IEC/TR 62351-10

Edition 1.0 2012-10

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 10: Security architecture guidelines

IEC/TR 62351-10:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TR 62351-10

Edition 1.0 2012-10

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 33.200

ISBN 978-2-83220-419-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 10: Security architecture guidelines

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62351-10, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1234/DTR	57/1265/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Cyber security becomes more and more a basic necessity in power control systems as standard IT and other forms of modern communication technology are being increasingly used for control and supervision of these systems. The application of IT communication technology demands the consideration of already existing vulnerabilities, which can be exploited by potential attackers, as recent intentional and unintentional cyber incidents on SCADA and other industrial control systems have shown. The increasing number of control system cyber incidents world-wide with medium to high impact underlines the importance of appropriate security measures (see [11][1]).

The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 (Power Systems Management and Associated Information Exchange) is responsible for developing international standards for power system data communications protocols. Standards developed within TC 57 comprise for instance IEC 60870-5, IEC 61850, and IEC 62351 just to state a few. Especially the latter addresses technical security controls within power systems.

A security architecture as targeted here does not only comprise technical means like the application of dedicated security entities, security protocols or security options in communication protocols to secure power system entities or the communication network. It also describes operational guidelines considering the available technical base as well as the personnel controlling the power systems. Moreover, interactions with existing (security) infrastructures also affect overall system security.

In this Technical Report hands-on guidelines are proposed for the implementation of security mechanisms based on deployment examples, rather than a lecture or reference book for security in general. Therefore, available resources of information related to security of power systems or more general to security in Smart Grid are utilized and will be referenced as much as possible, without repeating their content here. Thus this Technical Report addresses both, the power system engineer and the traditional IT security engineer.

The examples used throughout this Technical Report are intended to better explain the influences of and the interactions with security. They are used as descriptive examples without the claim to be complete.

Clause 4 of this Technical Report specifies the specifics of the power systems industry, comprising differences in the security requirements compared to office systems as well as an overview about related standardization. It also introduces the TC 57 reference architecture as one base for the security architecture discussion.

Clause 5 establishes a general approach to a security architecture by using security domains and dedicated security controls within these domains and maps this approach to the power system domain based on examples use cases. Clause 5 also addresses the mapping of the NIST identified interface categories with the TC 57 architecture interfaces.

Clause 6 maps security controls with the IEC TC 57 power system architecture based on example scenarios. It starts with an overview scenario of power systems and digs into dedicated sub-scenarios like a substation deployment, the communication between a substation and a control centre and so on.

---

1 References in square brackets refer to the Bibliography.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 10: Security architecture guidelines

1 Scope

This part of IEC 62351, which is a Technical Report, targets the description of security architecture guidelines for power systems based on essential security controls, i.e. on security-related components and functions and their interaction. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems is provided as a guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC/TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC/TS 62351-2, as well as the following apply.

3.1.1
de-militarized zone
DMZ
LAN segment / zone used to tier application/UI/file access between two other zones/segments

3.1.2
reliability
ability of a system to perform a required function under stated conditions for a specified period of time

3.1.3
security controls
technical or procedural security counter measures to avoid, counteract or minimize security risks

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ACL access control lists

BDEW	Bundesverband Für Energie- und Wasserwirtschaft
BES	bulk energy system
CA	certification authority that issues digital certificates
CSWG	cyber security working group
DHS	department of homeland security
DMZ	de-militarized zone
DoS	denial of service
DTLS	datagram transport layer security
DTR	draft technical report
HMAC	hashed message authentication codes
HTTPS	secure hypertext transfer protocol
HSM	hardware security module
IDS	intrusion detection system
IP	internet protocol
IPS	intrusion prevention system
LAN	local area network (it is the Ethernet IP network inside a security domain)
LDAP	lightweight directory access protocol
NTP	network time protocol
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NWIP	new work item proposal
OS	operating system
OTP	one time password authentication
RBAC	remote based access control
RDP	remote desktop protocol
PKI	public key infrastructure
SGIP	Smart Grid interoperability panel
SNMP	simple network management protocol
TCP	transmission control protocol
TPM	trusted platform module
TLS	transport layer security
TR	technical report
TS	technical specification
URL	uniform request locator
WIP	work in progress
WLAN	wireless local area network

4 Power systems – specifics and related standardization

4.1 Overview

Power generation, transmission, and distribution systems are characterized by the existence of two infrastructures in parallel, the electrical grid (1 in Figure 1), carrying the energy and the information infrastructure (2 in Figure 1) used to automate and control the electrical grid. Especially the information infrastructure is becoming more and more a critical part of power system operations as it is responsible not only for retrieving information from field equipment

but most importantly for submitting control commands. A dependable management of these two infrastructures is crucial and strongly relies on the information infrastructure as automation continues to replace manual operations. Hence, the reliability of the power system strongly depends on the reliability of the information infrastructure. Therefore the information infrastructure shall be managed to the level of reliability needed to provide the required stability of the power system infrastructure to prevent any type of outage.

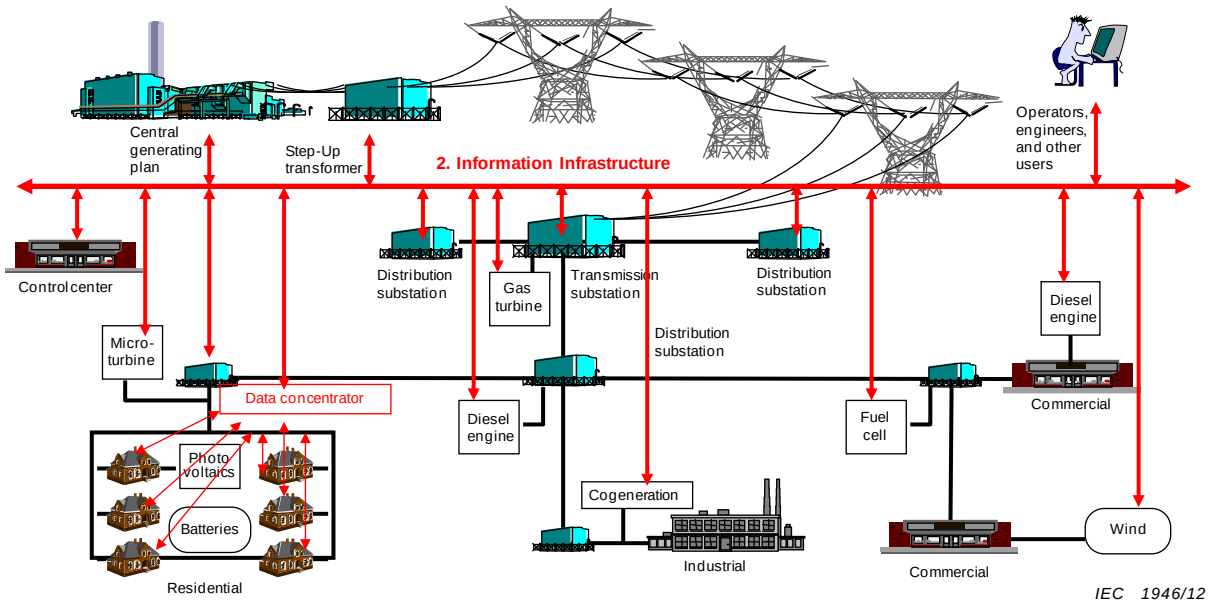


Figure 1 – Power systems – Management of two infrastructures (see Figure 11 of [40])

The present, rather centralized approach for power generation is evolving to a decentralized power generation involving existing power plants, power plants producing renewable energy (like wind parks) down to residences having their own micro power plants (e.g. solar cells). Moreover, electro mobility as potential energy storage will become more important and needs to be integrated into the current power system landscape. This increases the already high complexity of power systems even more. Furthermore, there is also the trend to interconnect the formerly closed and proprietary architectures with office environments and enterprise systems to allow new functionalities and increase cost effectiveness. The reverse side is that this may also lead to new vulnerabilities, which turn cyber security into a priority and a permanent challenge.

As the information infrastructure is the backbone of power system control, it needs appropriate protection to ensure the operation of power systems and support the required system reliability. Information security is the base for protecting the information infrastructure against intentional and unintentional cyber incidents but needs to take the power system specifics into account. These specifics are depicted in 4.2. Security as a major topic has been recognized by standardization bodies as outlined in 4.3, which does not provide a complete list of standards but lists the most important ones for the application domain. 4.4 focuses on the architecture of the IEC TC 57 spanning power systems management and associated information exchange.

4.2 Security specifics

The operational environment of the power systems information infrastructure differs from office environments or telecommunication environments in several aspects. Specific cyber security problems have been identified for instance in the NIST document set NIST IR 7628 (see [17], [18], and [19]). Volume 3 of NIST IR 7628 (see [19]) provides a list of evident and specific cyber security problems. These documents explain the enumerated operational, system, and device issues more specifically. Technical issues related to the definition of appropriate security measures have also been discussed as part of IEC/TS 62351-5 (see [43]).

The following list provides some examples for specifics in power systems out of the referenced documents and also provides additional examples (not a complete list):

– computer-constrained resources precluding many IT technologies;
– communication between components is often asymmetric and message oriented (like multicast);
– strict timing requirements (down to milliseconds);
– long lifetime or operation time of components (in the range of 10 to 30 years);
– based on the long operation time of the components, there are strong requirements for interoperability with legacy systems and for migration concepts;
– interoperability with legacy systems influences the maintainability of power systems and makes systems more complex, especially if maintenance and operation security is desired;
– limitations of connectivity of systems or system components to a central (control) network;
– higher availability and less latency requirements leading e.g. to missing or limited patch windows within customer facilities complicate the security patch process. Often customers do not or only reluctantly accept updates in their environment;
– interconnection of independent entities (producers / generators, other transport / distribution network operators and services);
– field devices may be installed in physically unprotected areas. Direct access to components by maintenance personnel is costly and often impractical as devices may be installed in widely distributed areas.

Figure 2 summarizes the differences for basic security services and practices between office networks and power system networks. The classifications low, medium, and high are comparable with the NISIR 7628 volume 1 (see [17]) impact levels.

	Energy Control Systems 	Office IT 
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	10-30 years	3-5 years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular / scheduled
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	High	Medium

IEC 1947/12

Figure 2 – Comparison office / power system security requirements

As seen, security objectives in power systems are focused on authentication and integrity protection rather than on confidentiality (which is typically the main objective in office and telecommunication environments). This is especially true for energy automation control and protection communication. Nevertheless, with the increased introduction of the advanced metering infrastructure (AMI) and the increasing demand for energy automation down to residential level, confidentiality is required to protect the user's privacy.

While the influences of the information infrastructure to the electrical infrastructure are obvious, there is also a feedback of the electrical infrastructure to the information

infrastructure. Information about states and events or engineering data in the electrical infrastructure can be used to derive relevant input for security controls in the information infrastructure. One example is the utilization of field device configuration data for the compilation of rules for intrusion detection/prevention systems (IDS/IPS) or firewall systems.

4.3 Relevant regulation and standardization activities

In this subclause 4.3 an overview of important domain specific regulation and standardization activities relating to security in Smart Grid systems is provided. This list is not complete and merely states the main standards considered in this report. For a survey on proposed standardization activities related to Smart Grid in general the IEC and NIST activities defining standardization roadmaps are referred to (the respective documents are referenced in the following list).

ISO/IEC

– ISO/IEC 27001 (see [5]), *Information technology – Security techniques – Information security management systems – Requirements*, specifies a set of information security management requirements designed to be used for certification purposes.

– ISO/IEC 27002 (see [6]), *Information technology – Security techniques – Code of practice for information security management*, establishes guidelines und general principles for initiating, implementing, maintaining, and improving information security management in an organization.

– IEC 62351 (all parts, see [25]) is being standardized by the IEC TC 57 WG 15 and defines data and communications security for power systems management and associated information exchange. It comprises security definitions for communication protocols, network and system management as well as role-based access control. IEC 62351 is extensible, thus allowing further parts to be added if necessary. The newest part will target the management of security credentials.

  Table 1 provides an overview of the different parts and their standardization status regarding Edition 1. There is currently work going on to provide an Edition 2 of selected parts to address comments received from public reviews such as from the Federal Energy Regulatory Commission (FERC) or the Smart Grid Information Security Working Group (SGIS) as well as recent advances in cryptography.

Table 1 – IEC 62351 parts

IEC 62351	Definition of security services for	Standardization status
Part 1	Introduction and overview	TS
Part 2	Glossary of terms	TS
Part 3	Profiles including TCP/IP	TS, edition 2 is currently under review targeting an IS
Part 4	Profiles including MMS	TS
Part 5	Security for IEC 60870-5 and derivatives	TS, work on edition 2 is almost finished
Part 6	Security for IEC 61850 profiles	TS, will be updated in edition 2 to align with IEC TR 61850-90-5
Part 7	Network and system management (NSM) data object models	TS
Part 8	Role-based access control for power systems management	TS
Part 9	Key management	WIP
Part 10	Security architecture guidelines	TR (this document)
Part 11	Security for XML Files	NWIP

An overview of the different parts of IEC 62351 is provided either in IEC/TS 62351-1 (see [40]) or in a TC 57 WG 15 White Paper (see [37]). These documents also provide an overview of security services necessary to protect against certain threats from a more

general point of view and their mapping to the power domain by using IEC 62351 defined security technology.

– IEC 62443 (see [26]) is being standardized by IEC TC 65 and will reflect the publications of ISA 99, i.e. ISA 99 documents will be submitted to the IEC voting process. Hence, parts of IEC 62443 are likely to be similar, if not identical, to ISA 99. The IEC version is currently likely to contain one more standard (IEC 62443-2-4) which is not developed by ISA.

– The IEC Smart Grid strategic group (SG3) has issued the *Smart Grid standardization roadmap report* (SMB/4175/R see [22]) which encompasses requirements, status and recommendations of standards relevant for the Smart Grid. Security is covered in detail in a separate section of [22]. An overall security architecture capturing the complexity of the Smart Grid is requested. Besides this, the following recommendations pertaining to open items and necessary enhancements are listed:

  - a specification of a dedicated set of security controls (e.g. perimeter security and access control);
  - a defined compartmentalization of Smart Grid applications (domains) based on clear network segmentation and functional zones;
  - a specification comprising identity establishment (based on trust levels) and identity management;
  - necessity to consider security of the legacy components within standardization;
  - the harmonization with IEC 62443 [26] to achieve common industrial security standards;
  - a recommendation to review, adapt and enhance existing standards in order to support general and ubiquitous security across wired and wireless connections.

– ISO/IEC 15408 (see [23]) describes common criteria to specify functional security requirements as well as assurance requirements for components, devices, or systems. ISO/IEC 15408 is being mentioned here, as there are currently attempts to provide protection profiles and associated technical guidelines for smart meter gateways in certain countries (Germany).

IEEE (Institute of Electrical and Electronics Engineers)

– IEEE 1686-2007 (see [30]) is the *Standard for substation intelligent electronic devices (IEDs) cyber security capabilities*. The standard defines functions and features that shall be provided in substation intelligent electronic devices to accommodate critical infrastructure protection programs. It addresses security in terms of access, operation, configuration, firmware revision, and data retrieval from IEDs. Encryption for the secure transmission of data, both within and external to the substation is not part of this standard.

– IEEE P2030 (see [31]) provides a *Guide for Smart Grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications, and loads*. The document is intended to provide guidelines for power system architectures, communication and information technology architectures related to Smart Grid targeting the interoperability of involved components.

