (XML) XML schemas (XSDs) mapped from MMS data objects.
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and derivatives (e.g., DNP3). These security standards cover both serial and networked profiles used by:
  - IEC 60870-5-7 (security details for IEC 60870-5-101 and 104).
  - IEEE 1815 (DNP3).
- IEC 62351-6: Data and Communication Security – Security for IEC 61850 peer-to-peer profiles. These security standards cover profiles in:
  - IEC 61850 that do not run over TCP/IP—generic object-oriented substation event (GOOSE) and sampled value (SV).

A.6.3 IEC 62351 Additional Cybersecurity Standards and Technical Reports

Additional IEC 62351 cybersecurity standards and technical reports cover additional areas:

- IEC 62351-7: Network and system management (NSM) of the information infrastructure, which defines abstract NSM data objects for the power system operational environment and reflects what information is needed to manage the information infrastructure as reliably as the power system infrastructure is managed. A mapping to Simple Network Management Protocol (SNMP) management information bases (MIBs) was also developed and made available as code components.
- IEC 62351-8: Role-Based Access Control (RBAC) for Power System Management. The purpose of this standard is to:
  - Introduce "subjects-roles-rights" as an authorization concept (in American National Standards Institute-International Committee for Information Technology Standards [ANSI INCITS] 359-2004, referred to as "users-roles-permissions").
  - Promote role-based access control for the entire pyramid in power system management.
  - Enable interoperability in the multi-vendor environment of the power industry.
  - IEC 61850-90-19 is developing the role-based access control (RBAC) requirements for IEC 61850.
- IEC 62351-9: Key Management. This standard specifies how to generate, distribute, revoke, and handle digital certificates and cryptographic keys to protect digital data and its communication. Included in the scope is the handling of asymmetric keys (e.g., private keys and X.509 certificates), as well as symmetric keys (e.g., session keys).
- IEC Technical Report (TR) 62351-10: Security Architecture. This technical report addresses the description of security architecture guidelines for power systems based on essential security controls (i.e., on security-related components and functions and their interaction).
- IEC 62351-11: Security for XML Files. This standard defines the security requirements for exchanges of XML-based documents that are used for IEC 61970, as well as for some types of information exchanges in IEC 61850.
- IEC TR 62351-12: Resilience for Power Systems with DER Systems. This technical report provides resiliency recommendations for engineering/operational strategies and cybersecurity techniques that are applied to DER systems. It covers the resilience requirements for the many different stakeholders of these dispersed cyber-physical generation and storage devices, with the goal of

enhancing the safety, reliability, power quality, and other operational aspects of power systems, particularly those with high penetrations of DER systems.

- IEC TR 62351-13: What Security Topics Should Be Covered in Standards and Specifications. This technical report provides guidelines that support the developers of standards by addressing cybersecurity at the appropriate levels for their standards. This document provides suggestions on what security topics should be covered in standards and specifications that are to be used in the power industry.
- IEC 62351-14: Cyber Security Event Logging. This part of the IEC 62351 series specifies technical details for the implementation of security logs: communication, content, and semantics.

A.6.4 IEC 62351 Technical Specifications for Conformance Testing

The IEC 62351 cybersecurity technical specifications for conformance testing are being planned and developed. They consist of the following:

- Part 100-1: Conformance Testing for Part 5: in progress as a Technical Specification (TS).
- Part 100-3: Conformance Testing for Part 3: in progress as a TS.
- Part 100-4: MMS (Common Test Cases); new work item proposal (NWIP) for a TS.
- Part 100-6-1: 61850-8-1/9-2, 100-6-2: ICCP, and 100-6-3: 61850-8-2 Conformance testing for IEC 61850: NWIP for a TS for 100-6-1 only.
- Part 100-7: Conformance testing for network management—start with discussion in 90-3 on what should (or should not) be included in conformance testing.
- Part 100-8-1: RBAC; Part 100-8-2: RBAC for 61850 in 90-19 (when included in an International Standard (IS) or a TS—maybe 62351-8-1 or 61850-xx).
- Part 100-9: Conformance testing for key management—Look at Protocol Implementation Conformance Statement (PICS) for certificate validation, revocation, and management as well as enhancements to Group Domain of Interpretation (GDOI).
- Part 100-14: Conformance testing for event logging.

