Technology Report

Cyber security and resilience guidelines for the smart energy operational environment

Executive summary

Cyber security has become an increasingly vital requirement for any business, particularly those dealing with critical infrastructure, such as power system operations responsible for managing the rapidly evolving electric system. These energy businesses must navigate their way through increasingly changing and risky business environments, while continuing to provide and improve their services to end users. Challenges include the transition to clean energy resources and society's increasing reliance on electrical energy.

At the same time, evolving regulations, breath-taking new technologies, and innovative market opportunities are impacting the existing business structures, including the interconnection of distributed energy resources owned and operated by third parties, the rapidly expanded use of electrical vehicles, the reorganization of the power system with microgrids, availability of cloud services, and increased utilization of the Internet of Things (IoT) technologies.

In parallel with the paradigm shifts in the energy business environment, the energy industry has accelerated its evolution toward digitization and is becoming increasingly reliant on cyber assets (systems, controllers, intelligent devices) to manage the delivery of electrical energy. These cyber assets are crucial to the safety, efficiency, and reliability of electrical energy.

However, these cyber assets present serious challenges: businesses must also determine how to cope with the reality of deliberate cyber attacks, such as the successful cyber attack against the Ukrainian SCADA system[1], as well as how to remain resilient to the more mundane but equally critical inadvertent cyber threats arising from personnel mistakes, the complexity of systems, the multitude of new participants in the energy market, equipment failures, and natural disasters. Energy businesses that used to address only the system engineering process (design, deployment, integration, procedures, and maintenance) must now include cyber security services and technologies into these engineering processes. As a result, the new systems could be significantly different in configurations, capabilities, and constraints.

In the energy operational environment, there are five critical concepts for cyber security that should be understood as these energy businesses struggle to implement the necessary cyber security policies, procedures, and technologies. These five critical concepts on cyber security and resilience for the smart energy are illustrated in Figure 1[2].

This IEC Technology Report provides guidelines based on these five cyber security concepts. They cover the cyber security issues that these businesses must address in order to mitigate the possible human safety, physical, functional, environmental, financial, societal, and reputational impacts of "successful" cyber attacks. The authors have focused on the electrical and gas operational environments[3], but almost all these cyber security issues apply also to other energy environments.

1 ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

2 All diagrams not otherwise noted, were developed by the authors of this report.

Figure 1 | Five cyber security concepts

Concept #1 Resilience should be the overall strategy for ensuring business continuity. When focusing on resilience in general, organizations must consider safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify and prevent), but also during such incidents (detect and respond) and after incidents have been resolved (recover). For resilience of cyber assets, organizations must similarly consider safety, security, and reliability for cyber assets. Resilience thus involves a continuous improvement process to support business continuity. Resilience is not just a technical issue but must involve an overall business approach that combines cyber security techniques with system engineering and operations to prepare for and adapt to changing conditions, and to withstand and recover rapidly from disruptions. Information sharing and interoperability within and across organizations is also becoming a crucial part of resilience.

Concept #2 Security by design is the most cost-effective approach to security. Security is vital for all critical infrastructure and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented. This means that the products, the systems, the processes and the organization should be designed or set up from the beginning with security in mind. However, recognizing that security cannot easily be added to legacy

3 For this document, the electrical and gas operational environment covers transmission and distribution operations, field operations, electrical generation operations, and interactions with energy and ancillary markets. It is understood that there are "gray areas" as to which environment a particular system might belong to, and there are many interactions between operational systems and corporate systems which could affect operations. So the term "environment" is used as a general term to identify the differences between entities that can affect physical processes and systems and those that do not directly affect physical processes and systems. This includes any "IT" systems that could affect "OT" systems.

systems, particularly since system components may have different life cycles, it is crucial that even for these existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades. Security by design combines business organizational policies with security procedures and the supportive technologies. Organizational policies include security regulations, personnel training, and segregation of duties, while security procedures include CERT information sharing, backup and recovery plans, and secure operations. Security technologies include physical and logical techniques, such as physical site access locks, access control, authentication and authorization for all communications, and security logs.