ISA (International Society of Automation)

– ISA-99 (see [32]) defines a framework addressing *Security for industrial automation and control systems*. It covers the processes for establishing an industrial automation and control systems security program based on risk analysis, establishing awareness and counter measures, and monitoring cyber security management systems. It describes several categories of security technologies and also the types of products available in those categories along with preliminary recommendations and guidance for using those security technologies. The standard consists of several sub-parts, which are in different state of completion.

CIGRE (International Council on Large Electric Systems)

– The guideline *Security for information systems and intranets in electric power systems* presents the work of Joint Working Group D2/B3/C2-01 and focuses on the importance of

handling information security within an electric utility, dealing with various threats and vulnerabilities, the evolution of power utility information systems from isolated to fully integrated systems, the concept of using security domains for dealing with information security within an electric utility, and the use of ISO/IEC 17799 [39]).

– WG D2.22 “Treatment of information security for electric power utilities”: Three reports *Risk assessment of information and communication systems* (see [34]), *Security frameworks for electric power utilities* (see [35]), and *Security technologies guideline* (see [36]) provide practical guidelines and experiences for determining security risks in power systems and the development of frameworks including control system security domains. This is done by elaborating the specific security requirements of these types of domains, and also by giving a view of interrelated domains and high-level frameworks that are necessary to manage corporate risks. Domain-specific cyber security controls are being defined and guidance is provided on how these controls can be applied to electric utility networks.

– WG D2.31 “Security architecture principles for digital systems in electric power utilities (EPUs)”: The new working group advances the results of D2.22 by identifying and developing security architecture principles for digital systems in EPUs. Topics to be addressed are defence in depth and graded approaches (zoning principles) in EPUs, Smart Grid relevant security architecture principles, developments of security architecture for digital systems addressing newly discovered threat scenarios as well as business demands and the support of technical control structures of the IT security architecture.

– JWG B5/D2.46 “Application and management of cyber security measures for Protection and Control systems” aims at identifying threats to protection and control systems to map them with existing to evaluate their effectiveness in providing a defence against the identified threats. Also targeted are practical organizational and technical guidelines for implementing cyber security in protection and control systems that minimizes these differences.

NERC (North American Electric Reliability Corporation)

– NERC’s mission is to ensure the reliability of the bulk power system in North America. To achieve that, NERC develops and enforces reliability standards and monitors users, owners, and operators for preparedness. NERC is a self-regulatory organization, subject to oversight by the US Federal Energy Regulatory Commission and governmental authorities in Canada. NERC has established the Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002 through CIP–011 which are defined to provide a foundation of sound security practices across the bulk power system. These standards are not designed to protect the system from specific and imminent threats. They apply to operators of Bulk Electric Systems (see also [13]). The profiles originate in 2006. NERC-CIP provides a consistent framework for security control perimeters and access management with incident reporting and recovery for critical cyber assets and cover functional as well as non-functional requirements. Clause A.1 provides an overview of the different parts of NERC-CIP.

– The draft standard CIP-011 may not lead to new cyber security requirements, but it provides a new organization of the existing requirements in the current CIP standards and eliminates the non-routable protocol exception. The classification of Bulk Electric Systems (BES) into the three categories low, medium, and high impact BES cyber systems, and the mapping of these to security controls are new.

IETF (Internet Engineering Task Force)

– The IETF published RFC 6272, *Internet protocols for the Smart Grid* (see [38]), which contains an overview of security considerations and a fairly thorough list of potentially applicable security technology defined by the IETF. Several IETF standards are applicable in Smart Grid environments. These are enumerated in 5.4.4.

National activities

– The National Institute of Standards and Technology (NIST) is a US federal technology institute that develops and promotes measurement, standards, and technology. In 2009, NIST formed the Smart Grid interoperability panel (SGIP) as a public-private cooperation with over 600 members that develops frameworks and roadmaps, not standards. SGIP’s

security related work is carried out in the cyber security working group (CSWG). The following subset of NIST documents directly applies to security in Smart Grid environments:

- NIST special publication 800-39, *Managing information security risk: organization, mission, and information system view* (see [9]) provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e. mission, functions, image, and reputation), organizational assets, individuals, other organizations).
- NIST special publication 800-53, *Recommended security controls for federal information systems* (see [20]) provides guidelines for selecting and specifying technical and organizational security controls and connected processes for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200 (“Minimum Security Requirements for Federal Information and Information Systems”). It provides an extensive catalogue of security controls and maps these in a dedicated appendix to industrial control systems.
- NIST special publication 800-82, *Guide to industrial control systems (ICS) security*(see [21]) provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). It uses NIST SP 800-53 (see [20]) as a basis and provides specific guidance on the application of the security controls in NIST SP 800-53. This publication is an update to the second public draft, which was released in 2007.
- NIST special publication 1108R2, *NIST framework and roadmap for Smart Grid interoperability standards* (see [16]), describes a high-level conceptual reference model for the Smart Grid. It lists 75 existing standards that are applicable or likely to be applicable to the on-going development of the Smart Grid. The document also identifies 15 high-priority gaps and potential harmonization issues for which new or revised standards and requirements are needed.
- NIST IR 7628 (see [17], [18], and [19]) originates from the CSWG and targets the development of a comprehensive set of cyber security requirements building on NIST SP 1108 (see [16]), also stated above. The document consists of three subdocuments targeting strategy (see [17]), security architecture (see [18]), and requirements, and supportive analyses and references (see [19]).

– The US Department of Homeland Security’s (DHS) *Catalog of control systems security – recommendations for standards developers* (see [33]) presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber-attacks. The recommendations in this catalogue are grouped into 18 families, or categories, that have similar emphasis. It is a collection of recommendations to be considered when reviewing and developing cyber security standards for control systems. The recommendations in this catalogue are intended to be broad enough to provide any industry using control systems with the flexibility needed to develop sound cyber security standards specific to its individual security needs.

– The German Bundesverband für Energie- und Wasserwirtschaft (BDEW) was founded by the federation of four German energy-related associations: Bundesverband der Deutschen Gas- und Wasserwirtschaft (BGW), Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland (VRE), Verband der Netzbetreiber (VDN) and Verband der Elektrizitätswirtschaft (VDEW). The BDEW introduced a white paper (see [14]) defining basic security measures and requirements for IT-based control, automation and telecommunication systems, taking into account general technical and operational conditions. It can be seen as a further national approach targeting similar goals as NERC-CIP. The white paper addresses requirements for vendors and manufacturers of power system management systems and is used as an amendment to requests for proposals or requests for quotations.

– Within the European Union a dedicated expert group of the Smart Grid task force is currently working on *Regulatory recommendations for data safety, data handling and data protection* (see [8]). The goal of the Task Force is the identification and production of a set of regulatory recommendations to ensure EU-wide consistent and fast implementation of Smart Grids, while achieving the expected Smart Grids' services and benefits for all users

involved. The goal of the Expert Group for security is the identification of appropriate regulatory scenario and recommendations for data handling, security, and consumer protection to establish a data privacy and data security framework that both protects and enables. With the Smart Grid Coordination Group, a further European Group targets security in Smart Grids. The focus of this group follows the European Mandate M/490 requesting the definition of a reference architecture based on qualified use cases as well as the investigation into the Smart Grid coverage with available standards. Security is an integral part of this investigation and handled in an own sub group.

The maturity of selected standards and their applicability is presented in Figure 3 as proposed in the European funded project "European network for the security of control and real time systems" ESCoRTS (see [4]). Figure 3 is intended to provide a better overview for operators and manufacturers of which standards influence their business most. The different colours in the figure indicate the targeted audience.

While IEC 62351 addresses the energy sector, more specifically substation automation systems, NERC-CIP is generally targeting energy operators. While ISO 27000 and NIST 800-53 are mainly targeted to IT environments (thus targeted at protecting information), other standards such as ISA 99 or IEEE P1686 directly address (industrial) automation systems. NIST SP800-53, Appendix I, is explicitly for industrial control systems, as is NIST SP800-82.

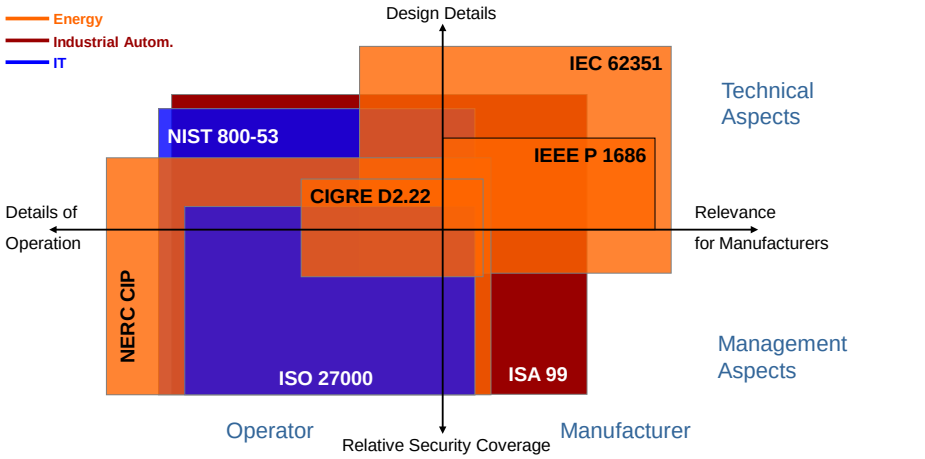


Figure 3 – Graphical representation of scope and completeness of selected standards (enhanced version of Figure 1 in 4.1 of [4])

Figure 3 provides a qualitative view on the scope and coverage of selected standards. Standards extending to the right in x-axis direction have relevance for manufacturers. Typically, such standards have detailed technical requirements up to the definition of dedicated security protocols, which must be implemented by the manufacturers. In contrast, the more a standard extends to the left of the x-axis, the more it is focused on secure operation. NERC-CIP, for example, prescribes specific actions for operators to comply with, thus providing implicit requirements to the manufacturers to support the operators.

Standards extending to the top of the y-axis list precise design details and leave little room for interpretation. IEC 62351, for instance, provides design details in such extend that device interoperability between various manufacturers can be guaranteed.

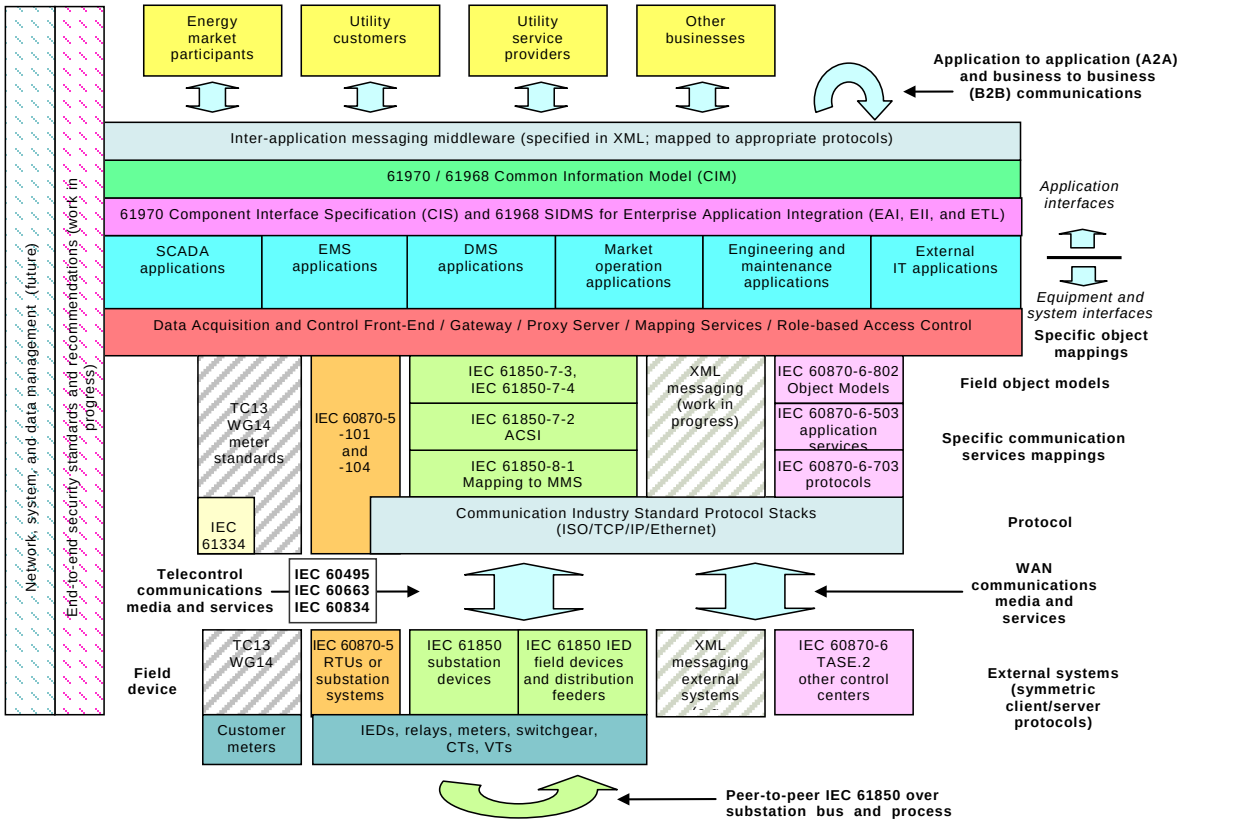
Standards extending to the bottom of the y-axis are covering a broad range of various security areas and can thus be consulted in order to get estimation on the overall security level.

4.4 Reference architecture for TC 57

IEC TC 57 is chartered with developing standards for EPS management and associated information exchange in the areas of generation, transmission and distribution real-time

operations and planning. The scope also includes information exchange to support wholesale energy market operations.

IEC 62357 (see [29]) provides a reference architecture explaining the interworking of various existing standards activities within IEC TC 57 and how they contribute to meet the objectives of TC 57. It also identifies areas where harmonization between TC 57 standards is needed and suggests possible approaches to achieve it in order to facilitate a single, comprehensive, optimal plan for deployment of these standards in product development and system implementations



IEC 1949/12

NOTE 1 Solid colours correlate different parts of protocols within the architecture.

NOTE 2 Non-solid patterns represent areas that are future work, or work in progress, or related work provided by another IEC TC.

Figure 4 – TC 57 reference architecture (see [29])

The TC 57 reference architecture shown in Figure 4 includes the following IEC TC 57 standards (responsible working groups are shown in parentheses):

- **IEC 60870-5:** standards for reliable data acquisition and control on narrow-band serial data links or over TCP/IP networks between SCADA masters and substations (WG 3).
- **IEC 60870-6:** standards for the exchange of real-time operational data between control centers over wide area networks (WANs). This standard is known officially as TASE-2 and unofficially as ICCP (WG 7).
- **IEC 61334:** standards for data communications over distribution line carrier systems (WG 9).
- **IEC 61850:** standards for communications and data acquisition in substations. They also include standards for hydroelectric power plant communication, monitoring, and control of distributed energy resources and hydroelectric power plants (WGs 10, 17, 18).

- **IEC 61970:** Standards to facilitate integration of applications within a control center, including the interactions with external operations in distribution as well as other external sources/sinks of information needed for real-time operations. These include the generation and transmission parts of the Common Information Model (CIM), the Generic Interface Definition (GID) interface standards, and eXtensible Markup Language (XML) standards for power system model exchange (WG 13).
- **IEC 61968:** Standards for Distribution Management System (DMS) interfaces for information exchange with other IT systems. These include the distribution management parts of the CIM and XML message standards for information exchange between a variety of business systems, such as asset management, work order management, Geographical Information Systems (GIS), etc. (WG 14).
- **IEC 62325:** Standards for deregulated energy market communications (WG 16).
- **IEC 62351:** Standards for data and communication security (WG 15).

