Federal Ministry
for Economic Affairs
and Energy

中国国家标准化管理委员会
Standardization Administration of the P.R.C.

中华人民共和国工业和信息化部

Security Standards White Paper for Sino-German Industrie 4.0/ Intelligent Manufacturing

Sino-German Industrie 4.0/Intelligent Manufacturing
Standardisation Sub-Working Group

STANDARDIZATION COUNCIL INDUSTRIE 4.0

国家智能制造标准化总体组

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Imprint

Publisher
Federal Ministry of Economic Affairs and Energy
Department of Public Relations
11019 Berlin
www.bmwi.de

Text
Standardization Council Industrie 4.0
DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik in DIN und VDE,
60596 Frankfurt am Main

Design and production
AKRYL digital agency, Hamburg

Status
April 2018

Zertifikat seit 2009 audit berufundfamilie

The Federal Ministry for Economic Affairs and Energy was awarded the audit berufundfamilie® for its family-friendly staff policy. The certificate is granted by berufundfamilie gGmbH, an initiative of the Hertie Foundation.

FSC www.fsc.org MIX Paper from responsible sources FSC® C106273

Content

International/Domestic Cyber Security Standards in the Context of Industrie 4.0 and Manufactured in China 2025

1 Introduction

The third meeting of the Sino-German Industrie 4.0 / Intelligent Manufacturing 2025 Standardisation Working Group (hereinafter referred to as the „Working Group“) was held in Berlin, Germany, from 28 to 30 Nov. 2016. The conference was organized by the Chinese Ministry of Industry and Information Technology and the German Federal Ministry of Economics and Energy. At the meeting, Sino-German partners decided to propose the white paper on the current status of security standards for Industrie 4.0/ Intelligent Manufacturing.

The white paper will consider the international / domestic (including Chinese and German) security standards in the context of Industrie 4.0/Intelligent Manufacturing 2025, especially the hierarchical structure of security standards ISO/IEC 27000 series and IEC 62443 series, and describe requirements and challenges of complying with these security standards (costs, migration, oversee production, etc.). Security standards regarding the following aspects, are involved:

- Communication security
- Security during product development
- Supplier relationship security
- Security incident management
- Asset management
- Interoperability

2 Overall Security Standards

This white paper will address the well-known international standards like ISO/IEC 27000 series, IEC 62443 series and specific national standards of China and Germany.

2.1 ISO/IEC 27000 series

The ISO/IEC 27000 series (also known as the ‚ISMS Family of Standards‘ or ‚ISO27k‘, for short) comprise information security standards that are jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
This standard series provides best practice recommendations for information security management - the management of information risks through information security controls, within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems.

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT/technical cyber security issues, and is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them (typically using information security controls) according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents.

This white paper focuses on ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019, which are closely related to Industrial Automation Control System (IACS).

1. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, monitoring, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature

2. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining ISMS. This standard contains 14 security control clauses, collectively containing a total of 35 main security categories and 113 controls. It gives guidelines for organizational information security standards and information security management practices, including the selection, implementation and management of controls taking into consideration the organization‘s information security risk environment(s).

3. ISO/IEC 27019 is intended to help organizations in the energy industry, to interpret and to apply ISO/IEC 27002 for securing electronic process control systems. Information security management presents fundamentally the same risk management challenges in all contexts, but the real-time nature of process control systems and the safety and environmental criticality make some of the challenges particularly extreme for organizations in the energy industry. This standard will therefore provide additional and more specific guidance on information security management, compared to that provided by ISO/IEC 27002.

The process of ISMS implementation and certification is clearly described in Figure 1.

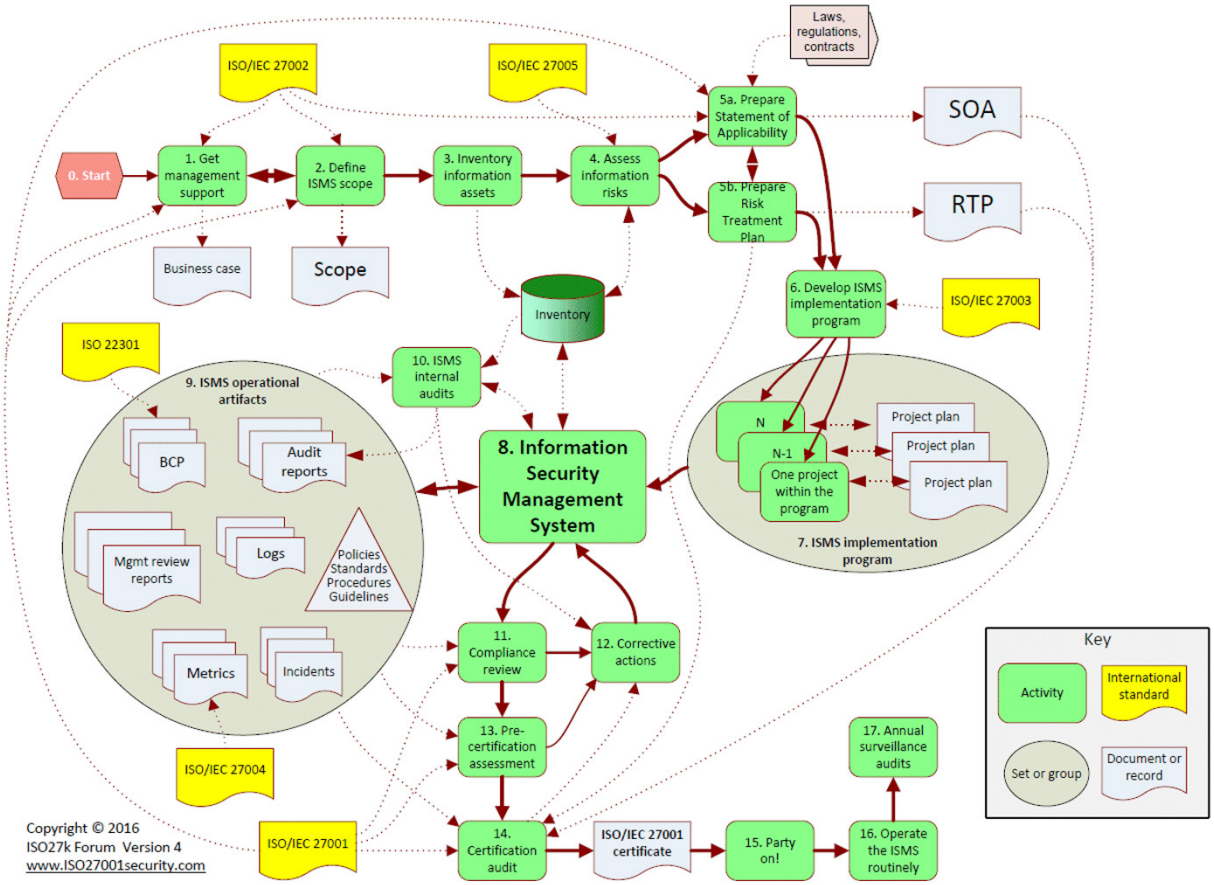

Figure 1 ISMS implementation and certification process flow chart

2.2 IEC 62443 series

Industry Safety includes functional safety, physical safety and information security. The IEC 62443 series focuses on the aspects of IACS. IACS includes control systems used in manufacturing and processing plants and facilities, as well as other controls systems related to Industrie 4.0.

IEC 62443 is a series of standards, technical reports and related information that define procedures for implementing electronically secure IACS. This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. IEC 62443 standards and technical reports are organized into four general categories, namely, General, Policies and Procedures, System, and Component, as described in Figure 2.

1. The first (top) category includes common or foundational information such as concepts, models and terminology. It also includes work products that describe security metrics and security life cycles for IACS.

2. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.

3. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core concept in this category is the zone and conduit design model.
According to IEC 61508, it is necessary to consider safety and security from the whole life cycle of a system. Therefore, it is necessary to define the SL (security level) when the system is defined, to clarify the security level required for that part (as in some areas, higher requirements are defined as SL4, while some requirements are not so critical are defined as SL1). Afterwards, corresponding risk analysis will be performed to determine the need for risk level reduction.

4. The fourth category includes work products that describe the specific product development and technical requirements of control system products. This is primarily intended for controlling product vendors, but can also be used by integrators and asset owners to assist the procurement of secure products.

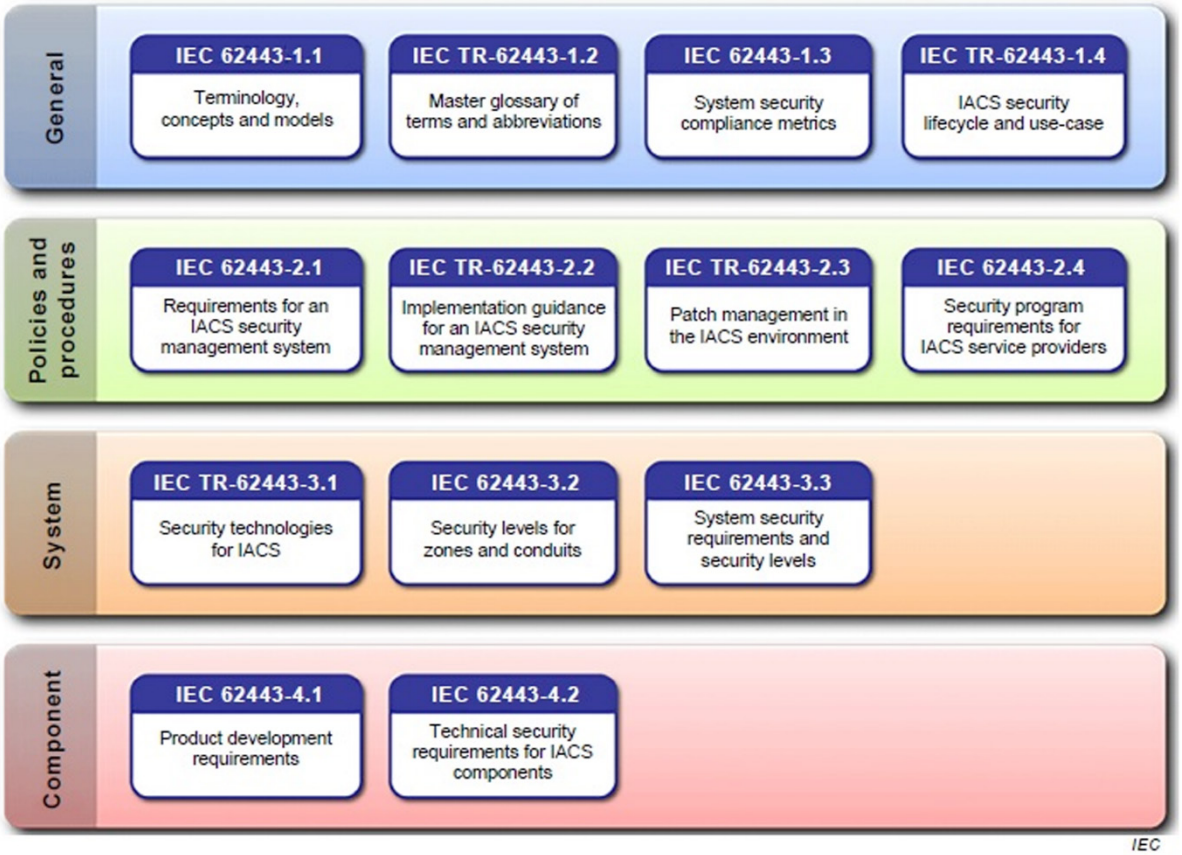

Figure 2 Structure of IEC 62443 standard series

Confidentiality (C), integrity (I) and availability (A) are the three main objectives of IT security. The priority of these three factors are in the order of CIA. However, the security priority in an IACS is AIC, as Figure 3 shows. Because industrial data is available in different vendor-specific format, it is necessary to work with the relevant environment for analysis to obtain its value. Besides, the availability of the system directly affects the production - production line downtime or misuse may lead to huge economic losses, as well as loss of human life or environmental damage.

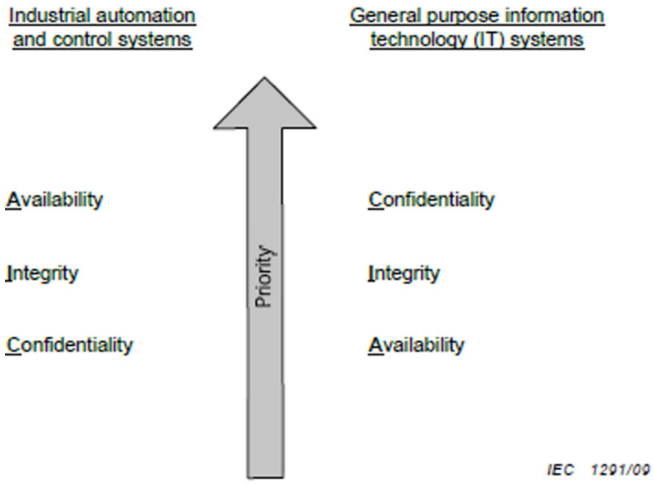

Figure 3 Difference of objectives priority between IACS and IT systems

2.3 China Specific Standards

Some of China national standards are localizations of ISO/IEC standards. For example, GB/T 22080 is a mirror of ISO/IEC 27001 and GB/T 22081 is a mirror of ISO/IEC27002. Some adopt the ISO/IEC standards partly. For example, GB/T 30976 overlaps partly with IEC 62443.

Classified protection standards are China specific ones. The aim is to improve China's information systems security construction, ensuring the coordination of information security and information construction. It is conducive to providing systematic, targeted, feasible guidance and services, effective control of information security construction costs. It is also conducive to optimizing the allocation of security resources, and to ensuring the security of critical infrastructure, effectively solving the information security threats and other security problems.

China has published the series of classified protection standards that covers the whole life-cycle of an organization's information security, including baseline requirement, design, implementation guide, testing and evaluation process, as listed below.

- GB 17859-1999 Classified criteria for security protection of computer information system
- GB/T 22239-2008 Information security technology - Baseline for classified protection of information system security
- GB/T 22240-2008 Information security technology - Classification guide for classified protection of information system security
- GB/T 25058-2010 Information security technology - Implementation guide for classified protection of information system
- GB/T 25070-2010 Information security technology - Technical requirements of security design for information system classified protection
- GB/T 28448-2012 Information security technology - Testing and evaluation requirement for classified protection of information system
- GB/T 28449-2012 Information security technology - Testing and evaluation process guide for classified protection of information system security

In GB 17859-1999, the security protection capability of information system is defined in five levels:

1. User independent protection level,
2. System audit protection level,
3. Security tag protection level,
4. Structured protection level, and
5. Access verification protection level.

At these five levels, a higher level of security capability includes those lower level(s).

2.4 Germany Specific Standards

The comprehensive BMWi Ministry guidance "IT-Sicherheit für die Industrie 4.0" [34] provides recommendations on addressing security for smart manufacturing, industrial internet of things and digital plants.

The VDI/VDE guidance "IT-security for industrial automation – General model" part 1 [35] and further parts provide in-depth considerations of the security aspects of product and platform development companies, engineering and integration companies and operation and maintenance utilities.

2.4.1 German BSI Guidance

German regulations are integrated in the regulations of the European Union.

Additionally, in Germany, the German Federal Office for Information Security as the national cyber security authority, shapes information security in digitalization through pre-

vention, detection and reaction for government, business and society.

According to the German name "Bundesamt für Sicherheit in der Informationstechnik", the prefix for the corresponding standards and guidance publications is BSI. Below, some of these standards are introduced, and are all available (in German) online at www.bsi.bund.de. The new versions have the numbers 200-1, 200-2 and 200-3.

BSI Standard 100-1 Information Security Management Systems (ISMS) [28]

BSI Standard 100-1 defines the general requirements for an ISMS. It is completely compatible with ISO/IEC Standard 27001 and moreover, takes into consideration, the recommendations in other standards of the ISO/IEC 2700x family. It provides readers with easily understandable and systematic instructions, regardless of which methods they wish to use to implement the requirements.

BSI presents the content of these ISO/IEC Standards in its own BSI Standard, to describe some issues in greater detail and therefore facilitate a more didactic presentation of the contents. In addition, the content was organized to be compatible with the "IT-Grundschutz" (Baseline Protection Profile) approach. The common headings in the two documents make orientation easier for the reader.

BSI-Standard 100-2: IT-Grundschutz Methodology [30]

The IT-Grundschutz Methodology progressively describes (step by step) how information security management can be implemented and operated in practice. The tasks of information security management and implementing a security organization are important subjects in this context. The IT-Grundschutz Methodology provides a detailed description of how to produce a practical security concept, how to select appropriate security safeguards, and what is important when implementing the security concept. The question as to how to maintain and improve information security in ongoing operation is also answered.

Thus, IT-Grundschutz interprets the very general requirements of the ISO/IEC 2700x family of standards, and helps the users to implement them in practice, with many notes, background expertise and examples. The IT-Grundschutz Catalogues not only explain what has to be done, they also provide very specific information as to what implementation (even at a technical level) may look like. The IT-Grundschutz approach is therefore a tested and efficient approach to meet all the requirements of the ISO/IEC Standards mentioned above.

BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz [32]

The IT-Grundschutz Catalogues of the BSI contain standard security safeguards required in the organizational, personnel, infrastructure and technical areas, which are generally appropriate for normal security requirements and for protecting typical information domains. Many users who are already working successfully with the IT-Grundschutz, are confronted with the question: how to deal with areas whose security requirements clearly go beyond the normal measure? It is important that the basic methodology does not produce a great deal of additional effort and expense, and reuses as many approaches as possible from the IT-Grundschutz.

To cover these issues, the BSI has formulated a method of analyzing risks, based on IT-Grundschutz. This approach can be used when companies or public authorities are already working successfully with the IT-Grundschutz Manual and would like to add an additional security analysis to the IT-Grundschutz analysis as seamlessly as possible. There may be different reasons for this:

- The protection requirements of the company or the public authority go beyond the normal measure (high or very high protection requirements).
- The institution operates important components, which are (still) not treated in the IT-Grundschutz Catalogues of the BSI.
- The target objects are operated in application scenarios, which are not designated within the framework of the IT-Grundschutz.

This approach is aimed both at the users of information technology (those responsible for information security) and at consultants and experts. However, it is usually advisable to rely on professional expertise when conducting risk analysis.

BSI-Standard 100-4: Business Continuity Management [34]

The BSI Standard 100-4 points out a systematic way to develop, establish and maintain an agency-wide or company-wide internal business continuity management system. The goal of business continuity management is to ensure that important business processes are only interrupted temporarily or not interrupted at all, even in critical situations. To ensure the operability, and therefore the survival, of a company or government agency, suitable preventive measures must be taken to increase the robustness and reliability of the business processes, as well as to enable a quick and targeted reaction in case of an emergency or a crisis.

2.4.2 European ENISA Guidance

Guidance on Maturity levels

ENISA (European Union Agency for Network and Information Security) has many publications in terms of several subtopics, e.g. cyber crisis management, data protection, incident reporting, IoT and smart infrastructures and threat and risk management etc.

ICS-SCADA maturity models

The ICS-SCADA environment is a fundamental component of European and national Critical Infrastructures. Critical infrastructure operators demand high quality, real time information to make more accurate and justified business decisions. The technological agenda of future plans is focused on the following topics: Internet of Things, Smart Infrastructures, E-Health, Connected Retail and Industrie 4.0, among other things. The ICS-SCADA Cyber Security Maturity Analysis [32] was conducted on the basis of publicly available information, and interviews with relevant national authorities in various Member States. For the purpose of this assessment of maturity levels in each Member State, an ICS-SCADA security maturity model was developed. Three tasks are desk research, series of interviews and a summary list of all security requirements. The ICS-SCADA model is illustrated in Figure 4.

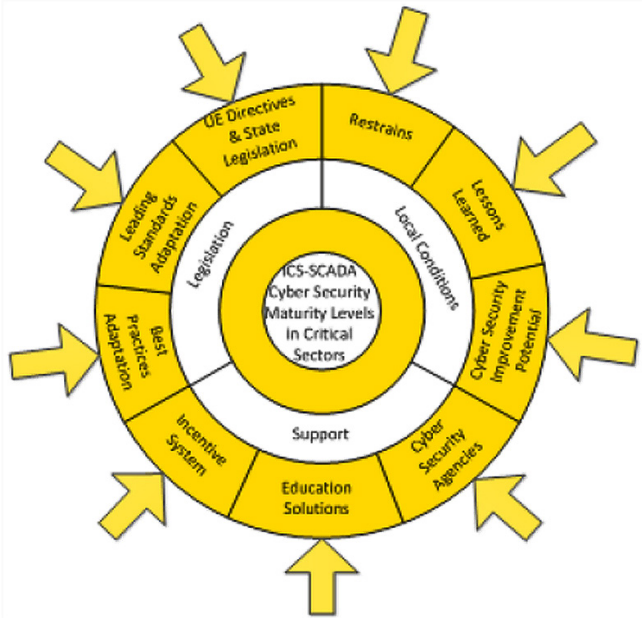

Figure 4 Dimensions of ICS-SCADA Security Maturity Model

The model was built from three major operating model dimensions, which are further divided into nine operating model sub-dimensions.