Concept #3 IT and OT are similar but different. Technologies in operational environments (called OT in this document) have many differing security constraints and requirements from information technology (IT) environments. The primary reason is that power systems are cyber-physical systems and security incidents can cause physical safety and/or electrical incidents, while such physical consequences are not usually a problem in corporate environments. For IT environments, confidentiality of sensitive business and customer information is usually the most important, but in comparison for OT environments, the availability, authentication, authorization, and data integrity of power system information are usually the more critical requirements, since power data is typically not sensitive. At the same time, the OT environment is increasingly relying on cyber technologies and is inheriting more and more devices and platforms from the IT world, while both IT and OT environments are increasingly converging on the use of well-known and ever evolving IoT technologies. This interconnection of IT/OT and increased dependence on IoT technology is leading to additional vulnerabilities and challenges on ensuring adequate security in the energy environment. Therefore the selection of appropriate security measures have to be focused on the security requirements as determined by risk assessment.

Concept #4 Risk assessment, risk mitigation, and continuous update of processes are fundamental to improving security. Based on an organization's business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, and reputational) for all its business processes. Risk assessment identifies the vulnerabilities of systems and processes to deliberate or inadvertent threats, determines the potential impacts, and estimates the likelihood that the incident scenarios could actually occur. The strategy for risk mitigations must take into account operational constraints, as well as looking to engineering designs and operational procedures for improving resilience, while also evaluating the cost for implementing such a potential risk mitigation strategy and degree to which it mitigates the risk. Risk assessment also requires that mitigation processes are re-evaluated during regular periodic security reviews or triggered by actual security incidents.

Concept #5 Cyber security standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programs and policies. Cyber security measures should not be re-invented. Key cyber security standards and best practice guidelines have already been developed for different areas and purposes of security. Cyber security planning should use these cyber security standards and guidelines to improve resilience, security, and interoperability throughout the energy OT environment, using the right standards, guidelines, and procedures for the right purposes at the right time.

This IEC Technology Report has been developed by the task force on cyber security in IEC Systems Committee on Smart energy Working Group 3.

Table of contents

Section 1

Resilience as the overall strategy for ensuring business continuity

Resilience must be the overall strategy for ensuring business continuity. Resilience covers measures that can mitigate impacts from safety, security, and reliability incidents, not only before such incidents (identify and prevent), but also during incidents (detect and respond) and after incidents have been resolved (recover). This report focuses on the cyber security aspects, while still taking into account safety and reliability as underlying requirements, since they can often mitigate security challenges. For example, the NIST Cyber Security Framework[4] and ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019 provide descriptions of these resilience concepts for cyber security (see Figure 2).

Cyber security is far more than preventing attacks launched by malicious hackers. Cyber security for smart energy improves the resilience[5] of the power system by mitigating the threats from security

Figure 2 | NIST framework for resilience (Credit N. Hanacek/NIST)

4 www.nist.gov/cyberframework

5 Resilience is defined as the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [SOURCE: US Presidential Policy Directive – Critical Infrastructure Security and Resilience].

An supplementary definition states that resilience includes "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."

"incidents" that affect cyber assets[6] that could disrupt operations.

Mitigation of threats to resilience combines cyber security techniques (such as access control, authentication, detection of anomalous behaviour, and incident logging) with organizational and engineering methods, which allow the organization to prepare for and adapt to changing conditions, as well as to withstand and recover rapidly from disruptions. These engineering methods would include traditional power system reliability measures, such as redundant equipment, contingency analysis, and backup systems, but would also include methods focused on addressing cyber asset vulnerabilities, such as planning for the loss of multiple cyber assets, isolation capability to limit cascading cyber attacks, and even training personnel in manual operations typically performed automatically.