Figure 5 shows where these standards can be applied in the utility operations environment.

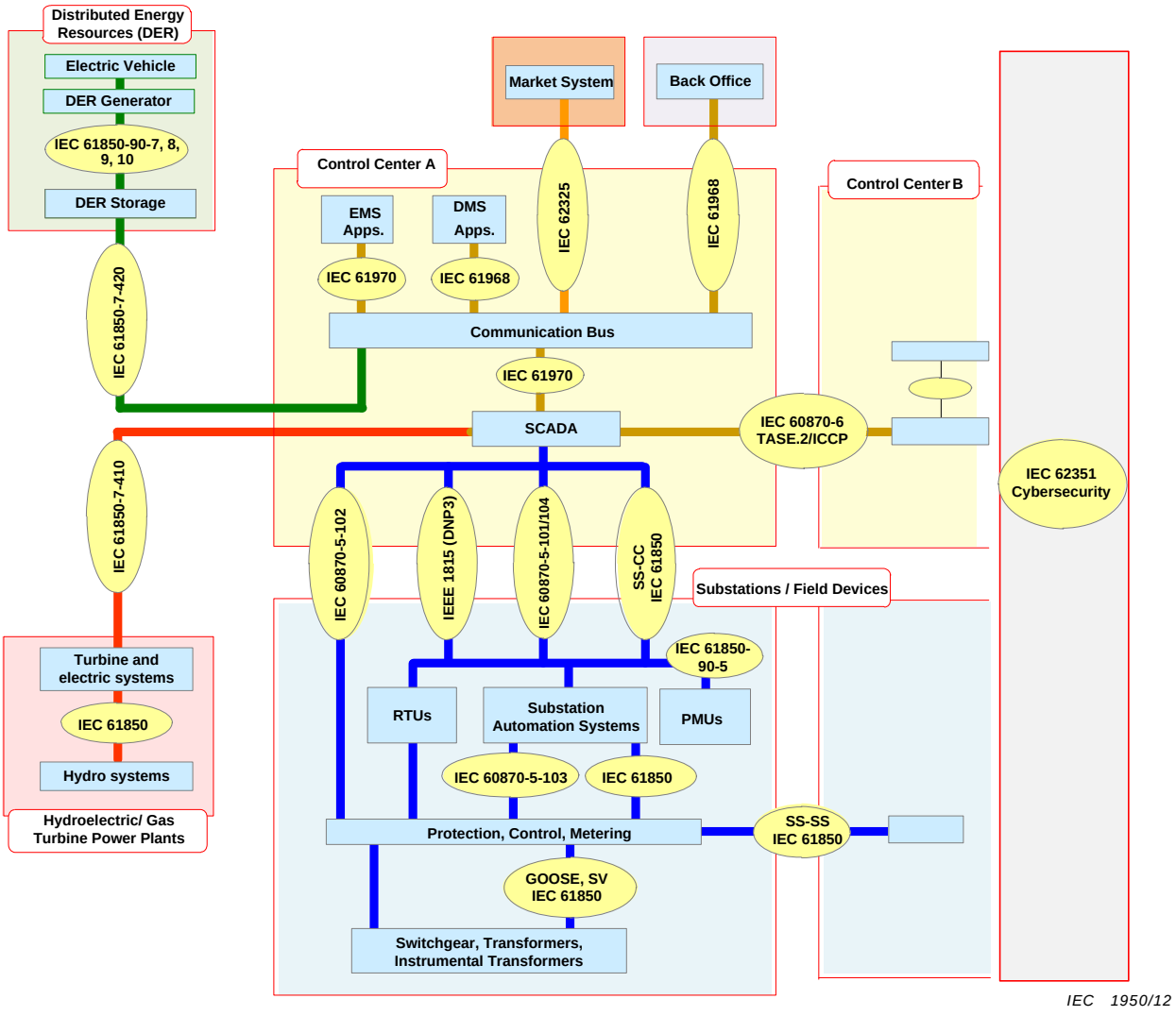


Figure 5 – Application of TC 57 standards to a power system (see [29], enhanced according to IEC/TR 61850-1)

The implementation and operation of this architecture in a secure manner requires an overall security architecture covering technical and operational means and showing especially how to apply TC 57 specific security measures. This will be the core of Clause 5.

5 Security architecture in power systems

5.1 General

ISO/IEC 42010:2007, 3.5 describes the architecture of a system as: “The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution” (see [7]).

A security architecture provides a framework and guidance to implement and operate a system using the appropriate security controls with the goal to maintain the system's quality attributes like confidentiality, integrity, availability, accountability and assurance. Appropriate security controls are typically determined by a risk and threat analysis of the target system based on technical and business related assets. Such a threat and risk analysis specifically targets the communication between different network elements with respect to their security requirements for confidentiality, integrity, and authentication. The target system itself may therefore be divided into different security domains, reflecting the different security needs of the single application domains. To provide a profiling of the security controls to the different domains, security policies define the mandatory and optional controls to be supported, while the enforcement of these security policies is part of the overall security process. The general process of defining a security architecture based on a threat and risk analysis is also outlined in IEC/TS 62351-1 (see [40]).

Generic security architectures have been discussed by several organizations and are provided for instance through Sherwood Applied Business Security Architecture (SABSA, see [2]) and The Open Group Architecture Framework (TOGAF, see [1]), which are shortly outlined in the following.

SABSA is a six-layer model covering all four parts of the IT lifecycle: strategy, design, implementation and management and operations. The SABSA matrix for security architecture development is intended to provide coverage for addressing the security questions and concerns within each domain. The intent is to also provide traceability and justification between the six layers (also known as views). For instance, from the logical layer (designer’s view) the creation of security policies should be based on the control objective’s defined in the conceptual layer (architect’s view); and likewise, the control objectives should be defined based on the business risk model defined in the contextual layer (business view). so if questioned why a particular policy exists in the organization, the decision should easily be traced back to the business layer. Likewise, if a control objective existed that did not have one or more security policies associated with it, a gap would easily be identified.

TOGAF is an exhaustive framework that describes itself as “providing methods and tools for assisting in the acceptance, production, use, and maintenance of enterprise architecture. It is based on an iterative process model supported by best practices and a re-usable set of existing architecture assets.” [1]. The enterprise framework is developed through several phases explained in its architecture development methodology (ADM). Security is addressed in the “ADM guidelines and techniques” section of TOGAF and is not intended to be a security architecture development method. The purpose of the security guidance in TOGAF is to inform the enterprise architect of security concerns within each phase of the ADM. Security is treated as a cross-cutting concern and leverages other security standards within ISO/IEC and NIST discussed in this document.

5.2 follows this approach by defining security domains and their mapping to power system domains. In a next step the interfaces of the power system domains are mapped against the interface categories provided by NIST IR 7628 to determine the communication interfaces to be secured. In a further step the security domains are then mapped to security controls to achieve the necessary security level. The results are used in Clause 6 to perform the mapping on a more detailed level, based on distinct scenarios.

5.2 Security domains and their mapping to power system domains

One method for managing the complexity of security is to define physical and/or virtual security domains. The perimeter of each security domain is maintained at the desired level of security, while within each domain the same level of security is assumed. Any information exchanges (including human users) crossing the perimeter are validated with the security level requirements within the security domain before they are allowed to enter.

As stated in 4.3, CIGRE WG D2.22 has already published an approach to describe security domains for electrical power utilities (see [35]) as well as potential security controls to be applicable in the different domains (see [36]). This approach will be used and evolved further on. Moreover, the approach is used in Clause 6 to provide a mapping to example deployment use cases of the TC 57 architecture.

The security model applied here defines four (logical) security domains, which relate to a dedicated protection level. These four domains are listed in Table 2. They are generally applicable to operational networks and can be mapped to power systems networks as well as office environments. The security domains comprise logical and physical characteristics. Thus, there are logical as well as physical security controls applied to achieve the required protection level.

Table 2 – Security domains (see also [35])

Security domain	Required protection level	Applies to	Example systems
Public	Low	Assets, supporting the communication over public networks.	Third party networks, Internet.
Corporate	Medium	Assets, supporting the business operation with baseline security not essential to the power system reliability and availability.	Office level business network.
Business Critical	High	Assets, supporting the critical operation, which are not critical to power system reliability and availability.	Finance network, human resource systems, ERP systems.
System operation critical	Very high	Assets directly related to the availability and reliability of power generation and distribution infrastructure.	Control systems, SCADA networks.

The different domains may be geographically distributed. This may have influence on the selection of security controls and needs to be considered appropriately.

From an abstract point of view, the power industry has been divided into seven different application domains in the NIST IR 7628 volume 1 document, as there are:

– **(Bulk) generation**

  Bulk power generation is the process of converting non-electrical energy into electricity, and is the first step in the process of delivering power to consumers. Besides classical energy generation like coal-fired power plants or nuclear power plants, decentralized energy generation using photovoltaic or windmills are getting more and more integrated into the power grid for bulk energy generation.

– **Transmission**

  Power transmission is the bulk transfer of electric power to substations. A power transmission network connects power plants generating electrical energy with substations and typically transports high voltage energy.

– **Distribution**

  Substations distribute the electrical energy further down to industrial, commercial, or residential consumers in the range of medium to low voltage energy.

– **Markets**

The market provides the facilities to exchange energy between different energy providers and network operators. As decentralized energy is more and more generated also within residential areas, the market functionality will be enhanced to also consider prosumers.

– **Operations**

Operations comprise the processes, infrastructure, and technology for the management of the bulk energy generation, storage, transport and distribution up to customer interactions. This also involves the handling of metering devices and connected services.

– **Service provider**

The service provider can act in different roles such as energy retailer or aggregator or as clearing house for billing and energy exchange purposes.

– **Customer**

The customer role was typically the endpoint for the energy transfer. Within the Smart Grid, this is changing from the pure consumer of energy to a producer of energy in residential areas. Hence the customer is becoming a prosumer.

Mapping the security domains stated in Table 2 to the seven application domains of the power industry listed above leads to Figure 6, combining approaches from CIGRE (see [35]) and NIST IR 7628.

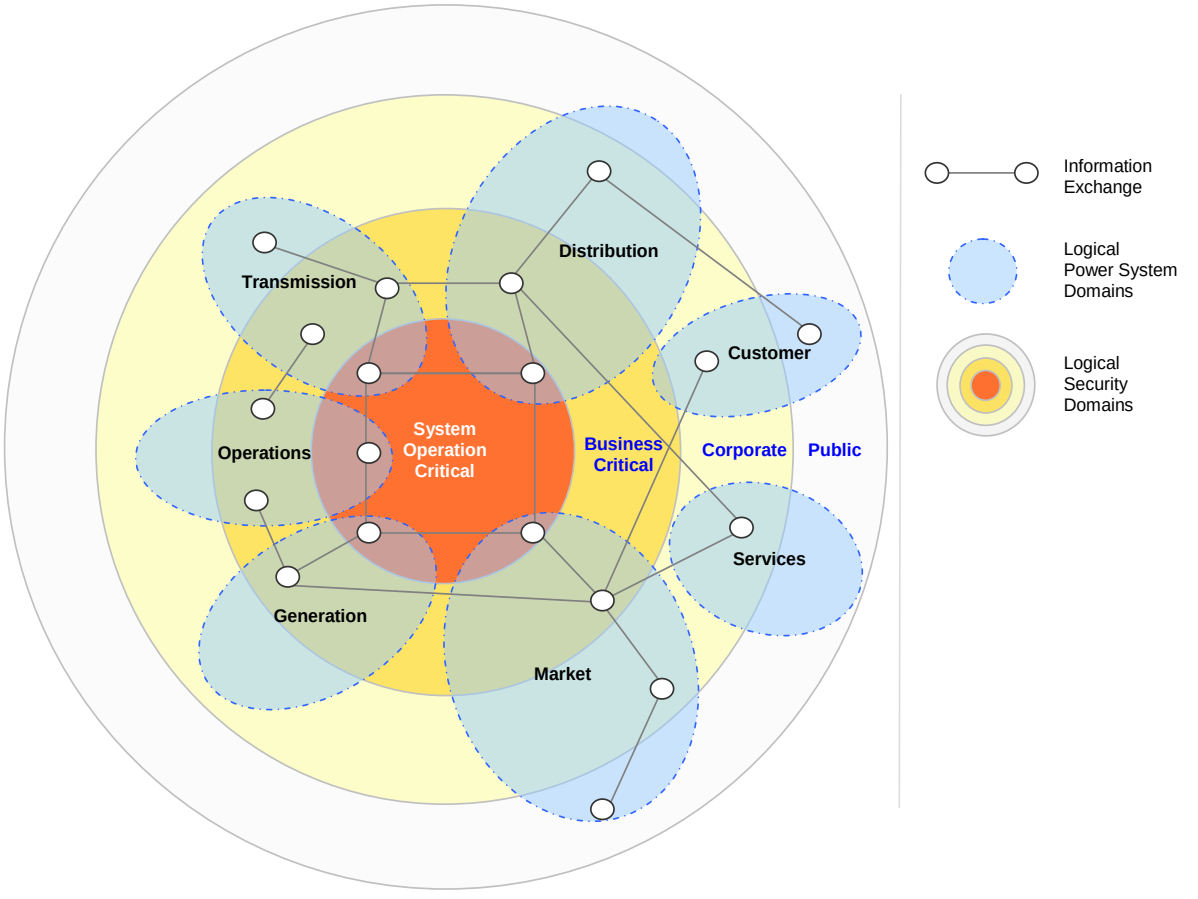


Figure 6 – Mapping of information security domains to power system domains

As shown in Figure 6, the power system domains span all of the security domains to a certain extent. Customer, distribution, services, and market do also connect to the public domain to take prosumers generating, consuming, and trading energy in residential areas into account targeting a Smart Grid. IEC protocols are used throughout the domains to facilitate Smart Grid control.

For each security domain dedicated security controls can be derived, which in turn can be mapped to the power system application domains. Ideally, this derivation is being done based on a security threat and risk assessment of a real target scenario, which addresses detected vulnerabilities and also takes the existing security measures into account.

As shown in 4.3, there are several guidelines and regulations already explaining security controls for power systems, but do not directly address the mapping to technical implementation details. This is the focus of 5.4 and Clause 6 discussing concrete realization examples of security controls in different power system domains.

5.3 System interface categories and their mapping to power systems

NIST IR 7628 vol. 1 (see [17]) defines logical interfaces categories, which are used to model the system interaction and thus build one base for the overall security architecture. These system interfaces are to be secured using the security controls.

The NIST IR 7628 interface categories are listed in the following table and mapped to power system interfaces based on the reference architecture description in 4.4.