The Legislation - Operating Model Dimension describes how advanced the legal model of a particular Member States is in terms of ICS-SCADA cyber security improvement. It covers responsibilities, regulations and policy activities in the area of ICS-SCADA cyber security at Member States level.

The Support - Operating Model Dimension captures how efficient Member States support critical service providers in improving ICS-SCADA cyber security by actively participating in cyber security assessments and development processes. It identifies actions aiming at increasing awareness, gathering and the propagation of information on existing good practices.

The Local Conditions - Operating Model Dimension reports the opportunities and challenges in terms of ICS-SCADA cyber security improvement and identifies focus areas for the future.

Communication network interdependencies in smart grids This report presents an analysis of the current situation of smart grid networks, considering the most relevant factors in this case, including: the role networks play in smart grid domains, the main threats affecting these communication infrastructure networks, and the interdependencies between networks. Several aspects are included:

- Review and analyze communication infrastructures in use in smart grids at different domains: end-user premises (HAN, IAN, and BAN), transmission grids, distribution grid, generation (bulk and DER), electric vehicle and other power storage facilities.
- Study connectivity interdependencies for smart grids among different domains in the electricity system within and between member states.
- Obtain a list of the main threats affecting communication networks in smart grids.
- Evaluate the current situation and possible network attacks with cascading effects on large parts of the population.
- Collect good security practices and measures for the communication networks (including different channels, technologies and protocols).
- Analyze, in relation to the identified good security practices, gaps in current implementations of communication networks in all smart grid domains.
- Explore limiting factors, impairments, constraints and potential incentives for the target audience to deploy these measures.

The study was carried out using a five-step methodology, as Figure 5 shows. From identification of experts to conclusions and recommendations.

Figure 5 Five-step methodology

2.5 Other Security Standards and Reports

2.5.1 NIST Security Standards

NIST Special publication 800-53 rev4, „Security and Privacy Controls for Federal Information Systems and Organizations", published in April 2013, specifically addresses the 194 security controls that are applied to a system to make it „more secure".

NIST Special Publication 800-82, Revision 2, „Guide to Industrial Control System (ICS) Security", revised in May 2015, describes how to secure multiple types of Industrial Control Systems against cyber-attacks, while considering the performance, reliability and safety requirements specific to ICS. The NIST Cyber Security Framework (NIST CSF) provides a high-level taxonomy of cyber security outcomes and a methodology to assess and manage those outcomes. It is intended to help private sector organizations that provide critical infrastructure, with guidance on how to protect this infrastructure, along with relevant protections for privacy and civil liberties.

2.5.2 Cyber security Report(s) within Industrie 4.0

The 2016 BSI Status Report provides a reliable and in-depth description of current developments in IT security. It covers the time period from September 2015 to February 2016. Software and hardware vulnerabilities are reported. During the investigation period, 404 incidents were recorded, 98% of which concerned the availability of cloud services. 78% of the service outages (317 incidents) occurred directly in the services layer of the cloud. The virtual resources layer was the second most frequent source of outages with a figure of 12% (46 incidents). Figure 6 is the comparison of incidence of vulnerabilities between this report and the previous one.

For the software vulnerability, BSI focuses on attack method and means, e.g. malware, ransomware, APT (Advanced Persistent Threats), Spam and Botnets etc. One of the examples is related to the I4.0—malicious software in a nuclear power plant in 2009. The virus Ramnit infects the visualization computer in SCADA in NPPs, and both virus Conficker and Ramnit use USB storage devices in order to infect other systems. Even though finally the Ramnit control server had been shut down by Europol, the cost was still significant in terms of the working time and fees.

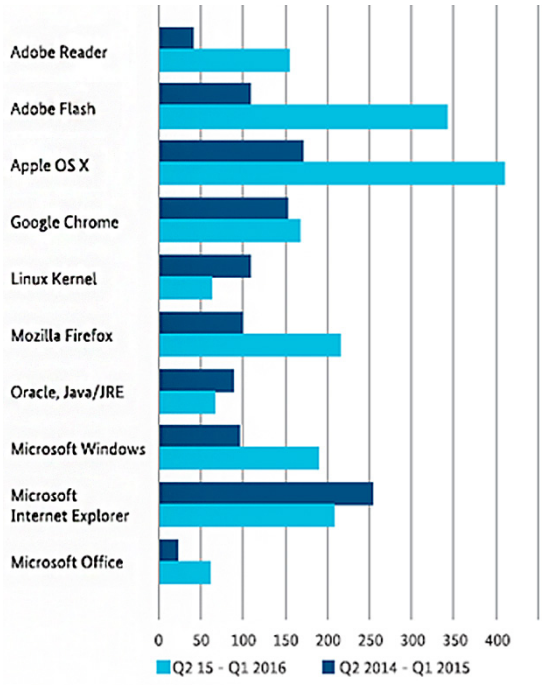

Figure 6 Incidence of vulnerabilities

Security in critical infrastructures has been referenced in the BSI report in 2016, which includes healthcare, power supply and voice and data transmission. One example for healthcare is a power outage that occurred in Ukraine in December 2015, which was evidently a consequence of a coordinated cyber-attack on several energy network operators. Approximately 225,000 inhabitants were affected. An example for power supply is the cyber-attacks on the SWIFT system. During the second half of 2016, several incidents came to light, in which unknown parties gained unauthorized access to 'Society for Worldwide Interbank Financial Telecommunication' (SWIFT) communication services. The Philippine news portal 'Inquirer.net' reported a cyber bank heist in March. According to this, attackers succeeded in removing 81 million US dollars from the Central Bank of Bangladesh without authorization. Three major disruptions occurred in Germany among ICT providers, which affected between 750,000 and 2.7 million people in each case, and resulted in the loss of Internet access, tele-

phone services and mobile communication.

Under the BSI Act, defending against attacks on the Federal Government IT systems is a core task incumbent on the BSI. For this purpose, BSI has developed requirements for a secure centralized remote maintenance service that takes into account, the operating requirements, in addition to security characteristics. The service is intended to protect the congeniality and integrity of sensitive data involved in remote maintenance work, using sufficiently strong cryptographic algorithms.

Another aspect of this report that refers to Industrie 4.0, is OPC UA. The networking of ICS is continually advancing, in particular, as part of Industrie 4.0 ICSs. Ensuring security and, at the same time, meeting the requirements of a modern and flexible smart factory, is a difficult challenge to overcome. The platform-independent and globally recognized communications protocol, OPC UA, provides the necessary cryptographic mechanisms for a secure factory, and is regarded as a key element on the road to Industrie 4.0. It enables the integration of industrial components and processes across different layers of the automation pyramid. BSI conducted an independent investigation on the security-relevant elements of OPC UA in 2015. Apart from some minor issues, OPC UA has implemented the 'Security by Design' principle consistently, and is facilitating the secure networking of industrial systems, when these are used correctly and with a comprehensively protected infrastructure.

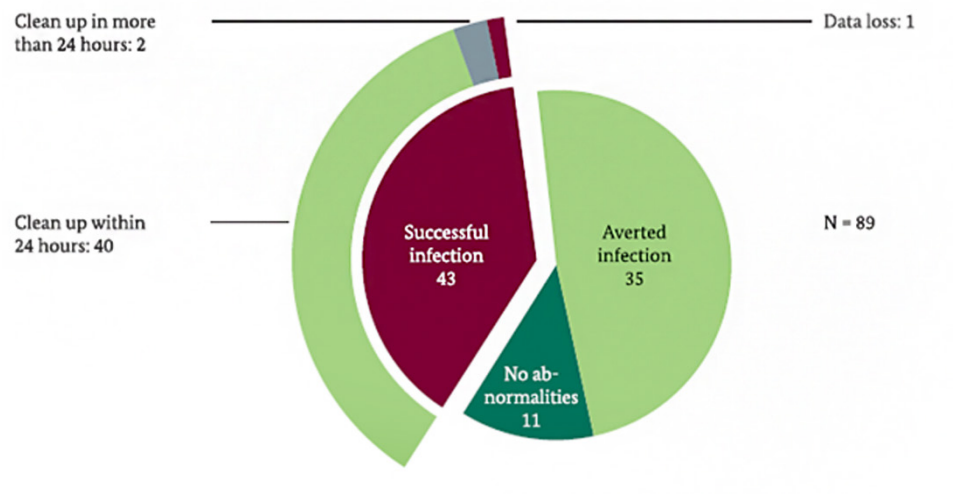

Figure 7 Result of the survey on concern due to ransomware in German healthcare

3 Communication Security

3.1 ISO/IEC 27033

The connection between different networks or inside a network, is an important factor for the implementation of Industrie 4.0, thus, incorporating network security as necessary during the design, implementation, management and operation of systems. The ISO/IEC 27033 series technical specification focuses on the network security, and provides the guidelines of design, implementation, management and operation of network security. Figure 8 is the architecture of ISO/IEC 27033 series technical specification. This specification gives several reference networking scenarios, which uses VPN (Virtual Private Networks), gateways, IP convergence and wireless and radio techniques to design a network.

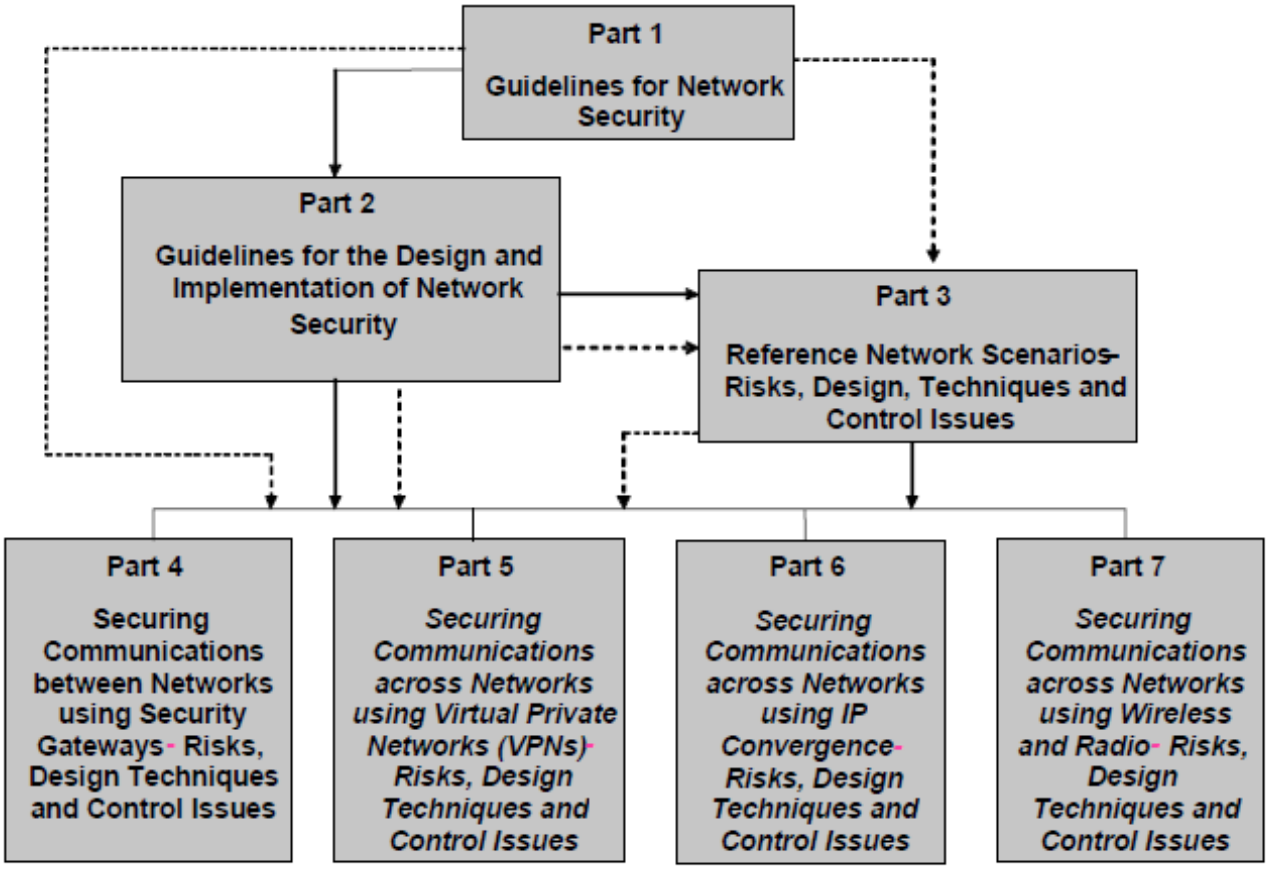

Figure 8 ISO/IEC 27033 Road Map

1. ISO/IEC 27033-1:2015: network security overview and concepts
   - Provides a roadmap and overview of the concepts and principles underpinning the remaining parts of ISO/IEC 27033.
   - Provides guidance on a structured process to identify and analyze network security risks and hence define network security control requirements, including those mandated by relevant information security policies.
2. ISO/IEC 27033-2:2012 Guidelines for the design and implementation of network security
   - Scope: planning, designing, implementing and documenting network security.
   - Defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where end-to-end security is a concern and independently of the network's underlying technology.
3. ISO/IEC 27033-3:2010 Reference networking scenarios -- threats, design techniques and control issues
   - Objective is "to define the specific risks, design techniques and control issues associated with typical network scenarios"
   - Discusses threats, specifically, rather than all the elements of risk.
4. ISO/IEC 27033-4:2014: Securing communications between networks using security gateways
   - Provides an overview of security gateways through a description of different architectures.
   - Guideline on securing communications between networks through gateways, firewalls, application firewalls, Intrusion Protection System etc. in accordance with a policy, including identifying and analyzing network security threats, defining security control requirements, and designing, implementing, operating, monitoring and reviewing the controls.
5. ISO/IEC 27033-5:2013: Securing communications across networks using Virtual Private Networks (VPNs)
   - Objective: to provide "guidelines for the selection, implementation and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks".
   - Provides guidance for securing remote access over public networks.
   - Introduces different types of remote access including protocols, authentication issues and support when setting up remote access securely.
6. ISO/IEC 27033-6: 2016 Securing wireless IP network access
   - Objective: "to define the specific risks, design techniques and control issues for securing IP wireless networks. This part is relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless networks (for example, network architects and designers, network managers, and network security officers)".
   - This is a generic wireless network security standard offering basic advice for WiFi, Bluetooth, 3G and other wireless networks.

During the design of network security, defense in depth is an important principle. Defense in depth is a way to protect one target to prevent attacks or mitigate the bad consequences, using different controls or measures. For example, in order to protect the date security, countermeasures can be taken from application level, host level, infrastructure level and perimeter level - the fine grain rises from the date level to perimeter level, as shown in Figure 9.

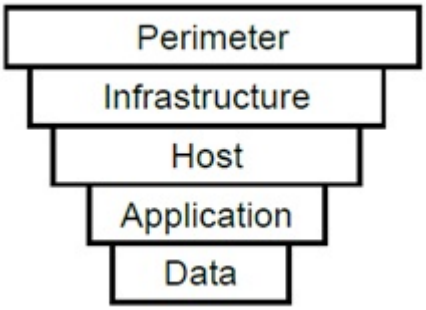

Figure 9 Defense in Depth

A real-world example for defense in depth is the loss prevention and robbery protection of banks.

Firstly, the remote monitoring and real time recording cameras have been set to deter bad people. If this is not enough, then there are guards with guns, protecting the bank. Additionally, the bulletproof glass and electronically locked doors are another protection measure to protect workers from shooting. If robbers happen to break through the doors, there is still a vault that is locked by several locks. To protect the vault, keys are distributed between two workers, who are rarely in the bank at the same time. Thus, for a successful bank robbery, the robbers must breach each protection measure, which will take some time and coordination. These defense in depth measures allow workers enough time to contact the police, in the event of a robbery.. All of these measures cannot prevent bank robberies, but can reduce the probability of a successful robbery.

3.2 IEC 62443

As mentioned above, the IEC 62443 series technical specification focuses on the security for IACS, which also suggests that before designing or redesigning a system, dividing the system into different zones and conduits of different Safety Levels (SLs) is necessary.
Figure 10 illustrates an example of a manufacturing system. According to the specification in this standard, this system is divided into four zones, which are enterprise network, industrial/ enterprise DMZ and two industrial networks. Three conduits are defined to implement the connection between different networks.

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure or ingress of network traffic into a control system, and to reduce the spread or egress of network traffic from a control system. This improves overall system response and reliability, as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

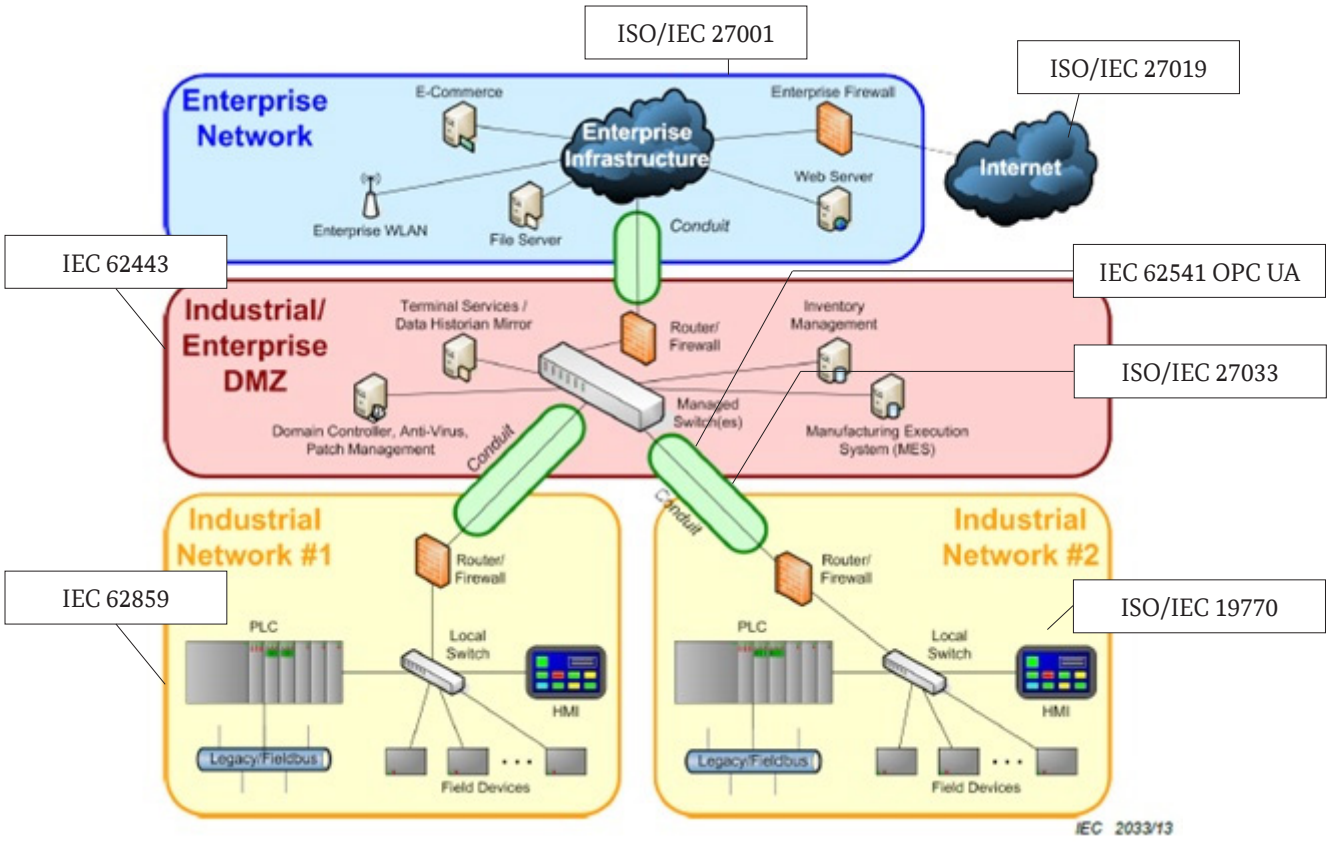

Figure 10 Network zones and conduits

After defining zones and conduits, the next step is to define SL for every zone and conduit, according to their security requirements or the tolerance of risks. If one zone or conduit is critical and has higher security demands, it can be defined with higher SL. The highest level is SL4, the lowest level is SL1. This process usually needs to be iterated multiple times.