Checks on data entry or control commands would be included in resilience support for the simple reason that mistakes are the most common "cyber incident". Since people with detailed knowledge of power system operations are the most dangerous attackers, additional cyber security and/or engineering methods may need to be deployed to mitigate this type of vulnerability, such as two-factor authentication, segregation of networks, and continuous monitoring for anomalous traffic. Backup generators, communication networks and spare cyber equipment should be located in secure sites, yet easily accessed when needed, because storms can affect not only the power system but also their cyber assets.

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

Section 2

Security by design as most cost effective approach

Designing security into cyber systems from the beginning is the most cost-effective approach to cyber security, since it minimizes risk and financial expenditure. 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 afterwards is costly because often they are *ad hoc* and require major modifications to system configurations, as well as significant retraining of personnel. If designed in 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, such as component designs, software implementations, 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 through security plan is critical for including security at each upgrade or replacement step.

Some of the security design aspects include becoming aware of potential threats and vulnerabilities through a risk analysis that takes into account the environments in which the component may be deployed before finalizing system and network configurations. For example, if some critical systems are located within a well-defined electronic security zone, then access to these critical systems can use the access and monitoring controls provided by the zone perimeters for crossing between different security zones (see Figure 3). Such a design reduces "attack surfaces" that could be exploited by malicious entities or simply misused by accident.

Security by design also permits more consistency across all systems with well-defined configurations of networks and information flows. Users would have consistent procedures to follow, rather than *ad hoc* security approaches. This consistency would therefore be easier to implement and maintain, less likely to have security gaps, and less costly to manage globally.

Security by design concepts can apply to planning for the inevitable "successful" security incidents (failure scenarios) which should trigger the development of procedures for coping, such as designing in degradation modes.

In security by design, access control can be implemented down to the data levels, not just 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 in the OT environment.

Flows of valid information to the right place within the right time are the most critical requirements for operational environments. Security by design, usually requiring new or updated applications, can ensure that this level of assurance can be provided by secure protocols which would be natively supported by systems and would be part of the core capabilities of the systems. For example, validating information can help mitigate the threat of people who have the knowledge to disrupt power system operations, by ensuring 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 institute 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 easily be designed into legacy systems, particularly since power system components may have vastly different life cycles. It is therefore crucial that even for existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades.

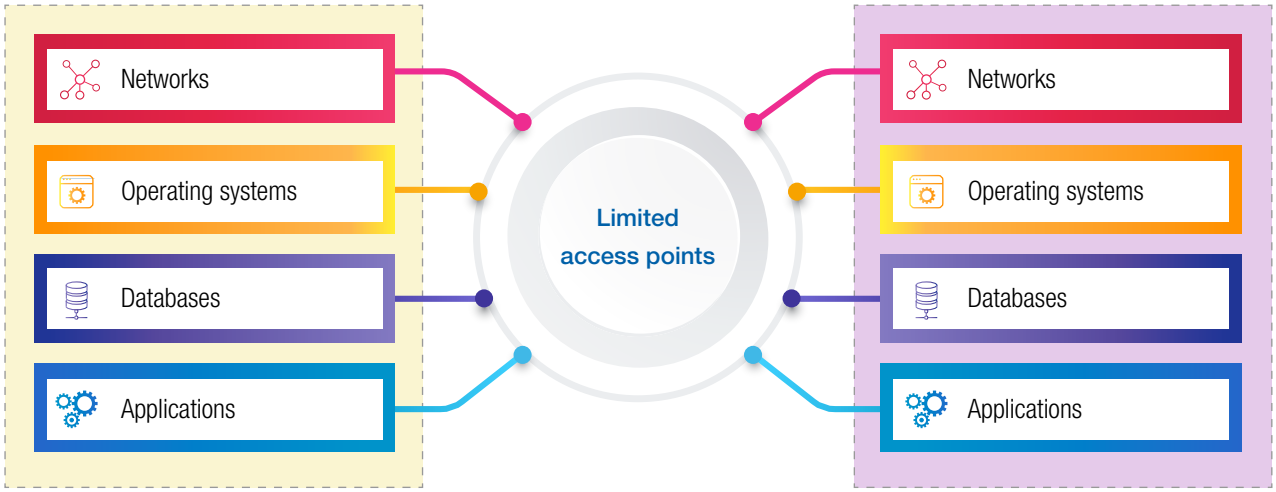

Figure 3 | Security by design example: electronic security perimeters with limited access points