Table 3 – Mapping of logical interface categories to TC 57 reference architecture

No.	Logical interface category	Mapping to TC 57 reference architecture (communication protocols, frameworks)
Control system related interfaces		
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints	Typically between substations or control center and substations – IEC 61850 – IEC 60870-5-101 and -104
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints	Typically between substations or control center and substations – IEC 61850 – IEC 60870-5-101 and -104
3	Interface between control systems and equipment with high availability, without compute or bandwidth constraints	Typically between substations or control center and substations – IEC 61850 – IEC 60870-5-104 – IEC 60870-6 (TASE.2)
4	Interface between control systems and equipment without high availability, without compute nor bandwidth constraints	Typically between substations or control center and substations – IEC 61850 – IEC 60870-5-104 – IEC 60870-6 (TASE.2)
5	Interface between control systems within the same organization	– IEC 60870-6 (TASE.2) – IEC 61850 – IEC 61968, IEC 61970
6	Interface between control systems in different organizations	– IEC 60870-6 (TASE.2) – IEC 61850 – IEC 61968, IEC 61970
Back office related interfaces		
7	Interface between back office systems under common management authority	– IEC 61968, IEC 61970
8	Interface between back office systems not under common management authority	– IEC 61968, IEC 61970
9	Interface with B2B connections between systems usually involving financial or market transactions	– IEC 61968, IEC 61970 – IEC 62325
10	Interface between control systems and non-control/corporate systems	– IEC 61968, IEC 61970
Sensor related interfaces		
11	Interface between sensors and sensor networks for measuring environmental parameters	– IEC 60870-5-101 – IEC 61850
12	Interface between sensor networks and control systems	Typically within a substation – IEC 61850
13	Interface between systems that use the AMI network	Involves metering devices, data concentrator and transaction handling – IEC 61968, IEC 61970
14	Interface between systems that use the AMI network with high availability	– IEC 61968, IEC 61970
Other interfaces		
15	Interface between systems that use customer (residential, commercial, and industrial) site networks	– IEC 61850 for load balancing – Web-based services (like IEC 61400-25) – IEC 61968, IEC 61970

No.	Logical interface category	Mapping to TC 57 reference architecture (communication protocols, frameworks)
16	Interface between external systems and the customer site	Involves metering devices, data concentrator and transaction handling – Possibly IEC 61850 – IEC 61968, IEC 61970
17	Interface between systems and mobile field crew laptops/equipment	Involves engineering connection via remote access using – Possibly IEC 61850
18	Interface between metering equipment	– IEC 61850 – IEC 61334 (PLC for metering) – IEC 62056 (DLMS/COSEM, IEC TC 13 WG 14)
19	Interface between operations decision support systems	– IEC 60870-6 (TASE.2) – IEC 61968, IEC 61970
20	Interface between engineering/maintenance systems and control equipment	Typically proprietary – IEC 60870-5-101 and -104 – IEC 61850
21	Interface between control systems and their vendors for standard maintenance and service	Typically proprietary – IEC 60870-5-104, – IEC 61850
22	Interface between security/network/system management consoles and all networks and systems	– IEC/TS 62351-7
NOTE Not all of TC 57's standards mentioned here are currently covered by IEC 62351. This shows the necessity to further evolve IEC 62351. 6.5 lists these standards as potential gaps in terms of coverage.		

IEC 62351 with its different parts has been developed to provide security controls to protect the communication protocols defined in TC 57. The scope and the functionality of these protocols is reviewed and enhanced as new use cases in the Smart Grid appear. Consequently IEC 62351 is constantly improved and enhanced to cope with new upcoming requirements. The current coverage of protocols and information modelling is shown in Figure 7.

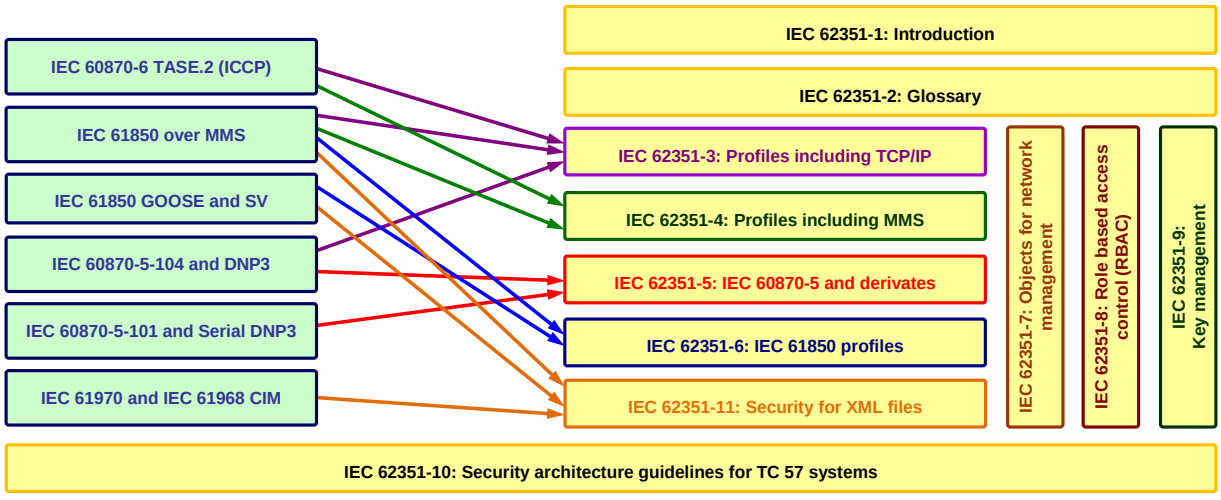
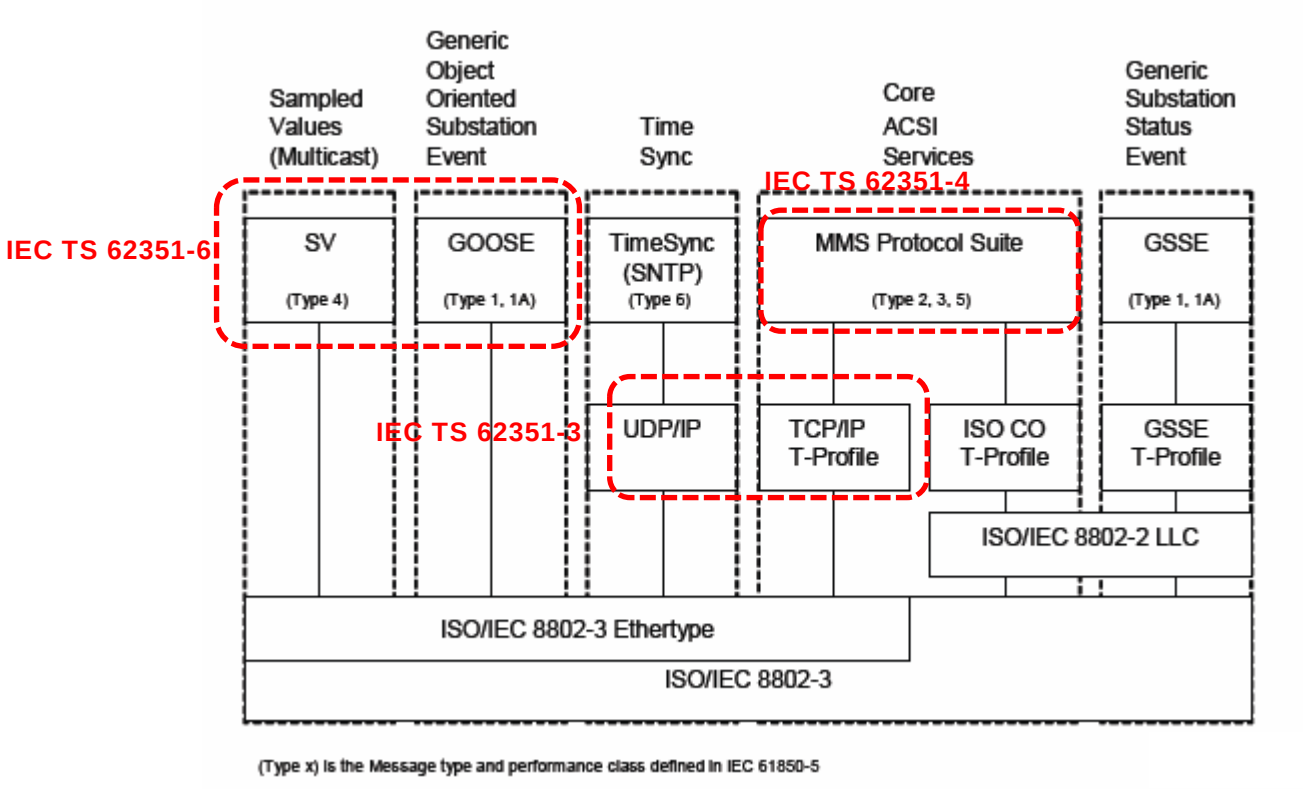


Figure 7 – Mapping of IEC TC 57 communication standards to IEC 62351 parts

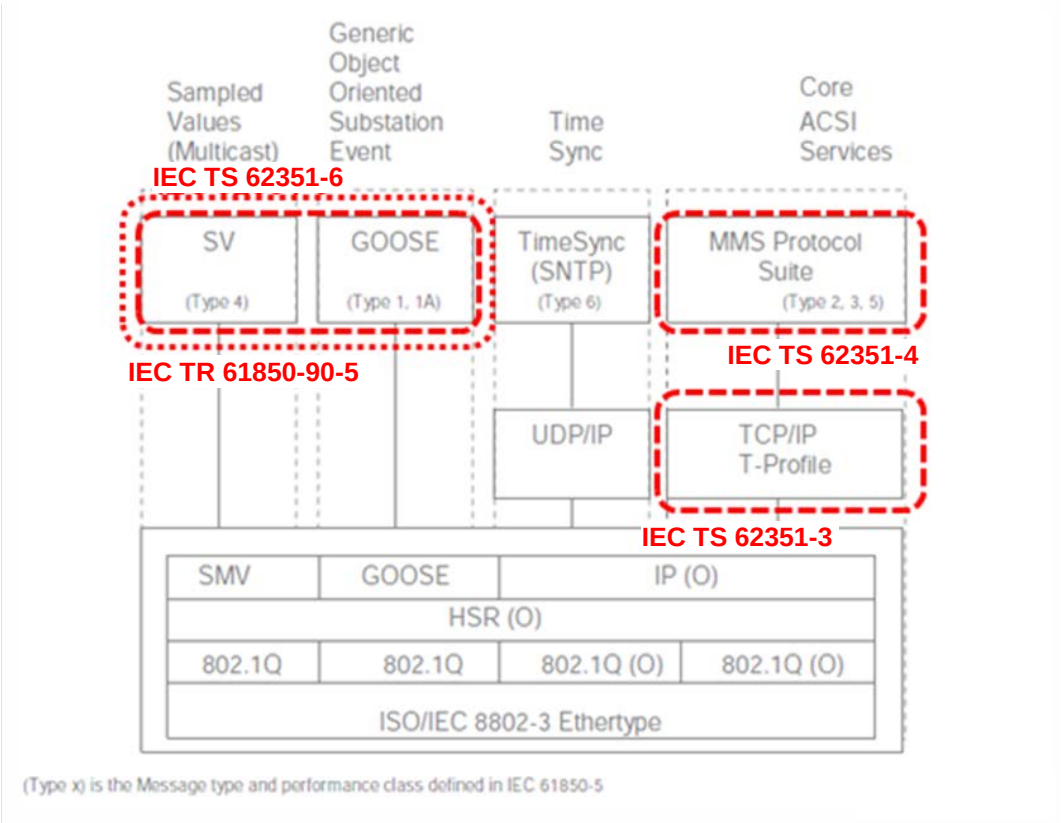
An overview of the different parts of IEC 62351 is provided as an overview in 4.3 and further elaborated in IEC/TS 62351-1 (see [40]). This part also covers the discussion of potential

security controls and their application and therefore builds a base for 3.3. Another base is provided by IEC/TS 62351-9 [47] giving the key management, which is essential for all other cryptography based security from the other IEC 62351 parts.

The mapping of the IEC 62351 parts relating to the layers they address can also be depicted as in Figure 8 showing them in relation to the IEC 61850 protocol stack. The security functionality provided in IEC TR 61850-90-5 has been added to the picture.



IEC 1953/12



IEC 1954/12

Figure 8 – Mapping of IEC 62351 protocol related parts to the IEC 61850 stack

5.4 Security controls

5.4.1 General

Security controls describe security counter measures to avoid, counteract or minimize security risks. Within the context of this document security controls are categorized into:

– physical controls e.g. fences, doors, locks targeting the definition of a physical security perimeter;

– procedural controls e.g. incident response processes, management oversight, security awareness and training;

– technological security controls necessary for operation e.g. user authentication (login) and logical access controls, malware software, security protocols, firewalls. They apply for instance to the interface categories stated in Table 3;

– operational security controls like state analysis or contingency analysis;

– legal and regulatory or compliance controls e.g. privacy laws, policies and clauses.

Orthogonal to all security controls is the security management, which has interfaces to and interactions with all security controls. As stated earlier, the choice of security controls should be dependent on a threat and risk assessment to address explicit target security requirements and also be aligned with the targets reliability and latency requirements.

As already stated in 4.3 there are several documents providing catalogues for security controls, which can be taken as reference here, such as:

– NIST special publication SP800-53 (see [20]) specifies a security control catalogue for federal information systems and organizations;

– Department of Homeland Security Catalog of Control Systems Security gives *Recommendations for standards developers* of the US (see [33]);

– NIST IR 7628 (see [17], [18], and [19]) originates from the Smart Grid interoperability panel (cyber security WG);

– IEC 62443 (see [26]) addresses “security for industrial automation and control systems” describing several categories of security technologies and also the types of products available in those categories along with preliminary recommendations and guidance for using those security technologies. This work is being done in cooperation with ISA-99 (see [32]);

– ISO/IEC 27002 (see [6]) provides general guidance on commonly accepted goals of information security management. Taking the specifics of process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the connected processes into account, argues for a domain specific mapping of these guidelines. This would support the implementation of an information security management system explicitly. The German DIN just provided a domain specific version as technical report with DIN SPEC 27009 (see [58]).

In power systems, there are already a number of existing utility processes to protect the system’s reliability that can be leveraged for security purposes. Examples of reliability ensuring controls are fault location, isolation, sectionalization and recovery (FLISR), redundant control centres, periodic polling, alarm reporting, contingency analysis, state analysis, and revenue protection schemes.

The focus of this document is placed on cyber security and procedural controls which are applicable to TC 57 related technology. Legal and regulatory security controls are referenced by the documents stated in 4.3.