The control system shall provide the capability to logically segment control system networks from non-control system networks, and to logically segment critical control system networks from other control system networks.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture used by an asset owner in their facility, and even system integrators within their control systems. Logically segmenting networks based on their functionality provides some measure of protection, but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure, but will

lead to a more complex and costly network design. These trade-offs will need to be evaluated during the network design process.

In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local Certification Authorities (CAs). It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.

3.3 Overlapping between ISO/IEC 27033 and IEC 62443

The ISO/IEC 27033 mainly focuses on four parts. It includes four ways to secure the communications between networks, e.g. using gateway, VPN, IP convergence, wireless and radio.
The IEC 62443 series standards can be divided into four parts, the basic part mainly introduces the general concept and models of security; whilst the second part focuses on the management level, which introduces the requirements, implementation guidance of IACS security management system and patch management. The third part introduces the concept and implementation of zones and conduits, using risk matrix to assess the security risk in different levels of system security; and in the last part, IEC 62443 describes requirements of product development and technical security from the layer of component.

Both standards focus on network communication security. However, each has its own emphasis. IEC 62443 is the specification that tends to the management level, whereas the ISO/IEC 27033 tends to report more on specific technical points. For example, the zone and conduits concepts have been provided in IEC 62443, however, there is no detailed information on how to implement the zone or conduit on a specific system of plant. Even which specific technique or protocol will be used here are unknown. ISO/IEC 27033, however, provides several methods that can be used to implement the communication between two zones (say in the conduit), e.g. gateway and VPN. ISO/IEC 27033 also refers the IP convergence, wireless and radio to secure the communication network.

The difference between them is that ISO/IEC 27033 introduces the detailed methods to realize the security of network. Whereas, IEC 62443 does not include all of these methods, e.g. VPN is not modeled through zone or conduit. The communication protocols used in ISO/IEC 27033 are higher than those in IEC 62443, which use TCP/IP to secure the network in layer 4 (OSI model). Whilst, the protocols referred in IEC 62443 are industrial communication protocols in MAC layer.

A further overlapping between ISO/IEC 27033 and IEC 62443 is the concept of conduits, which is introduced in the IEC 62443-3-2. ISO/IEC 27033 also addresses the communication via secure methods in a conduit (without using the term), e.g. the gateway. They are different concepts, but the purpose is similar.

3.4 IEC 62351

The international standard IEC 62351 titled “Power systems management and associated information exchange – Data and communications security” considers security aspects of Smart Grids with the focus on communication security. Overall, it consists of 11 parts that are already published, except for part 9, which will focus on credential management. The first part of IEC 62351-1 gives not only an overview of the other parts of this standard, but also of the requested security services (availability, authentication, confidentiality and nonrepudiation), possible attacks on the system and possible countermeasures. The main part of the standard describes the communication between the components of the system. IEC 62351 introduces specified security measures for the protocols of IEC 61850 (automation of substations), IEC 61400-25 (communication and monitoring in wind power plants) IEC 60870-5 (protocols of remote control of equipment) and IEC 60870-6 (telemetry, TASE.2/ ICCP uses MMS according to ISO 9506). While IEC 60870-6 and IEC 60870-5-x cover wide parts of the Smart Grid including Inter-control center communication and station automation down to field devices, IEC 61850 covers substation automation and is extended to cover additional areas like hydro-power plants and distributed energy resources. IEC 62351 refers directly to these standards, which makes it an important security standard for a wide range of Smart Grid Applications. Additionally, IEC 62351 introduces security concepts like role-based access control, key management and security architectures. Some of these concepts are also closely related to other standards. For example, IEC 62351-8, which introduces Role-based access control, refers to the IEC 61850 data model.

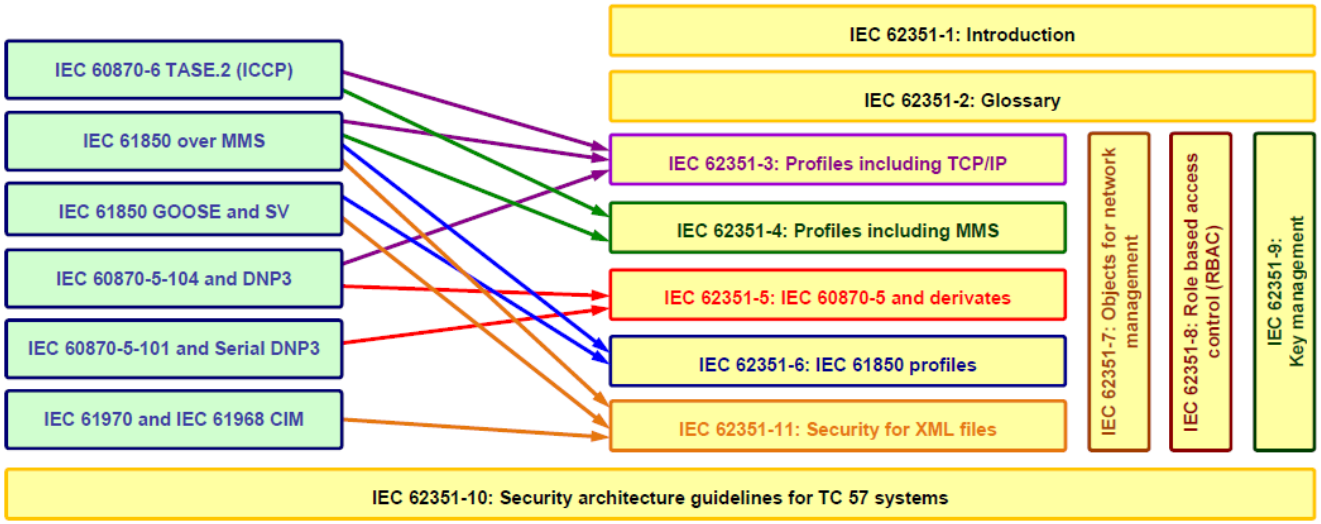

Figure 11 Relationship

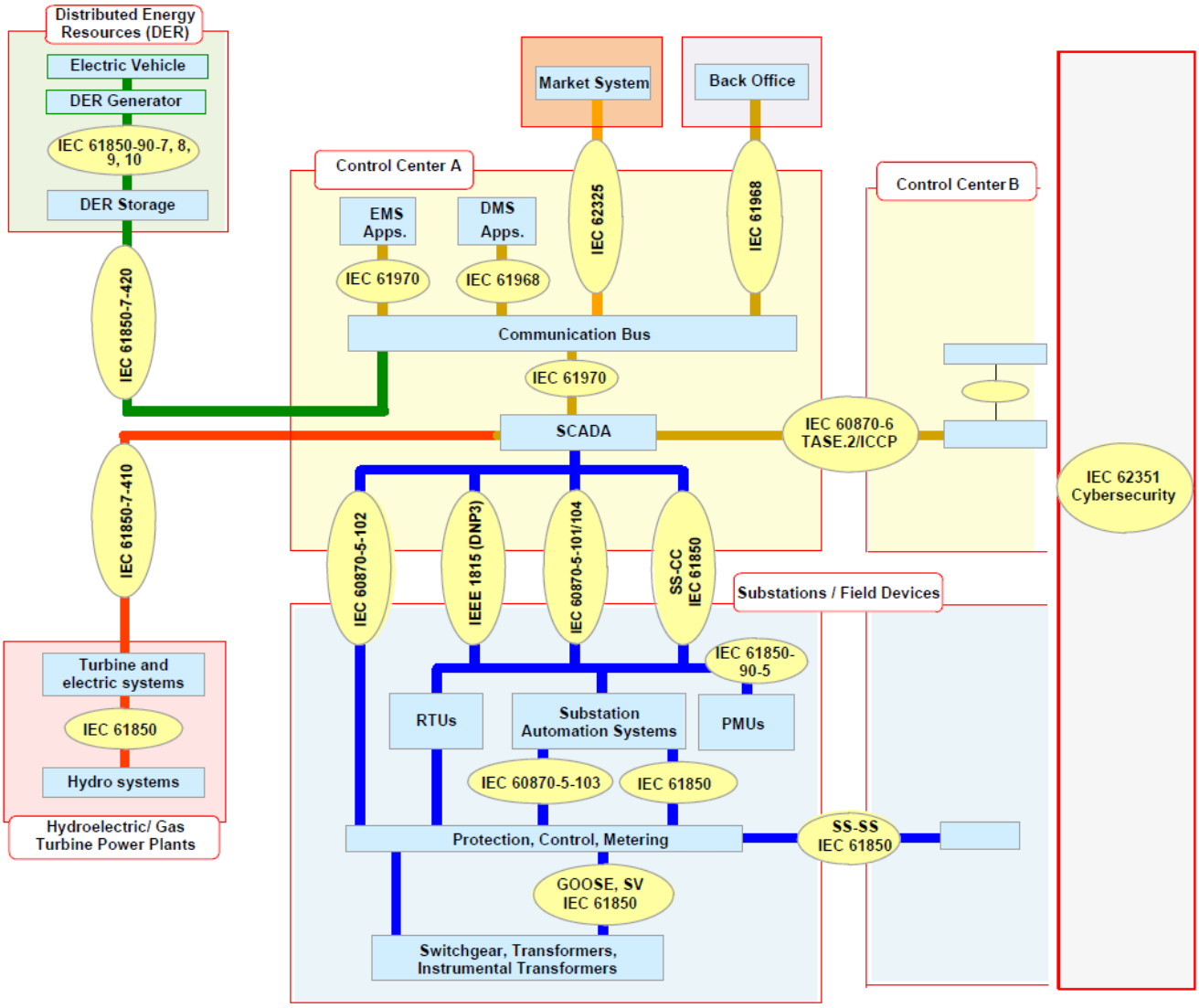

Figure 12 Scope and Usage

3.5 Other Network Security Standards

3.5.1 Chinese Standards

3.5.1.1 Information security technology - Application guide to industrial control system security control (GB/T 32919-2016)

This standard provides basic methods of safety control applications for industrial control systems that are used in various industries to guide organization selection; and tailoring, compensation and replenishment of industrial control system safety controls to obtain a safety control baseline suitable for the organization's demands, meet the organization's industry control system security needs, and help organizations to achieve effective control of industrial control systems risk management.

3.5.1.2 Information security technology - Security management fundamental requirements for industrial control systems

This standard references are NIST SP 800-53v4 and NIST SP 800-82v1. It analyzes the main security management activities of industrial control system and summarizes the fundamental requirements of industrial control system network security management, technology and operation. In addition, it provides the security management requirements correspondence tables of industrial control systems, with different safety levels in the appendix.

This standard regulates the safety related concepts, reference models and safety management requirements of industrial control systems, and provides support and basis for industrial safety classification, evaluation and inspection for the demand of establishing industrial control system network security inspection system and evaluation system.

3.5.1.3 Information security technology - Information security classification specifications of industrial control systems

This standard analyzes the information security level protection, IEC 62443 industrial control system classification, telecommunications, Internet level protection and other standards. The main considerations of the system classification include: the importance of industrial control system assets, the threat of seriousness, the possibility of threat occurrence, the inherent vulnerability of industrial control systems and other aspects of comprehensive consideration, put forward four security levels.

3.5.1.4 Information security technology - Implementation guide to risk assessment of industrial control systems

This standard guides the safety protection work of the industrial control system in the important industrial areas of the national economy. It ensures the safety and reliability of the industrial control system and achieves the autonomy of the industrial control system. In order to achieve this goal, China's industrial sectors take full account of the specificity of industrial control systems and different levels of security requirements, carefully sorting out the unit of industrial control system assets. Analyzing the threats to industrial control systems stemming from environmental and human factors, and analyzing the vulnerabilities of industrial control systems stemming from both technical and managerial aspects. By combining existing security measures, analyzing existing risks of industrial control systems, balancing benefits and costs to develop risk disposal plans it keeps the residual risk of industrial control systems within acceptable levels.

3.5.1.5 Information security technology - Technical requirements for vulnerability detection of industrial control systems (Under development)

This standard is used to guide the development of safety products for vulnerability scanning of industrial systems and equipment. It stipulates the technical requirements of industrial control system vulnerability detection products, puts forward the safety objectives and environment of industrial control system vulnerability detection products, gives the product safety guaranteed requirements, basic / enhanced functional grading requirements and product performance requirements.

3.5.1.6 Industrial automation and control system security - Programmable logic controller (PLC) - Part 1: System requirements (GB/T 33008.1-2016)

This standard specifies cyber-security requirements for PLC system, including cyber-security requirements of direct and indirect communication with other systems. The standard applies to engineering designers, equipment manufacturers, system integrators, users, as well as evaluation and certification institutions. In consideration that systems realized by programmable logic controllers are faced with varying cyber-security threats in the whole life-cycle, including design, development, installation, operation, maintenance and exit stage, technical and management requirements are provided to lower cyber-security risk to an acceptable level.

3.5.1.7 Industrial automation and control system security - Distributed control system (DCS) - Part 1: Protection requirements (GB/T 33009.1-2016)

This standard stipulates required security capability, protective technical requirements and secure zone partition for distributed control system in process of operation and maintenance, and puts forward specific requirements for

protection key points, protective equipment and protection techniques of process monitoring layer, field control layer and field equipment layer. The standard applies to critical infrastructure field related to distributed control system security protection, e.g. electric power, petrochemical industry, water conservancy, metallurgy, construction material. It aims to guide enterprise users to improve security of in-service and newly-added distributed control system. It also provides guidelines for system security design to distributed control system manufacturers and integrators.

3.5.1.8 Industrial automation and control system security - Distributed control system (DCS) - Part 2: Management requirements (GB/T 33009.2-2016)

This standard stipulates cyber security management system of distributed control system as well as specific requirements of relevant security management factors. The standard applies to security management of distributed control system in the process of operation and maintenance. It aims to guide relevant enterprises and organizations to establish and implement cyber security management system combined with distributed control system's practical application situation.

3.5.1.9 Industrial automation and control system security - Distributed control system (DSC) - Part 3: Assessment guidelines (GB/T 33009.3-2016)

This standard describes the classification, target of evaluation and implementation process of distributed control system's security risk assessment, as well as validity test of security arrangement. The standard applies to security risk assessment activities carried out for distributed control system of critical infrastructure field, such as electric power, petrochemical industry, water conservancy, metallurgy, construction material, etc. It aims to guide users to improve and enhance security capability of distributed control system in the manufacturing system during system maintenance activities.

3.5.1.10 Industrial automation and control system security - Distributed control system (DCS) - Part 4: Risk and vulnerability detection requirements (GB/T 33009.4-2016)

This standard normalizes risk and vulnerability detection of distributed control system (DCS) before and after being put into operation, and puts forward specific requirements for that of DCS software, Ethernet network communication protocol and industrial control network protocol. The standard applies to following targets in DCS: application software e.g., monitoring software, configuration software, database software operation systems e.g., operator station, control station function and components with network protocol implementation as well as network communication capability.

This standard does not apply to vulnerability detection of intelligent instruments and wireless industry.

3.5.2 ENISA guidance on communication network dependencies

Communication network dependencies for ICS/SCADA Systems report is addressed by ENISA in [33]. The guidance addresses the architectures and technologies, especially the protocols in use within and between levels and the security tools for SCADA systems. The attack scenarios address the compromise of SCADA systems, the insider threat and malware infections.

Security of critical assets and critical infrastructure is addressed from the state perspective and from the operator perspective. The main objective is to provide insight into the communication network interdependencies currently present in industrial infrastructures and environments, mapping critical assets, assessing possible attacks and identifying potential good practices and security measures to apply.

4 Security during Product Development

The whole life-cycle of products needs to be protected and traced. Considering the threat likelihood, we focus on Software during the research. However, similar tests or approaches can be applied with hardware or firmware.

4.1 IEC 62443 life-cycle management

IEC 62443-4-1 specifies process requirements for the secure development of products used in industry automation and control systems. It defines a secure development life-cycle (SDL) including security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products.

4.1.1 General principles

Figure 13 illustrates how secure by design principles are combined with a defense in depth strategy for the product. Although not shown, defect management and security update management provide verified repairs to the secure implementation.

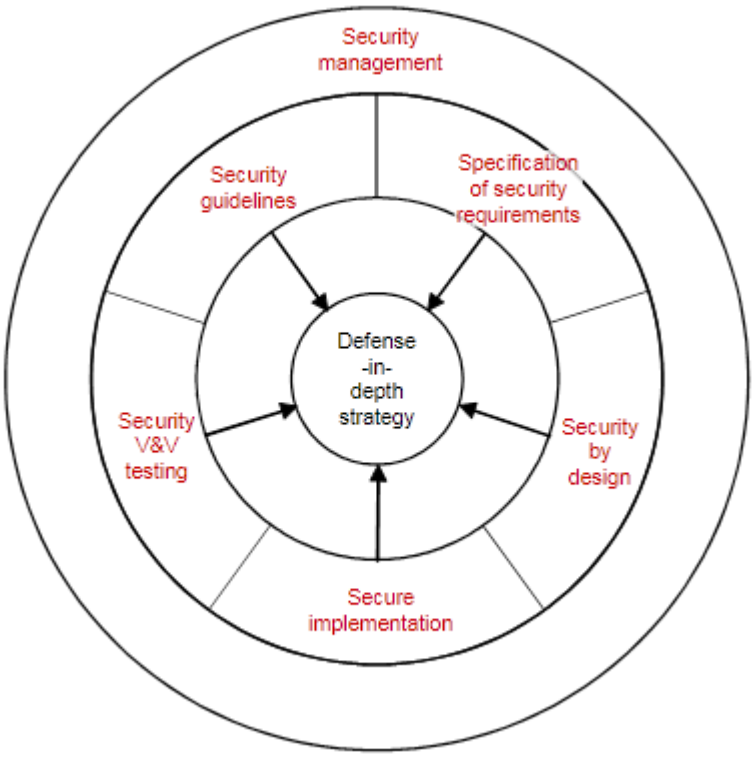

Figure 13 Defense in depth strategy & the secure product life-cycle

In IEC 62443-4-1, it defines a maturity model that sets benchmarks for meeting the secure requirements during the whole product life-cycle. These benchmarks are defined by maturity levels. The maturity levels are based on the Capability Maturity Model Integration (CMMI) for Development (CMMI-DEV) model.

4.1.2 Security management

The purpose of the security management practice is to ensure that the security-related activities are adequately planned, documented and executed throughout the product's life-cycle. If these are not adhered to in planning and supporting the activities related to security, then those activities may be rendered ineffective due to inadequate resources, insufficient time or process inefficiencies. Similarly, misalignment of the product's security requirements with related organizational processes such as configuration management, information technology policies and procedures and supply chain management can jeopardize the effectiveness of the secure product development life-cycle.

4.1.3 Specification of security requirements

The processes specified by this practice are used to document the security capabilities that are required for a product along with the expected product security context. Security capabilities may include such items as authentication, authorization, encryption, auditing and other security capabilities a product needs to include. The product security context may include items such as physical security level, protection of external interfaces via a firewall, etc. These security requirements may be defined at the product-level or they may supplement product-level requirements.

4.1.4 Secure by design

The processes specified by this practice are used to ensure that the product is secure by design, including verification of defense in depth measures. Defense in depth provides one or more layers of security to thwart security threats. Each layer of the defense in depth strategy is designed to protect the assets from attack in the case that other layers have been compromised.

The processes required by this practice are required to be applied to all stages of product design, from conceptual design to detailed design, and to all levels of product design from the overall architecture to the design of individual components.

4.1.5 Secure implementation

The processes specified by this practice are used to ensure that the product features are implemented securely.

4.1.6 Security verification and validation testing

The processes specified by this practice are used to docu-

ment the security testing required to ensure that all the security requirements have been met for the product and security of the product is maintained when it is used in its product security context and configured to employ its defense in depth strategy.
Security testing can be performed at various times by various personnel during the SDL based on the type of testing and the development model used by the vendor. For example, fuzz testing could be performed during software development by the software development team and later in the cycle by a test team.
Four types of security testing are addressed in practice:

- Security requirements testing,
- Threat mitigation testing,
- General vulnerability testing,
- Penetration testing.

4.1.7 Security defect management

The processes specified by this practice are used for handling security-related issues of a product that has been configured to employ its defense in depth strategy within the product security context.