Bibliography

[1] ENEL. "Enel Cyber Security Risk Management," Presentation by Yuri Rassega, slide 38, October 2018, personal communication.

[2] IEC (International Electrotechnical Commission). "WG15 Public Site." IECTC57. IEC. Last modified 2016. http://iectc57.ucaiug.org/wg15public/default.aspx

[3] IEC. "Search results for '62443.'" Webstore. IEC. Accessed February 13, 2020. https://webstore.iec.ch/searchform&q=62443

[4] IEC. "IEC 62351:2020 SER Series." Webstore. IEC. Published January 10, 2020. https://webstore.iec.ch/publication/6912

[5] International Society of Automation (ISA). ISA99, Industrial Automation and Control Systems Security, https://www.isa.org/isa99/

[6] ISO (International Organization for Standardization). Information Technology—Security Techniques—Code of Practice for Information Security Controls. ISO/IEC 27002. Paris: ISO, 2013. https://www.iso.org/standard/54533.html

[7] ISO. Information technology — Security techniques — Information security risk management. ISO/IEC 27005:2018 https://www.iso.org/standard/75281.html

[8] ISO. Information Technology—Security Techniques—Information Security Controls for the Energy Utility Industry. ISO/IEC 27019. Paris: ISO, 2017. https://www.iso.org/standard/68091.html

[9] ISO. Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. ISO/IEC 27000. Paris: ISO, 2018. https://www.iso.org/standard/73906.html

[10] Lewis, James. Economic Impact of Cybercrime: No Slowing Down. Santa Clara, CA: McAfee and the Center for Strategic and International Studies, 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

[11] Morgan, Steve. "Cyber Crime Costs Projected to Reach $2 Trillion by 2019." Forbes. Last modified January 17, 2016. https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/ - 5bd5bcc43a91

[12] NARUC (National Association of Regulatory Utility Commissioners). Cybersecurity Evaluative Framework for Black Sea Regulators. NARUC, 2017. https://pubs.naruc.org/pub.cfm?id=E20048B4-155D-0A36-3117-F2F0A7A692F4

[13] NERC (North American Electric Reliability Corporation). CIP-002-5.1a—Cyber Security—BES Cyber System Categorization. NERC, 2013. https://www.nerc.com/pa/Stand/Reliability Standards/CIP-002-5.1a.pdf.

[14] NERC. "CIP Standards." Standards. NERC. Accessed February 13, 2020. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[15] NIST (National Institute of Standards and Technology). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST, 2018. https://doi.org/10.6028/NIST.CSWP.04162018.

[16] NIST. "Cybersecurity Framework." NIST. Accessed February 13, 2020. https://www.nist.gov/cyberframework.

[17] NISTIR 7628 Revision1: Guidelines *for Smart Grid Cybersecurity*. NIST, 2014. https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

[18] OWASP Foundation. "Security by Design Principles." OWASP Foundation Wiki. OWASP Foundation. Last modified August 3, 2016, 12:35. https://wiki.owasp.org/index.php/Security_by_Design_Principles

[19] Ragazzi, Elena, Alberto Stefanini, Daniele Benintendi, Ugo Finardi, and Dennis K. Holstein. Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators. NARUC, 2020.

For questions regarding this publication, please contact
Erin Hammel (ehammel@naruc.org).

National Association of Regulatory Utility Commissioners (NARUC)
1101 Vermont Ave NW, Suite 200
Washington, DC 20005 USA
Tel: +1-202-898-2210
www.naruc.org