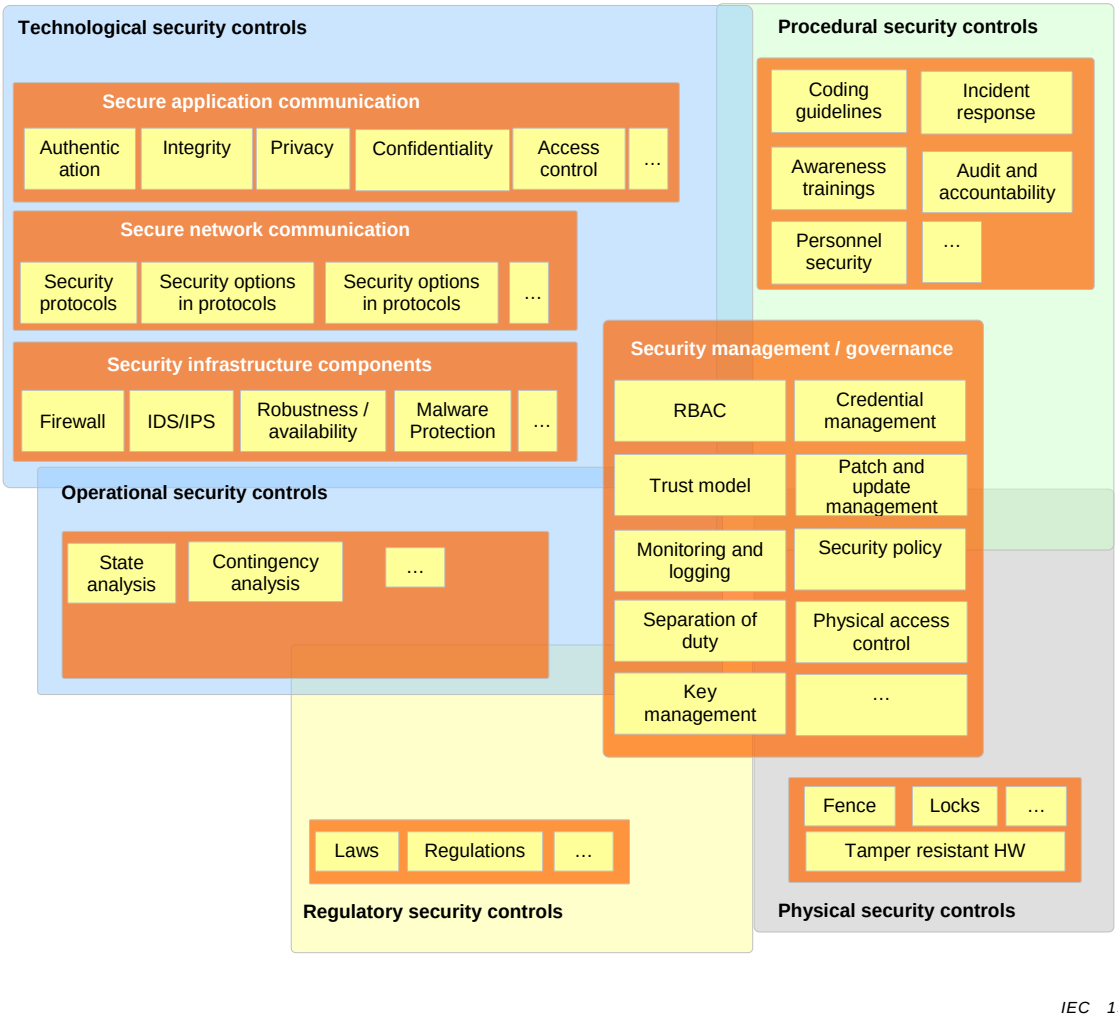


Figure 9 – Security controls overview

Figure 9 provides an overview of the interrelationship of security controls emphasizing security management as a common part. The controls shown in Figure 9 only provide examples and the list does not claim to be complete. As shown in Figure 6, the power system application domains span multiple security domains, which are interconnected up to the public security domain. This requires the support of basic security paradigms like layered defence or defence in depth for the design of a security architecture.

Defence in depth can be described as the application of security controls in layers and at different levels. “Layers” imply multiple security barriers between the attacker and the target, while “levels” relate to the different levels in the communications infrastructure underlying any cyber system (transport, application, etc.). This concept ensures that if one security barrier is broken (for instance the lock on a door), the next layer may prevent the attack (the attacker does not have the correct password) or it may just deter the attack until it is detected (such as video surveillance or an alarm notifies personnel that an excess of passwords have been attempted).

Technological security controls are typically a combination of different security mechanisms. An example may be a secured transport channel (as provided, e.g. by IEC/TS 62351-3 (see [41])), which authenticates the communicating peers and uses integrity mechanisms and encryption to protect the contents of a message on transport level. This may be sufficient for several use cases, but application level security may be required by others. One example is role-based access control on application level, e.g. to ensure that certain actions can only be executed by authorized personnel (IEC/TS 62351-8 provides a solution for this).

5.4.2 Domain mapping of security controls

Using the concept of layered defence, necessary security controls for each security domain can be defined. As mentioned, security controls represent counter measures supporting dedicated security requirements resulting in the application of distinct security services. Since the security requirements differ between the four security domains, Table 4 provides a list of examples for typical security controls and realization examples mapped to the three security domains (Corporate – C, Business Critical – B, and System Operation Critical – O) as introduced in 5.2. This list is not complete but shows potential minimum realization variants per domain.

Table 4 – Security controls applicable to the different security domains

Security control	Realization example, notes	Security domain		
		C	B	O
Authentication	Strong user-to-device and user-to-application authentication (local and remote)	X	X	X
	User authentication and single sign-on (SSO) either using user-id and password, e.g. by accessing a directory (ISO/IEC 9594 or LDAP plus SSO addition) or using Kerberos	X	X	
	Support of two-factor user authentication technologies (e.g. smart token, OTP)		X	X
	Device-to-device authentication, e.g. Client-Server-Authentication via X.509 based certificates		X	X
	Enforcement of mutual authentication according to IEC/TS 62351-3, -4, -5 and -6 in IEC based communication protocols			X
	(Physical) ID check through plant security	X	X	X
Access control	Definition and enforcement of a physical security perimeter supported through security personnel, locks, fences, video surveillance, etc.		X	X
	Definition of a logical security perimeter supported through application of firewalls, remote access gateways, etc. (for local and remote access)	X	X	X
	Enforcement of least privilege escalation	X	X	X
	Definition and enforcement of role-based access control (RBAC)		X	X
	Application of IEC/TS 62351-8 RBAC for access controlled engineering and operation			X
	Application of secure authentication options in DNP3 communications			X
	Password policy, e.g., complexity criteria, aging, etc., e.g. as provided by ISO/IEC 9594	X	X	X
	Network Segmentation (applying Firewalls and DMZ)	X	X	X
Integrity protection	Integrity protection of communicated data between different data network components (e.g., geographically dispersed data networks) using security appliances or security functionality in routers to protect communicated traffic		X	X
	Application of integrity protection options in SCADA and ICS protocols		X	X
	Application of IEC/TS 62351-3, -4, -5 and -6 integrity protection features in IEC based communication protocols		X	X
	Application of secure authentication options in DNP3 communications			X
	Integrity protection of stored data (e.g. disk, tape)		X	X
Confidentiality	Confidentiality protection of sensitive data during communications between different data network components using security appliances or security functionality in routers to protect communicated traffic		X	X
	Application of confidentiality protection options in SCADA and ICS protocols		X	X
	Confidentiality protection of stored live data; disk encryption for engineering and control systems		X	X

Security control	Realization example, notes	Security domain		
		C	B	O
	Confidentiality protection of stored backup data (e.g. disk, tape)		X	X
	Application of IEC/TS 62351-3, -4, and -5 confidentiality protection using TLS in IEC based communication protocols		X	X
	Access to confidential data following the need to know principle	X	X	X
Monitoring and logging	Maintenance and monitoring of computer and network security components, e.g. system event log auditing or SNMP v3 application to monitor system events		X	X
	Anomaly/intrusion prevention/detection (IDS/IPS deployment)		X	X
	Login/account management on control and engineering systems		X	X
	Auditing / logging of all automated / scripted login sessions		X	X
	Logging of control application access, including user ID, event time		X	X
	User activity on control systems while logged in			X
Security management	Personnel risk assessment, e.g. security clearance of technical personnel		X	X
	Separation of duty for control, operation, safety, and security	X	X	X
	Security training of personnel (incident handling, security process handling, etc.)		X	X
	System hardening according to security measurement plans	X	X	X
	Security documentation (for processes and systems)	X	X	X
	Regular security assessments of components (e.g., vulnerability scans)	X	X	X
	Key- and credential management (addressed in new work item IEC/TS 62351-9)			X
	IEC/TS 62351-7 application to describe power system objects to be managed			X
	Definition and maintenance of roles to support IEC/TS 62351-8		X	X
	Incident response (events and alarming)	X	X	X
	Backup and recovery of business and operation relevant information	X	X	X
	Patch management (organizational part)	X	X	X
	Establishment of a security organization with defined responsibilities and responsible persons (e.g. for incident handling)	X	X	X
	Definition of identification and authentication procedures	X	X	X
Availability and robustness	Redundancy concepts for IT infrastructure		X	X
	Firewall concepts (DoS protection)	X	X	X
	IDS/IPS systems (DoS protection)	X	X	
	Connection limitations (Bandwidth, number of connections, etc.)			X
	Malware protection software/appliances, white listing	X	X	X
	Backup and restore concepts and procedures		X	X
	Emergency concept		X	X
	Quality Control (e.g. NERC Compliance of used products, etc.)		X	X
	Application of products supporting a secure lifecycle (product selection should obey security requirements covering the complete product lifecycle)	X	X	X
Privacy protection	Protection of person (user, customer, etc.) related information in AMI	X	X	X
	Protection of business relevant data (e.g. generation data, system status)	X	X	

Not all controls may be applicable to components in a Smart Grid infrastructure. An example is given through malware protection on field devices. While these devices have limited

capabilities they also often use proprietary operating system for which malware protection software does not (yet) exist.

Security of information exchanges implies end-to-end security from the sender of the information all the way across through all intermediate communication paths, computer systems, software applications, and databases, to the final receiver of the information. Thus information security shall not only address physical components but also the virtual paths from end to end.

End-to-end also covers cascading or chains of security, where the compromise of one type of information has cascading effects. For instance, if substation data incorrectly indicates that a breaker has tripped when actually it is still closed, inappropriate operator and power system reactions can cause more impacts than the original false signal might itself warrant.

5.4.3 Determination of necessary security controls

To determine the actual need for certain security controls and their placement within the architecture, a security assessment is the typical starting point. This assessment may target both the system's general design based on a conceptual assessment of the use case-specific data model, the data exchange and its derived security requirements as well as practical tests on dedicated components. This analysis should be performed on a regular base; at least whenever the general functionality of the target system is enhanced or new components are added. The general approach is depicted in Figure 10.

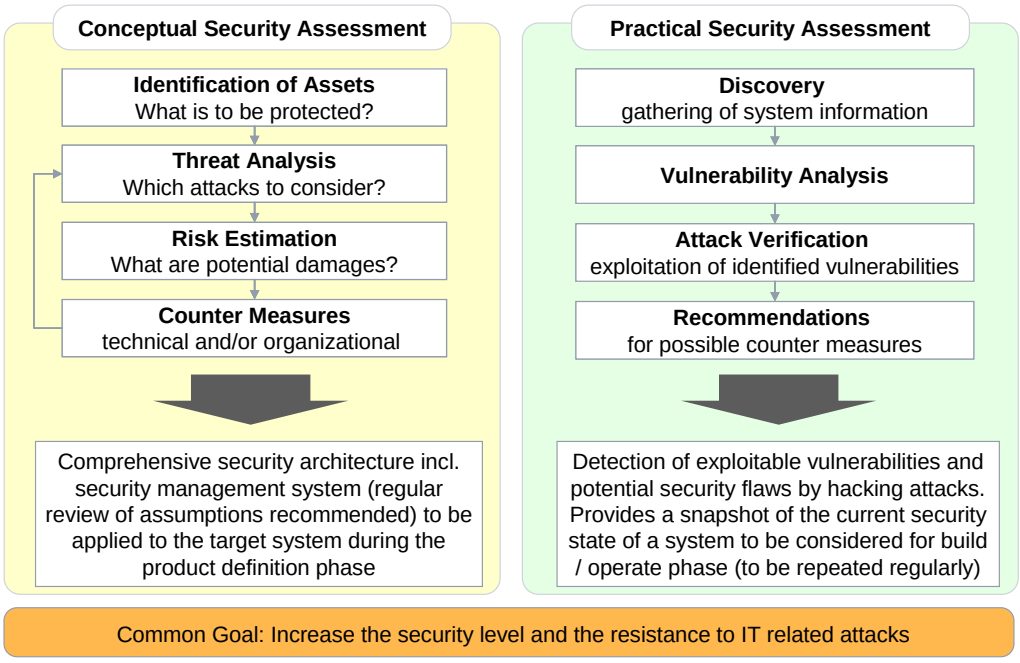


Figure 10 – Generic system security assessment approach covering design and implementation

This security assessment itself is only one part of a security oriented design, development, and operation process as shown in Figure 11. The process of determining the actual security needs based on a specific system architecture including the determination of assets and connected risks to the assets are further explained in the NIST SP 800-30 (see [10]).

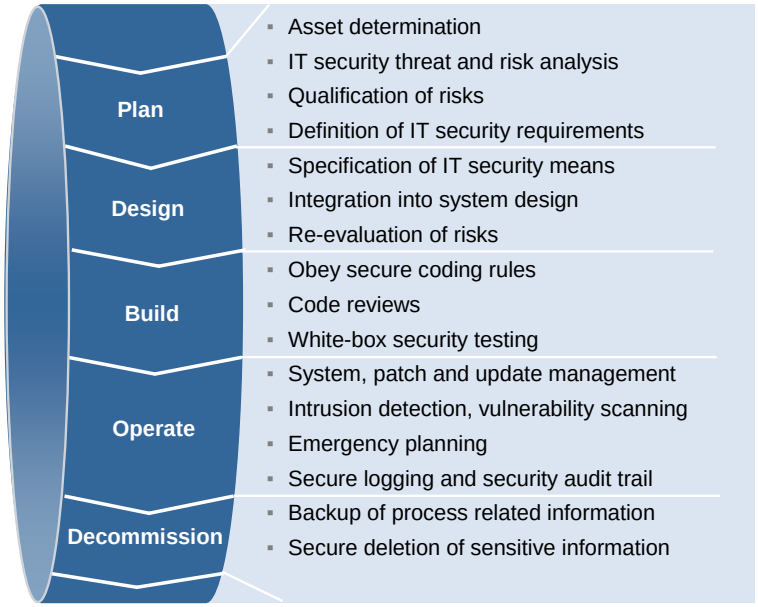


Figure 11 – Secure design, development, and operation process

5.4.4 Network-based security controls

An increasing number of endpoints as well as interconnected systems within typical power system installations on one hand and the underlying network topologies on the other raise the bar for network security in general. Based on the Internet Protocol (IP) suite as the foundation to meet these requirements, the following key objectives need to be addressed in the scope of a network and security architecture:

– **Strong network segmentation and Quality of Service (QoS)** – An appropriate network architecture should be applied in order to segregate traffic based on functionality. As an example, control traffic for automation and monitoring purposes shall be prioritized over other, less important traffic. This approach ensures reliability and helps to isolate traffic based on a multi-service communication architecture. It is much easier to monitor and restrict isolated traffic at the endpoints. Network router for instance can be logically divided into three functional planes: data plane (control, monitoring, measurements), management plane (management protocols and other interactive access protocols like secure shell protocol, LDAP and SNMP) and control plane (routing control protocols, keep-alive, ICMP, etc.). Based on this, a methodical approach for network security following the defence in depth approach described in the beginning of 5.4 is much easier to implement and to perform. To respect cyber security, network isolation is an appropriate means of separating security relevant functionalities like authentication server or remote access devices. QoS policies can help to detect traffic abnormalities and offer additional Denial-of-Services (DOS) prevention.

– **Availability and survivability** – The network architecture should be able to defend or gracefully handle DoS and/or DDoS attacks in general and especially on single points of failure like authentication servers, etc. QoS policies can help to detect traffic abnormalities and offer DOS prevention. Techniques to achieve network device resiliency are based on hardening (disabling unnecessary services), strict access control lists (ACL), port security, control plane protection and redundancy, to name but a few.

– **Pervasive network awareness and proactive network health monitoring** are important to detect an attack as early as possible in order to initiate incident response and network forensics. An immediate response in the event of a cyber-attack is essential and can trigger counter measures like isolation of network segments and rerouting.

– An IP-based network architecture fosters a **seamless integration of physical security with cyber security controls** in order to protect typical remote deployment scenarios. These capabilities should be used to connect physical access control, video surveillance as well as other physical security controls with an overall security management to respond

to security breaches quickly and efficiently. In addition, logs should be collected across devices, systems, and applications and correlated with Intrusion Prevention System (IPS) events to identify security incidents, followed by mitigation steps.