Section 3

IT vs OT: different security requirements in the IT environment and technologies in OT environments

In traditional business environments, the IT department is considered the expert in all things termed “cyber security”. For most corporate cyber assets, this IT expertise is well placed to understand and address the threats, and to design methods to minimize vulnerabilities and respond to attacks. In general, corporate cyber assets are mostly concerned about the confidentiality of the information contained within computer systems, with the result that most IT security focuses on preventing access to this sensitive data.

However, technologies in the operational (OT) environment can affect the management of the cyber-physical power system and can thus affect safety and reliability. Therefore, technologies in the OT environment have different requirements and constraints when applying security measures to ensure that these systems can continue to support the same power system safety and reliability levels. For instance, security measures must take into account the time latency requirements of systems in the OT environment. For example, in substations the information flows can have latencies of less than a few milliseconds, while SCADA systems in control centres may need time latencies of seconds.

In the OT environment, deliberate cyber security incidents or inadvertent mistakes and failures of cyber assets can have physical repercussions since power systems are “cyber-physical systems”. The repercussion with the greatest consequence is safety: the deliberate or inadvertent mis-operation of a cyber asset could cause harm or even death. The second most important repercussion is the reliability of the power system to provide electrical energy or the gas system to provide gas energy to customers. Although these OT infrastructures have always been built with reliability of their physical assets (generators, breakers, transformers, power lines, gas lines) as the most critical design requirement, the reliability of the supporting cyber assets must nowadays also be designed to the same degree.

As illustrated in Figure 4, for IT environments, confidentiality of sensitive business and customer information is usually the most important, but in comparison for OT environments, the availability, authentication, authorization, and data integrity of power system information are usually the more critical requirements, since power data is typically not sensitive. With their experience in focusing on energy system reliability, it is often the experts in 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 methods and operations of the “physical” energy systems to minimize the impacts of such cyber asset incidents.

Operational environments have some very specific security challenges. For instance, high availability of both physical and cyber assets requires engineering designs with the focus on redundancy, high reliability, high performance requirements of these assets. The security requirements of the OT environment may necessitate changes in network configurations and information flows, such as 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 to those typically used in IT, for instance, requiring only authentication and not encryption.

At the same time, operational constraints must be taken into account in these designs. For instance, constraints on equipment resources (timing, bandwidth, network access) can impact the cyber security procedures and technologies that could be used. In particular, heavy encryption techniques or online access to certificate authorities are generally not possible for operational assets. Additionally, 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 for such updates.

Another constraining element for applying cyber security measures reflects the large numbers of legacy equipment with long life cycles that cannot be easily upgraded to include cyber security techniques. Therefore, other security measures must be found, such as virtual private networks or methods to isolate or segregate the devices. In addition, given the criticality of power system operations, security should not prevent operational actions, particularly emergency actions, meaning that “break the glass” scenarios must also be built into security procedures.

Another major change 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 (DERs) and communicating with smart meters. This use of IoT implies that utilities can no longer rely only on their own proprietary communication networks but must nonetheless still apply cyber security techniques to the interactions across public networks using well-known communication technologies.