4.1.8 Security update management

The processes specified by this practice are used to ensure security updates associated with the product, are tested for regressions and made available to product users in a timely manner.

4.1.9 Security guidelines

The processes specified by this practice are used to provide documentation that describes how to integrate, configure, and maintain the defense in depth strategy of the product in accordance with its product security context.
Applying and maintaining the defense in depth strategy for a specific installation will typically address the following:

- policies and procedures associated with the product security context;
- architectural considerations, such as firewall placement and use of compensating mechanisms including security measures;
- configuring security settings/options, such as configuring firewall rules and managing user accounts (for example, setting their privileges/permissions); and
- Using of tools to assist in the hardening.

4.2 ISO/IEC TR 24772 Vulnerabilities in Programming Language

4.2.1 General Description

ISO/IEC TR 24772 specifies software programming language vulnerabilities, which should be avoided in the development of systems where assured behavior is required for security, safety, mission critical and business critical software.
In general, this guidance is applicable to software developed, reviewed, or maintained for any application. ISO/IEC 24772 does not address software engineering and management issues.

ISO/IEC 24772 seeks to avoid the debate about where low-level design ends and implementation begins, by treating selected issues that some might consider design issues rather than coding issues.

The body of ISO/IEC 24772 provides users of programming languages with a language-independent overview of potential vulnerabilities in their usage.

4.2.2 Intended audience

The intended audience for ISO/IEC 24772 are those who are concerned with assuring the predictable execution of the software of their system. In particular those, who are developing, qualifying, or maintaining a software system and need to avoid language constructs that could cause the software to execute in a manner other than intended.

Developers of applications that have clear safety, security or mission-criticality are expected to be aware of the risks associated with their code and could use ISO/IEC 24772 to ensure that their development practices address the issues presented by the chosen programming languages.

A weakness in a non-critical application may provide the route by which an attacker gains control of a system or otherwise disrupts co-hosted applications that are critical. It is hoped that all developers would use ISO/IEC 24772 to ensure that common vulnerabilities are removed or at least minimized from all applications.

Specific audiences for this International Technical Report include developers, maintainers and regulators of:

- Safety-critical applications that might cause loss of life, human injury, or damage to the environment.
- Security-critical applications that must ensure properties of confidentiality, integrity, and availability.
- Mission-critical applications that must avoid loss or damage to property or finance.
- Business-critical applications where correct operation is

essential to the successful operation of the business.
- Scientific, modeling and simulation applications which require high confidence in the results of possibly complex, expensive and extended calculation.

4.2.3 Main contents

ISO/IEC 24772 gathers descriptions of programming language vulnerabilities, as well as selected application vulnerabilities, which have occurred in the past and are likely to occur again. Each vulnerability and its possible mitigations are described in the body of the report in a language-independent manner, though illustrative examples may be language specific. In addition, it describes the vulnerabilities and their mitigations in a manner specific to the language. ISO/IEC 24772 contains descriptions that are intended to be language-independent to the greatest possible extent, and the generic guidance applied to particular programming languages.

The descriptions include suggestions for ways to avoid the vulnerabilities. Some are simply the avoidance of particular coding constructs, but others may involve increased review or other verification and validation methods. Source code checking tools can be used to automatically enforce some coding rules and standards.

1. Vulnerability Issues, provides rationale for ISO/IEC 24772 and explains how many of the vulnerabilities occur.
2. Programming Language Vulnerabilities, provides language-independent descriptions of vulnerabilities in programming languages that can lead to application vulnerabilities. Each description provides:
   - a summary of the vulnerability,
   - characteristics of languages where the vulnerability may be found,
   - typical mechanisms of failure,
   - techniques that programmers can use to avoid the vulnerability, and
   - Ways that language designers can modify language specifications in the future to help programmers mitigate the vulnerability.
3. Application Vulnerabilities, provides descriptions of selected application vulnerabilities that have been found and exploited in many applications, as well as those that have well known mitigation techniques, and those that result from design decisions made by coders in the absence of suitable language library routines or other mechanisms. For these vulnerabilities, each description provides:
   - a summary of the vulnerability,
   - typical mechanisms of failure, and
   - Techniques that programmers can use to avoid the vulnerability.
4. New Vulnerabilities, provides new vulnerabilities that have not yet had corresponding programming language text developed.
5. Vulnerability Taxonomy and List, is a categorization of the vulnerabilities of this report in the form of a hierarchical outline and a list of the vulnerabilities arranged in alphabetic order by their three-letter code.
6. Language Specific Vulnerability Template, is a template for writing programming language specific annexes that explain how the vulnerabilities from clause 6 are realized in that programming language (or show how they are absent), and how they might be mitigated in language-specific terms.
7. The annexes, each named for a particular programming language, list the vulnerabilities of Programming Language and Application Vulnerabilities, and describe how each vulnerability appears in the specific language and how it may be mitigated in that language, whenever possible. All of the language-dependent descriptions assume that the user adheres to the standard for the language as listed in the sub-clause of each annex.

4.2.4 Guidance in the I4.0/IM context

Web technologies play an important role within the context of Industrie 4.0 and Intelligent Manufacturing. ICT innovations, like the always evolving web services, may help the industry to handle the information exchanges, as well as processing data flows among distributed systems within dynamic adapting infrastructures, such as cloud services. However, considering the restricted safety and security requirements in the industry field, IT solutions need to be analyzed and adapted to be suitable solutions for industry. In this trade-off, the balance between light-weighted systems and safety/security requirements need to be considered.

As an example, TypeScript, which is developed as a superset of JavaScript, is introduced as a new programming language for developing robustness and scalable web solutions. It is an object-oriented programming language designed to be compatible with the 6th ECMAScript standard published in 2015. In addition, TypeScript supports optional static typing which enables static code analysis. These features eliminate some security vulnerabilities from the new programming language, which could be a suitable candidate for the software development within the I4.0/IM context.

In the academic world, there is already an example for involving web technology (JavaScript) into the industry field. Based on the OPC UA framework, a research project has been conducted at the University of Dresden since 2009. It provides a solution for using smartphones or tablets as terminals of smart meters. The work is based on a new proposed Framework (JSUA), which itself is based on the OPC UA Framework, and incorporates a communication stack developed using JavaScript [26].

5 Supplier Relationships Security

5.1 IEC 62443-2-4

5.1.1 General Description

IEC 62443-2-4 specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner. Figure 14 illustrates how the integration and maintenance capabilities relate to the IACS and the control system product that is integrated into the Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3. The service providers must ensure that these are supported in the Automation Solution (either included in the control system product or separately added to the Automation Solution).

5.1.2 IACS Service Providers

IEC 62443-2-4 also defines requirements for security capabilities to be supported by security programs of integration and maintenance service providers. Support for these capabilities means that the service provider can provide them to the asset owner upon request. The terms and conditions for providing these capabilities are beyond the scope of this standard. In addition, IEC 62443-2-4 can be used by these IACS service providers to structure and improve their security programs.

In addition, IACS service providers can use IEC 62443-3-3 and IEC 62443-4-2 in conjunction with IEC 62443-2-4, to work with suppliers of underlying control systems/components. This collaboration can assist the service provider in developing policies and procedures around a capability of a system/component, e.g. backup and restore based on the recommendations from the suppliers of the systems/components used.

The security programs implementing these requirements are expected to be independent of different releases of the control system that is embedded in the Automation Solution. That is, a new release of the control system product does not necessarily require a change to the service provider's security program. However, changes to the security program will be required when changes to the underlying control system make the existing security program deficient with respect to these IEC 62443-2-4 requirements.

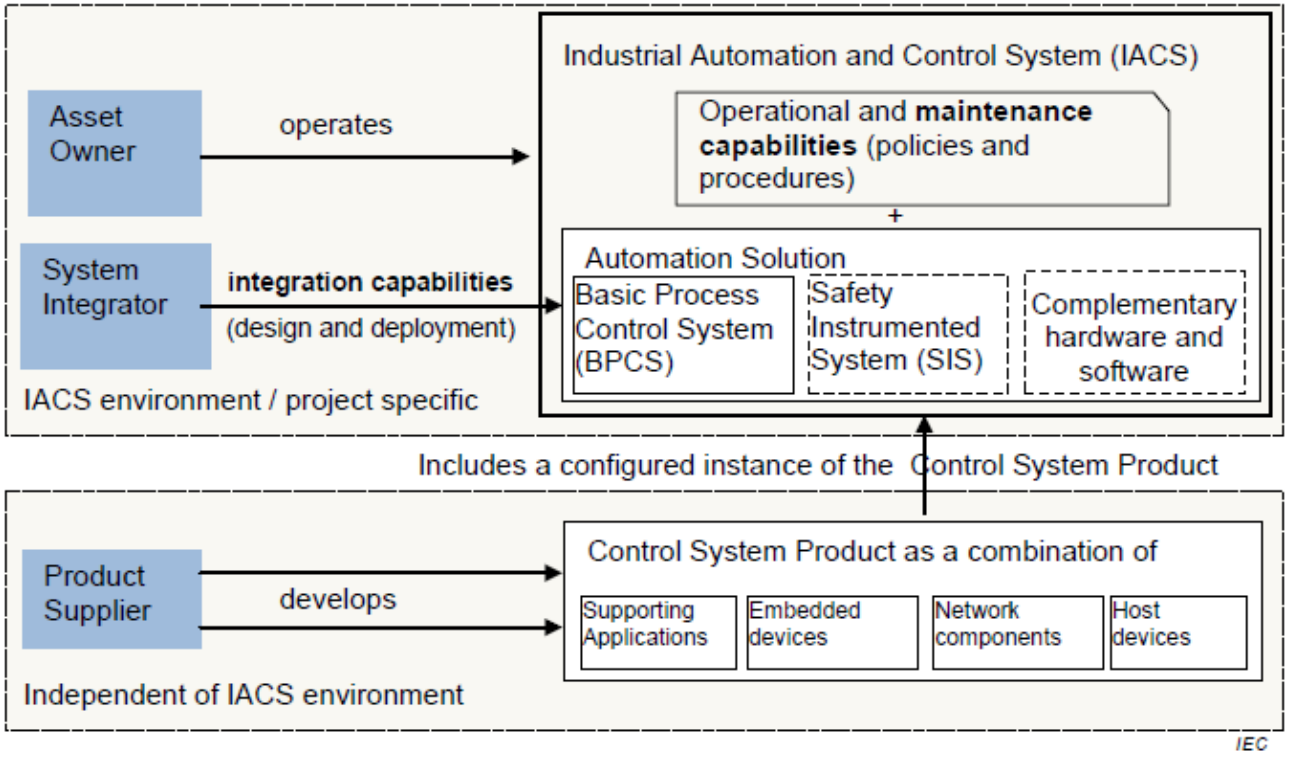

Figure 14 Scope of service provider capabilities

In Figure 14, the Automation Solution is illustrated to contain a Basic Process Control System (BPCS), optional Safety Instrumented System (SIS), and optional supporting applications, such as advanced control. The dashed boxes indicate that these components are "optional".

5.1.3 IACS Asset Owners

IEC 62443-2-4 can be used by asset owners to request specific security capabilities from the service provider. More specifically, prior to such a request, IEC 62443-2-4 can be used by asset owners to determine whether or not a specific service provider's security program includes the capabilities that the asset owner needs.

In general, IEC 62443-2-4 recognizes that asset owner requirements vary, so it has been written to encourage service providers to implement the required capabilities so that they can be adaptable to a wide variety of asset owners. The maturity model also allows asset owners to better understand the maturity of a specific service provider's capabilities.

5.1.4 Negotiations between IACS asset owners and IACS service providers

Prior to the IACS service provider starting work on the Automation Solution, the asset owner will normally issue a Request for Quote (RFQ) that includes a document, e.g. a Statement of Work (SOW), which defines its security policies and requirements, including which of the requirements.

Service providers respond to the RFQ and negotiations follow, in which the service provider and the asset owner come to agreement on the details of the SOW (or similar document). Typically, the specific responsibilities and capabilities of the service provider for supporting asset owner security policies and requirements will be included in or referenced by this agreement/contract between the IACS service provider and the asset owner.

Additionally, the asset owner does not normally specify how its security requirements (e.g. backup and restore) will be implemented - that is what the service provider has already specified in its policies and procedures. However, the asset owner may define constraints and parameters (e.g. password timeout values) for how the service provider's policies and procedures will be applied in its specific project.
In cases where the asset owner does not specify security requirements, the service provider may propose them to the asset owner based on its own security analysis, and then negotiate which are included in the SOW.

It is also expected that the IACS service provider will have some ability to customize its capabilities to meet the needs of the asset owner.

5.1.5 Profiles

Profiles are capability sets defined by selecting a specific subset of requirements. Profiles are intended to be written for different industry groups/sectors and other organizations to define one or more capability sets most appropriate to their needs.
It is anticipated that asset owners will select existing profiles to specify the requirements that they need for their Automation Solutions.

5.1.6 IACS integration service providers

An IACS integration service provider is an organization, typically separate from and under contract to the asset owner. It provides capabilities to implement/deploy Automation Solutions according to asset owner requirements. Integration service provider activities generally occur in the time frame starting with the design phase and ending in handover of the Automation Solution to the asset owner. IACS integration service provider activities typically include:

- Analyzing the physical, electrical, or mechanical environment that the Automation Solution is to control (e.g. the physical process to be controlled, such as those used in manufacturing, refining and pharmaceutical processes),
- Developing an Automation Solution architecture in terms of devices and control loops and their interconnectivity with engineering and operator workstations, and possibly the inclusion of a Safety Instrumented System (SIS),
- Defining how the Automation Solution will connect to external (e.g. plant) networks,
- Installing, configuring, patching, backing up, and testing that lead to the handover of the Automation Solution to the asset owner for operation.
- Gaining approval of the asset owner for many of the decisions made and outputs generated during the execution of these activities.

This description of integration service provider activities is abstract and may exclude some of these activities or include other activities that generally precede the handover of the Automation Solution. Also, these activities include participation of the asset owner to ensure the asset owner requirements are met.

From the perspective of IEC 62443, integration service providers are also expected to participate in the assessment of security risks for the Automation Solution or to use the results of such an assessment provided by the asset owner. The service provider is also expected to use capabilities required by 62443-2-4 in its security program to address these risks.

5.1.7 IACS maintenance service providers

An IACS maintenance service provider is any organization, typically separate from and under contract to the asset owner, which performs activities to maintain and service Automation Solutions according to asset owner requirements.
Maintenance activities are separate from activities used to operate the Automation Solution and generally fall into two categories, those that apply specifically to maintaining the security of the Automation Solution, and those that apply to maintaining other aspects of the Automation Solution, such as device and equipment maintenance, but that have the responsibility to ensure that security is not degraded as a result of these activities.

Maintenance activities generally start after handover of the Automation Solution to the asset owner has occurred and may continue until the asset owner no longer requires them. They are typically short and frequently recurring, and typically include one of more of the following:

- Patching and anti-virus updates,
- Equipment upgrades and maintenance, including small engineering adjustments not directly related to control algorithms,
- Component and system migration,
- Change management,
- Contingency plan management.

All maintenance activities include some level of security awareness, independent of whether or not they are directly security related. No activity should reduce the security posture of the system after it has been completed.

This description of maintenance activities is abstract and may include other activities generally following the handover of the Automation Solution. Furthermore, these activities include participation with the asset owner to ensure the asset owner requirements are met.

From the perspective of the IEC 62443 series, maintenance service providers, like integration service providers, are expected to participate in the assessment of security risks for the Automation Solution (such as for proposed changes) or to use the results of such an assessment provided by the asset owner. The service provider is also expected to use capabilities required by 62443-2-4 in its security program to address these risks.

5.2 ISO/IEC 27036

ISO/IEC 27036 includes 4 parts:

1. ISO/IEC 27036-1 — Information security for supplier relationships - Part 1: Overview and concepts
2. ISO/IEC 27036-2 — Information security for supplier relationships - Part 2: Requirements
3. ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
4. ISO/IEC 27036-4 — Information security for supplier relationships - Part 4: Guidelines for security of cloud services

ISO/IEC 27036 offers guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers. The implied context is business-to-business relationships.

It includes the following contents:

1. IT outsourcing and cloud computing services;
2. Other professional services e.g. security guards, cleaners, delivery services (couriers), equipment maintenance/servicing, consulting and specialist advisory services, knowledge management, research and development, manufacturing, logistics, source code escrow and healthcare;
3. Provision of ICT hardware, software and services including telecommunications and Internet services;
4. Bespoke products and services where the acquirer specifies the requirements and often has an active role in the product design (as opposed to commodities and standard off-the-shelf products);
5. Utilities such as electric power and water.

It covers:

1. Strategic goals, objectives, business needs and compliance obligations in relation to information security and assurance when acquiring ICT-related or information products;
2. Information risks such as:
   - Acquirer's reliance on providers, complicating the acquirer's business continuity arrangements (both resilience and recovery);
   - Physical and logical access to and protection of second and third party information assets;
   - Creating an 'extended trust' environment with shared responsibilities for information security;
   - Creating a shared responsibility for compliance with information security policies, standards, laws, regulations, contracts and other commitments/obligations;
   - Coordination between supplier and acquirer to

adapt or respond to new/changed information security requirements;

3. Information security controls such as:
   - Relationship management covering the entire lifecycle of the business relationship;
   - Preliminary analysis, preparation of a sound business case, Invitation to tender etc., taking into account the risks, controls, costs and benefits associated with maintaining adequate information security;
   - Creation of explicit shared strategic goals to align acquirer and provider on information security and other aspects (e.g. a jointly-owned 'relationship strategy');
   - Specification of important information security requirements (such as requiring that suppliers are certified compliant with ISO/IEC 27001 and/or use standards such as ISO27k) in contracts, service level agreements etc.;
   - Security management procedures, including those that may be jointly developed and operated such as risk analysis, security design, identity and access management, incident management and business continuity;
   - Special controls to cater for unique risks (such as testing and fallback arrangements associated with the transition/implementation stage when an outsourcing supplier first provides services);
   - Clear ownership, accountability and responsibility for the protection of valuable information assets, including security logs, audit records and forensic evidence;
   - A 'right of audit' and other compliance controls, with penalties or liabilities in case of identified non-compliance, or bonuses for full compliance;
4. The entire relationship lifecycle:
   - Initiation - scoping, business case/cost-benefit analysis, comparison of insource versus outsource options as well as variant or hybrid approaches such as co-sourcing;
   - Definition of requirements including the information security requirements, of course;
   - Procurement including selecting, evaluating and contracting with supplier(s);
   - Transition to or implementation of the supply arrangements, with enhanced risks around the implementation period;
   - Operation including aspects such as routine relationship management, compliance, incident and change management, monitoring etc.;
   - Refresh - an optional stage to renew the contract, perhaps reviewing the terms and conditions, performance, issues, working processes etc.;
   - Termination and exit i.e. ending a business relationship that has run its course in a controlled manner.

5.3 NIST SP800-161

NIST SP800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations

5.3.1 General Description

Information and Communications Technology (ICT) relies on a complex, globally distributed, and interconnected supply chain ecosystem that has geographically diverse routes, and consists of multiple tiers of outsourcing.

Commercially available ICT solutions present significant benefits including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. These commercial off-the-shelf (COTS) solutions can meet the needs of a global base of public and private sector customers. However, the same globalization and other factors that allow for such benefits also increase the risk of a threat event, which can directly or indirectly affect the ICT supply chain.

These ICT supply chain risks may include insertion of counterfeits, unauthorized production, tampering, and theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain.

Threats and vulnerabilities created by malicious actors (individuals, organizations, or nation states) are often especially sophisticated and difficult to detect, and thus provide a significant risk to organizations.

ICT Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.

NIST SP800-161 can provide guidance on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage ICT supply chain risks. In SP800-161, it addresses the overlap of the four pillars of ICT SCRM - security, integrity, resilience, and quality - as depicted in Figure 15.

Figure 15 Four Pillars of ICT SCRM

5.3.2 ICT Supply Chain Risk

ICT supply chain risks include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware (e.g. GPS tracking devices, computer chips), as well as poor manufacturing and development practices in the ICT supply chain. These risks are realized when threats in the ICT supply chain exploit existing vulnerabilities.

Figure 16 depicts ICT supply chain risk resulting from the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impact.

5.3.3 ICT SCRM Activities in Risk Management Process

Risk management is a comprehensive process that requires organizations to:

- Frame risk (i.e., establish the context for risk-based decisions);
- Assess risk;
- Respond to risk once determined; and
- Monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.

Figure 17 depicts the interrelationships among the risk management process steps, including the order in which each analysis may be executed and the interactions required to ensure that the analysis is inclusive of the various inputs at the organization, mission, and operations levels.

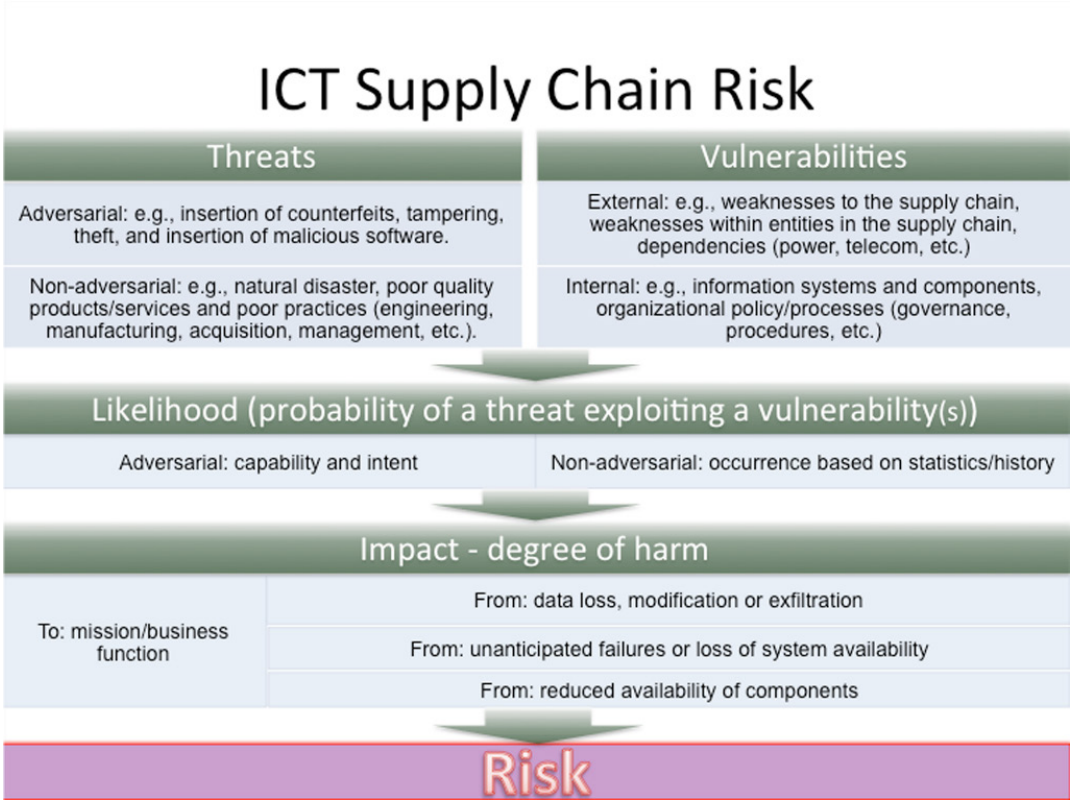

Figure 16 ICT Supply Chain Risk

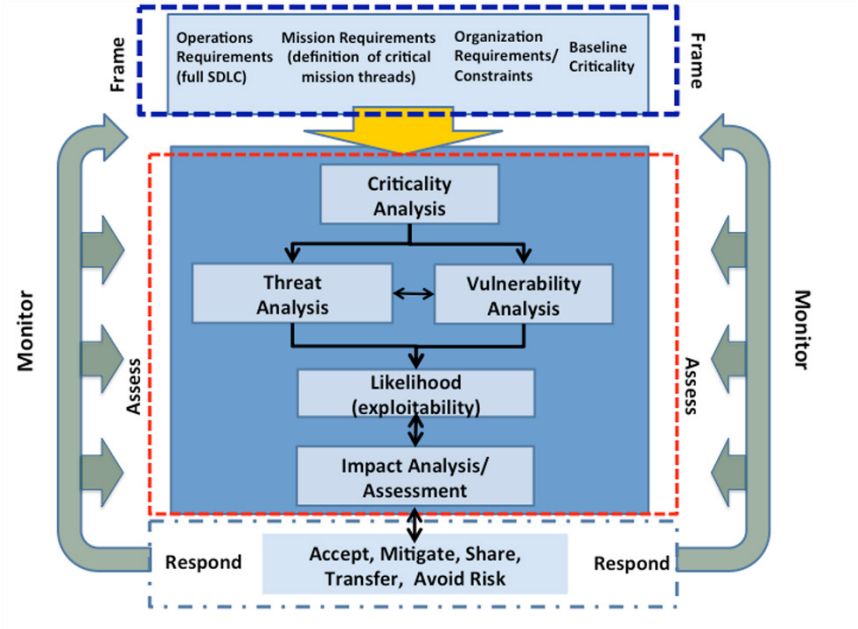

Figure 17 ICT SCRM Risk Management

5.4 UTC (Utilities Telecom Council)

The "Cyber Supply Chain Risk Management for Utilities— Roadmap" outlines these ten basic principles for implementation:

- Identify critical assets, systems, and processes, and prioritize them
- Identify critical data/information about your business and customers
- Identify your suppliers
- Assess supplier risk and prioritize suppliers
- Establish general security requirements by priority
- Establish how you will want to share information with suppliers on vulnerabilities and incidents
- Establish how you will want to monitor supplier adherence to requirements
- Get the people within your organization up to speed
- Make arrangements for contingencies
- Conclude supplier relationship in a risk-conscious way

5.5 Comparison of different standards

IEC 62443-2-4 is a report about the relationship between automation solution providers, maintenance service suppliers and asset owners, which describes the work period of each role. The task assignment as Figure 14 shows.

Before the asset owner receives the asset, the service provider designs and finishes the solution and subsequently tests it and assesses its risks. The asset owner should record requirements (including security policy, capabilities and responsibilities). After handing over the solution to asset owner, the maintenance service supplier will start work. They are in charge of patching the solution and updating anti-virus software, equipment updates and general maintenance.

However, in ISO/IEC 27036-Information technology — Security techniques — Information security for supplier relationships focuses on information security risks that acquirers and suppliers can pose to each other, including both software and hardware components. It analyzes risks on supply chain in more detail, and considers the more complex situation in reality. For example, the components of ICT supplier are not the one who supply the ICT, so the supply chain between all suppliers and acquirer is complex and the security among them is more difficult to manage. Based on this situation, this standard analyzes the content from the motivation of managing security in supply chain, different types of supplier relationships, information security risks in supplier relationships and associated threats to managing information security risks and ICT supply chain. At last, in order to secure the supply chain, this standard divides the relationship between acquirer and supplier into five types. It takes into account the security of supply chain from the whole lifecycle aspect, e.g. agreement process, organizational project-enabling process, project process and technical process. In addition, this standard also considers the security of supply chain in cloud computing.

As for NIST SP800-161, the basic difference with previous standards is that this publication is based on the federal agency information systems, which provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations.

This publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitier, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities. For more details, please refer to the section 5.3.1.

6 Security Incident Management

6.1 ISO/IEC 27035

6.1.1 General Description

Information security controls are imperfect in various ways: controls can be overwhelmed or undermined (e.g. by competent hackers, fraudsters or malware), fail in service (e.g. authentication failures), work partially or poorly (e.g. slow anomaly detection), or be more or less completely missing (e.g. not [yet] fully implemented, not [yet] fully operational, or never even conceived due to failures upstream in risk identification and analysis). Consequently, information security incidents are bound to occur to some extent, even in organizations that take their information security extremely seriously.

Managing incidents effectively involves detective and corrective controls designed to recognize and respond to events and incidents, minimize adverse impacts, gather forensic evidence (where applicable) and in due course 'learn the lessons' in terms of prompting improvements to the ISMS, typically by improving the preventive controls or other risk treatments.

Information security incidents commonly involve the exploitation of previously unrecognized and/or uncontrolled vulnerabilities, hence vulnerability management (e.g. applying relevant security patches to IT systems and addressing various control weaknesses in operational and management procedures) is part preventive and part corrective action.

It includes 5 key stages in security incident management:

1. Prepare to deal with incidents e.g. prepare an incident management policy, and establish a competent team to deal with incidents;
2. Identify and report information security incidents;
3. Assess incidents and make decisions about how they are to be addressed e.g. patch things up and get back to business quickly, or collect forensic evidence even if it delays resolving the issues;
4. Respond to incidents i.e. contain them, investigate them and resolve them;
5. Learn the lessons - more than simply identifying the things that might have been done better, this stage involves actually making changes that improve the processes.

6.1.2 ISO/IEC 27035-1:2016 Principles of incident management

This section outlines the concepts and principles underpinning information security incident management, and introduces the remaining parts of the standard. It describes an information security incident management process consisting of five phases, and states how to improve incident management.

The incident management process is described in five phases:

1. Plan and prepare: establish an information security incident management policy, form an Incident Response Team etc.
2. Detection and reporting: someone has to spot and report "events" that might be or turn into incidents;
3. Assessment and decision: someone must assess the situation to determine whether it is in fact an incident;
4. Responses: contain, eradicate, recover from and forensically analyze the incident, where appropriate;
5. Lessons learned: make systematic improvements to the organization's management of information risks as a consequence of incidents experienced.

6.1.3 ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response

This section concerns assurance that the organization is in fact ready to respond appropriately to information security incidents that may yet occur. It addresses the rhetorical question "Are we ready to respond to an incident?" and promotes learning from incidents to improve things for the future. It covers the Plan and Prepare and Lessons Learned principles.

It includes 8 main clauses:

1. Establish an information security incident management policy
2. Update information security and risk management policies
3. Create an information security incident management plan
4. Establish an Incident Response Team (IRT) [aka CERT or CSIRT]
5. Define technical and other support
6. Create information security incident awareness and training
7. Test (and train) the information security incident management plan
8. Learn lessons

6.2 Digital Forensics

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form, while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events [27]. In ISO/IEC 27K standards, the ISO/IEC 27042 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence and ISO/IEC 27043 Information technology — Security Techniques — Incident investigation principles and processes focus on the digital forensics.

ISO/IEC 27042

In this technical report, which provides a general framework to analyze and explain the elements of information system security incident handling. One structured approach has been developed to obtain more findings, as Figure 18 shows.

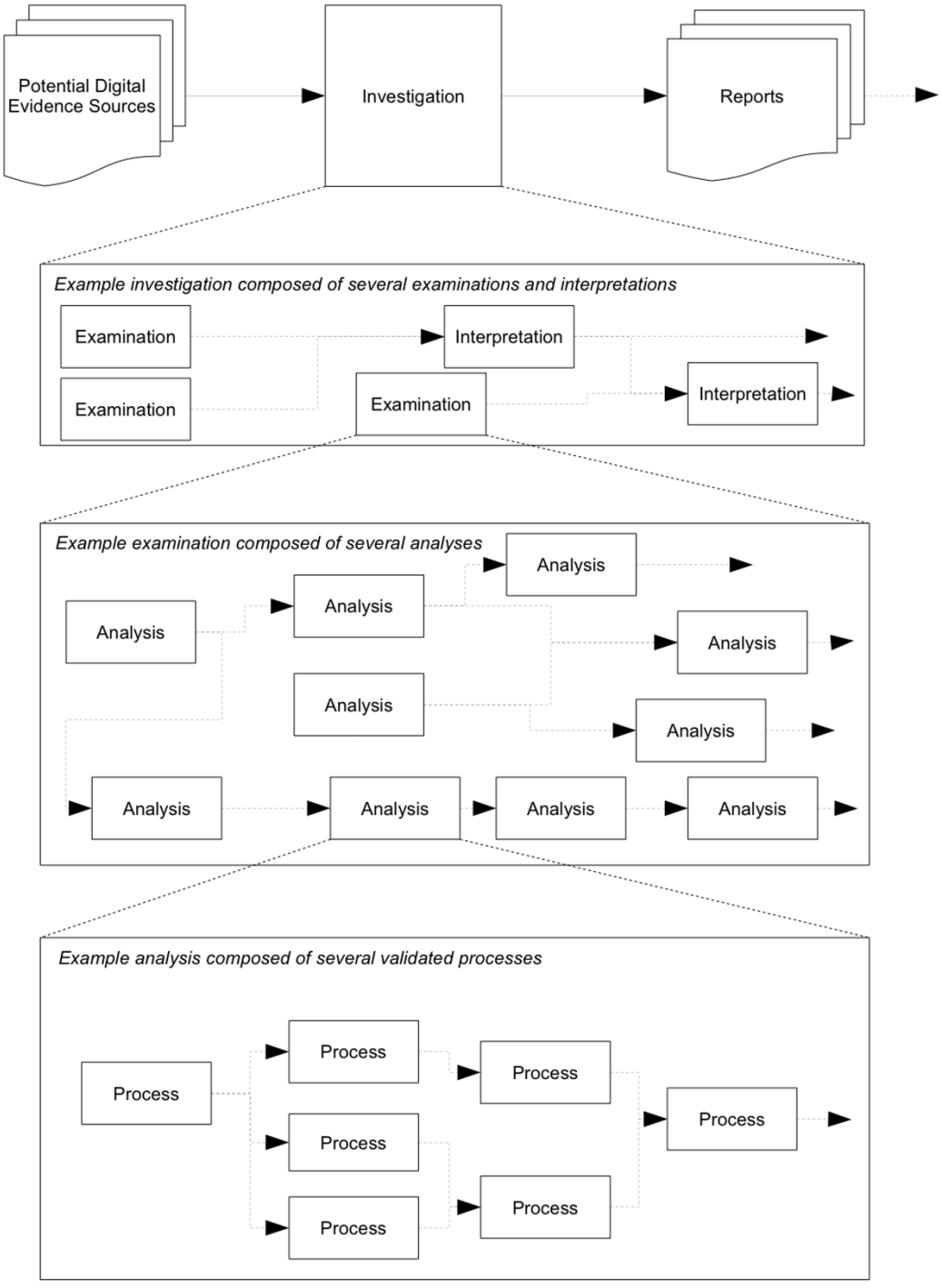

Figure 18 Structured approach of digital forensic

Using this structure, we can analyze digital artifacts. However, during the analysis process, some rules should be followed. For example, processes used to carry out the examination of items of potential digital evidence should be fully validated and they should not change the contents of any sources of potential digital evidence under examination. If a member of the investigative team believes that he/she has found evidence of another incident, he/she should inform the investigative lead of this fact and await further instructions. For the analysis tools (combinations of software, hardware and firmware), these should be based on the agreed requirements and the processes (see ISO/IEC 27041), which make up the analysis. The user should be competent to use the tools in the context of the relevant process.

There are two models to analyze the digital evidence: one is static analysis model and the other is live analysis model. The static analysis model is particularly appropriate for the analysis of consequential data (e.g. contents of log files, contents of network packets, contents of memory dumps) and meta-data (e.g. file permissions and timestamps). The live analysis model concerns both non-imaginable (cannot be copied/reproduced) and imageable systems. The difference between them is that live analysis of non-imaginable systems which cannot be imaged or copied, however, the live analysis of non-imageable systems can be copied or imaged. Another point in this standard is the requirement of interoperation and the format of the report. The investigative team should remember that their primary responsibility is to provide a fair and accurate interpretation of the facts as they are determined. So, when assessing evidence, care must be taken to distinguish facts that have been found and information that has been inferred. The report templates, with standardized format, drop-down selection lists and placeholders for common text with associated descriptions of the text, can be used to assist finish the report.

ISO/IEC 27043

This standard is mainly about the general view of digital forensics investigation process and principles. This standard, from an abstract level, divides the whole process into 4 sub-processes (readiness process, initialization process, acquisition process and investigative process), so that it can be used more universally. The detailed steps and relationships between different processes are shown in Figure 19.

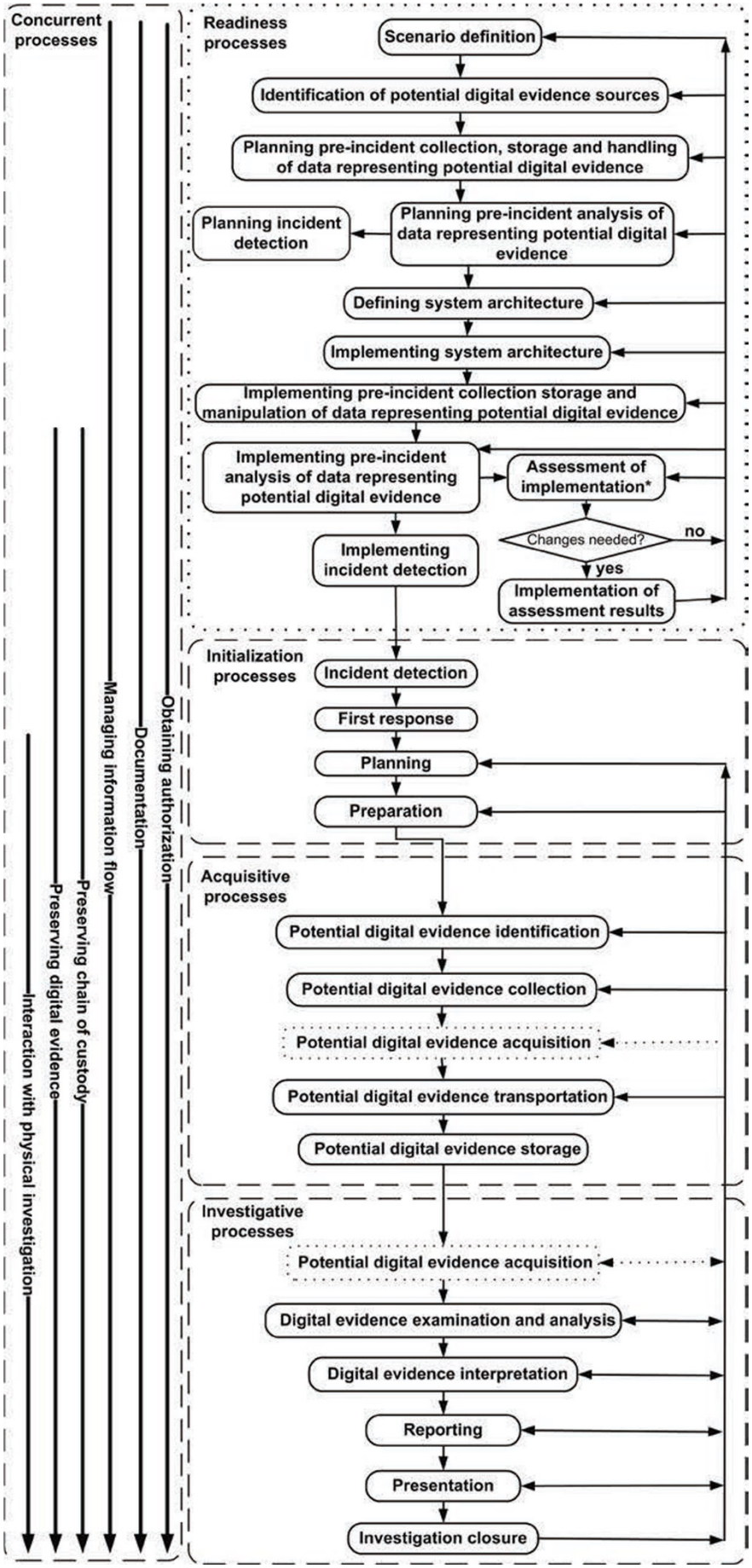

Figure 19 Steps and relation between different processes

Concurrent processes are defined as the principles which should be applied throughout the digital investigation process, because such concurrent processes are applicable to many other processes within the digital investigation process.

Readiness processes

Readiness processes include that class of processes dealing with setting up an organization in such a way that, in case that a digital investigation is required, such organizations possess the ability to maximize their potential to use digital evidence, whilst minimizing the time and costs of an investigation. This class of processes is optional for the digital investigation process, since it is the prerogative of the organization to implement it rather than the task of the investigators.

Initialization processes

Initialize the digital investigation by handling the first response of an incident and planning as well as preparing for the remainder of the incident investigation process.

Acquisition processes

Consists of processes that are concerned with acquisition of potential digital evidence.

Investigative processes

The basis of the digital investigation. It is concerned with analyzing evidence, interpreting results from the analysis, reporting on results of the digital evidence interpretation process and presenting these results in a court of law or to the relevant parties involved. Finally, the digital investigation draws to a close within the investigation closure process.

6.3 Security Information and Event Management (SIEM) systems

Currently, there is no standard about SIEM system exactly, the standard which focuses on SIEM is ISO/IEC 27044, but it has already been withdrawn, so there is a gap on this point now. Nevertheless, there are SIEM solutions in SPLUNK and QRadar (IBM).

7 Asset Management

7.1 ISO 55000

The ISO5500x Standard Series defined the basement of Asset Management.

7.1.1 Definition of asset

An asset is any entity that has potential or actual value to an organization. The considered assets could be a factory in the large scale or a device in the detailed view. In refined views, an asset could be the combination of hardware and software. Furthermore, it could be an employee, some intellectual properties and even the “know-how” of running approaches.

7.1.2 Assets need to be managed

These assets need to be put under appropriate management in order for the organization, as the owner, to sustainably benefit from them. More specifically, according to ISO 55000, the organization may improve its financial performance by e.g. tracking its device assets and deploying a preventive maintenance strategy. During the process of investment decisions, proper asset management system can provide reliable data and even simulate asset changes with new investment, e.g. the setup of a new factory and replacement of one production line. Furthermore, a good asset management system may provide the information for managing known and analyzing potential risks. For example, it may indicate and estimate the results when a production process has to be interrupted due to accidents or system failures.

7.1.3 Benefit of asset management

At last, the asset management may help to increase customers’ satisfaction as well as the organization’s public reputation. More practically, a clear demonstration of the assets and their status can show compliance easily to regulators, which is also a very important topic in the compliancy of security standards/controls.

7.1.4 Relations between the key elements of asset management

Figure 20 illustrated the relations between the key elements of an asset management system. The figure is adapted from ISO 5000 by remarking its most important elements with red rectangles.

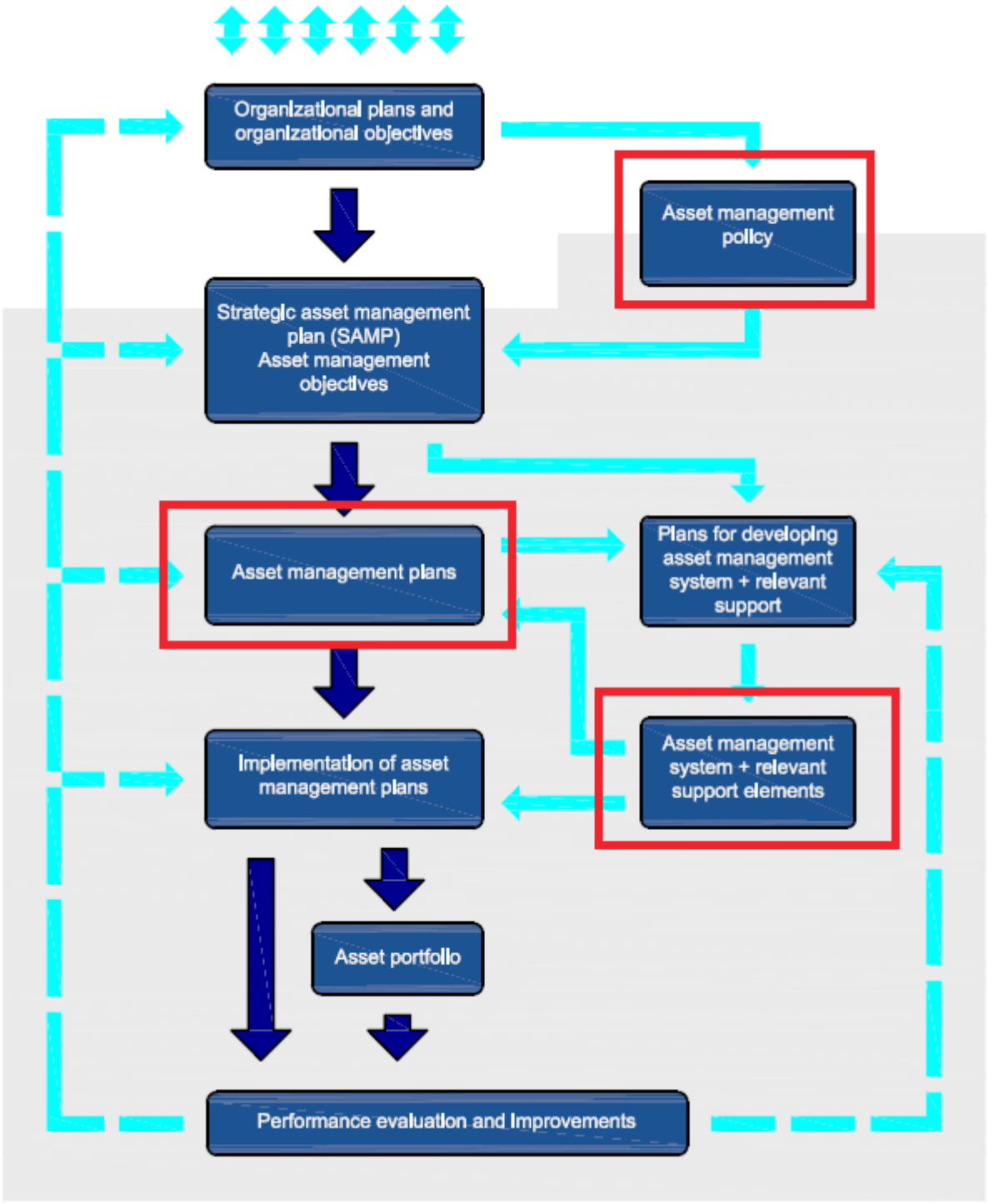

Figure 20 Relations between the key elements of an asset management system

1. First of all, besides the three elements surrounded by the red rectangles, the definition and identification of assets plays an important role in the management system. Normally the organization manages these assets according to a set of policies.
2. Assets will be categorized into different groups. Each group needs to comply with one or several asset management policies. Such a group could consist of assets that share similar responsibilities, e.g. all computers, printers and switchers/routers in the office area. A group may also contain homogenous systems carrying similar functionalities, e.g. all same type controllers within a modern factory. According to the group-based policies, each asset under management will be assigned a concrete asset management plan, which will be executed and monitored by the asset management system.
3. The asset management system tracks the life-cycle of an asset and monitors whether it complies with assigned policies. When actions are needed, e.g. maintenance is required, the asset management system will notify the

engineers to deal with the specific issue. The asset management system should continuously observe the status of assets. In the case the features of an asset change, e.g. the asset is defect due to aging problems, the asset needs to be evaluated to decide whether a maintenance is required or that the device should be removed from the asset list. Traditionally, the status of assets will be examined in a periodic way. Nowadays the deployment of new IT technologies such as IoT, enables a real-time monitoring of asset status.

7.1.5 Relations between asset management systems and other systems

The real-time feature of asset management systems shows the overlap with security information and event Management (SIEM) systems. Meanwhile, the asset management system also assists with risk management, which is also one major consideration of security standards [2700x] [62443-x-x]. More importantly, the identification of assets, as well as their features, provides a firm basement for security considerations. It is easy to setup the asset management system or to improve existing management system to develop a powerful and reliable ISMS in the future.

7.2 ISO/IEC 19770

7.2.1 ISO/IEC 19770 focus on IT and Software asset management

Compared to the ISO 5500x series standard, the ISO/IEC 19770 series standard provides a more detailed view focused on the sub-disciplines of asset management: IT Asset Management and Software Asset Management in ISO 55005. The scope of this series standard aims for all IT assets within an organization, and especially considers the management of software assets, since more difficulties need to be considered when compared to asset management for hardware components.

7.2.2 Difficulties to manage IT and Software Asset

At the outset, the number of software assets is normally much bigger than other kind of assets, especially in a modern smart factory. Due to the module design concept, multiple types of software (which may come from different suppliers) are typically built together to implement a required functionality. Meanwhile, in general cases, this software needs to be executed on operating systems, which are themselves also software asset with huge complexity. Furthermore, the introduction of Open Source software, regardless of regular software or operating systems like Linux, brings more impacts to the IT-security considerations. License management is also a big challenge in modern manufacturing. For improving the performance while reducing the costs, which is one major target of asset management systems, customers might require sharing licenses between devices installed with the same software, in a time-division manner. When these devices located in a large scale, e.g. in different factories that were built in different cities, the relevant license has to be transferred between distributed locations through network.

7.2.3 Patching and Version Management increase difficulty

The patching of software increases security concerns. Improper patching may cause the failure of a whole system due to unmatched interfaces. Heterogeneous versions of the same software may cause potential errors that are very difficult to diagnose. Before updating/patching of the production system, an integration test helps to partly avoid these problems. However, software asset management still plays an important role by tracking the patching actions and determining the version of the running software. In some scenarios with high security demands, the software itself, as well as its patches, needs to be authenticated to avoid tampering or the insertion of fake stubs from cyber-attackers.

7.2.4 A system of software identification tags (SWIDs)

Similar to the asset management system described in ISO 50000, software assets, which could be a dedicated software, an operating system, a patch or even a software snapshot, need to be identified as software assets with unique identifiers. Considering different modules in a software system, relevant assets should be able to link each other for testing their compatibility. One part of the series standard 19770-5 provides the guidelines for building a system of software identification tags (SWIDs).

Figure 21 illustrated an example of relations between software and its related patches. Here, the software product and all patches (patch 1 to 7) have their own SWIDs, thus they can be identified in the software asset management system.

- On one side, all the applied patches will be recorded in the correspondent attribute in the SWID of the software product.
- On the other side, for each patch, its patching targets will be recorded too.

Through this record, we can easily check whether all relevant software within our system have already patched. Besides, Figure 21 also demonstrates the relationships between patches: requiring or superseding. Requiring means the current patch needs the installation of a previous patch, e.g. patch 4 requires that patch 3 is already installed. Superseding means the new patch already contains all its previous patches. In this case, when recovering by a new installa-

tion, its preceded patches can be skipped without changing the status of the software asset.

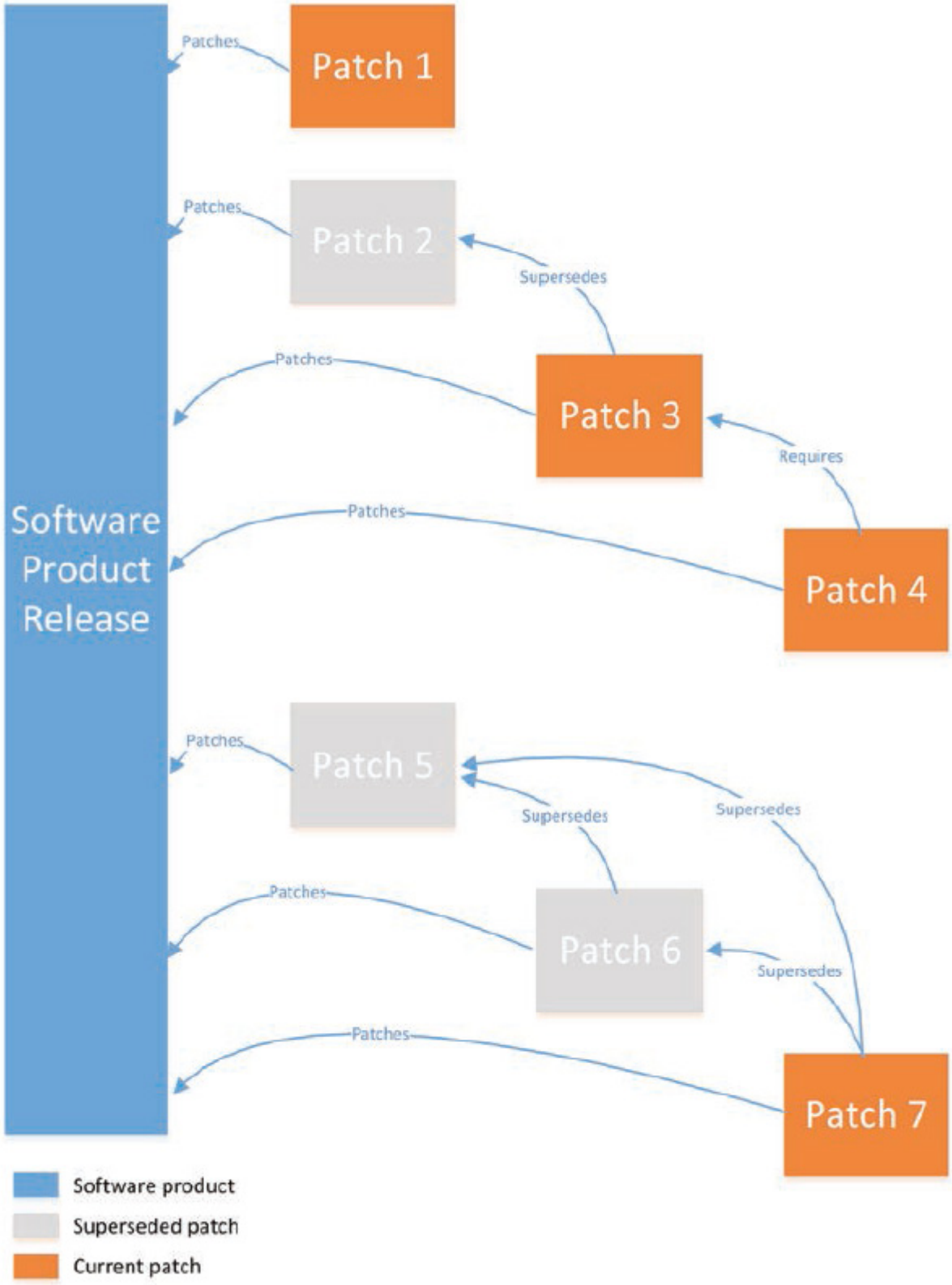

Figure 21 Representation of patch and product relationships (from ISO/IEC 19770-2)

7.2.5 Challenges for IT and Software asset management

The software asset management is still facing challenges. For example, the replacement of a software asset is not modeled in detail yet. Due to the refurbishment of a system, a software asset might be replaced by a new one provided by another company with similar functionalities. This kind of replacements bring potential risks to the whole system and may significantly change its security confidence while an additional security analysis of the whole system means additional cost that is difficult to be evaluated.

8 Interoperability

8.1 IEC 62541 OPC UA

8.1.1 General Description

OPC unified architecture (OPC UA) is a series of technical specifications that provide a way for considering security, reliability in data transport as well as compliance and portability. This standard can be used in different automation systems (e.g. HMI, MES), as well as by different suppliers. It is a common situation that automation systems provided by different suppliers do not always use the same communication protocol. But users usually integrate several systems into the same plant to fulfill their own requirements. Thus, the communication between systems from different vendors becomes a problem. In this situation, interface applications must be developed, which normally means additional costs. Based on this background, OPC UA provides a platform independent specification, using OPC UA client and server to implement the data transport security between different platforms without a need for additional specialized interface applications. It can reduce the integration costs and greatly improve the interoperability.

OPC UA does not only target at SCADA, PLC and DCS interfaces, but also acts as a way to provide better interoperability between higher level functions, including the interface applications (such as HMI, report or alarm center), enterprise management and decision-making platforms (ERP and big data platforms), Internet of Things systems (such as MES or SCADA with CPS) or CPS devices such as the RFID reader to coordinate with the PLC, etc.)

8.1.2 OPC UA specification organization

Figure 22 shows the architecture of this series specification. The left side (part1-part7) of the figure is the core part, which includes the specification about access type and utility. In these core specifications, important models (e.g. security model, address space model and information model) and key techniques (e.g. service set) are described.

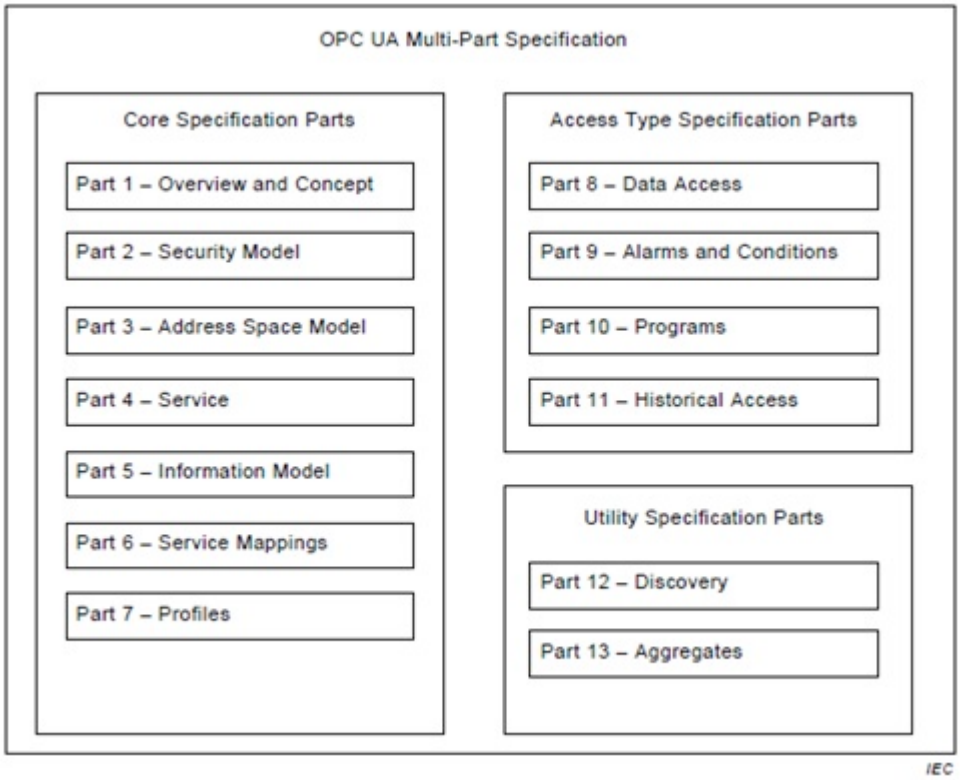

Figure 22 OPC UA specification organization

8.1.3 OPC UA system architecture

OPC UA uses client/server (C/S) architecture defined in IEC 62541-1. As illustrated in Figure 23, client requests service and server responses the service request.
This standard focuses on securing the data exchanged between applications, while other aspects of security are also considered when developing the system.

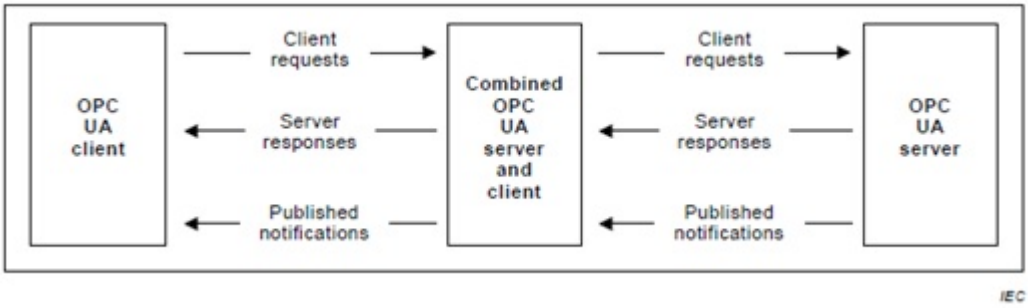

Figure 23 OPC UA system architecture

8.1.4 OPC UA client architecture

The OPC UA client architecture is shown in Figure 24. The client application is the code that implements the functionality of the client side. It employs the OPC UA client API to send and receive OPC UA service requests and responses. The "OPC UA client API" is an internal interface that isolates the client application code on top of the OPC UA communication stack. OPC UA communication stack takes OPC UA client API calls and sends formatted messages through the underlying communication entity to the server side. The OPC UA communication stack also receives response or notification messages and delivers them to the client application according to the OPC UA client API.

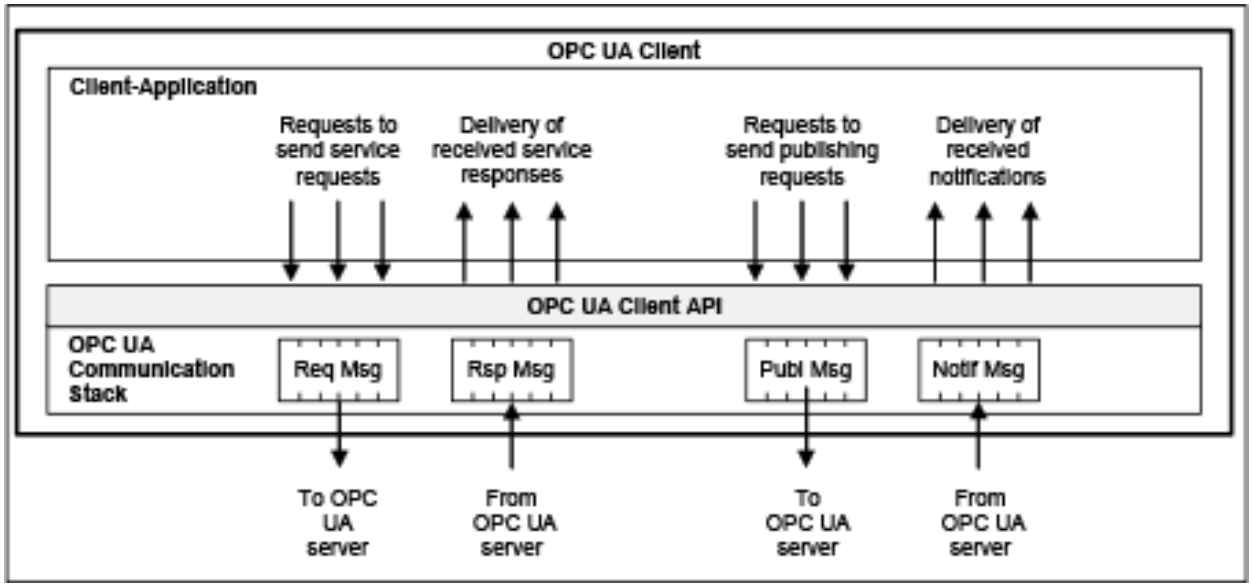

Figure 24 OPC UA Client Architecture

8.1.5 OPC UA server architecture

The OPC UA server architecture model represents the server endpoint in the client/server interactions. Figure 25 illustrates the major elements of the OPC UA Server and how they are related to each other.

8.1.5 OPC UA server architecture

The OPC UA server architecture model represents the server endpoint in the client/server interactions. Figure 25 illustrates the major elements of the OPC UA Server and how they are related to each other.

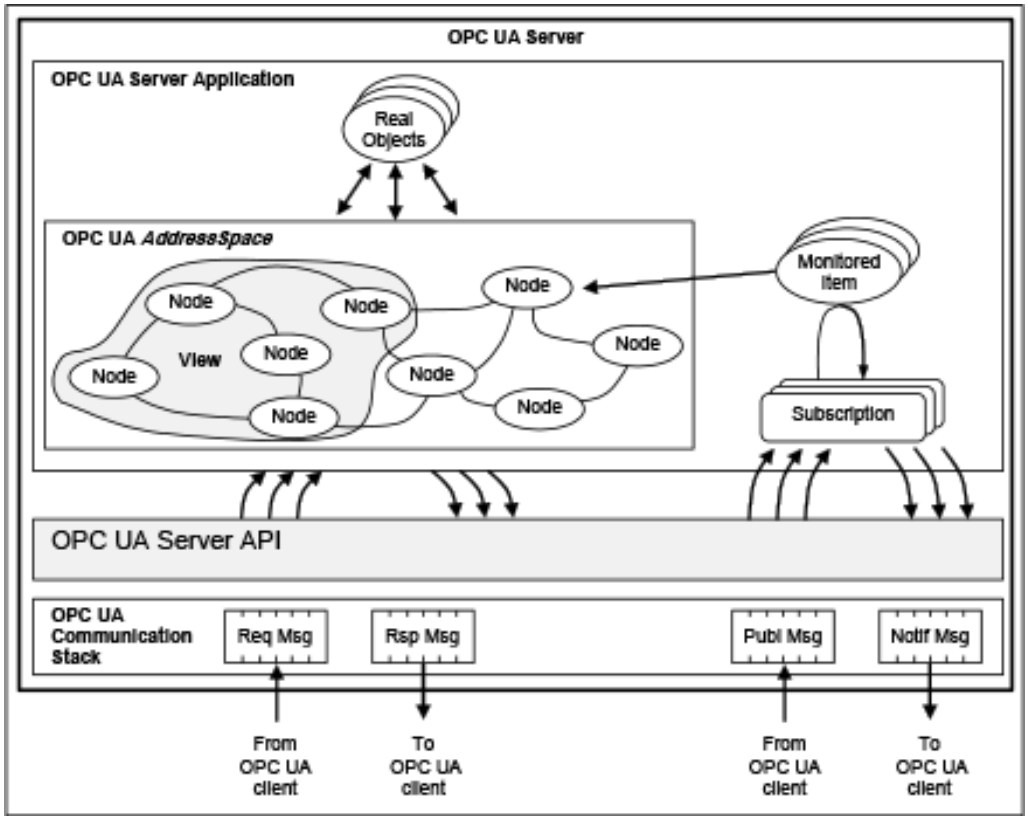

Figure 25 OPC UA Server architecture

8.1.6 OPC UA security architecture

The OPC UA security architecture is a generic solution that allows implementation of the required security features at various places in the OPC UA application. The OPC UA security architecture is structured on the application layer, a communication layer and the transport layer as shown in Figure 26.

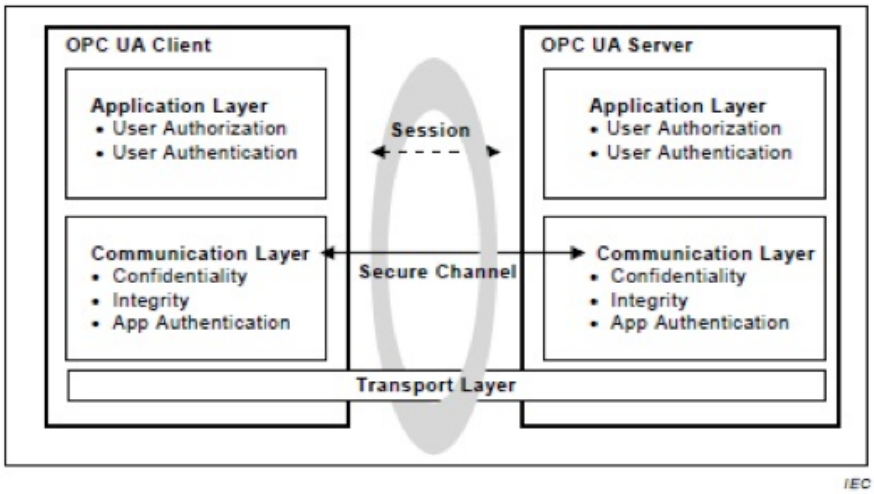

Figure 26 OPC UA security architecture

The routine work between a client and a server for transmitting information, settings and commands is done in a session on the application layer. The application layer also manages the security objectives like user authentication and user authorization.

A session in the application layer communicates over a secure channel that is created on the communication layer (lower layer) and relies upon it for secure communication. All of the session data is passed to the communication layer for further processing.

The communication layer provides a security mechanisms to meet confidentiality, integrity and application authentication as security objectives.

One essential mechanism to meet the above mentioned security objectives is to establish a secure channel that is used to secure the communication between a client and a server. The secure channel provides encryption to maintain the confidentiality of data, message signatures to maintain data integrity and digital certificates to provide application authentication for data that comes from the application layer and passes the "secured" channel down to the transport layer.

The transport layer handles the transmission, reception, and the transport of data that is provided by the communication layer.

To survive the loss of transport layer connections (e.g. TCP connections) and to resume with a new connection, the communication layer is responsible for re-establishing the transport layer connection without interrupting the logical secure channel.

8.1.7 OPC UA Security Policy

A security policy is derived from a security profile and specifies which security mechanisms are to be used. Security policies are used by the server to announce which mechanisms it supports and are used by the client to select one to cooperate with the secure channel as it wishes. Security Policies include the following information:

- algorithms for signing and encrypting
- algorithm for key derivation

Since computing power increases every year, specific algorithms that are considered as secure today can become insecure in the future. Therefore, it is reasonable to support different security policies in an OPC UA application and to be able to adopt more as they become available.

8.2 IEC 61850

IEC 61850 is a standard for vendor-agnostic engineering of the configuration of intelligent electronic devices for electrical substation automation systems to be able to communicate with each other. IEC 61850 is a part of the International Electrotechnical Commission's (IEC) Technical Committee 57 (TC57) reference architecture for electric power systems. The abstract data models defined in IEC 61850 can be mapped to a number of protocols. Current mappings in the standard are to MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event), SMV (Sampled Measured Values), and soon to Web Services. These protocols can run over TCP/IP networks or substation LANs using high speed switched Ethernet to obtain the necessary response times below four milliseconds for protective relaying.

The IEC 61850 standard can be used in different industry domains as shown in Figure 27.

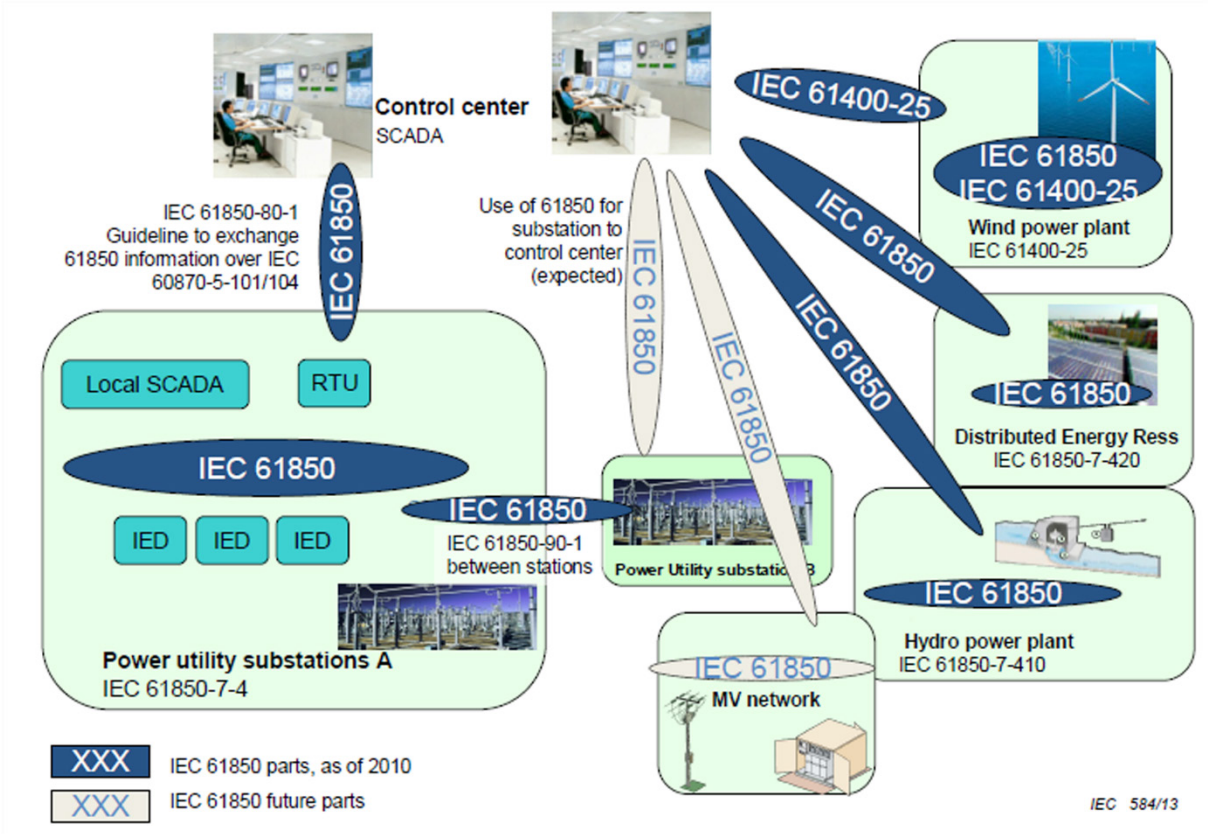

Figure 27 Scope of application of IEC 61508

One obvious feature of IEC 61850 is the idea of communication independence from the application by specifying a set of abstract level of services and objects. In this way applications can be written in a manner which is independent from the specific protocol. This abstraction allows both vendors and utilities to maintain application functionality and to optimize this functionality when appropriate as explained in Figure 28.

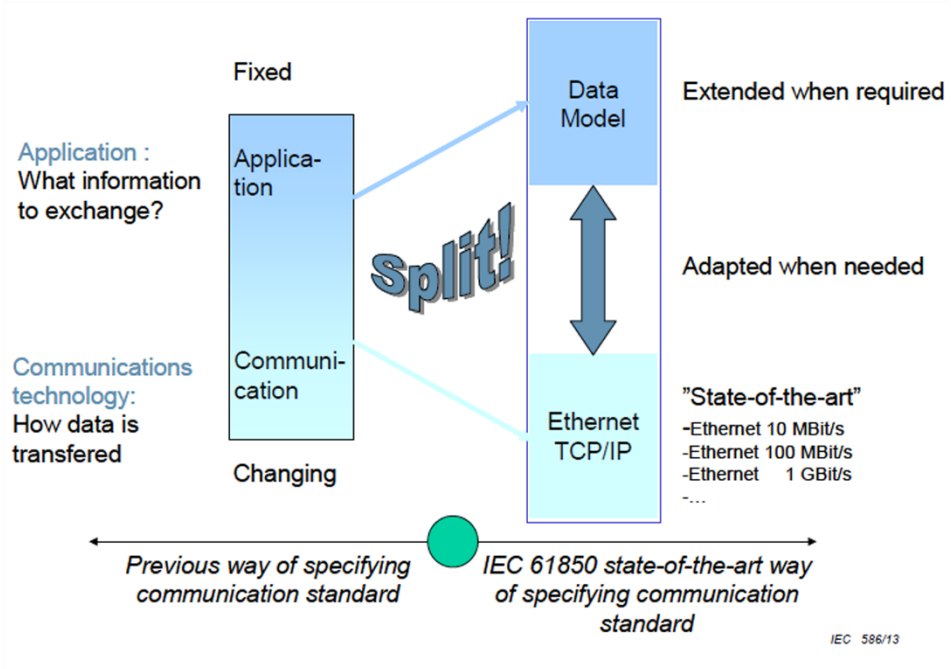

Figure 28 IEC 61850 specifying approach

The IEC 61850 information model is based on two main levels of modeling (see below):

- The breakdown of a real device (physical device) into logical devices
- The breakdown of logical device into logical nodes, data objects and attributes

Figure 29 gives an example of how each level is included into the upper layer.

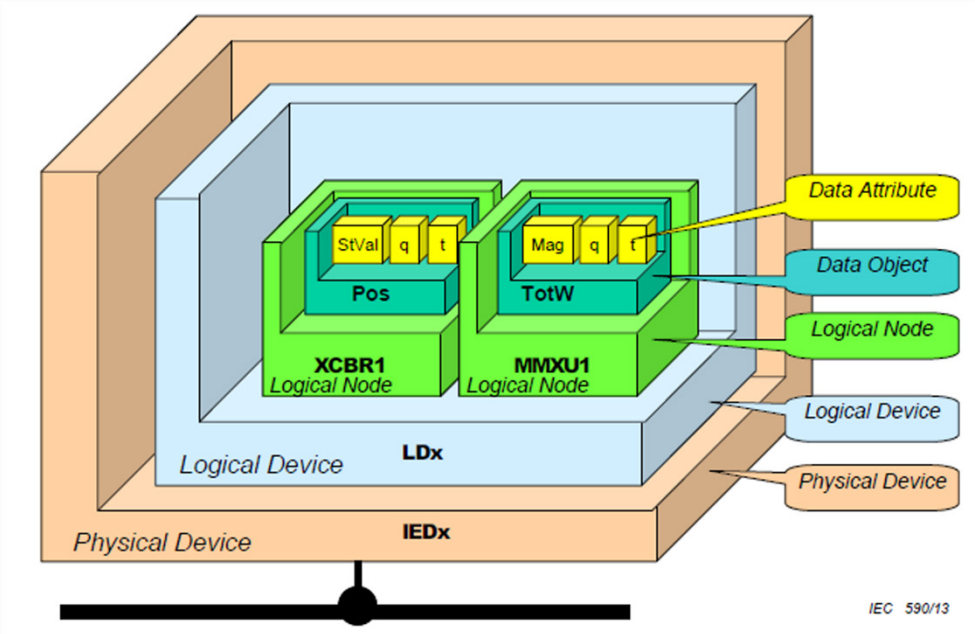

Figure 29 Data modeling

IEC 61850 offers three types of communication models:

1. Client/Server type communication services model
2. Fast and reliable system-wide distribution of data, based on a publisher-subscriber model (GSE Management). Two control classes are defined for that purpose.
   - GOOSE – analogue and digital multicast
   - GSSE – digital data exchange over multicasts (deprecated)
3. Sample Values (SMV) model for multicast measurement values

The IEC 61850 series provides an assortment of mappings which can be used for communication within the substation. The selection of an appropriate mapping depends on the functional and performance requirements.

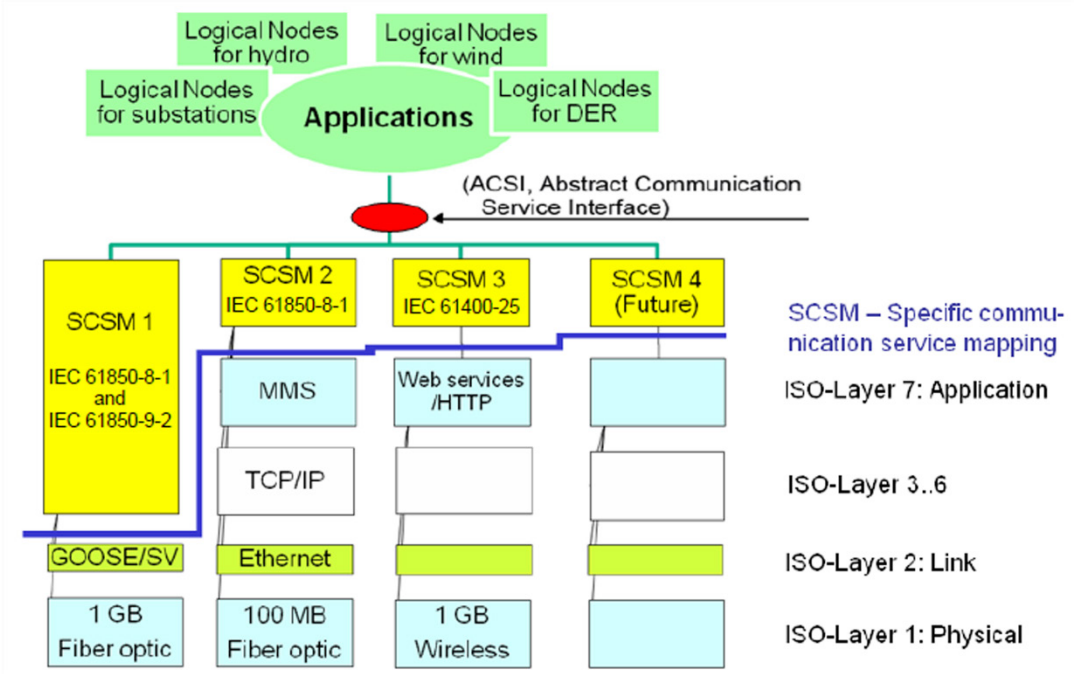

Figure 30 Basic reference model

This mapping is shown in Figure 30 as "SCSM". According to the facilities of the related application layer, the extent of the mapping can be different.

In order to ensure the data can be exchanged in between tools of different manufacturers in a compatible way, IEC 61850-6 defines a System Configuration description Language (SCL). The SCL language itself is based on XML, this language can implement the system functional specification, IED capability description, power Utility automation system description.

8.3 NIST SP800-162

This document describes the functional components of ABAC (Attribute Based Access Control), as well as a set of considerations for employing ABAC within a large enterprise without taking Identity Management into account, thus assuming subjects are bound to trusted identities or identity providers. This report provides detailed information to understand ABAC, basic and core concept of ABAC, it also explains the life cycle principle of initiation, acquisition/development, implementation/assessment, and operations/maintenance phases.

The concepts of IBAC (identity based access control) and ACL (access control lists) were introduced first. As networks grew, the need to limit access to specific protected objects spurred the growth of identity based access control (IBAC) capabilities. IBAC employs the use of access control lists (ACLs) to capture the identities of those allowed to access the object. If a subject presents a credential that matches the one held in the ACL, the subject is given access to the object. Individual privileges of the subject to perform operations (read, write, edit, delete, etc.) are managed on an individual basis by the object owner. Each object needs its own ACL and set of privileges assigned to each subject. In the IBAC model, the authorization decisions are made prior to any specific access request and result in the subject being added to the ACL.

8.3.1 Definition of ABAC

Attribute Based Access Control (ABAC) is an access control methodology, where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. Attributes are characteristics that define specific aspects of the subject, object, environment conditions, and/or requested operations that are predefined and reassigned by an authority. Attributes contain information that indicates the class of information given by the attribute, a name, and a value (e.g., Class=HospitalRecordsAccess, Name=PatientInformationAccess, Value=MFBusinessHoursOnly).

Concept of ABAC

The basic access control scenario of ABAC as Figure 31 shows, includes the concept of policy, attribute management, access control mechanism.

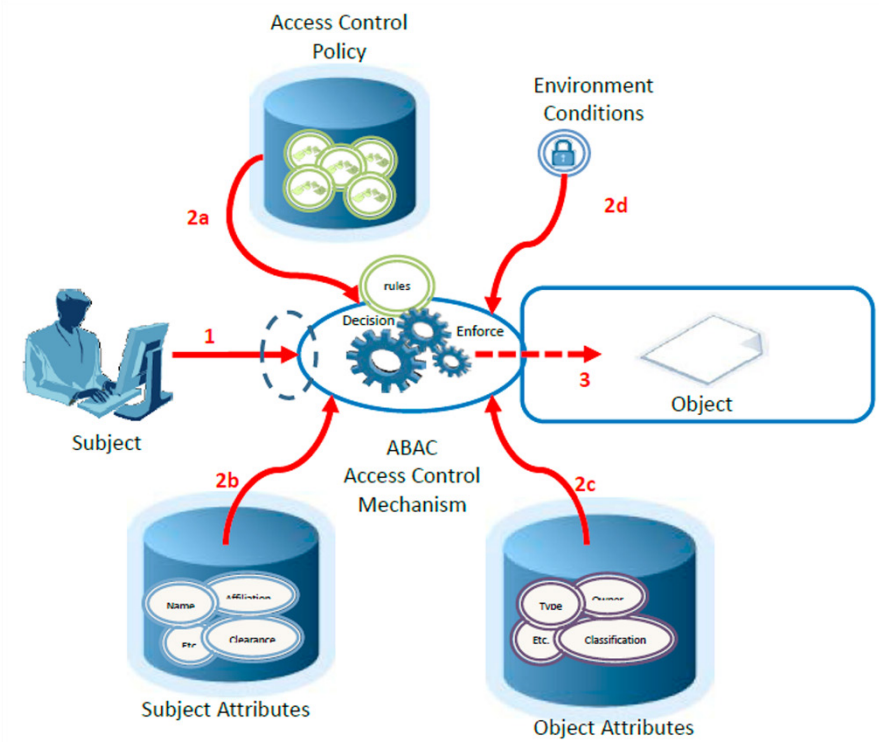

Figure 31 Basic ABAC Access Control Scenario

First, the Subject requests access to the Object;
Second, the Subject should satisfy the ABAC Mechanism, e.g. (2a) Access Control Policy, (2b) Subject Attributes, (2c) Object Attributes, and (2d) Environment Conditions to determine authorization;

Third, if Subject satisfies all the mechanism in step 1, then the Subject can get the right to assess to the Object, otherwise, it will be denied.

ABAC relies heavily upon the evaluation of attributes of the subject, attributes of the object, environment conditions, and the formal relationship or access control rule or policy defining the allowable operations for subject-object attribute combinations. All ABAC solutions contain these basic core capabilities to evaluate attributes and enforce rules or relationships between those attributes (see Figure 32).

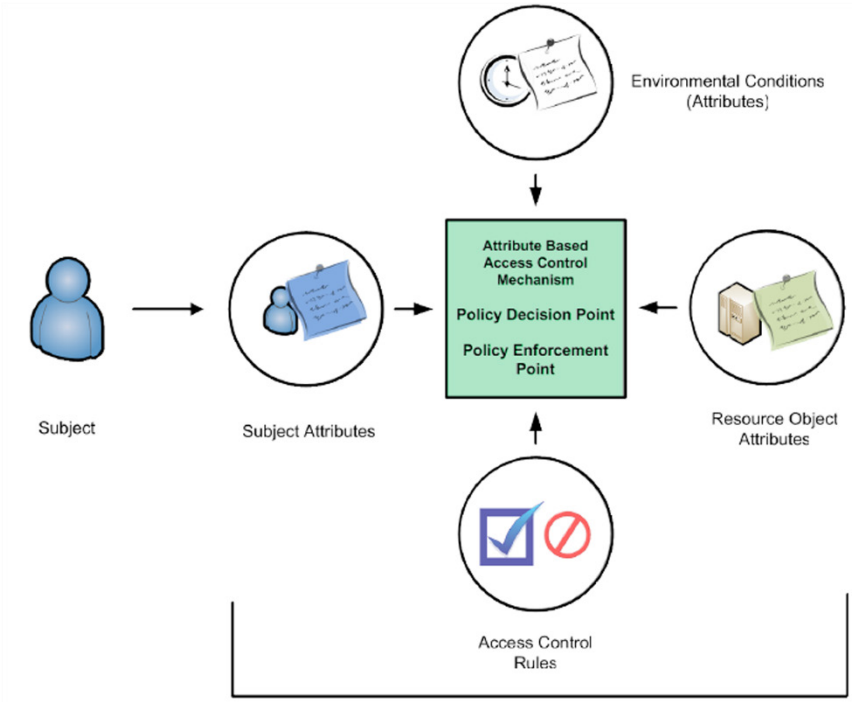

Figure 32 Core ABAC Concept

From Figure 32 we can see that whenever there is an access request, which will be evaluated by the ABAC Mechanism to decide whether it can be allowed or not. In this ABAC basic form, the Access Control Mechanism contains Policy Decision Point and Policy Enforcement Point.

8.3.2 Guideline of Deploying an ABAC

The concept based on the NIST life cycle

Many factors must be considered before deploying an ABAC system across an enterprise. This section attempts to consolidate available guidelines based on the state of the technology to date and lessons learned through multiple attempts within the Federal Government to deploy ABAC capabilities throughout a large enterprise. The guidelines are presented according to the phases of the NIST System Development Life Cycle (SDLC), as Figure 33 shows. For more general information regarding the definitions of the phases and expected outputs, please refer to NIST SP 800-100: Information Security Handbook: A Guide for Managers. Most considerations for employment of enterprise ABAC fall within the first four phases: Initiation, Acquisition/Development, Implementation/Assessment, and Operations/Maintenance. As such, this section focuses on those phases exclusively.

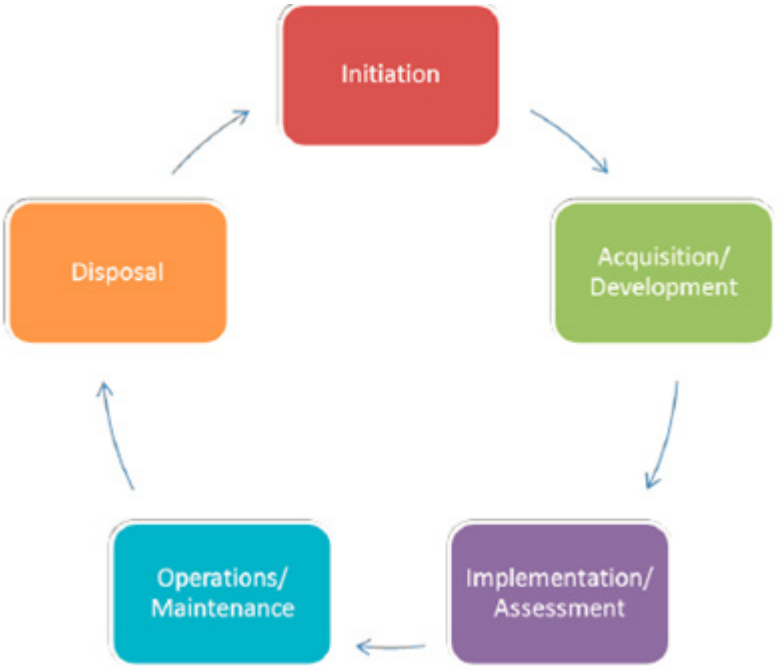

Figure 33 ACM NIST System Development Life Cycle (SDLC)

Initiation Phase

The organization establishes the need for an ABAC system and documents its purpose. It is often determined whether the ABAC system will be an independent information system or a component of an already-defined system. Once these tasks have been completed and a need has been recognized for ABAC capabilities, several processes must take place before the ABAC system is approved, to include clearly defining goals and defining high-level requirements. Typically, during this phase, the organization defines high-level business and operational requirements as well as the enterprise architecture for the ABAC system.

Acquisition/Development Phase

During the acquisition/development phase, the system is designed, purchased, programmed, developed, or otherwise constructed. Typically, during this phase, the organization prepares the business processes needed for enterprise-wide execution and defines the systems to be deployed and integrated. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle. During the first part of this phase, the organization should simultaneously define the system's security and functional requirements. During the last part of this phase, the organization should perform developmental testing of the technical and security features/functions to ensure that they perform as intended prior to launching the implementation/assessment phase.

Implementation/Assessment Phase

In the implementation/assessment phase, the organization configures and enables system security features, tests the functionality of these features, installs or implements the system, and finally, obtains a formal authorization to operate the system. Most of the considerations during this phase are focused on optimizing performance and ensuring security features work as expected.

Operations/Maintenance Phase

In the operations/maintenance phase, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. During this phase, the organization should continuously monitor performance of the system to ensure that it is consistent with pre-established user and security requirements, and needed system modifications are incorporated.

The advantage of ABAC is that it is well suited for large and complex enterprises. Its capabilities will allow an unprecedented amount of flexibility and security, while promoting information sharing between diverse and often disparate organizations. An ABAC system can implement existing role-based access control policies and can support a migration from role-based to a more granular access control policy based on many different characteristics of the individual requester.

9 Conclusion

This whitepaper contains an overview of different international and national Chinese and German security standards and guidelines that are considered to be significant in the context of I4.0/IM. The document structure is according to key topics and sub-topics, like network security, supplier relationships, interoperability, access control schemes, patch management, asset management, risk management etc. with indications of the contributions that different standards and guidelines bring to the respective topics. As indicated in some sections, several standards are still under development. Also, some of the examples, e.g. the distribution of security incident types in a given time period, as analyzed by the German BSI, are bound to change over time. Accordingly, in a few years, an update of this whitepaper may be needed, in order to reflect the Sino-German security Standardisation landscape, e.g. in 2020.

10 Reference

[1] http://www.iso27001security.com/index.html

[2] IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

[3] IEC/TR 62443-1-2, Industrial communication networks - Network and system security - Part 1-2: Master glossary of terms and abbreviations1

[4] IEC/TR 62443-1-3, Industrial communication networks - Network and system security - Part 1-3: System security compliance metrics

[5] IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

[6] IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment

[7] IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

[8] IEC TR 62443-3-1:2009 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems

[9] IEC 62443-3-2 ED1 Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design

[10] IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

[11] IEC 62443-4-1 ED1 Industrial communication networks - Security for industrial and control systems - Part: 4-1: Product development requirements

[12] IEC 62443-4-2 ED1 Industrial communication networks - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

[13] GB17859-1999 Classified criteria for security protection of computer information system

[14] NIST SP800-53 rev4, Security and Privacy Controls for Federal Information Systems and Organizations

[15] NIST SP800-82, Rev2, Guide to Industrial Control System (ICS) Security

[16] NIST SP800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations

[17] NIST Cyber-security Framework

[18] ISO/IEC 27033 Information technology - Security techniques - Network security Part 1 ~ Part 6

[19] IEC TR 62541□OPC Unified Architecture Part 1 ~ Part 13

[20] ISO/IEC TR 24772:2013 Information technology - Programming languages - Guidance to avoiding vulnerabilities in programming languages through language selection and use

[21] ISO/IEC 27036 Information security for supplier relationships Part 1 ~ Part 4

[22] UTC (Utilities Telecom Council), Cyber supply chain risk management for utilities - roadmap for implementation ten basic practices

[23] ISO/IEC 27035:2016 Information technology — Security techniques — Information security incident management, Part 1 ~ Part 2

[24] ISO 55000:2014 Asset management - Overview, principles and terminology

[25] ISO/IEC 19770-1:2012 Information technology - IT asset management (ITAM) - Part1 ~ Part8

[26] http://www.opcfoundation-events.com/uploads/media/OPC-UA-Wegbereiter-der-IE40-DE-v2.pdf

[27] https://www.techopedia.com/definition/27805/digital-forensics

[28] BSI Standard 100-1 Information Security Management Systems (ISMS)

[29] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1

[30] BSI-Standard 100-2: IT-Grundschutz Methodology https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1
BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile&v=1

[31] BSI-Standard 100-4: Business Continuity Management
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

[32] Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, ENISA, 2015, https://www.enisa.europa.eu/publications/maturity-levels

[33] Communication network dependencies for ICS/SCADA Systems, ENISA, 2016, https://www.enisa.europa.eu/publications/ics-scada-dependencies

[34] IT-Sicherheit für die Industrie 4.0, BMWi, 2016, https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.html

[35] IT-security for industrial automation – General model, VDI/VDE 2182 Blatt 1, 2011

11 Annex

11.1 ISO/IEC 27000-series information security standards

The following ISO/IEC 27000-series information security standards (the "ISO27k standard") are either published or being developed:

Standard	Published	Title	Notes
ISO/IEC 27000	2016	Information security management systems - Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary.
ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant.
ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls.
ISO/IEC 27003	2010	Information security management system implementation guidance	Basic advice on implementing ISO27k.
ISO/IEC 27004	2016	Information security management – Measurement	.
ISO/IEC 27005	2011	Information security risk management	Discusses risk management principles without specifying particular methods.
ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies.
ISO/IEC 27007	2011	Guidelines for information security management systems auditing	Auditing the *management system* elements of the ISMS.
ISO/IEC TR 27008	2011	Guidelines for auditors on information security management systems controls	Auditing the *information security* elements of the ISMS.
ISO/IEC 27009	2016	Sector-specific application of ISO/IEC 27001 - requirements	Guidance for those developing new ISO27k standards.
ISO/IEC 27010	2015	Information security management for inter-sector and inter-organizational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure".
ISO/IEC 27011	2016	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051".
ISO/IEC 27013	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL.
ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"

Standard	Published	Title	Notes
ISO/IEC TR 27015	2012	Information security management guidelines for financial services	Applying ISO27k in the finance industry.
ISO/IEC TR 27016	2014	Information security management - Organizational economics	Economic theory applied to information security.
ISO/IEC 27017	2015	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing.
ISO/IEC 27018	2014	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing.
ISO/IEC TR 27019	2013	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry).
ISO/IEC 27021	DRAFT	Competence requirements for information security management professionals	Guidance on the skills and knowledge necessary to work in this field.
ISO/IEC TR 27023	2015	Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002	Belated advice for those updating their ISMSs from the 2005 to 2013 versions.
ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (*i.e.* resilience, incident management and disaster recovery) for ICT, supporting general business continuity.
ISO/IEC 27032	2012	Guidelines for cybersecurity	
ISO/IEC 27033	-1 2015	Network security overview and concepts	Various aspects of network security, updating and replacing ISO/IEC 18028.
	-2 2012	Guidelines for the design and implementation of network security	
	-3 2010	Reference networking scenarios - threats, design techniques and control issues	
	-4 2014	Securing communications between networks using security gateways	
	-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
	-6 2016	Securing wireless IP network access	
ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard. Promotes the concept of a reusable library of information security control functions, formally specified, designed and tested
	-2 2015	Organization normative framework	

Standard	Published	Title	Notes
	-3 DRAFT	Application security management process	
	-4 DRAFT	Application security validation	
	-5 DRAFT	Protocols and application security control data structure	
	-6 2016	Case studies	
	-7 DRAFT	Application security assurance prediction framework	
ISO/IEC 27035	2016	Information security incident management	Replaced ISO TR 18044; now being split into three parts.
ISO/IEC 27036	-1 2014	Information security for supplier relationships - Overview and concepts	Information security aspects of ICT out sourcing and services.
	-2 2014	Common requirements	
	-3 2013	Guidelines for ICT supply chain security	
	-4 2016	Guidelines for security of cloud services	
ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	First of several IT forensics standards.
ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents.
ISO/IEC 27039	2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	IDS/IPS
ISO/IEC 27040	2015	Storage security	IT security for stored data.
ISO/IEC 27041	2015	Guidelines on assuring suitability and adequacy of incident investigative methods	Assurance of the integrity of forensic evidence is absolutely vital.
ISO/IEC 27042	2015	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
ISO/IEC 27043	2015	Incident investigation principles and processes	The basic principles of eForensics.
ISO/IEC 27050	-1 2016	Electronic discovery - overview and concepts	More eForensics advice.
	-2 DRAFT	Guidance for governance and management of electronic discovery	Advice on treating the risks relating to eForensics.
	-3 DRAFT	Code of practice for electronic discovery	A how-to-do-it guide.
ISO 27799	2016	Health informatics — Information security management in health using ISO/IEC 27002	Information security advice for the healthcare industry.

11.2 Acronyms and Abbreviations

ABAC	Attribute Based Access Control
ACL	Access Control List
ANSI	American National Standards Institute
API	Application Programming Interface
APT	Advanced Persistent Threats
BAN	Business/Building Area Network
BMWi	Bundesministeriums für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy)
BPCS	Basic Process Control System
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
C/S	Client/Server
CA	Certification Authority
CERT	Computer Emergency Response Team
CIA	Confidentiality (C), Integrity (I) and Availability (A)
CMMI	Capability Maturity Model Integration
COST	Commercial-off-the-Shelf
CSIRT	Computer Security Incident Response Team
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
ECMAS	European Computer Manufacturers Association
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
GB/T	GuoBiao/Tui (Chinese National Standard Recommendation)
GB	GuoBiao (Chinese National Standard)
GOOSE	Generic Object Oriented Substation Event
GPS	Global Positioning System
GSSE	Generic Substation State Event
HAN	Home Area Network
HMI	Human Machine Interface
I4.0	Industry 4.0
IACS	Industrial Automation Control System
IAN	Industrial Area Network(smart grid)
IBAC	Identity Based Access Control
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control System
ICT	Information Communications Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IM	Intelligent Manufacturing
IMSG	(Chinese) National Intelligent Manufacturing Standardization Administration Group
IRT	Incident Response Team
ISA	International Society for Automation
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MES	Manufacturing Execution System
MMS	Manufacturing Message Specification
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cyber Security Framework
NIST SP	NIST Special Publication
OPC	Object Linking and Embedding (OLE) for Process Control
OPC UA	OPC Unified Architecture
OSI	Open System Interconnection
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SCI4.0	Standardization Council Industrie 4.0
SCL	Substation Configuration Description Language
SCRM	Supply Chain Risk Management
SCSM	Specific Communication Service Mapping
SDL	Secure Development Life-Cycle
SIS	Safety Instrumented System
SMV	Sampled Measured Value
SWID	Software Identification Tag
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TASE	Telecontrol Application Service Element
TCP/IP	Transmission Control Protocol / Internet Protocol
UTC	Utilities Telecom Council
VDI/VDE	Verein Deutscher Ingenieure/Verband Deutscher Elektrotechniker
VPN	Virtual Private Networks
XML	Extensible Markup Language

List of Contributors to the IT Security White Paper

Chinese experts	German experts
Jianjun Yang, National Information Security Standardization Technical Committee (TC260)	Dr Karl Waedt, Framatome GmbH
Kefeng Fan, National Information Security Standardization Technical Committee (TC260)	Yuan Gao, Framatome GmbH
Lin Li, China Electronics Standardization Institute	Xinxin Lou, Framatome GmbH
Xiangang Liu, China Electronics Standardization Institute	Edita Bajramovic, Framatome GmbH
Xiangzhen Yao, China Electronics Standardization Institute	Venesa Watson, Framatome GmbH
Junjie Gan, China Electronics Standardization Institute	Jochen Link, ING-LINK Ingenieurbüro
Dajiang Zhang	Christiane Gabbe, innogy SE
Ji Xia, China Electronics Standardization Institute	Prof Dr Christoph Ruland, University Siegen
Jiezhong Gong, China Electronics Standardization Institute	Prof Dr Ding Yongjian, University of Applied Sciences Magdeburg-Stendal
Ruikang Zhou, China Electronics Standardization Institute	Martin Kaiser, Industrieanlagen-Betriebsgesellschaft mbH
Sha Wei, China Electronics Standardization Institute	Prof Jan de Meer, smartspacelab
Gaofeng An	Dr Wolfgang Klasen, Siemens AG
	Robert Fischer, Otto von Guericke University Magdeburg
	Jörn Edlich, CETECOM
	Volker Jacumeit,DIN

Members of the Sino-German Experts Working Group

Standardization Council Industrie 4.0 (SCI4.0)
Dr. Jens Gayko, Managing Director SCI4.0
E-Mail: jens.gayko@vde.com
Yves Leboucher, Manager International Cooperations
E-Mail: yves.leboucher@vde.com

Chinese Lead Expert
Dr. Kefeng Fan, National Information Security Standardization Technical Committee (TC260)

German Lead Expert
Dr. Karl Waedt, Framatome GmbH