– Strong perimeter security is the basis for any zone-based concept and shall be enforced by strict rule definitions in the firewalls used to protect the segments. Invalid access alarm based on integrated firewall capabilities should be correlated with event management.

– In the domains of advanced metering infrastructure (AMI), distribution automation and distributed energy resources, device and platform integrity are important requirements. It shall be ensured that devices, especially meters, are protected in order to be resistant to cyber-attacks and cannot be compromised easily. Tamper-resistant design, digitally signed firmware images, approved cryptographic algorithms, secure storage of cryptography credentials, and secure code development practices are approved measurements to achieve this.

In general, the existing capabilities of advanced network-based security should be fully exploited to protect all connected systems and devices within power system installations. Network-based security encapsulates all security measures that are deployed in the network. These technical security controls are especially important because of the current status of TC 57 based systems and protocols for power automation:

– Many devices do not have technical security controls implemented. They may be called legacy which is probably not true for the automation and protection features they need to fulfil (because these objectives are met completely). In order to integrate them in a secure manner, security measurements provided by the network play a key role. There are already solutions in place to protect so called ‘legacy devices’ by means of a “bump-in-wire” approach. Besides this, legacy device virtualization by network-based means is a flexible solution to safeguard unprotected devices.

– Furthermore, embedded devices with critical tasks within the electrical grid, like Protection-IEDs, are limited in memory and processing power when it comes to functions beyond control and protection. This shall be addressed by the security architecture in order to disburden these devices from security features that can be realized by the network or network- based devices, like centralized key management.

– Network-based solutions for secure connectivity are needed to protect the traffic between devices and systems, for remote access solutions or other communication links. Especially solutions based on virtual private networks (VPN) support a stringent approach to protect confidentiality and integrity of control data and other important messages. VPNs can be used to supplement existing communication security based on parts of IEC 62351 or to establish it where implementations of these standards are not available in the devices connected to the network. Especially tunnel less VPN solutions are highly scalable in any-to-any scenarios by supporting native multicast routing. Furthermore, tight policy integration as well as customized, per-application based encryption are features that support a typical TC 57 specific system and the underlying network architecture.

– Intrusion detection systems (IDS) as well as intrusion prevention systems (IPS) are providing pro-active and reactive detection capabilities, especially when adjusted to power system network specifics. Signatures are available for domain specific protocols like SCADA or telecontrol protocols. In this regard, security architects have to evaluate the pro and cons of “higher-layer” encryption, sometimes even defined on the application layer. In such a case, packet inspection and any other checks on the payload are not possible with direct impact on important preventive measures. Furthermore, behaviour-based techniques can help to respond successfully to even new and unknown threats.

– Device authentication based on authentication, authorization, and accounting (AAA) solutions is an appropriate way to define and control who is allowed to access specific parts of the network. It provides a flexible and scalable means to handle installations with hundred or even thousands of end-points. Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos, can be used to establish access control based on user (device) or service basis. Protocols like LDAP can be used to query directories and fetch user credentials.

In essence, the ultimate solution is a best of breed mix of device and network-based security leveraging the respective strengths by achieving a layered defence (or defence in depth, see 5.4.2). The maturity of existing network-based security solutions provides excellent opportunities to support the requirements for end-to-end security of power systems. Furthermore, network-based security shall be built on a stable and extensible framework of standards. The most relevant standards to protect communications links as well as the underlying infrastructure are listed and described in IETF RFC 6272 (*Internet protocols for the Smart Grid*, see also 4.3). These standards are already used and implemented at any scale in many industries. The most prominent standards are listed in Table 5.

Table 5 – General security standards applicable to network security

Standard	Content	Note / application example
RFC 4101, RFC 4102, RFC 4103	Base standards for IP Security (IPSec)	Layer 3 Security, typically used for VPNs or for remote access. The listed RFCs describe general architecture as well as the two modes AH (Authentication Header) and ESP (Encapsulated Security Payload).
RFC 5246	Transport layer security (TLS)	Layer 4 security for TCP/IP based communication, currently used in IEC 62351.
RFC 5746	Transport layer security (TLS) renegotiation indication extension	Extension to TLS to avoid certain injection when renegotiating an existing connection. A cryptographic binding between the current and the former session is being provided.
RFC 4962	Authentication, authorization, and accounting	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management. Provides an architecture allowing the centralized control of AAA functionality.
RFC 5247	Extensible Authentication Protocol (EAP) Key Management Framework	Framework for EAP, single EAP methods are defined in separate RFCs. EAP is typically used for controlling device (or human) access to networks.
RFC 6347	Datagram transport layer security v1.2 (DTLS)	Layer 4 security for UDP/IP based communication. May be applied in scenarios, where TLS is not applicable.
RFC 6407	Group domain of interpretation (GDOI)	Group based key management, currently used in IEC/TR 61850-90-5.
RFC 5280	Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile	Base specification for X.509 certificate and certificate handling.
ISO/IEC 9594-8	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks	Basic specification for certificates, certification authorities, revocation, validation, etc.
IEEE 802.1X	Port based network access control	Specifies port based access control, allowing the restrictive access decisions to networks based on dedicated credentials. It defines the encapsulation of EAP over IEEE 802, also known as EAP over LAN or EAPOL. Includes also the key management, formally specified in IEEE 802.1AF.
IEEE 802.1AE	MAC security	Specifies security functionality in terms of connectionless data confidentiality and integrity for media access independent protocols. Specifies a security frame format similar to Ethernet.
IEEE 802.1AR	Secure device identity	Specifies unique per-device identifiers and the management and cryptographic binding of a device to its identifiers

6 Mapping security controls to the TC 57 architecture

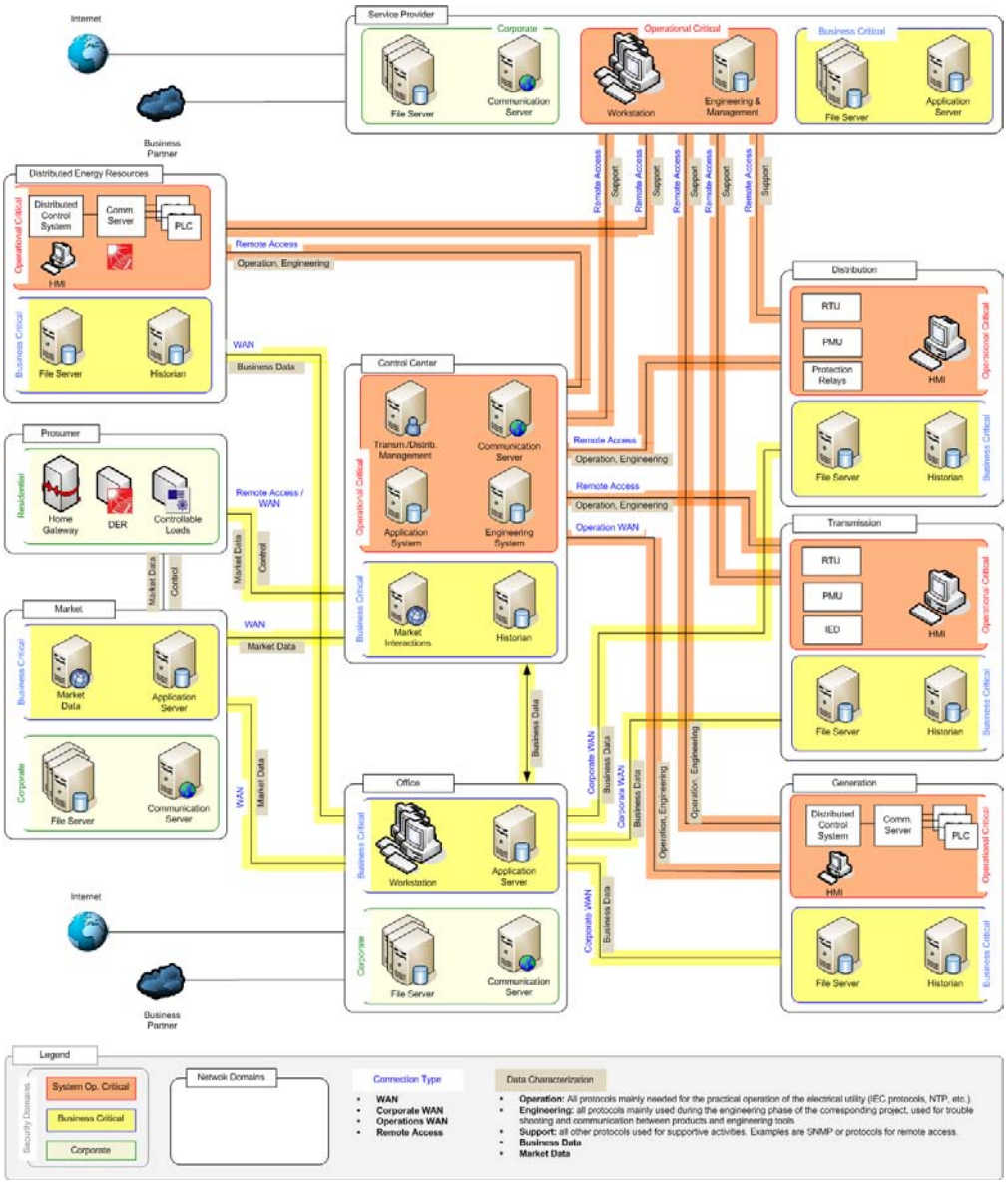
6.1 General

Clause 6 maps security controls introduced in Clause 5 to TC 57 architecture examples. It will start with an abstract generic scenario incorporating all power system domains used to map the four security domains. Based on this, cyber security controls are incorporated into this generic architecture scenario to provide insight into necessary steps to build secure power systems. Moreover, dedicated use cases for parts of the overall scenario are being discussed providing more detailed information about the security architecture in use cases like substation communication or control centre to substation communication. 6.2 to 6.5 can be taken as guidelines to select the security controls to cope with given security requirements.

The selected use cases are examples and may not apply in the described manner to every power system deployment. Therefore, a typical approach for selecting the appropriate security controls is a threat and risk analysis based on the explicit target use case to determine the security needs.

6.2 Security domains within a generic power system architecture

Figure 12 shows a generalized scenario for power systems following the CIGRE approach (see [35]) including the mapping of the logical security domains to the power system architecture. As stated before, power systems architectures easily span all four security domains.



IEC 1958/12

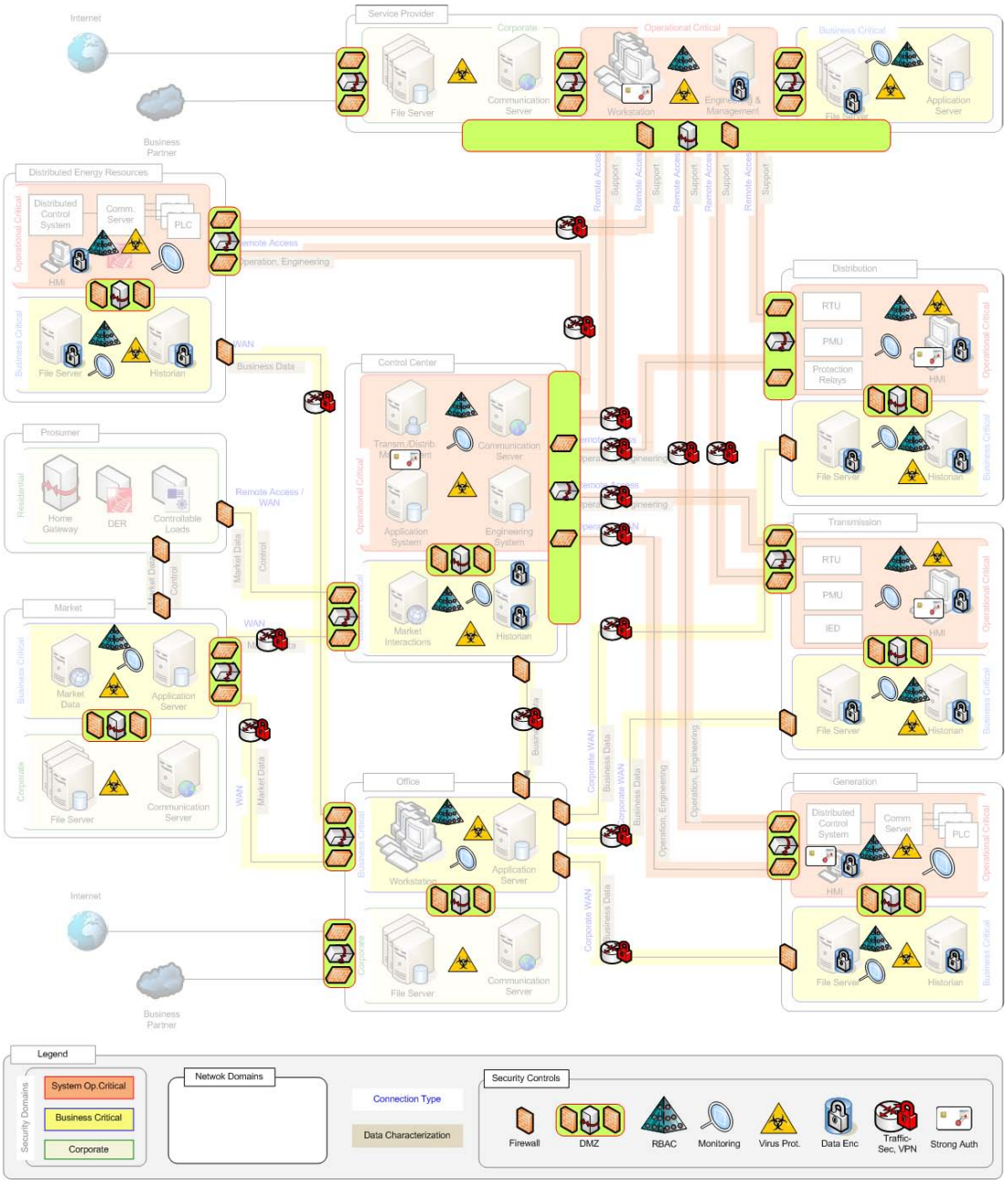
Figure 12 – Generic power systems architecture

Figure 12 depicts the different domains of power systems for generation, transmission and distribution, and the control centre. Additionally it shows the service provider domain, which may connect the service provider and the third party equipment manufacturer to the operational domain for engineering, maintenance and remote administration. Prosumers are depicted here, as they may be the endpoint of IEC 61850 based communication, e.g. for load reductions or distributed energy resources (DER) information. The control may be done via the market, but can also be done via the network operator directly (not shown in Figure 12).

Based on this overall scenario, cyber security controls (see Table 4) are incorporated addressing given security requirements for the security domains as part of 6.3.

6.3 Application of security controls to a generic power system architecture

Security controls have been discussed as part of 5.3. This subclause maps security controls to the generic power systems architecture showing the need for action in dedicated parts of the power system architecture. The list of applied security controls is not complete here. Figure 13 instead shows main security controls on an abstract level applied to achieve protection of communicated data as well as access protection to different security domains.