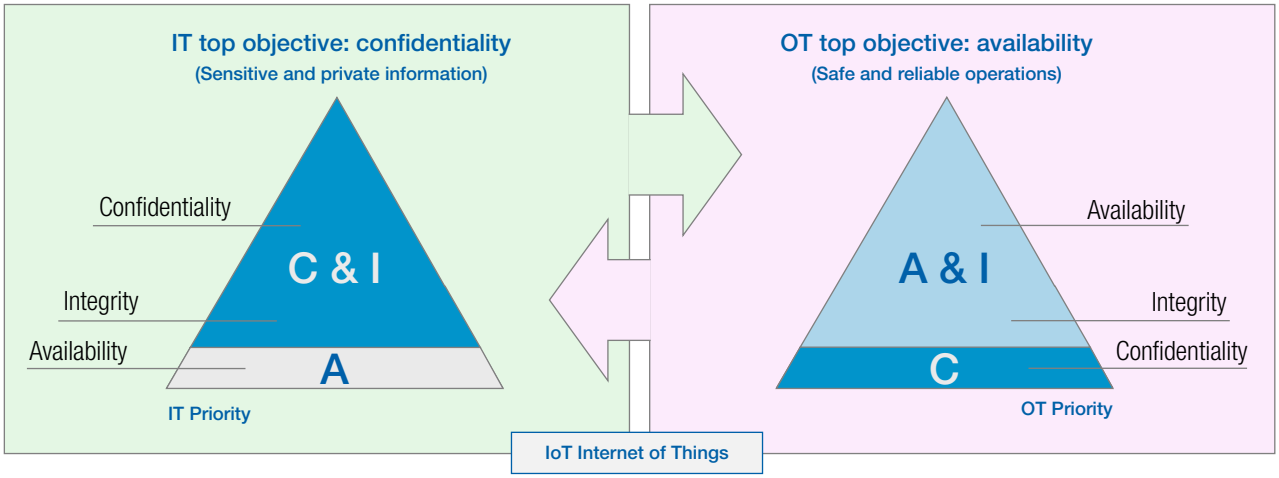

Figure 4 | Example of the different priorities of IT and OT primary security objectives

Section 4

Risk assessment, risk mitigation and risk life cycle processes

Risk assessment, risk mitigation, and life cycle continuous update of processes are fundamental methodologies for providing security. Using business requirements (financial, brand, operation, societal) as inputs, thanks to proven methodologies defined in international standards that are applicable for OT environments, organizations can determine security risk exposure, select and apply appropriate security measures, follow them closely and update them when needed, in a continuous improvement process.

Risk assessment involves both objective and subjective analyses. There are many risk assessment methods and guidelines that can be used to identify the risks in the OT environment. The choice of which risk assessment method to apply to different situations and environments could be quite challenging, depending on different constraints in different organizations, such as national regulations, time constraints, and executive directives.

There is no single or perfect way for mitigating risks. In the OT environment, the principles chosen for addressing risk mitigation must absolutely integrate the operational constraints of the systems in order to take into account personal safety, to provide protection of physical assets, and to ensure the required performance of these systems.

For the best risk assessment process, it is key to integrate the experts of each utility domain directly as part of the cyber security team, not only as contributors to risk mitigation methods, but also as contributors to risk assessment life cycle updates.

A risk can be described 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.

- Consequences may include safety, financial, environmental, societal, etc. of an event (e.g. failed process, loss of information, personnel harm)
- Risks should be identified, quantified or qualitatively described, and prioritized against risk criteria and objectives relevant to the organization

Risk assessment should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. Risk assessment should include:

- The systematic approach of estimating the magnitude of risks (risk analysis); and
- The process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation)

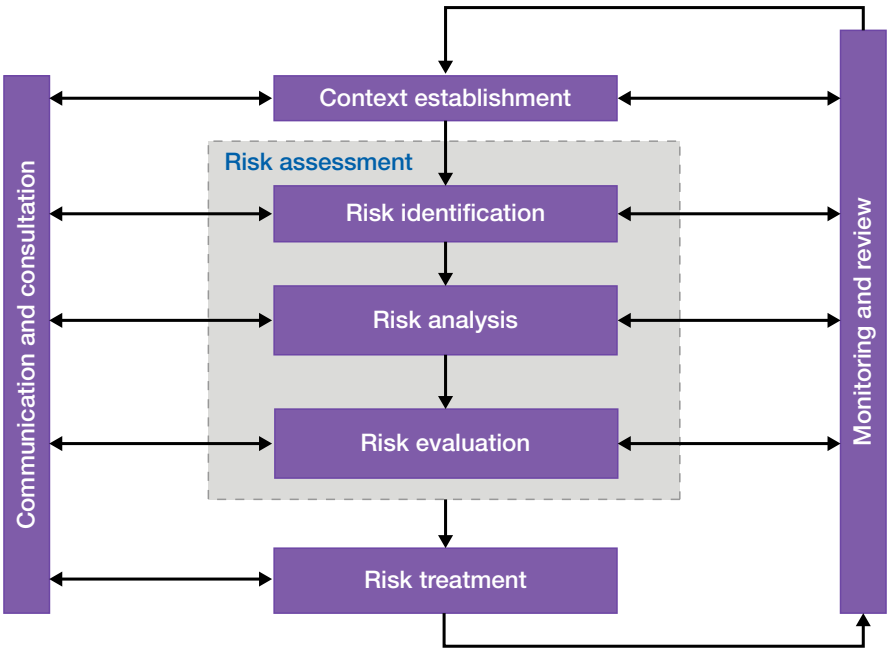

Figure 5 | Risk management process (ISO/IEC 27005:2018)

Figure 5 illustrates the general risk management process, while the key steps of any risk assessment method include:

- 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 the 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
- Threats can be associated with physical equipment, information, processes, interactions, configurations, and other assets
- Risk mitigation involves balancing the risk against the mitigation costs for reducing that risk to an acceptable level. Internal security policies must determine what are acceptable risks. 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[7] to mitigate the risks that were identified:
  - Security control solutions may consist of organizational measures, processes, and/or technologies that are implemented in the systems
  - The efficacy of the security control solutions could be assessed to determine if they have actually mitigated the risk acceptably

7 Control (from ISO/IEC 27000:2018): measure that is modifying risk. Note 1 to entry: Controls include any process, policy device, practice, or other actions which modify risk. Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.

  - These security control solutions could include both cyber security measures as well as power engineering measures (procedures, technologies, and/or real-time operations)
- Once the risk assessment has been completed and the risk mitigation control solutions have been selected, these solutions are implemented on the systems
  - Verify over time that the applied controls have been applied correctly and really provide the expected mitigations
  - Include an assurance process, such as an audit, possibly by a different group
- 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
  - Some security control solutions may not be able to be implemented in some systems, particularly for legacy systems (e.g. anti-virus applications or secure patching procedures)
  - Constraints on these control solutions should be identified, given the variety of issues associated with diverse OT environments, such as different constraints in a substation environment (long times between the ability to patch systems) or a DER environment (poor on-site security knowledge)
- Over time, all of these control solutions should be monitored to ensure that they are continuing to be effective or if possible attacks have potentially overcome the control solutions
  - In all cases, possible security events identified by this monitoring should be sent to a central CERT site
  - The CERT should be capable of filtering and assessing the importance of any security event or sequence of security events

Section 5

Cyber security standards and best practices

Given the complexity of business processes and the wide variety of cyber assets used in the smart energy environment, no existing single cyber security standard can address all security requirements, security controls, resilience strategies, and technologies. Some standards and guidelines are focused on the high level organizational security requirements and more detailed recommended controls (what), while other standards focus on the technologies that can be used to supply these cyber security controls through validated techniques and with a focus on interoperability (how).

While many additional documents and regulations are applicable to national and local regions, the key IEC, ISO, IEEE, NIST, and IETF cyber security standards and best practices are illustrated in Figure 6, organized by type (what, how, process towards compliance) and by level (high general level, high energy-specific level, detailed technical level).

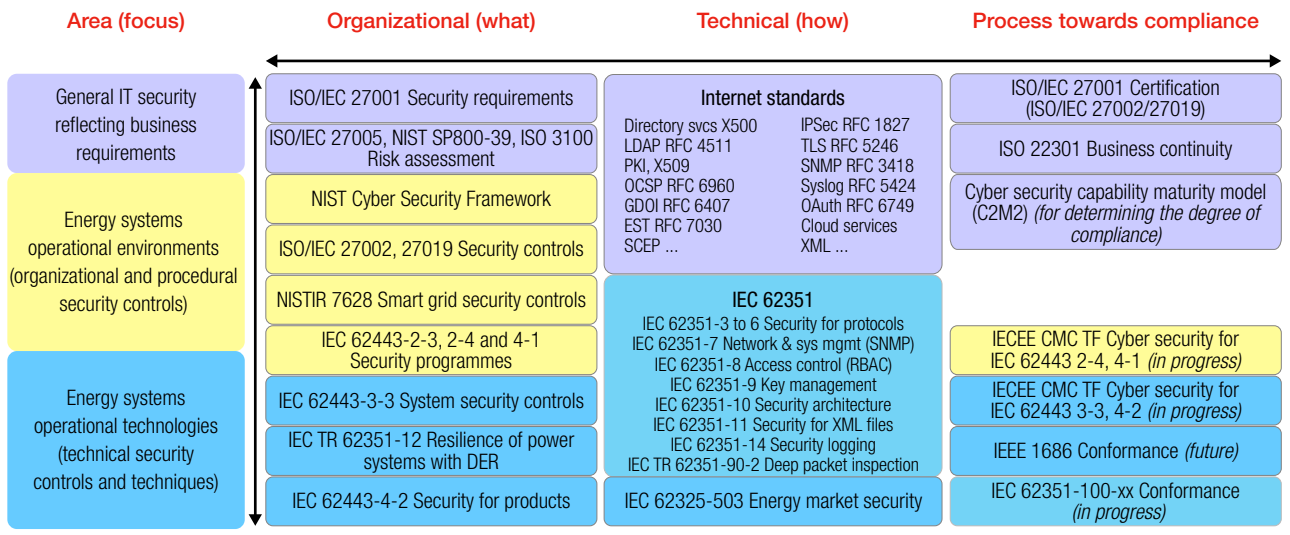

Figure 6 | Key cyber security standards and guidelines

Section 6

Conclusions

As cyber security has become an increasingly vital requirement for any business to survive in an increasingly automated environment, corporate executives must become cognizant of the key security and resilience characteristics of their business since the security culture must start from the top of an organization. Security policies, security procedures, and security technologies can only be effective if security and resilience is seen as critical by top management and is promulgated down to all levels. This requirement is particularly important for businesses that are deemed critical infrastructures, particularly those in the energy operational environment.

Five concepts for cyber security are critical for executives in the energy operational environment to understand as their businesses struggle to implement the necessary cyber security policies, procedures, and technologies.

Concept #1 Resilience should be the overall strategy for ensuring business continuity. When focusing on resilience in general, organizations must consider safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify and prevent), but also during such incidents (detect and respond) and after incidents have been resolved (recover).

Concept #2 Security by design is the most cost-effective approach to security. Security is vital for all critical infrastructure and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented. However, it is recognized that security cannot easily be added to legacy systems, so it is crucial that even for these existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades.

Concept #3 IT and OT are similar but different. Technologies in operational environments (called OT in this document) have many differing security constraints and requirements from information technologies (IT) environments. The primary reason is that energy systems are cyber-physical systems and security incidents can cause physical safety incidents and/or vital losses of energy. Therefore, availability, authentication, authorization, and data integrity of operational information are usually more critical requirements than confidentiality. Nonetheless, both IT and OT environments are increasingly relying on IoT technologies.

Concept #4 Risk assessment, risk mitigation, and continuous update of processes are fundamental to improving security. Based on an organization's business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, and reputational) for all its business processes. Risk assessment identifies the vulnerabilities of systems and processes to deliberate or inadvertent threats, determines the potential impacts of incidents, and estimates the likelihood that the incident scenarios could actually occur.

Concept #5 Cyber security standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programmes and policies. Cyber security measures should not be re-invented: key cyber security standards and best practice guidelines have already been developed

for different areas and purposes of security. Cyber security planning should use these cyber security standards and guidelines to improve resilience, security, and interoperability throughout the energy OT environment, using the right standards, guidelines, and procedures for the right purposes at the right time.

Taking these 5 concepts into account, some key conclusions include:

- The executive level must take the lead on cyber security. Many cyber security issues must be addressed at the executive level, such as security policies, system architectures, personnel organization, security procedures, and types of security technologies:
  - In particular, security education and training programmes need to be developed, as well as policies on sharing security vulnerabilities, threats, and solution information with other corporations such as through CERTs
  - For example, just encrypting communications does not mean that the systems are secure: stolen or guessed passwords can still permit dangerous actions to be instigated in cyber-physical systems
- The existing cyber security standards and best practices related to security requirements and controls are quite mature and should be the start of any cyber security process. However, implementing the security procedures and technologies to meet the requirements of these existing standards may not be completely effective:
  - Cyber standards are regularly reviewed and updated to reflect new security issues and may not be available and/or complete
  - New technologies are always introducing new threats and/or vulnerabilities, for which new standards or guidelines need to be developed
  - Cyber hackers are always inventing new ways of exploiting vulnerabilities which can cause cyber incidents. Standards or guidelines may not have yet had time to address these new threats
  - Compliance with cyber security standards provide a large level of assurance, but this does not mean that the systems are necessarily completely secure, partly because the complexity of systems and their configurations may make it impossible to address all cyber issues, and partly because there will always be successful attacks
  - Cyber security standards can support the interoperability of these increasingly complex communicating systems, by defining validated and limited sets of security technologies and procedures
- Continuous monitoring and improvement of security measures is vital, given that technologies are always changing, new vulnerabilities are being found daily, and cyber hackers are always one step ahead of cyber security solutions

About the IEC

The IEC, headquartered in Geneva, Switzerland, is the world's leading publisher of international standards for electrical and electronic technologies. It is a global, independent, not-for-profit, membership organization (funded by membership fees and sales). The IEC includes 173 countries that represent 99% of world population and energy generation.

The IEC provides a worldwide, neutral and independent platform where 20 000 experts from the private and public sectors cooperate to develop state-of-the-art, globally relevant IEC International Standards. These form the basis for testing and certification, and support economic development, protecting people and the environment.

IEC work impacts around 20% of global trade (in value) and looks at aspects such as safety, interoperability, performance and other essential requirements for a vast range of technology areas, including energy, manufacturing, transportation, healthcare, homes, buildings or cities.

The IEC administers four conformity assessment systems and provides a standardized approach to the testing and certification of components, products, systems, as well as the competence of persons.

IEC work is essential for safety, quality and risk management. It helps make cities smarter, supports universal energy access and improves energy efficiency of devices and systems. It allows industry to consistently build better products, helps governments ensure long-term viability of infrastructure investments and reassures investors and insurers.

A global network of 173 countries that covers 99% of world population and electricity generation

Offers an affiliate country programme to encourage developing countries to get involved in the IEC free of charge

Develops international standards and runs four conformity assessment systems to verify that electronic and electrical products work safely and as they are intended to

IEC International Standards represent a global consensus of state-of-the-art know-how and expertise

A not-for-profit organization enabling global trade and universal electricity access

Key figures

173
members and affiliates

>200
technical committees

20 000
experts from industry, test and research labs, government, academia and consumer groups

10 000
international standards published

4
global conformity assessment systems

>1 million
conformity assessment certificates issued

>100
years of expertise

ISBN 978-2-8322-7544-3

CHF 50.-

International Electrotechnical Commission

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

IEC TEC Cyber security:2019-10(en)