IEC 1959/12

Figure 13 – Power systems architecture with security controls

The security controls applied to the power system architecture in Figure 13 target:

– **Network segmentation** (see 5.4.4) is a powerful protection mechanism grouping network elements with frequent and sensitive communication needs into the same subnet with the goal to physically and logically providing explicit access control to this subnet. By this approach the security requirements for subnet internal communication can be often reduced compared to large open networks. Mechanisms to support network segmentation are provided through:

  - Firewalls to control inbound and outbound traffic into/from different zones (e.g. as stand-alone appliance or as router with firewall functionality)
  - DMZ providing distinct access control to information between two zones. The DMZ is located behind a firewall, and spans a semi-trusted zone between the internal and external network. The DMZ contains applications that are accessible from the inside and the outside. The DMZ symbols depicted in Figure 13 simply show the necessity of a DMZ to support network segmentation but not which components have to be placed

into a DMZ. All external communication should be routed through a dedicated proxy application in the DMZ. The hosts and applications within a DMZ have to be hardened to reduce their attack surface.

- VLANs provide a logical separation of networks and can be done on different layers, most common on layer 2. The membership to a VLAN is typically determined through configuration (e.g. a VLAN ID on Ethernet level). Note that VLANs as such do not provide cryptographic based security. IEC/TS 62351-6 [44] defines VLANs tags for dedicated application to logically separate GOOSE and SV traffic.

– **Strong authentication and access control** to operations and engineering services
  - Strong authentication using e.g., authentication based on X.509 certificates, which may also carry the role information for RBAC. The role in a public-key certificate could be signalled by creating a certificate policy document for each role. The object identifier identifying the certificate policy also indicates the role. For attribute certificates, the role attribute should be used.
  - RBAC based on IEC/TS 62351-8 to provide distinct access to equipment for control and engineering tasks. This includes the necessary definition of roles and rights in a security policy, as well as the enforcement in the components.
  - Mutual authentication in security protocols as described in IEC/TS 62351-3, -4, and -5 applying X.509 certificates in security TCP based communication using TLS. Authentication based on X.509 certificates typically requires a PKI.

– **Data security** for transmitted and stored information
  - Data encryption of stored information like engineering and control data or backup data. This may be done by using hard disc encryption tools at the lower layer or database encryption tools providing in combination with access control to the stored information.
  - Traffic encryption using:

    a) security protocol options of used communication protocols, i.e. the consequent application of protocol inherent security measures, e.g. IEC 62351, secure DNP3, etc.;

    b) security protocols to protect individual connections (TLS, DTLS, IPSec).

    Table 6 lists example protection options for communication protocols or applications.

Table 6 – Example security approaches to power system communication protocols

Service	Applied Protocol (s) or Applications	Recommendations for security controls
Remote desktop	RDP	Use VPN or IPSec option. RDP has built-in encryption (RC4) and authentication from Windows operating system.
Web-monitor	HTTP	Application of HTTPS for secure Web access.
Web-monitor	Java Applets/Servlets	Application of HTTPS for secure Web access.
Reporting / MMS	IEC 61850	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Time synchronization	NTP	NTPv3 offers security. Can be deployed using auto-key for key management
Substation – control center communication	IEC 60870-5-104	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Control center communication	IEC 60870-6 TASE 2 (ICCP)	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Control center and substation – control center communication	DNP3	Application of DNP3 security measures.
Network management	SNMP	Application of SNMPv3 security measures, support of IEC/TS 62351-7 defined NSM objects, SNMPv2 should only be allowed for monitoring.
File transfer	FTP	Use secure variants like SFTP instead of FTP.

c) Separate (additional) security appliances like VPN gateways: This approach is typically transparent to the other components and can be applied, e.g. between a substation router and the control center core firewall. It protects the traffic only between the VPN gateways, not on the whole communication path.

– **Security monitoring and preventive measures** to ensure reliability and availability of operations and engineering services:

- Monitoring tools like IPD/IPS systems to detect / counteract unusual communication traffic. This applies to all shown network domains;
- Malware protection to protect against viruses, Trojan horses, etc. influencing the operation of power systems for commercial or common operating systems (if malware protection software is available);
- White listing to allow only dedicated applications or services to be executed;
- Quality Management, e.g. definition and enforcement of secure coding guidelines during product development as explicit requirement to third party product vendors.

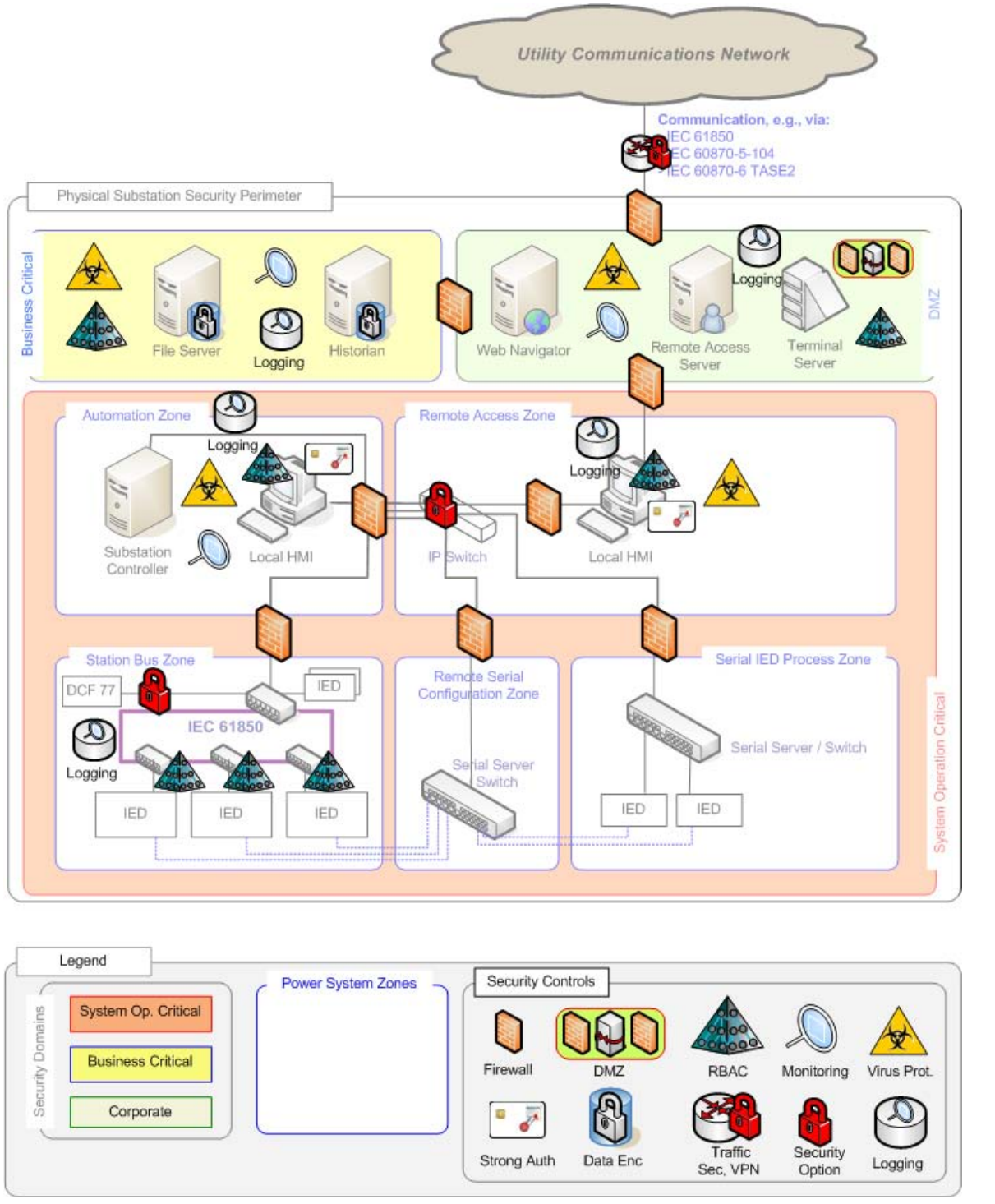
6.4 Application of security controls to specific power system scenarios

6.4.1 General

6.4.2 to 6.4.4 provide information about dedicated use cases, which are part of the generic power system architecture described above. The goal is to have a more detailed description of the application of dedicated security controls using the examples substation automation, control centre – substation communication, and advanced metering. Security controls are not restricted to the examples. There are further examples such as wide area situation awareness and demand-response, etc.

6.4.2 Substation automation

This subclause depicts security controls applied in an example substation communication scenario to protect substation internal communication as well as connectivity to external power system entities.



IEC 1960/12

Figure 14 – Example substation automation deployment with security controls

Substation automation shall be engineered ensuring not only the integrity of information exchanged within the substation but also crossing different security domains. This is especially important if access to control to field devices is carried out remotely, influencing the general availability of power, e.g. in business or residential areas. Hence, the security

controls applied to the substation system shown in Figure 14 target the protection of control and signalling information as well as access control and comprise:

– **Network segmentation** using a DMZ to provide distinct access control to the file server, server holding historian data as well as the automation and process bus zone down to the field devices and IEDs. This approach also supports remote administration by providing access via a terminal server located in the DMZ, which avoids direct access from a remote location to a field device. Network separation as shown in Figure 14 can also be supported using multiple firewalls to separate different zones, which may not necessarily be physical separated zones.

– **Strong authentication:**

  - to local engineering service computer based on X.509 credentials (certificates and associated private keys), which may be provided on smart tokens;
  - mutually for operation related machine-to-machine communication based on IEC 61850, IEC 60870-5-104 or DNP according to IEC/TS 62351-3, -4, and -5 applying X.509 credentials (for TCP based communication protected with TLS as T-Profile security means);
  - for GOOSE messages communicated between field devices using IEC/TS 62351-6.

– **Role-based access control based on IEC/TS 62351-8 to provide distinct access to equipment for control and engineering tasks down to the field device level:**

  - if X.509 certificates (identity or attribute certificates) are used, they may be carried on the smart token and can be combined with the certificate used for authentication;
  - definition and engineering of a minimum set of roles as suggested in IEC/TS 62351-8. The definition of additional roles is possible if needed;
  - security screening of personnel before assigning security roles;
  - definition of the area of responsibility for service personnel to allow only distinct access;
  - utilization of PKI services to issue and maintain security credentials for RBAC as targeted in IEC/TS 62351-9. This includes the engineering of dedicated root certificates on the components performing RBAC as well as the provisioning of revocation information to enable the verification of presented RBAC credentials.

– **Data security** for transmitted and stored information:

  - data encryption of stored information like engineering and control data or backup data in the DMZ;
  - traffic encryption used for sensitive communication with external system entities:

    a) security protocol options of used communication protocols, i.e. the consequent application of protocol inherent security measures, e.g. IEC 62351, Secure DNP3, etc.,

    b) security protocols to protect individual connections (TLS, DTLS, IPSec),

    c) separate security appliances like VPN gateways, e.g., providing a secure tunnel based on IPSec for IP-based communication. Using separate security appliances is typically transparent to the other components, but needs to be taken into account for the engineering.

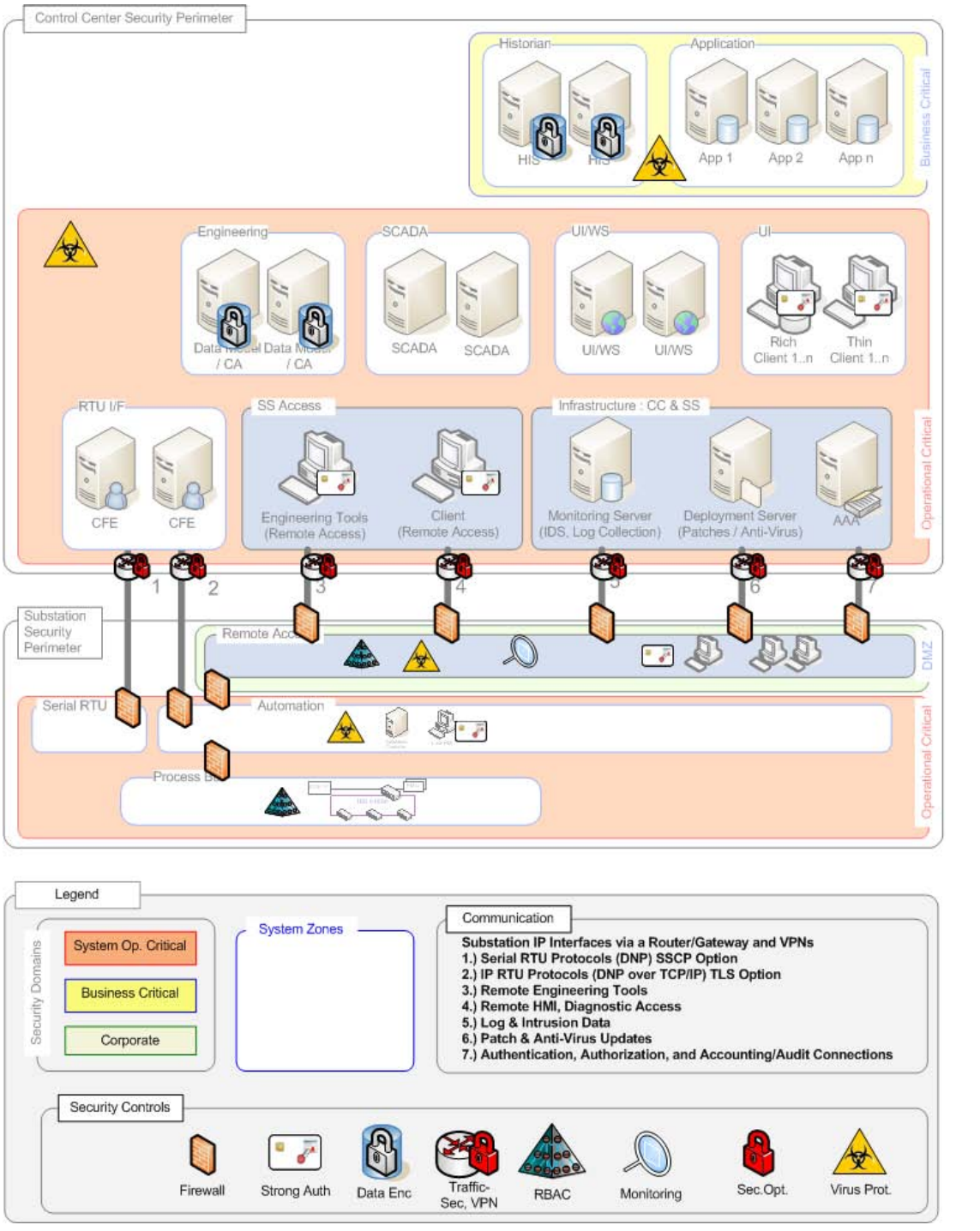
– **Communication security**: Application of security options in used supporting protocols, e.g.:

  - network time: NTPv3;
  - SMNP: SNMPv3 security options.

– **Security monitoring and preventive measures** to ensure reliability and availability of operations and engineering services. Additionally to the examples stated in 6.3, engineering information from the power system may also be used to configure IDS/IPS systems to better consider the target architecture and thus to decrease the probability of false positives.

6.4.3 Control center – substation communication

This subclause depicts security controls applied in an example control centre substation communication scenario. Figure 15 shows potential parts of a control centre communicating with a substation. Here it is assumed that all system zones are within the control centre security perimeter. With the integration of new business roles, certain responsibility may be moved out of the control centre security perimeter to a separate entity with an own security perimeter. In Figure 15, this may apply to the infrastructure control centre and the substation zone.



IEC 1961/12

Figure 15 – Example control center substation communication with security controls

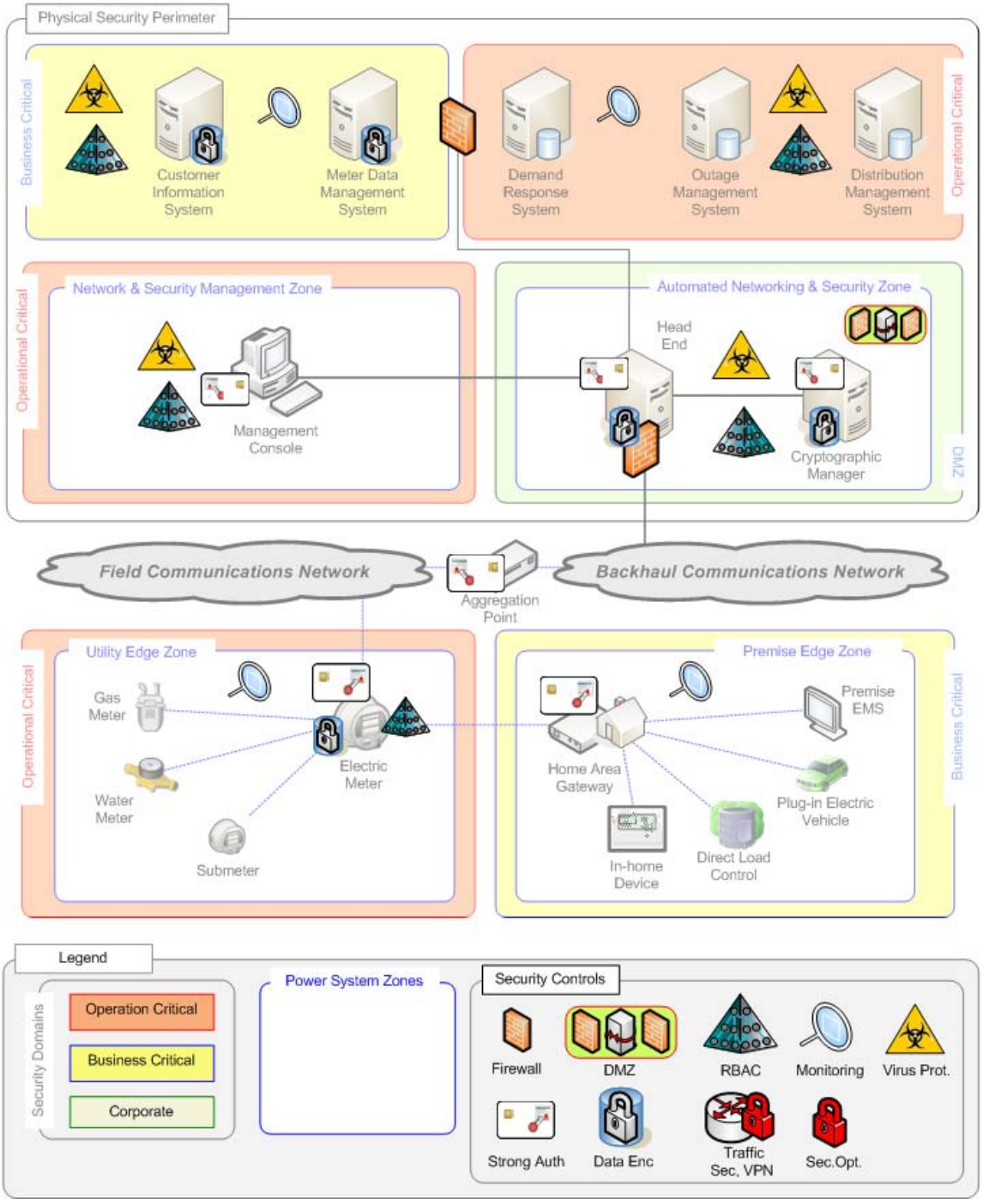
As seen in Figure 15, there are different communication channels between a substation and a control centre, which are typically provided via a router/gateway including:

– operational communication, e.g.:
  - serial RTU Protocols (e.g. DNP),
  - IP-based RTU Protocols (e.g. IEC 61850 over TCP/IP);
– engineering communication via:
  - proprietary protocols,
  - Web-based remote engineering tools using HTTPS or HTTP,
  - Remote HMI, diagnostic access using protocols like HTTPS, HTTP or RDP;
– security management related communication, e.g.:
  - log and intrusion data using, e.g. SNMP,
  - patch and anti-malware updates for commercial or common OS (if malware protection software is available),
  - authentication, authorization, and accounting/audit connections.

Security controls applied for the protection of communicated information and also RBAC as described for the substation automation scenario in 6.4.2 apply here as well. Additionally security credential related communication is expected, e.g., to maintain security credentials used in the substation. Examples are key renewal for components and most importantly the update of certificate revocation information.

6.4.4 Advanced metering

This subclause depicts security controls applied in an example Advanced Metering Infrastructure (AMI) scenario (as shown in Figure 16) to protect two-way communications between the utility back office and metering endpoints as well as those devices and systems beyond the meter that depend upon or utilize the meter as the communications channel to the utility.



IEC 1962/12

Figure 16 – Example advanced metering infrastructure deployment with security controls

AMI components and systems will most likely be closely integrated with other utility systems involved in the operation of the distribution system such as a demand-response control system, an outage management system, and a distribution management system. The AMI will also need to integrate with critical utility business systems such as billing and the customer information system. The AMI shall provide a strong defence for back-office applications where it bridges the utility's physical security perimeter and connects to other communication systems such as wide-area backhaul and field-area networks.

Field components shall be engineered in such a way that the utility is able to ensure the integrity of information crossing organizational boundaries and protect the confidentiality of sensitive customer information. Information integrity becomes especially important in cases

where load may be affected by either direct load control or delegated decision-making shaped by pricing information. Aggregation points shall therefore ensure only authorized utility personnel are able to access field traffic information and management controls. Home area gateways shall likewise ensure that signals affecting program enrolment, software updates, and pricing information come only from authenticated and authorized sources. The meter itself faces a multitude of concerns as it shall protect the aforementioned channels to the field area and home area networks as well as potentially other utility end-point devices such as submeters and other utility infrastructure (i.e. water and gas meters).

6.5 Identified gaps

This subclause lists gaps which have been identified and which need to be addressed either by further standardization or by guidelines or regulation. Some of the identified gaps may already be tackled by existing activities. This is mentioned per gap.

– To support cyber security measures security credentials are a necessary prerequisite. These credentials may be symmetric keys (shared keys) or based on the concept of public and private keys (PKI). There are certain requirements to these credentials, which comprise distribution, utilization, and management. The description of these requirements and a solution approach for the context of IEC 62351 security functionality will be addressed in IEC/TS 62351-9 targeting credential management and potentially identity management. These management tasks require technical and procedural support.

– Liaison with groups responsible for the PKI development within ITU-T or IETF and ISO/IEC should be established.

– Configuration and system management is being addressed by a task force from TC 57 WG 10 and WG 15 targeting a vendor independent solution to manage especially IEC 61850 devices.

– Application of RBAC according to IEC/TS 62351-8 [46]. IEC/TS 62351-8 describes the format and the handling of access tokens. IEC/TS 62351-8 can be directly applied in several use cases, e.g. by authentication and authorization as part of TLS in case of the push model or for local HMI access for the pull model. There are still more scenarios, in which the utilization of the access token needs more specification for the application (layer) or protocol using the access token. In the easiest case, additional fields necessary to carry the access token need to be defined in protocols utilizing RBAC.

– New scenarios in the advent of Smart Grid may require additional security mechanisms on the application layer, if the transport layer trust spans entities with different trust levels along the application layer path. This issue needs to be considered when working on new editions of existing and upcoming IEC/TS 62351 parts.

– Integration of security into CIM (IEC 61968, IEC 61970) to ensure that the security properties of a CIM object can be bound to the CIM object. This allows the security properties of the CIM object can be obeyed during the handling of the CIM object independently whether it is in transport or at rest.

– The following standards are stated in Table 3 in the mapping of logical interfaces to the TC 57 reference architecture but not covered by IEC 62351 so far. The standards may need investigation by IEC TC 57 WG 15: IEC 61334, IEC 62056, IEC 62325, IEC 61400-25.

Annex A
(informative)

Further related material

A.1 NERC CIP

Subclause 4.3 references the NERC CIP profiles. Table A.1 provides more information on the different profiles defined (see also [13]).

Table A.1 – NERC CIP overview

CIP	Title / Content
001	Sabotage reporting Reporting disturbances or unusual occurrences, suspected or determined to be caused by sabotage to appropriate authorities.
002	Critical cyber asset identification Identification and documentation of critical cyber assets using risk-based assessment methodologies.
003	Security management controls Documentation and implementation of cyber security policy reflecting commitment and ability to secure critical cyber assets.
004	Personnel and Training Maintenance and documentation of security awareness programs to ensure personnel knowledge on proven security practices.
005	Electronic security protection Identification and protection of electronic security perimeters and their access points surrounding critical cyber assets.
006	Physical Security Program Creation and maintenance of physical security controls, including processes, tools, and procedures to monitor perimeter access.
007	Systems security management Definition and maintenance of methods, procedures, and processes to secure cyber assets within the electronic security perimeter to do not adversely affect existing cyber security controls.
008	Incident reporting and response planning Development and maintenance of a cyber security incident response plan that addresses classification, response actions and reporting.
009	Recovery plans for critical cyber assets Creation and review of recovery plans for critical cyber assets.
010	Bulk electrical system cyber system categorization (draft) Categorization of BES systems that execute or enable functions essential to reliable operation of the BES into three different classes.
011	Bulk electrical system cyber system protection (draft) Mapping of security requirements to BES system categories defined in CIP-010.

A.2 SABSA

Clause 5 refers to SABSA and TOGAF as example for generic security architectures approaches. Table A.2 provides more information about the SABSA security architecture development. More information is available in [2].

Table A.2 – The SABSA matrix for security architecture development

	Asset (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	TIME (WHEN)
Contextual (business view)	The Business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual (architect's view)	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetime and deadlines
Logical (designer's view)	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical (builder's view)	Business data model	Security rules, practices, and procedures	Security mechanisms	Users, applications and user interface	Platform and network infrastructure	Control structure execution
Component (tradesman's view)	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational (facility manager's view)	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites and platforms	Security operations schedule

Bibliography

General material

[1] TOGAF, Industry standard architecture framework, available at <http://www.opengroup.org/architecture/togaf/>

[2] SABSA – Sherwood Applied Business Security Architecture, available at <http://www.sabsa-institute.org/>

[3] Open Security Architecture, available at <http://www.opensecurityarchitecture.org>

[4] ESCoRTS project, *R&D and standardization road map, final deliverable 3.2*, available at <ftp://ftp.cen.eu/CEN/Sectors/List/ICT/D32finaldelivery.pdf>

[5] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements* , see <http://www.iso27001security.com/html/27001.html>

[6] ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management*, see <http://www.iso27001security.com/html/27002.html>

[7] ISO/IEC 42010:2007, *Systems and software engineering – Recommended practice for architectural description of software-intensive systems*

[8] EU task force Smart Grid, expert group 2: *Regulatory recommendations for data safety, data handling and data protection*, available at <http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf>

[9] NIST SP 800-39, *Managing information security risk: organization, mission, and information system view*, March 2011, available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

[10] NIST SP 800-30, *Risk management guide for information technology systems*, July 2002, available at <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[11] Department of Homeland Security, see <http://www.dhs.gov>

[12] ISO/IEC 9594-8 (ITU-T X.509), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

Power systems related standards and guidelines

[13] NERC, North American Reliability Corporation, standards, available at <http://www.nerc.com/page.php?cid=2|20>

[14] BDEW, *White paper requirements for secure control and telecommunication systems*, available at <http://www.bdew.de/bdew.nsf/id/DE_Datensicherheit>

[15] NIST, National Institute of Standards and Technologies, *Smart Grid interoperability project*, available at <http://www.nist.gov/smartgrid/>

[16] NIST 1108R2, *Framework and roadmap for Smart Grid interoperability standards*, release 2.0, February 2012, available at <http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf>

[17] NIST IR 7628, *Guidelines for Smart Grid Cyber Security, Vol. 1 Smart Grid Cyber Security Strategy*, August 2010, available at <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf>

[18] NIST IR 7628, *Guidelines for Smart Grid Cyber Security, Vol. 2 Security Architecture and Security Requirements*, August 2010, available at <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf>

[19] NIST IR 7628, *Guidelines for Smart Grid Cyber Security, Vol. 3 Supportive Analyses and References*, August 2010, available at <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf>

[20] NIST SP 800-53, *Recommended security controls for federal information systems and organizations*, Revision 4, February 2012, available at <http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>

[21] NIST SP 800-82, *Guide to industrial control systems (ICS) security*, Draft, September 2008, available at <http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf>

[22] IEC *Smart Grid standardization roadmap*, prepared by SMB Smart Grid strategic group (SG3), June 2010, available at <http://www.iec.ch/zone/smartgrid/grid_sg3.htm>

[23] ISO/IEC 15408 (all parts), *Information technology – Security techniques – Evaluation criteria for IT security*

[24] IEC 61850 (all parts), *Communication networks and systems in substations*

[25] IEC 62351 (all parts), *Power systems management and associated information exchange – Data and communications security*

[26] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

[27] IEC 61400-25-4, *Wind turbines – Part 25-4: Communications for monitoring and control of wind power plants – Mapping to communication profile*

[28] IEC TC 57, *Power systems management and associated information exchange*, see <http://tc57.iec.ch/index-tc57.html>

[29] IEC/TR 62357:2003, *Power system control and associated communications – Reference architecture for object models, services and protocols*

[30] IEEE 1686-2007, *IEEE Standard for substation intelligent electronic devices (IEDs) cyber security capabilities*

[31] IEEE P2030, *IEEE draft guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications, and loads*

[32] ISA 99 standards framework, available at <http://www.isa-99.com/>

[33] DHS *Catalog of control systems security – recommendations for standards developers*, June 2010, available at <http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf>

[34] CIGRE Report, *Risk assessment of information and communication systems*, WG D2.22, August 2008, Electra

[35] CIGRE Report, *Security frameworks for electric power utilities*, WG D2.22, December 2008, Electra

[36] CIGRE Report, *Security technologies guideline*, WG D2.22, June 2009, Electra

[37] Frances Cleveland, *IEC TC 57 security standards for the power system's information infrastructure – beyond simple encryption*, WG 15 White Paper, June 2007

[38] IETF RFC 6272, *Internet protocols for the Smart Grid*, F. Baker, D. Meyer, June 2011

[39] ISO/IEC 17799, *Information technology – Security techniques – Code of practice for information security management*

[40] IEC/TS 62351-1:2007, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

[41] IEC/TS 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

[42] IEC/TS 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

[43] IEC/TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

[44] IEC/TS 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

[45] IEC/TS 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models*

[46] IEC/TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

[47] IEC/TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

[48] IEC 60870-5-101, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

[49] IEC 60870-5-104, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profile*

[50] IEC 60870-6 (all parts), *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations*

[51] IEC 61334 (all parts), *Distribution automation using distribution line carrier systems*

[52] IEC 61968 (all parts), *Application integration at electric utilities – System interfaces for distribution management*

[53] IEC 61970 (all parts), *Energy management system application program interface (EMS-API)*

[54] IEC 62056 (all parts), *Electricity metering – Data exchange for meter reading, tariff and load control*

[55] IEC 62325 (all parts), *Framework for energy market communications*

[56] IEC/TR 61850-90-5, *Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*

[57] ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[58] DIN SPEC 27009:2012-04, *Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002* (title in English: *Guidance for information security management of power supply control systems based on ISO/IEC 27002*) available at <http://www.beuth.de/en/technical-rule/din-spec-27009/151100155>

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch