IEC TR 62357-1

Edition 2.0 2016-11

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Part 1: Reference architecture

IEC TR 62357-1:2016-11(en)

International Electrotechnical Commission

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.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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 62357-1

Edition 2.0 2016-11

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Part 1: Reference architecture

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-3764-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE –

Part 1: Reference architecture

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 62357-1, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This new edition cancels and replaces the first edition published in 2012 and constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) The new edition provides updates and defines layered Reference Architecture to help direct longer term goals and activities, specifically to ensure compatibility of all new

standards developed in the IEC by benefitting from lessons learned during development of the current standards and their application to actual utility projects as well as through application of other internationally recognized architecture standards.

b) This edition reflects the progress recently achieved with the international Smart Grids (SG) initiatives and the CIGRE D2.24 large system architecture vision. It also leverages the work done by NIST-SGIP, CEN-CELELEC-ETSI SGCG M490, IEC SG3 Smart Grids Roadmap, and IEC SyC Smart Energy working groups.

The edition also reflects the most recent editions of the IEC standards relating to power systems management and associated information exchange, including the IEC 61850 series and the IEC 61968, IEC 61970 and IEC 62325 Common Information Model (CIM) standards.

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

Enquiry draft	Report on voting
57/1688/DTR	57/1745/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.

In this technical report, the following print types are used:

– *obligations: in italic underlined type.*

A list of all parts in the IEC 62357 series, published under the general title *Power systems management and associated information exchange*, 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 website 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.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE –

Part 1: Reference architecture

1 Scope

Electricity grids from generation to consumers, including transmission and distribution, as well as energy markets are facing many new challenges while integrating an increasing variety of digital computing and communication technologies, electrical architectures, associated processes and services. The new challenges lead very often to support an increasing level of interaction between involved actors, components and systems.

Thus, it is key for the IEC to propose a clear and comprehensive map of all standards which are contributing to support these interactions, in an open and interoperable way.

The purpose of this document is to provide such a map (as available in 2016), but also to bring the vision of the path which will be followed by the concerned IEC technical committees and working groups in the coming years, to improve the global efficiency, market relevancy and coverage of this series of standards.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*

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

IEC 61850 (all parts), *Communication networks and systems for power utility automation*

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

IEC 61970 (all parts), *Energy Management System Application Program Interface (EMS-API)*

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

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

IEC TR 62357-200, *Power systems management and associated information exchange – Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6)*

IEC 62361 (all parts), *Power systems management and associated information exchange – Interoperability in the long term*

IEC 62746 (all parts), *Systems interface between customer energy management system and the power management system*

3 Terms, definitions and abbreviated terms

3.1 Terms

3.1.1 Architecture

The purpose of architecture is to define or improve systems. The architectural process encompasses understanding the scope of interest, understanding stakeholder requirements, and arriving at a design to satisfy those requirements.

The two word-senses in which architecture is used are:

- A set of models with the purpose of representing a system of interest.
- The activity and/or practice of creating the set of models representing a system.

Model Driven Architecture advocates the application of modelling to the architectural process and formalizes the resulting artefacts such that the realization or improvement of the system may be more actionable, less expensive and less risky.

3.1.2 Reference Architecture

A Reference Architecture describes the structure of a system with its element types and their structures, as well as their interaction types, among each other and with their environment. Describing this, a Reference Architecture defines restrictions for an instantiation (concrete architecture). Through abstraction from individual details, a Reference Architecture is universally valid within a specific domain. Further architectures with the same functional requirements can be constructed based on the Reference Architecture. Along with Reference Architectures comes a recommendation, based on experiences from existing developments as well as from a wide acceptance and recognition by its users or per definition. [ISO/IEC 42010]

3.1.3 System

A system is a collection of parts and relationships among these parts that may be organized to accomplish some purpose.

In Model Driven Architecture, the term ‘system’ can refer to an information processing system but it is also applied more generally. Thus a system may include anything: a system of hardware, software, and people, an enterprise, a federation of enterprises, a business process, some combination of parts of different systems, a federation of systems – each under separate control, a program in a computer, a system of programs, a single computer, a system of computers, a computer or system of computers embedded in some machine, etc.

One of the key strengths of modelling, and one that distinguishes it from implementation technologies like software source code, is that it is an excellent way to represent, understand and specify systems.

In Smart Grids Architecture Model (SGAM) a system is a boundary which include all layers of SGAM

3.1.4 Functional Architecture / Concept

- A “function” represents a logical entity which performs a dedicated function. Being a logical entity, a function can be physically implemented in various ways (in devices or applications).
- A “function group” is a logical aggregation of one or more functions.

- An “interaction” of two or more functions is indicated by a connecting line between these functions. Interaction is realized by information exchange via the interfaces of functions and communication means.
- A “functional architecture” identifies the functional elements of a system and relates them to each other.

3.1.5 Service

This is the contract to perform a certain task, with certain deliverables (output) and other agreements on what is included (external view)

3.1.6 Function

This is when the service is carried out (internal view)

3.1.7 Application

This is the implementation of a service providing a certain functionality

3.1.8 Model

A model in the context of Model Driven Architecture (MDA) is information selectively representing some aspect of a system based on a specific set of concerns. The model is related to the system by an explicit or implicit mapping. A model should include the set of information about a system that is within scope, the integrity rules that apply to that system and the meaning of terms used.

A model may represent the business, domain, software, hardware, environment, and other domain-specific aspects of a system.

3.1.9 Modelling language

To be useful, any model needs to be expressed in a way that communicates information about a system among involved stakeholders that can be correctly interpreted by the stakeholders and supporting technologies. This requires that the model be expressed in a language understood by these stakeholders and their supporting technologies. Well-known modelling languages include Unified Modelling Language (UML), Structured Query Language (SQL), Business Process Model and Notation (BPMN, E/R, Ontology Web Language (OWL), EXtensible Mark-up Language (XML) Schema.

3.1.10 Elements

Elements are systems and a system may contain subsystems applications and devices. An element can also be a function or group of functions. An element can also be a service or group of services.

3.1.11 Profile

Generally a profile defines a subset of an entity (e.g. standard, specification or a suite of standards/specifications). Profiles enable interoperability and therefore can be used to reduce the complexity of a given integration task by:

- selecting or restricting standards to the essentially required content, e.g. removing options that are not used in the context of the profile
- setting specific values to defined parameters (frequency bands, metrics, etc.)

A standard profile for communications standards may contain a selection of communication capabilities applicable for specific deployment architecture. Furthermore a profile may define instances (e.g. specific device types) and procedures (e.g. programmable logics, message

sequences) in order to support interoperability. It may also provide a set of engineering guidelines to ease the deployment of new technologies.

3.2 Abbreviated terms

AMM	Advanced Metering Manager
BPMN	Business Process Model and Notation
CEN/CENELEC	European Committee for Electrotechnical Standardization
CIGRE	Conseil International des Grands Réseaux Electriques
CIM	Common Information Model
COSEM	Companion Specification for Energy Metering
DER	Distributed Energy Resources
DR	Demand Response
DSO	Distribution System Operator
ebIX	European forum for energy Business Information eXchange
EFET	European Federation of Energy Traders
ENTSO-E	European Network of Transmission System Operators for Electricity
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
FERC	Federal Energy Regulatory Commission
GIS	Geographic Information System
ISO	International Standardization Organization
ITU	International Telecommunications Union
MDA	Model Driven Architecture
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OWL	Ontology Web Language
RA	Reference Architecture
RDF	Resource Description Framework
SCADA	Supervisory Control And Data Acquisition
SDO	Standards Development Organization
SG	Smart Grid
SGAC	Smart Grids Architecture Committee
SGAM	Smart Grids Architecture Model
SGIP	Smart Grids Interoperability Panel
SGTCC	Smart Grids Testing & Certification Committee
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TC	Technical Committees
TOGAF	The Open Group Architecture Framework
TSO	Transmission System Operator
UML	Unified Modelling Language
XML	Extensible Markup Language
XSD XML	Schema Definition

4 Drivers and objectives for Reference Architecture

The Reference Architecture drivers are:

- Need to manage the increase of intermittent and distributed energy resources

The objective is to anticipate the new usage of electricity and support the new business models attached to these new usages.

Electricity paradigms are changing due to the introduction of intermittent distributed resources, as well as a higher and higher presence of active users, modifying their behaviour to make the most of electricity.

It is the role of the IEC to enable the emergence of these new ways of using electricity.

It shall enable meaningful data to flow freely across the system as the energy flows in various directions and ensure any information is available anywhere it is needed.

The Reference Architecture shall consider and represent the specifics of intermittent and distributed energy resources. It shall support meaningful information exchanges and communication within the power system and to external parties to facilitate their integration.

- Need for sustainable and efficient energy

The objective is to make the best of available energy and preserve natural resources

The contribution of the Reference Architecture is to facilitate and consider specific requirements for interactions between or within involved players, renewable energy producers, markets, utilities and consumers to reach such a goal.

The Reference Architecture must provide a means to leverage energy efficiency potentials.

- Need for safe, secure, and reliable energy to have a resilient power system

The objective is to support the needed functions to provide the expected quality to consumers such as voltage and frequency regulation and outage reduction

The objective is to provide a resilient power management system complying with the reliability objective of the utility

Cyber security supports the reliable operation of power systems coping with technical, physical, and organizational security requirements related to specific use cases. The derivation of security requirements is typically based on a threat and risk analysis. Further security requirements may also stem from regulation. The security counter measures need to be appropriate to address the security requirements.

The Reference Architecture provides a framework for identifying risk and providing security counter measures.

- Need for economic efficiency

The objective is to support flexibility while maximising the use of existing foundations

Architecture flexibility refers to its ability to adapt to dynamic changes mostly through incremental changes.

This may lead the architecture to add/remove/update services/functions/components at different level of depths.

The market is requiring more and more flexibility and standardization should help the users in managing these needed evolutions.

Increasing flexibility through international standards will increase the value and the duration of concerned assets.

Backward compatibility with an easy migration from the existing appears among the main properties to consider reaching such an objective.

The objective is to support interoperability by design and offer multi-vendor system capabilities

It is one of the main properties of the Reference Architecture to support interoperable architecture enabling mixing components, sub-systems and systems coming from different vendors.

This also includes properties of the Reference Architecture to allow any market player to have an equal opportunity to participate in this architecture.

The needed property of such a Reference Architecture to meet this objective relies on the availability of common data model across a maximum number of levels of the architecture.

The Reference Architecture shall support the “customization” of standard usage – also known as “profiling” − if it helps to reach a better level of interoperability in a specific context.

It is important to recognize that the focus of the IEC in this domain is standards for interoperability among different utility organizations and/or different vendor products. Neither the IEC nor its working groups design or build applications, and the internals of applications are deliberately left open to competition and are not part of the IEC scope for standardization. The policy is to maximize opportunities for creativity by restricting standardization to points where exchange of information is required.

The objective is to maximise the re-use of off-the-shelf technologies, especially the technologies coming from the IT and communication domain

Offering capabilities to exchange data between components, sub-systems and systems requires the use of information and communication technologies.

Considering that the use of this technology is not specific to the electricity domain, it is the challenge of the Reference Architecture to maximize the re-use of opened transverse technologies which are used in other domains.

However it is also the challenge to pick from these the most open, sustained and used ones, and in any case to make the Reference Architecture resilient to changes in this domain, which is known as a fast moving one.

The objective is to reduce power management systems total costs around their life cycle

- Need to cope with faster changing context

The objective is to support assets agility while preserving the existing ones

Agility means the ability to support a new user’s objectives driven by internal (new user’s company objectives) or external pressures (technological change, regulatory changes).

A second objective is to support flexibility to adapt to local regulatory frameworks

The objective for the Reference Architecture is to partition systems to identify the interfaces for communication standards such as CIM, IEC 61850, Tase-2, IEC 60870 to minimize the dependencies. Then changing one function will minimize the effect on the others.

- Need to cope with increasing complexity

The interaction of systems and markets interactions are increasing and becoming more complex. Regulatory requirements increase the number and variety of market players and require much more sophisticated, forecasting and faster reacting systems.

The objective is to provide sustained foundations to existing and future systems

The expectation of standard users is to get longer lasting assets; it is an expected top priority of the Reference Architecture to guarantee the most stable technical principles and resilience to future changes.

The principle is for standardization to provide all needed means to define and manage in a sustained way the data models, which are considered as the most stable part of the Reference Architecture.

The objective is to reduce integration efforts while anticipating an increased complexity of the systems

The cost of integration is really one of the main challenges in making system smarter. It is the role of the IEC Reference Architecture to offer to the market the most efficient way to integrate such a system, and then consider the processes and services needed to support the full system cycle from its specification down to its deconstruction.

One way to reach this objective is relying on the ability of systems, sub-systems and components to support pre-defined meaningful data models (meaningful, means with a defined standard semantic).

The objective is to make as easy as possible the use of the proposed set of standards

For most of the stakeholders, moving to smarter systems raises the need for this market player to get the needed knowledge as quickly as possible and at the lowest costs and to adapt its processes and tools to manage the new set of technologies.

It is the role of the Reference Architecture to provide the easiest access to the standard technologies and to foresee better ways to support the needed process and tools to make the life of the user the easiest.

Among one of the main challenges of the expected properties is to focus on the most limited number of semantic domains.

5 Overview

5.1 Standardisation context

Power Systems are mainly based on the standards shown in Figure 1:

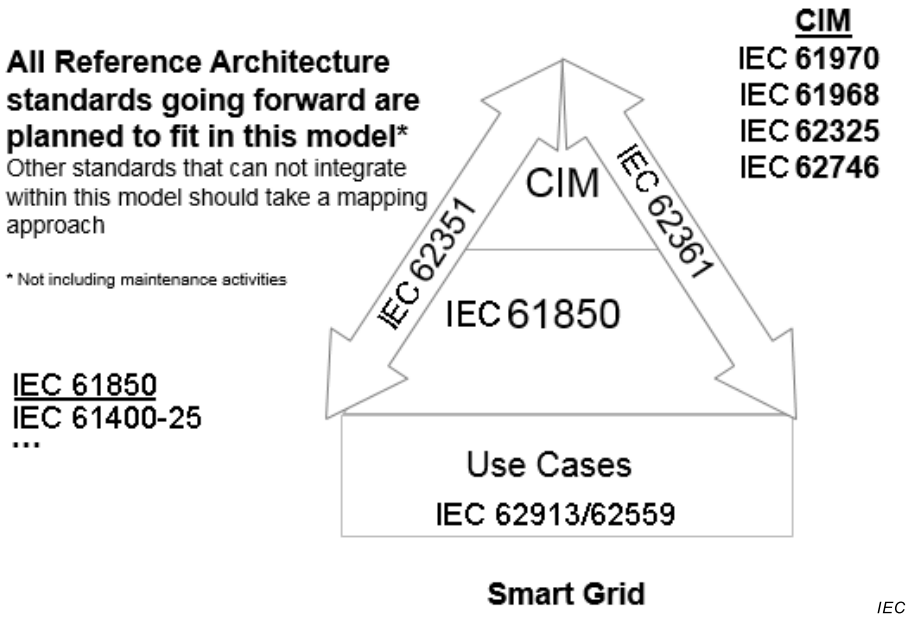


Figure 1 – Core domain of Reference Architecture

These key standards, with other related standards will be spread over the Reference Architecture. The core domain of Reference Architecture revolves mostly around IEC standards and has connection to other semantic domains such as Electric Vehicle (EV) or metering[1].

5.2 Relevant business domains

During the coming years the structure, operation and management of the power system will undergo fundamental changes. In order to define standards that support this transition in a consistent way, a generic conceptual model is required. This conceptual model is to be regarded as the starting point for all modelling activities, and for all other models, frameworks, and architectures, which are used to arrive at standards required for Smart Grids and Markets.

The IEC System Committee Smart Energy is the coordinator for the development of these Generic Smart Grid requirements in collaboration with the various IEC Technical Committees. SyC Smart Energy promotes a system perspective.

The IEC TS 62913 series[2], proposed by SyC Smart Energy WG6 (Generic Smart Grid Requirements), has broken down the scope of Smart Grids applications into domains[3]. This is an arbitrary yet necessary split, and it has been inspired by existing conceptual models which have been drafted previously, such as the National Institute of Standards and Technology (NIST) Smart Grids conceptual Model or the conceptual model developed as part of the European mandate M/490 Smart Grids Coordination Group.

A conceptual model can be defined as the grouping of roles and actors (systems, components, operators etc.) within coherent domains related to a general system. It provides

---

1 Some Technical Committees have chosen to extend IEC 61850: TC 38 (IEC 61869), TC 88 (IEC 61400-25), SC 17C (IEC 62271), etc.

2 Under preparation.

3 Excerpt from IEC 62913-1:−, Clause 2, Conceptual Models.

a high-level Reference Architecture model and proposes a decomposition of a system in domains and sub-domains.

This facilitates the description of Smart Grids systems and interoperability analysis. The roles and systems of each domain interact with each other, as well as with the roles and systems of other domains.

Based on the commonly accepted breakdown and other existing Conceptual models (NIST conceptual model, European Union (EU) M/490 Smart Grids conceptual model), IEC TS 62913 has organised the Smart Grids domains in five clusters:

– Grid-related domains – these include the Transmission Grid domain, the Distribution Grid domain, and the Micro-Grids domain,
– Market-related domain – this consists of the Market domain,
– Resources-connected-to-the-Grid domains – these domains are the Bulk Generation domain, the Distributed Energy Resources domain, the Smart Home / Commercial / Industrial / Demand Response (DR)-Customer Energy Management domain, and the Energy Storage domain,
– Electric Transportation domain – this consists of the Electric Transportation domain (DCT8),
– Support functions domains – these include the Smart Substation Automation domain, Advanced (Smart Grids and) Smart Metering Infrastructure domain and the Asset Management domain.

Figure 2 provides an overview of the Smart Grids domains and their high-level interactions. It represents a conceptual model for IEC TS 62913:

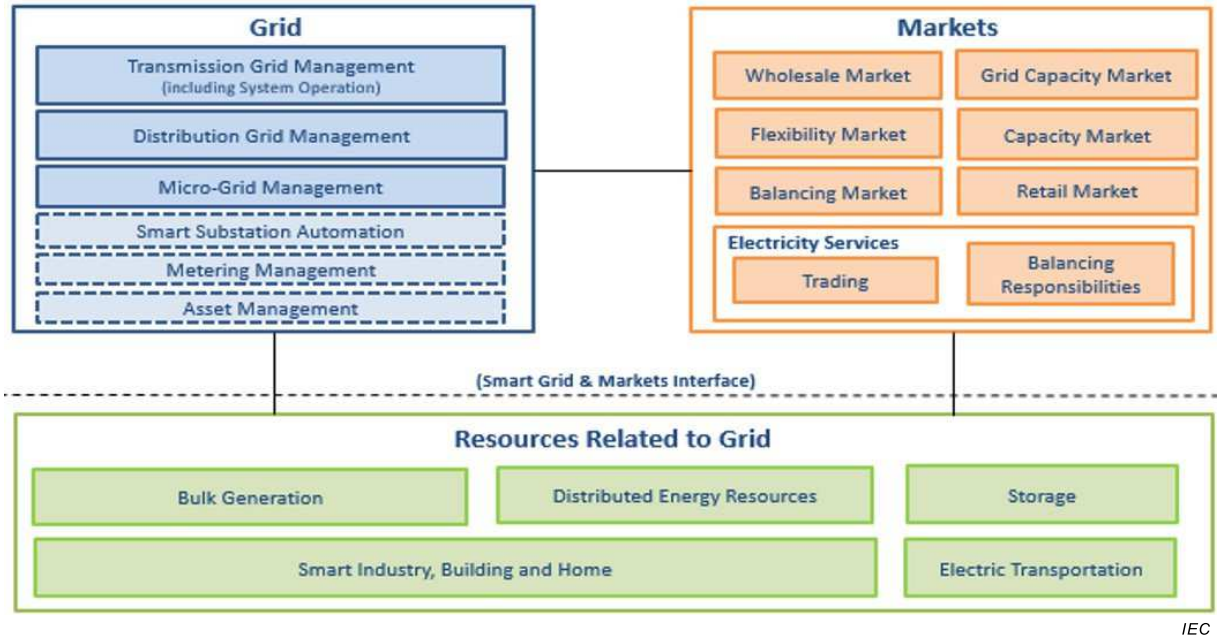


Figure 2 – IEC TS 62913 conceptual model

Its main underpinning is the analysis of roles and responsibilities. While this model is based on an electricity market structure, the roles and responsibilities are clearly defined and provide a solid basis; new parties may enter certain markets, responsibilities may be redistributed, but the fundamental roles and their respective responsibilities are expected to remain constant.

Reference Architecture facilitates the conceptual model of Smart Grids Use Case (UC and requirements enabling the different UC to be implemented and describing links between, Grid, Markets and Grid Users domain.

Both the conceptual model and the Reference Architecture plan to use the same methodology and the same definition of actors and roles.

The term IT (Information Technology) is typically connected with devices used to perform business operations, for example product life cycle management, enterprise resource planning, business planning, billing, asset tracking, and/or maintaining customer information. The devices used are mainly located in offices and data centres. In contrast OT (Operation Technology) is associated with field level devices, used to perform actual operations like discrete or continuous control, metering, etc. These OT systems are based on vendor-specific and often proprietary technologies operating in a real time or near to real time environment. The meaningful convergence or the bridging of both (IT and OT) relates to the integration of operational technologies like Supervisory Control And Data Acquisition (SCADA), Meters/Sensors working in real time with IT systems allowing an end-to-end management of both. This allows for cost and risk reductions (burden sharing) on the economic side and on reuse of existing technologies on the other. The Reference Architecture aims to support this IT/OT interoperability shown in Figure 3.

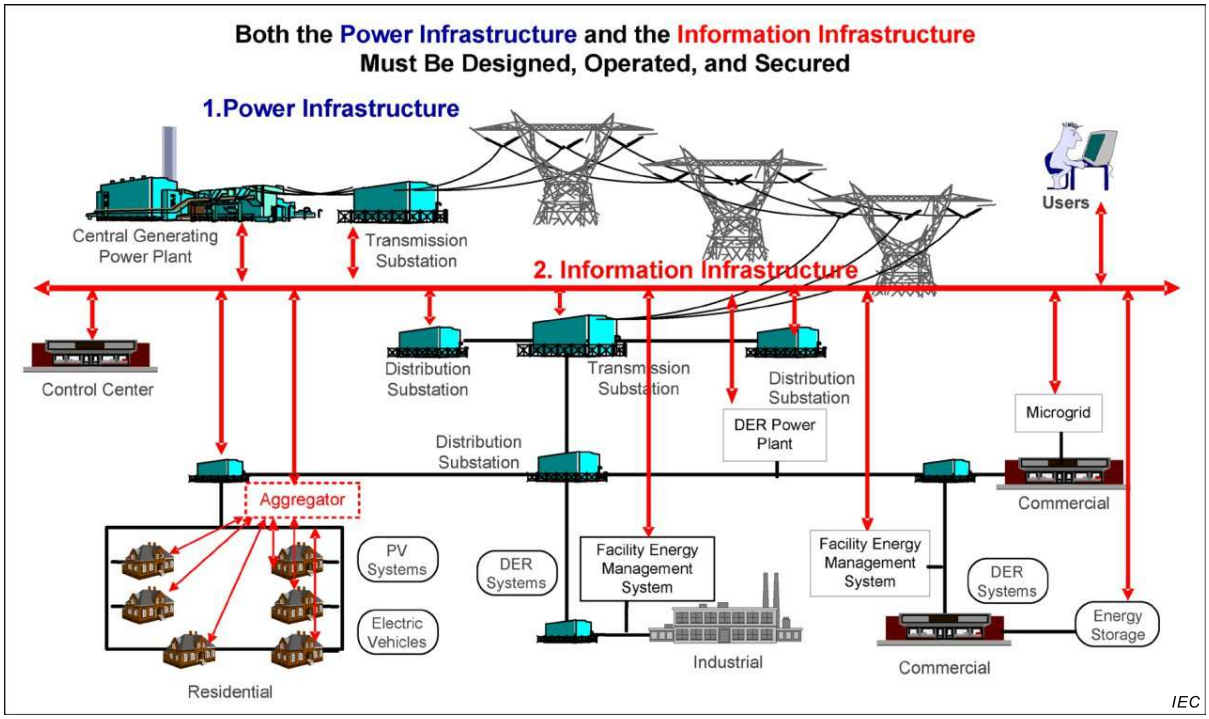


Figure 3 – Two infrastructures (OT/IT) must be designed, operated, and secured

For instance high performance automation on distribution will provide more and more data at higher levels (IT level) in order to conduct data analytics. Therefore the OT/IT paradigm is still a stake for many utilities.

The problem of aligning and integrating business processes and OT/IT is hampering many companies in their strategic and tactical development. Constructing integrated architecture models contributes to tackling this problem. In current business practice, an integrated approach to business processes and OT/IT is indispensable.

5.3 Intended audience

5.3.1 General

The Reference Architecture provides the high level assumptions about how systems should interoperate.

The main purposes of the Reference Architecture are:

– To guide designers of standards for data exchange, by clarifying the purpose of data exchanges between systems, applications, components.
– To guide application designers by clarifying what the overall vision expects from their systems.
– To guide utilities in establishing implementation architecture that will accomplish their tasks effectively.

The role of the Reference Architecture is to support and assist standardization groups and to provide them with easily applicable methods and architectures and ensure an easy understanding of the approach. Though the main intended audience is standardization technical committees, it can also be used by other actors like research projects testing new concepts or engineers developing Smart Grids products, or even the legislator in order to check the legislative framework.

The intended audience is based on key roles described in Reference Role Model. It is not intended to go through all Roles. For a detailed Role Model description please refer to IEC TS 62913-1[4].

5.3.2 Implementing actors

5.3.2.1 Transmission System Operators and Grid Operators

The increased penetration of generation capacities, mostly connected to the distribution network, as well as the development of new usages of electricity will tend to intensify the need for cooperation between system operators at distribution and transmission level. If Transmission System Operators (TSO) were traditionally responsible for the overall system stability and Distribution System Operators (DSO) for operating their respective network, they will need to strengthen their coordination at different timeframes in order to ensure the security of the system.

TSO business processes are impacted by new regulations that are coming into force and developed by regulatory authorities.

5.3.2.2 Distribution System Operators and Grid Operators

The Distribution Grid Management (DGM) domain today faces several challenges, which tend to significantly change the way its actors operate. These changes and their combination contribute to transform in depth Distribution Grid Operators. They already started and will continue to impact their roles, business models and business processes.

The distribution domain will also see more and more self-healing grids, micro-grids and interconnected micro-grids.

It includes business processes and functions related to:

- The long-term planning and development of the electricity distribution system, including connection and access;

4 Under preparation. Stage at the time of publication: IEC/CDM 62913-1:2016.

- The operational planning and scheduling of the electricity distribution system;
- The operation and maintenance of the electricity distribution system;
- The facilitation of electricity markets;
- The possibility to provide regulated services based on data management and provision to external roles such as TSOs, Energy Regulators, or local authorities, in order to facilitate national and local public policies and enable customer empowerment.

5.3.2.3 Resources related stakeholders

Different resources are connected to the Grid (Distributed Energy Resources, Smart Home / Commercial / Industrial / DR-Customer Energy Management, Energy Storage, and Bulk Generation, These resources are managed by different stakeholders. This document must help concerned stakeholders in order to identify which standards will be used to connect these resources to the Grids, which standards can be used to define these resources in order to have them interoperable.

5.3.2.4 Market players

Market players are numerous: Balance Responsible Party, Billing Agent, Consumer, Electricity trader / Broker, Flexibility Aggregator/Operator, Imbalance settlement responsible, Service Provider, (Electricity) Supplier / Retailer. The business processes of the Market domain, especially those related to the contribution to system security, need to comply with the applicable Grid/Network Codes. This document will help market players understand the big picture, identify potential new developments and identify which main standards they have to comply with.

5.3.2.5 Vendors

This document supports vendors as a guide to workable standards useful for developing best state of the art products and solutions fitting business requirements. It shall help vendors to understand that their respective product will have to interoperate with other vendor product using a recognized international standard.

5.3.3 Standardization actors

5.3.3.1 Regulators

This document should help regulators as a guide to workable standards useful to delivering the best value for consumers by ensuring that technical investments by energy providers utilize standards wisely, and introduction to standards related to Smart Grids privacy and security.

Regulators are defining Grid Codes which have an impact on different stakeholders' business processes, and as a consequence on their supporting architecture.

5.3.3.2 Standard Development Organisations

The IEC has several liaisons within its own Technical Committees (TC) and with external Standards Development Organizations (SDOs) (International Standardization Organization (ISO), International Telecommunications Union (ITU), UN-CEFACT, etc.). This document shall help SDOs to identify their boundaries and needs for harmonisation.

5.4 Reference to relevant sources

Figure 4 describes the main relevant sources of input to this document. Refer to these documents as complementary documents:

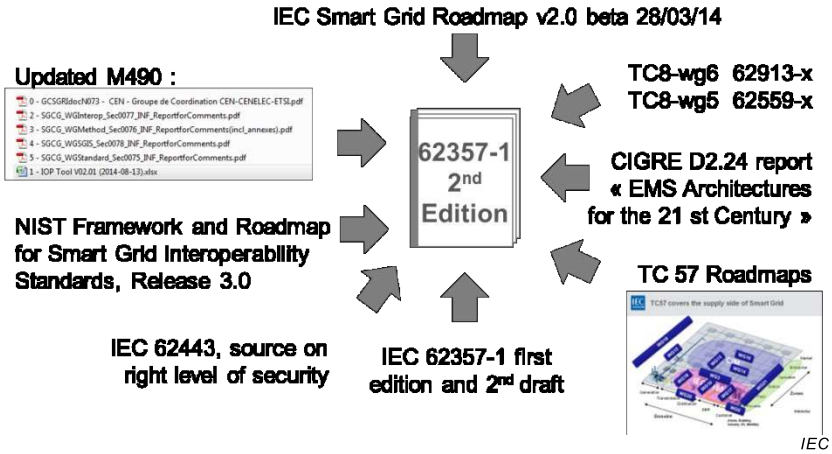


Figure 4 – Relevant sources for IEC TR 62357-1:2016

Refer also to the bibliography.

6 Reference Architecture

6.1 Underlying methodology

6.1.1 General

The development of system requirements is a key ingredient for the development of information exchange standards for the Smart Grids and their Markets. Identifying the actors of and their interactions within Smart Grids and Markets is an important step therein from the market level to the technology level.

Power system management distinguishes between electrical process and information management. These viewpoints can be partitioned into the physical domains of the electrical energy conversion chain and the hierarchical zones for the management of the electrical process (refer to IEC TR 62357-1:2016, IEC TR 62357-200:2015 and IEC 62264-1:2013).

“Zones” illustrate the physical and management aspects of the grid. The notion of zones is derived from IEC 62264-1 manufacturing process interfaces. Zones describe the process hierarchy from the power system through the various entities that participate in the production, transmission, and consumption of electricity.

Applying this concept to the Smart Grids conceptual model allows the foundation of the *Smart Grids Plane* that spans in one dimension the complete electrical energy conversion chain, partitioned into five domains: Generation, Transmission, Distribution, Distributed Energy Resources (DER) and Customers Premises. And in the other dimension the hierarchical levels of power system management, partitioned into six zones: Process, Field, Station, Operation, Enterprise and Market. Figure 5 shows the domains and zones.

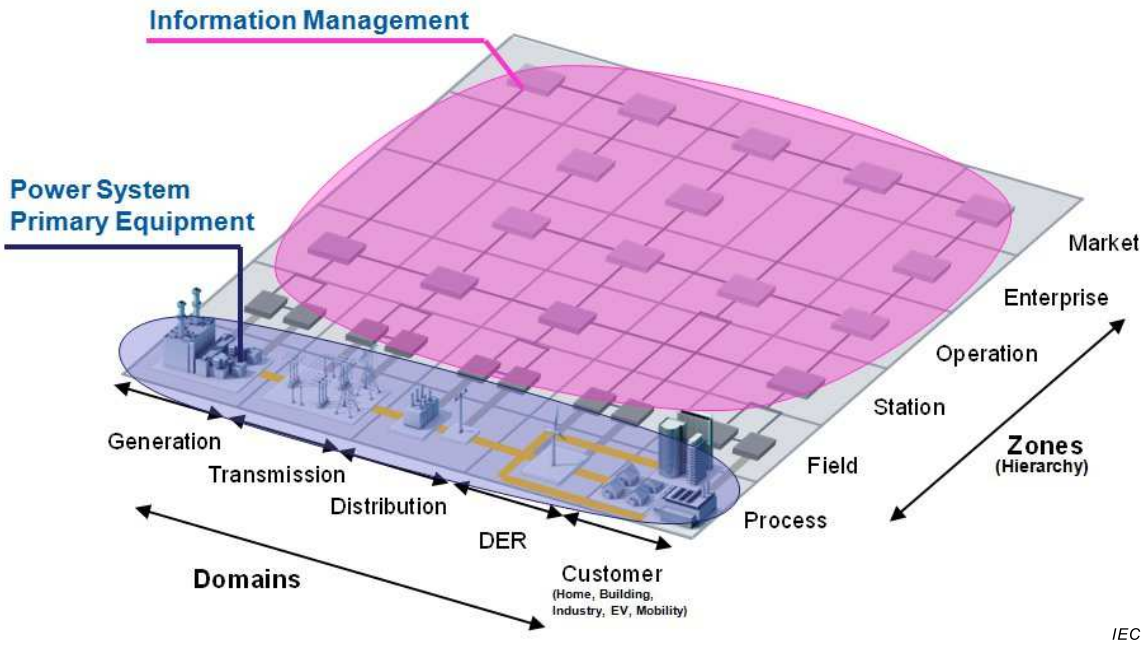


Figure 5 – SGAM plane

6.1.2 The Smart Grids architectural methodology

The Smart Grids is a complex system of systems, serving the diverse needs of many stakeholders. It must support:

- Devices and systems developed independently by many different solution providers
- Many different utilities
- Millions of industrial, business, and residential customers
- Different regulatory environments

Moreover, these systems must work together not just across Smart Grids' technical domains but across stakeholder communities in enterprises which are not part of the existing utility industry. Achieving interoperability in such a massively scaled, distributed system requires architectural guidance, which is provided by SGAM described in this clause/subclause?.

Interoperability as a key enabler for Smart Grids is inherently addressed in SGAM by the five superimposed layers Component, Communication, Information, Function and Business. It aims at decomposing the Electric Power System by interoperability layers, Domains, and Zones as depicted in Figure 6:

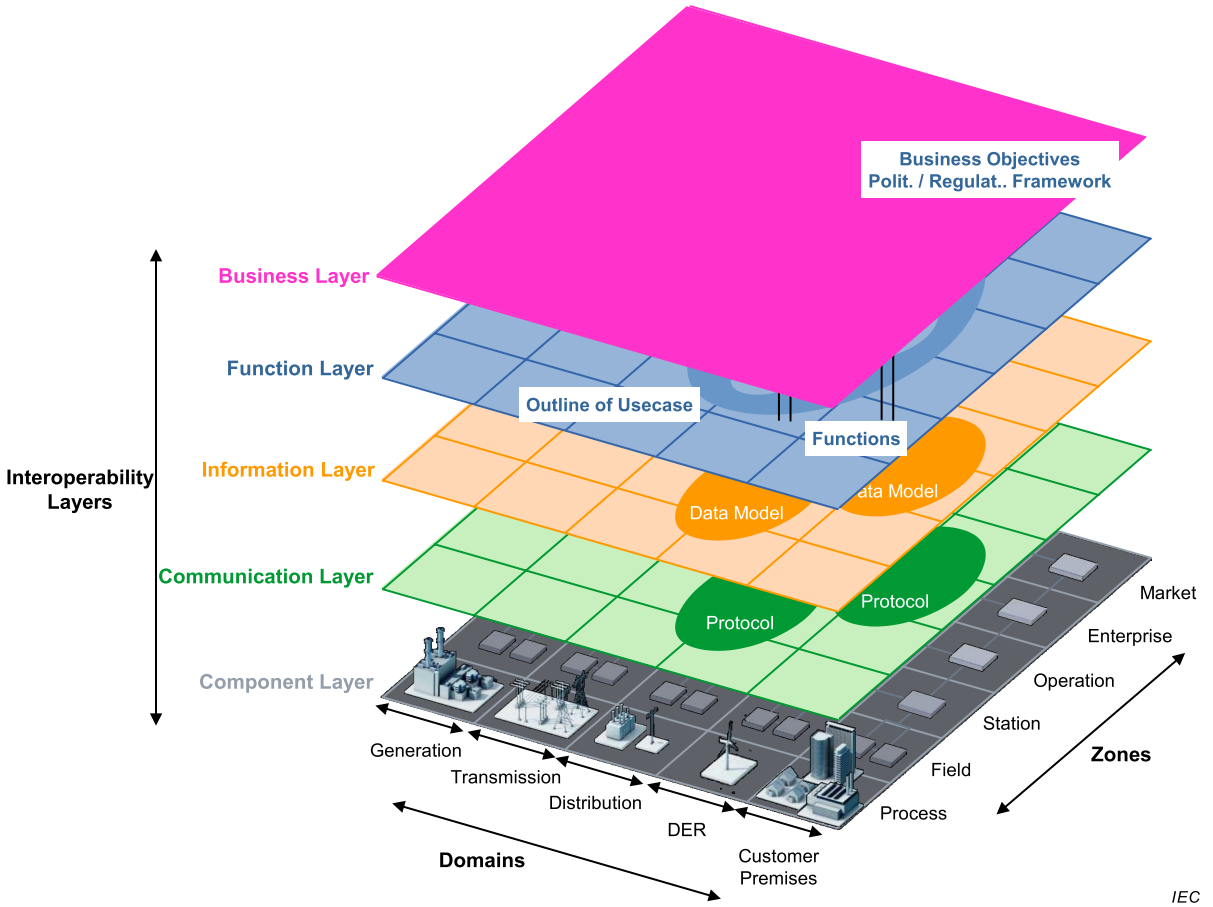


Figure 6 – SGAM Model

The SGAM is a template for architects to follow while building aspects of a Smart Grids architecture, regardless of an architect's speciality (such as in areas of transmission, distribution, IT, back office, communications, asset management, and grid planning).

The SGAM Interoperability Layers allow the modelling of different views from business as well as technical viewpoints. On the business layer SGAM can be used to map regulatory and economic (market) structures and policies, business models, business portfolios (products and services) of market parties involved. Also business services and processes can be represented in this layer. In this way it supports business executives in decision making related to (new) business models and specific business projects (business case) as well as regulators in defining new market models.

The business perspective is modelled in SGAM on the first upper layer:

- The Business layer represents business models and regulatory requirements.

The technical perspectives are modelled in SGAM on the four lower layers:

- The Service/Function layer (OSI 6/7) describes functions and services including their relationships following business needs. Functions are represented independent from their physical implementation in systems or devices (implementations are represented in the component layer).
- The Information layer describes the information that is being used and exchanged between functions. It contains information objects and the underlying canonical data models.

- The emphasis of the Communication layer is to describe mechanisms and protocols for the interoperable exchange of information between functions.
- Finally, the Component layer shows the physical distribution of all participating components. This includes power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches) and any kind of computers. For a specific implementation of a use case the identified functions can be mapped onto components complementing the relationships between all layers.

6.1.3 SGAM levels of abstraction

This subclause provides an overview for each interoperability layer in the SGAM on different levels of abstraction on which a SGAM analysis can be applied. These SGAM analysis patterns are intended to provide guidance on how to model with the SGAM on a level of abstraction chosen, starting from a concept up to a detailed level required for implementation. There can be different abstraction levels defined for each layer. Ideally a fixed number of abstraction levels are defined per SGAM layer including respective concepts that are relevant in a specific SGAM development iteration. In addition to that, there could also be interrelations between the abstraction levels on different layers. However, generally the number of abstraction levels depends on the purpose of the modelling effort/project and interrelations between abstraction levels must not necessarily exist.

An overview of exemplary abstraction levels is given in Figure 7. Each layer therein depicts some concepts (examples) used in steps of successive model refinements that can be carried out on the respective interoperability layer. The identification may then finally support a definition of interoperability requirements. The abstraction levels on different layers depicted in Figure 7 do not necessarily relate to abstraction levels on the same level of abstraction on other layers.

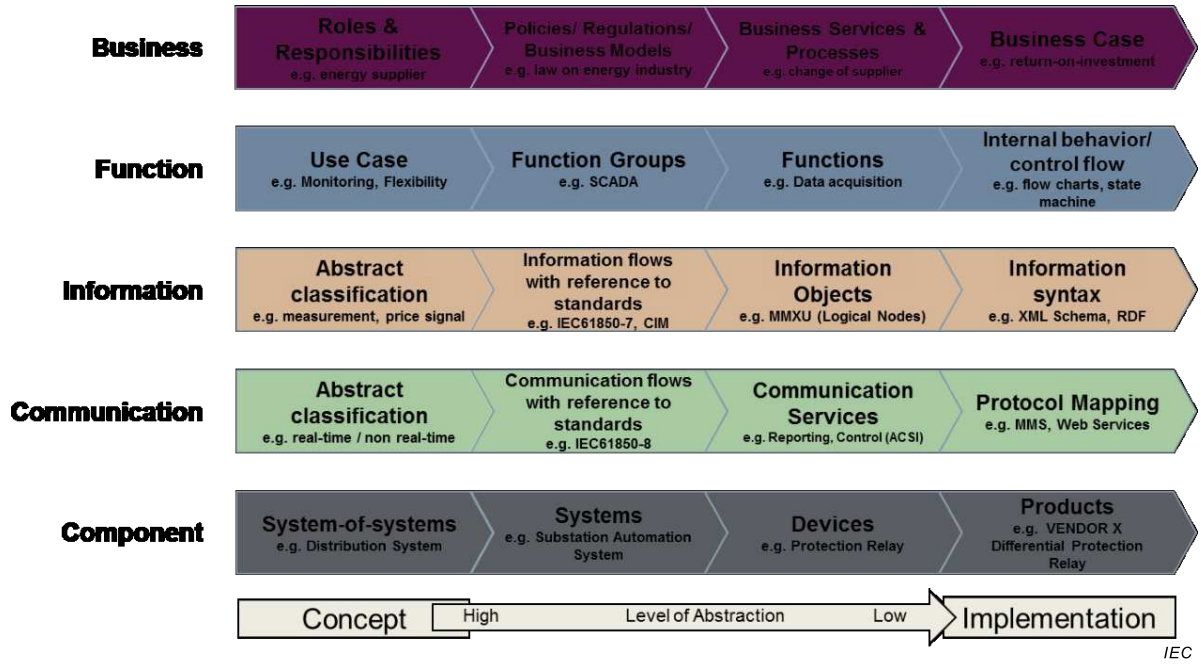


Figure 7 – SGAM levels of abstraction

Complete description of SGAM and SGAM usage can be found in SG-CG/F] SG-CG/M490/C_ Smart Grids Reference Architecture, [SG-CG/F] SG-CG/M490/F_ Overview of SG-CG Methodologies.

6.1.4 The use case methodology

According to IEC TR 62390:2005, a use case is a “class specification of a sequence of actions, including variants that a system (or other entity) can perform, interacting with actors of the system”. The concept has been further defined by IEC 62559-2 as “a specification of a set of actions performed by a system which yields an observable result that is of value for one or more actors or other stakeholders of the system”. In other words, it describes, in text format, how one or several actors interact within a given system to achieve goals. In order to clearly explain the definition, it seems important to further detail the different concepts used.

The notion of ‘Role’ is fundamental in the use case methodology. A role may be defined as “an intended behaviour of a business party”[5]. It is associated with responsibilities. A business party, when carrying out a business transaction, takes on a certain role. According to European Network of Transmission System Operators for Electricity (ENTSO-E) Role Model (ENTSO-E, European Federation of Energy Traders EFET, and European forum for energy Business Information eXchange ebIX, 2011), “the objective of decomposing the electricity system into a set of autonomous roles and domains is to enable the construction of business processes where the relevant role participates to satisfy a specific transaction (service). Business processes should be designed to satisfy the requirements of the roles and not of the parties.”

Roles should be differentiated from Actors, which are more general and include Roles, information systems, or devices.

- An actor can be defined as anyone or anything with behaviour. It can include:
  - Roles, which are the external intended behaviour of a business party which cannot be shared – examples: Distribution System Operator, Grid User, DSO Network development unit;
  - Persons – examples: SCADA operator;
  - Information Systems – examples: SCADA, Active Demand Management System;
  - Physical components – examples: Energy Storage, network captor.
- The system defines the scope of a use case or a set of use cases, i.e. its boundaries. It can be an organisation, a project, or an information system for instance.

Use cases are above all a textual description. Existing literature on the methodology has provided several use case templates. The use case template proposed by IEC 62559-2:2015 is the most widely accepted within the Smart Grids community. Any Smart Grids project can use this template to describe its Business Use Case as well as its System Use Case.

Use cases literature (Cockburn, 2001) highly recommends distinguishing different levels of goals. Indeed, goals the actors are pursuing are not necessarily on the same level, some being very high-level and others really specific, related to the task the user of a system may perform. In order to structure these goals in a consistent way and avoid producing use cases which do not have the same granularity and/or overlap, the literature has identified two types of use cases, corresponding to two levels of details:

- Business Use Cases describe business processes and their associated requirements, which are included in the present document,
- System Use Cases detail functions or sub-functions supporting the business processes, and their associated requirements.

Table 1 highlights the differences between these two types of use case.

5 SG-CG/M490/C:2012-12.

Table 1 – Business and System Use Case

	Description	Involved actors
Business Use Cases	A business process implementing a service	Roles (organisations or organisational entities)
System Use Cases	A function or sub-function supporting one or several business processes	Systems and Persons (operators of an information system)

In Business Use Cases, aspects related to technology are treated using a 'black-box' approach, i.e. by focusing on the functions required to enable / execute the business process and their associated requirements – the 'what' –, but not on their implementation from a technical perspective – not the 'how'. By describing business needs and business rules related to the activities of a business process,

Business Use Cases writers contribute to define requirements which might impact the tools or systems needed to implement the identified functionalities. However, they "must never pre-empt designers and try to use the use-case model to design the system" (Bittner and Spence, 2003). In other words, Business Use Cases should not describe solutions, but only express requirements.

Based on the SGAM method and according to the literature on use case methodology:

- Business Use Cases describe Business Processes and their activities/steps (Business Layer), their execution within different Domains and Zones, as well as their interactions with Functions (Function Layer);
- System Use Cases describe Functions (Function Layer) supporting the Business Processes described on the Business Layer and their interactions with data models (Information Layer), protocols (Communication Layer), and components (Component Layer).

A business-driven and top-down approach to describe new and relevant business processes of the electric power system impacted by Smart Grids technologies from which details on the needed Smart Grids functions supporting these processes are given. These requirements will serve as input for the development of Smart Grids standards (data models, protocols etc.), like the ones developed by the IEC.

Figure 8 shows the interactions between the Business and Function layers and their associated concepts – roles, services, business processes, activities, functions and systems.

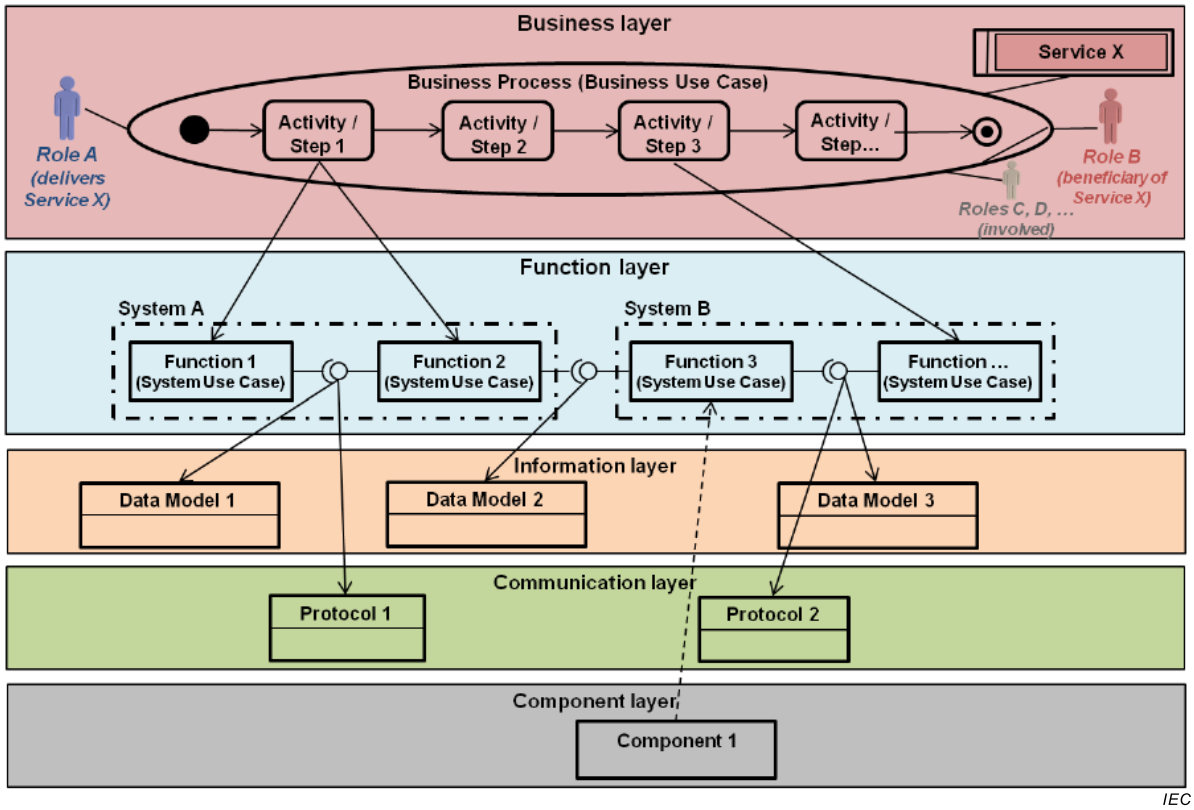


Figure 8 – Interactions between the Business and Function layers

A generic actor list, derived from generic use cases, includes the role-actor relationships. This supports the analysis of the business context when defining requirements of Smart Grids systems from use cases, as the first step towards standards. Moreover, it ensures the required applicability of standards based on these requirements in all market models.

In 2012, SG-CG/F] SG-CG/M490/E_ Sustainable Process Annex A proposed a list of Actors. NIST SGIP consolidated an actor list. IEC Smart Energy System Committee WG6 will provide a consistent list of actors, in coordination with other IEC technical committees.

The system use cases which are developed at the functional layer will have to be developed according to the Interface Reference Model concept defined by IEC 61968-1, and which is going to be extended to new Smart Grids business domains.

Complete description of Use Case methodology can be found in IEC 62913-1, and "SGCG/M490/K_SGAM User Manual", 6.2.

6.1.5 Data modelling

Because of the increasing need of Smart Grids stakeholders, to deploy solutions offering a semantic level of interoperability, data modelling appears as the corner stone and foundation of the Smart Grids framework.

In addition data modelling seems much more stable than communication technologies, which makes this foundation even more important.

Currently the IEC framework relies on three main pillars, as far as data modelling is concerned, represented in Figure 9.

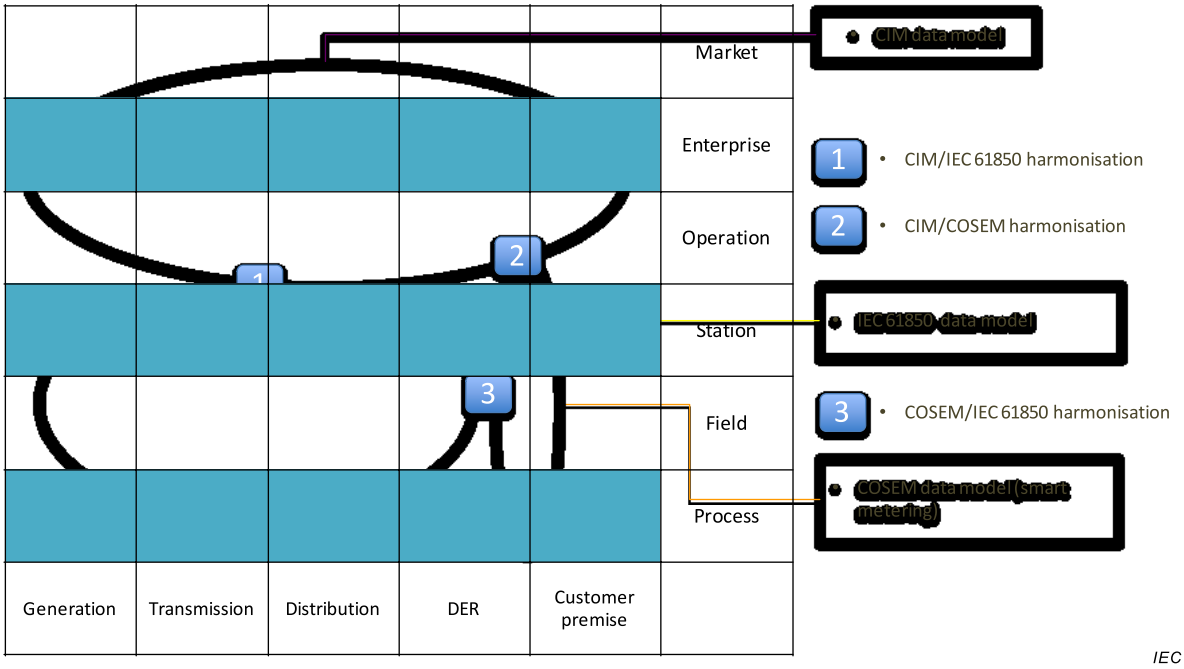


Figure 9 – Data modelling and harmonization work mapping

CIM (IEC 61970, IEC 61968, IEC 62325) provides the information model containing equipment and functions and their properties for power system management, analysis and related use cases (Generation, market and grid).

The Companion Specification for Energy Metering (COSEM) provides the information model containing equipment and functions and their properties for metering and related use cases.

Figure 9 also represents the three harmonisation works (i.e. the definition of unified shared semantic sub-areas, or formal transformation rules) which need to be performed in order to allow an easy bridging of these semantic domains:

- Harmonization between CIM and IEC 61850, mostly to seamlessly connect the field to operation and enterprise level[6]
- Harmonisation between CIM and COSEM, mostly to seamlessly interconnect electricity supply and grid operation[7]
- Harmonisation between COSEM and IEC 61850, where smart metering may co-habit with Power Utility Automation systems[8]

6.1.6 Profiling methodology

A profile is a specification that governs information exchanged within a specific business exchange context. Profiles can be developed to serve the information needs of specific user groups. These user groups can be diverse and can be characterized either by geographic context or by application domain. Examples of such user groups could be for instance regional or country specific. Individual companies i.e. utilities or manufacturers can also develop their own profiles, as subsets of the more generic profiles of a user group.

6 See IEC 62361-102.

7 See IEC 62056-6-9.

8 See IEC TS 61850-80-4.

One of the most important purposes of a profile is to help improve interoperability between systems. By adopting and implementing an accepted profile, one is, in a sense, entering into an informal agreement with entities that have adopted the same profile. Adopting a profile means increasing the possibilities for seamless information exchange and interoperability between systems. Open standards sometimes can be vague or have ambiguous specifications; the use of profiles can enforce one possible interpretation.

As an example, related to the CIM environment, each noun used in a 61968 message identifies a payload type. Payload types are typically derived from the IEC CIM or other semantic models. Payload types used by the parts of IEC 61968 are always derived from the IEC CIM and have design artefacts (e.g. XML Schema Definition XSDs) that describe their structure. Cases where XSDs are not required include:

- Messages using Resource Description Framework (RDF) payloads as defined by IEC 61968-13 and the IEC 61970-45x series.
- Response messages from services that dynamically generate XML (as in the case of SQL XML result sets).
- Non-XML compressed and encoded payloads.
- Encoded binary data (where XML formatting is not efficient as in the case of 'high speed data')

If an XSD is not available to describe the payload, it is the responsibility of the sender and receiver(s) to agree upon the specific formatting.

The CIM logical information model is described as a set of UML packages. The diagram in Figure 10 shows the use of the CIM from the perspectives of UML modelling and generation of design artefacts needed by integration tools. It illustrates the relationships between information models and contextual profiles that are used in conjunction with assembly rules in order to derive design artefacts.

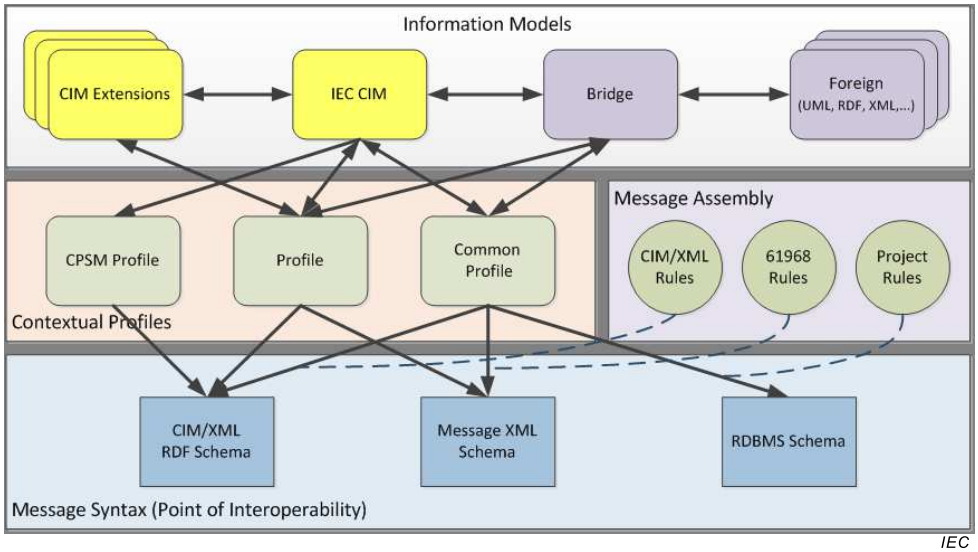


Figure 10 – Information Models, Profiles and Messages

Profiling is also envisaged with IEC 61850, COSEM, etc.

6.2 Reference Architecture overview

Using SGAM Domain & Zones, Figure 11 describes TC 57 standards, with some other TC related standards (TC 13 for Smart Metering Systems, TC 69 for electro-mobility).

The Reference Architecture is based on the “Elements” (blue and red bordered boxes) and the “relationships / interactions” between the “Elements” mirrored on use cases. Elements and relationships have been mapped to SGAM domains and zones in Figure 11.

The Reference Architecture covers e the information and communication layer in a high level abstraction view.

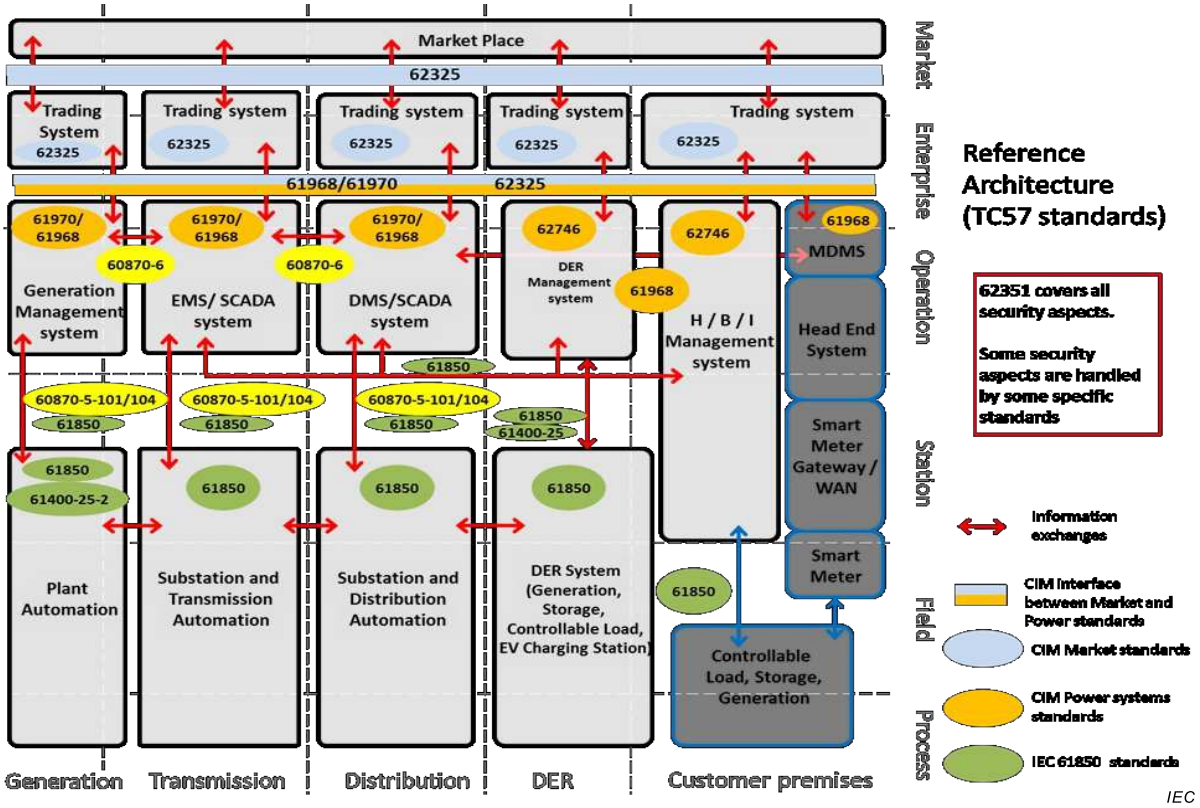


Figure 11 – Reference Architecture

Complementary standards are proposed by the IEC or other organisations. See D12 for a list of some of these complementary standards.

6.3 Elements of Reference Architecture

6.3.1 General

Figure 12 describes the power systems related standards that will be used by some of the following elements:

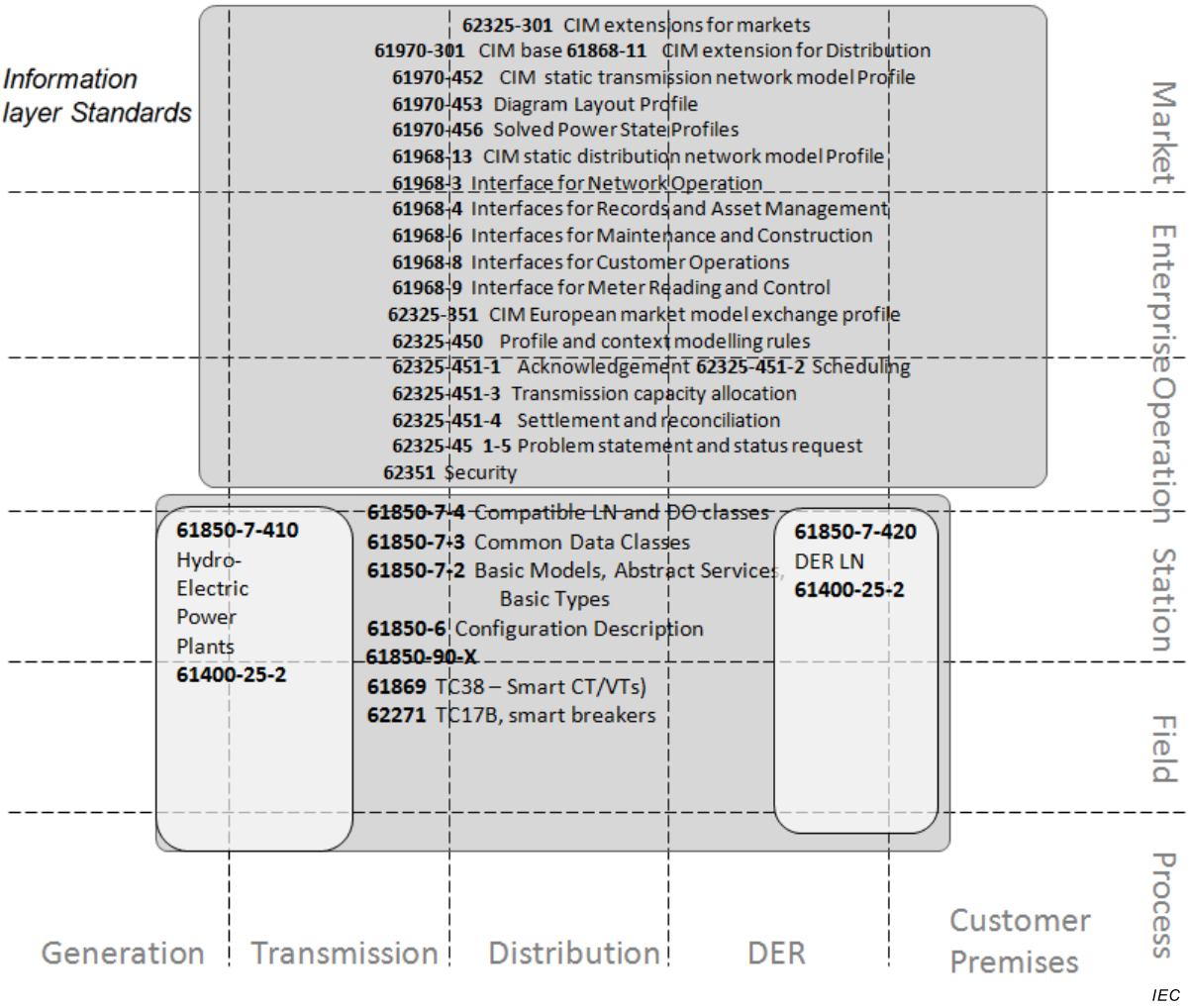


Figure 12 – Power systems information related standards

The following parts of IEC 62351 define security information elements like a MIB or a credential:

- IEC TS 62351-7: definition of information elements for network management in terms of (system or security) events (Management Information Base MIB-elements) Transport of these elements based on mapped protocols, IEC TS 62351-7 focusses on Simple Network Management Protocol (SNMP)
- IEC TS 62351-8: Information element for carrying role information to be used for role-based access control (basically an extension to X.509 certificates) Transport of this information is also targeted in IEC TS 62351-8
- IEC 62351-9: Information elements in terms of certificates needed for authentication described also the handling of certificates

Other parts of IEC 62351 (3, 4, 5, 6, 11) simply use them to achieve a dedicated protection goal.

6.3.2 Elements as Interface Reference Model abstract components

Various organizations cooperate to perform the planning, design, construction, operation, management and use of the Smart Grids. This segmentation by business function is provided

in the Interface Reference Model (IRM) standard (IEC 61968-1). The IRM for Distribution[9] is presented in Figure 13:

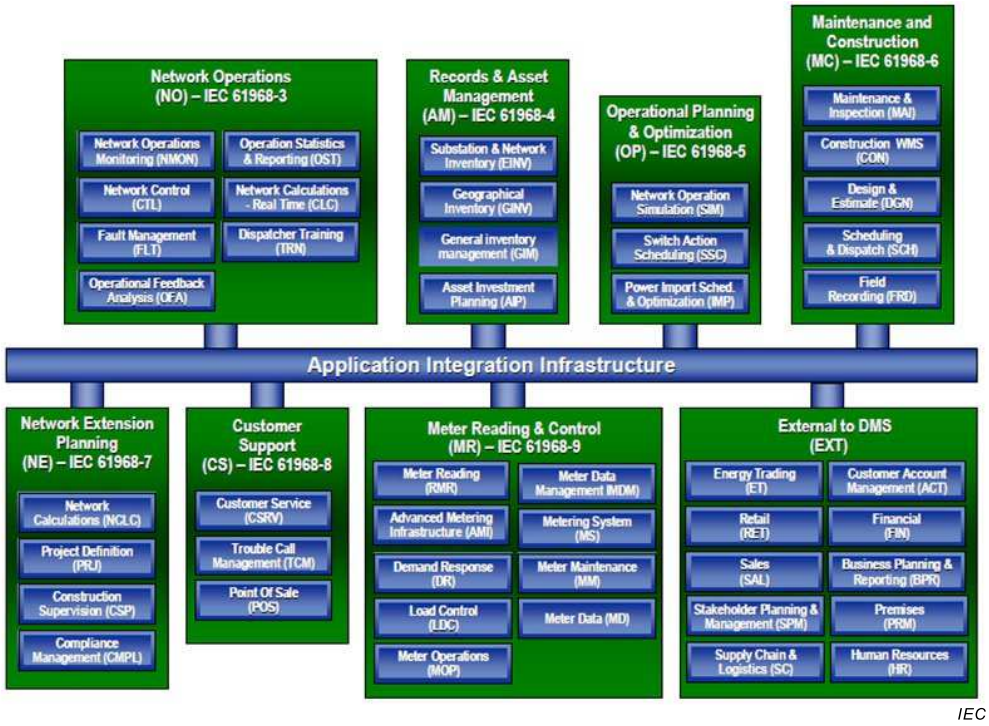


Figure 13 – Distribution IRM Model

In addition to providing an organizational framework for defining industry information exchange standards, use of a business-related model helps ensure independence from vendor-produced system solutions.

It is expected that a concrete (physical) application will provide the functionality of one or more abstract (logical) components as listed in IEC 61968-1. These abstract components are grouped by the business functions and sub-functions of the IRM. In the IEC 61968 series, the term abstract component is used to refer to that portion of a software system that supports one or more of the interfaces defined in the CIM-based standards. It does not necessarily mean that compliant software is delivered as separate modules.

Some abstract components may be used by several different business functions. For example, a component like power flow can be used for network operation, short term operational planning and optimization, and long term network extension planning. Much of the information exchanged for power flow purposes in each of these areas will therefore use many of the same Information Exchange Message Types.

Applications from different vendors package the functionality of these abstract components in different ways. To use the IEC 61968 services, each application must support one or more of the interfaces for the abstract components.

When the functions are implemented this lead to Application, when the applications are distributed on components this lead to Systems. The “IEC Mapping Tool” is a concrete example as described in http://smartgridstandardsmap.com/.

9 IRM is extended for Transmission and Markets.

As another example, as described in M490 C-Reference Architecture, Figure 14 illustrates the flexible assignment of element, as functions, to SGAM segments.

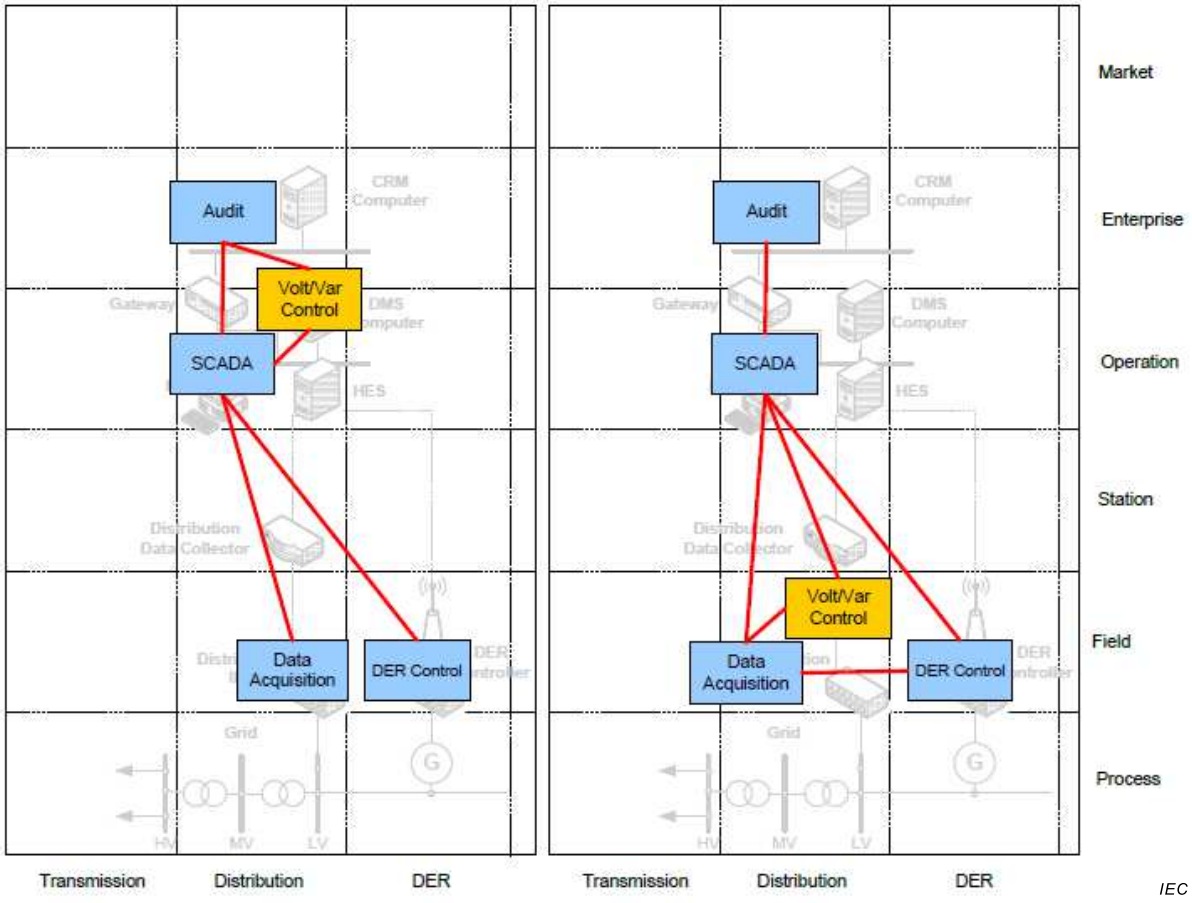


Figure 14 – Flexibility for assignment of element "Volt/Var Control" to SGAM segments (M490 C-Reference Architecture)

6.3.3 Elements as some typical Smart Grids Systems

Some typical Smart Grids systems are described in SGCG/M490/G as follow, and a list of Smart Grids components (SGCG/M490, Table 12) is provided in Figure 15.

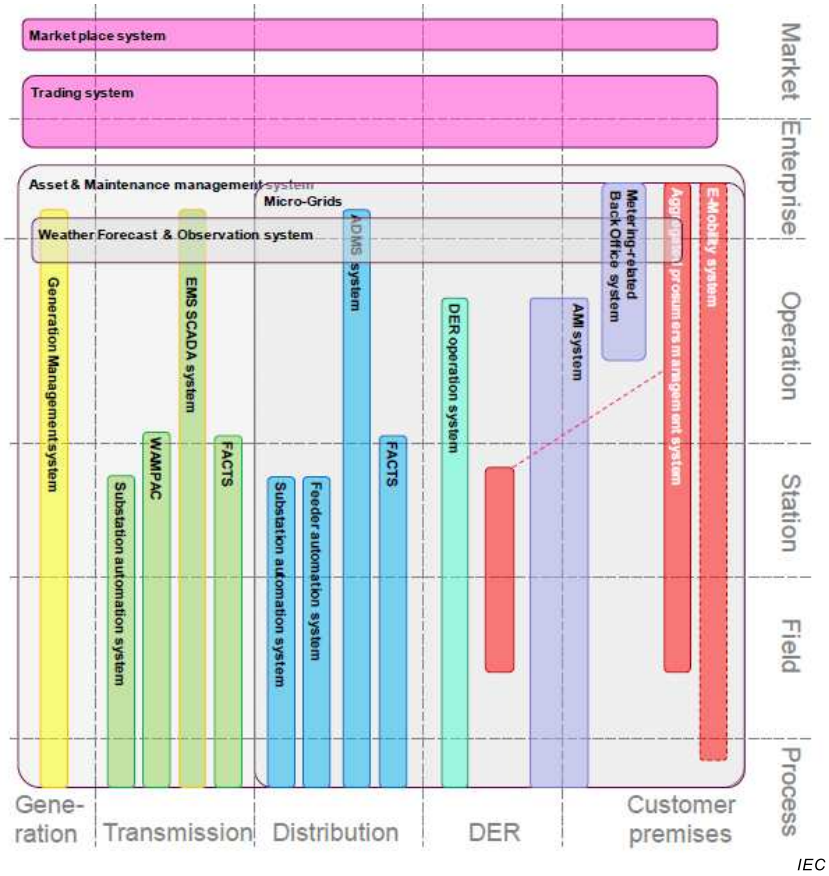


Figure 15 – SGCG/M490 Smart Grids systems on SGAM Plane

Some use cases will refer to IRM abstract components, as others will be application use cases and will use system names like SCADA, Geographic Information System (GIS), Training System, Reliability System and Advanced Metering Manager (AMM), etc. It is recommended to use IRM abstract component terms as it provides an abstraction layer. The IEC has mapped its IRM abstract components to typical system actors.

6.3.4 Elements as 61850 Intelligent Electronic Devices

The IEC 61850 information model is based on two main levels of modelling – explained below:

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

Figure 16 shows an example of how each level is included into the upper layer.

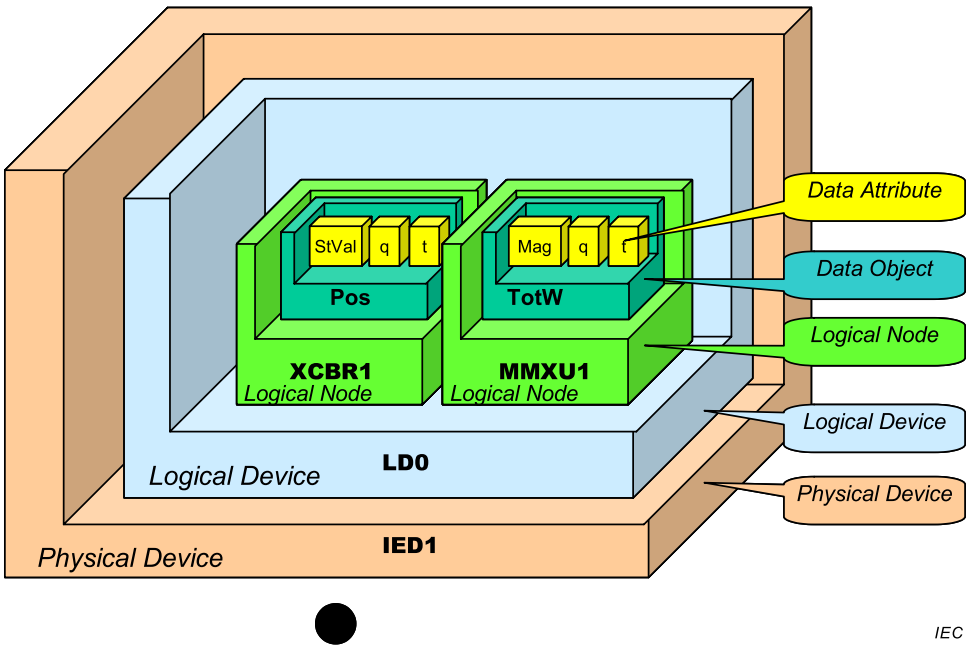


Figure 16 – IEC 61850 Data Modelling

The approach of IEC 61850 as defined in IEC TR 61850-1 is to decompose the application functions into the smallest entities which are used to exchange information. The granularity is given by a reasonable distributed allocation of these entities to dedicated devices (IED).These entities are called Logical Nodes (for example, a virtual representation of a circuit breaker class, with the standardised class name XCBR). Other examples may be a distance protection function, PDIS or a measurement value, MMXU. The logical nodes are first defined from the conceptual application point of view in IEC 61850-5 and then modelled in Parts 7-4 and 7-4xx.

Then several logical nodes comprise a logical device as defined above (for example, a representation of a Bay unit). Based on their functionality, a logical node contains a list of data (for example, position) with dedicated data attributes. The data have a structure and a well-defined semantic and are fully defined in IEC 61850-7.

The different elements are also related to security in terms of access protection. Role-based Access Control (RBAC) as defined in IEC TS 62351-8 is related to logical devices and data objects. A subject (client) is identified by the authentication parameters passed to the IEC 61850 server. Based on these parameters a session is established. Based on the role, a subject shall then be permitted access to an IEC 61850 data object simply if the required access right (of that data object) is associated with at least one of the roles used in the current session. There are two areas in which access control shall be applied according to IEC TS 62351-8, the service-access-point (logical device) and data objects.

Other elements are described in 7.1.2.

6.4 Relationships of Reference Architecture

6.4.1 General

Relationships in the context of the Reference Architecture mean interaction; an interaction of two or more functions is indicated by a connecting line between these functions. Interaction is realized by information exchange via the interfaces of functions and communication: information exchange between elements.

Relationships, or interaction, between elements can be explained through use cases.

Transmission and Distribution domains relationships can be structured as follows:

The functions of a substation automation system may be allocated logically on three different levels (station, bay/unit, or process). These levels are shown by the logical interpretation of Figure 17 together with the logical interfaces 1 to 11.

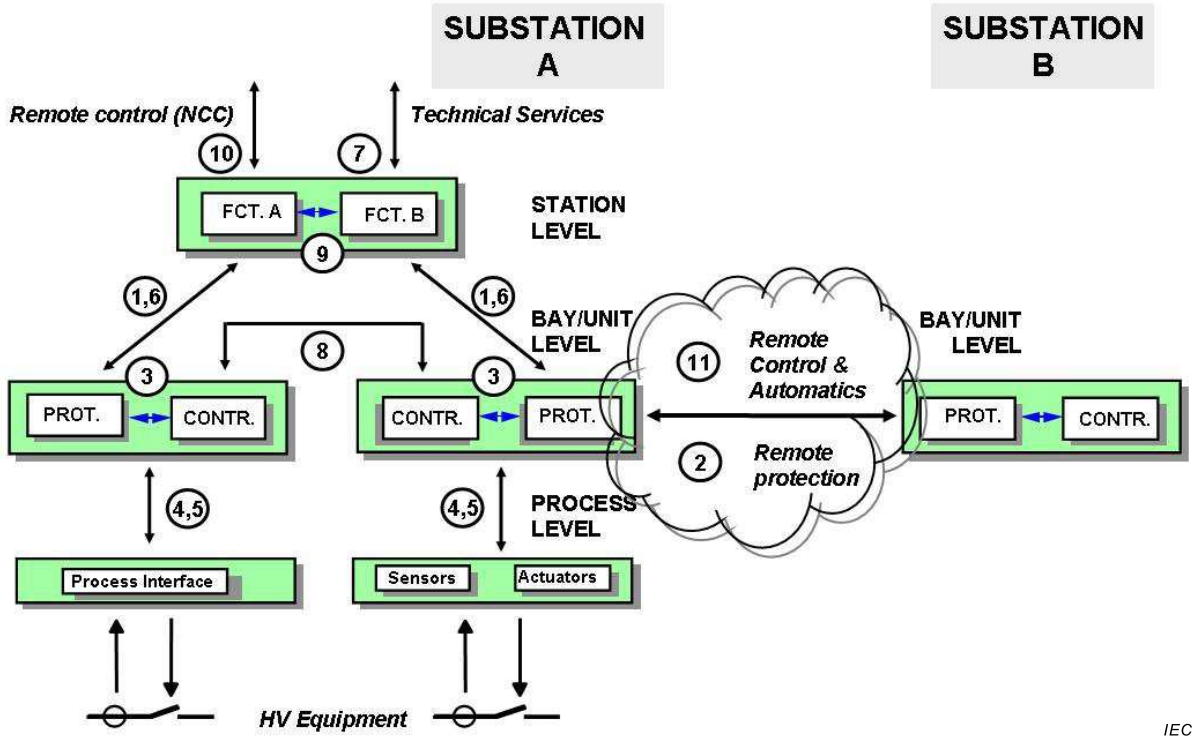


Figure 17 – Functions of a substation automation system allocated logically on three different levels (station, bay/unit, or process)

The interfaces 1, 3 to 6, and 8 to 9 are connecting functions of the substation automation system inside the substation. Interface 10 represents as TCI (telecontrol interface) the communication of the SA system to the remote control centre, interface 7 represents as TMI (telemonitoring interface) the communication to remote engineering, monitoring and maintenance places. Interface 2 represents as TPI (teleprotection interface) the protection related function between substations, interface 11 represents the same for control related functions.

The list of interfaces is described as follow:

- IF1: protection-data exchange between bay and station level
- IF2: protection-data exchange between substations. This interface refers both to analog data e.g. for line differential protection and binary data e.g. for line distance protection
- IF3: data exchange within bay level
- IF4: Current transformer (CT) and Voltage Transformer (VT) instantaneous data transport (especially samples) from the process to the bay level. This comprises in the reverse direction also the protection trip
- IF5: control-data exchange between process and bay level
- IF6: control-data exchange between bay and station level
- IF7: data exchange between substation (level) and a remote engineer's workplace
- IF8: direct data exchange between the bays especially for fast functions like interlocking
- IF9: data exchange within station level

- IF10: control-data exchange between the substation and remote control centre(s)
- IF11: control-data exchange between substations. This interfaces refers to binary data e.g. for interlocking functions or inter-substation automatics

Figure 18 describes the IEC 61850 communication standards.

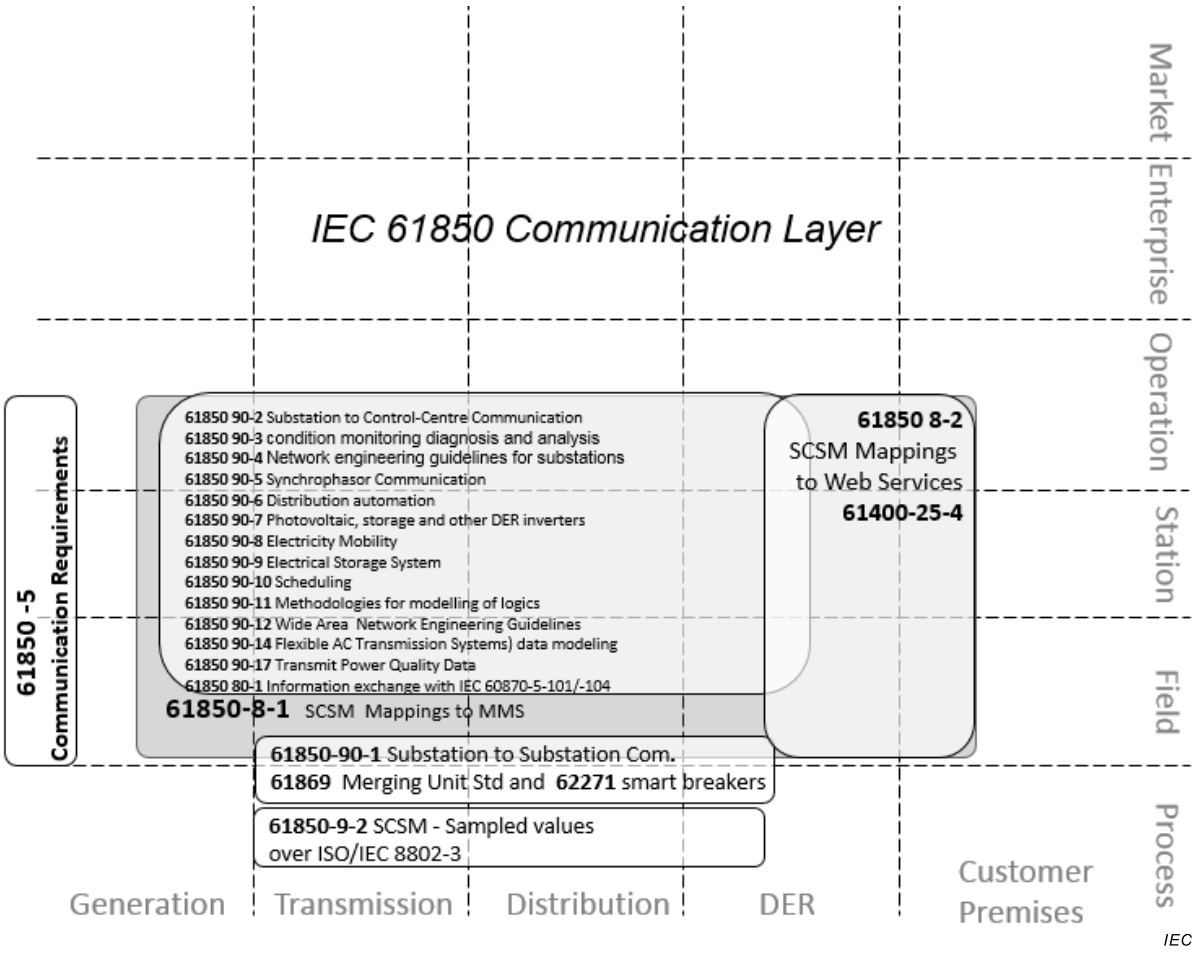


Figure 18 – IEC 61850 related standards

6.4.2 Communication inside substation

IEC 61850 Parts 1 to 10

Communication protocols, described in Figure 19, can be used either:

- Within the substation, IEC 61850-8-1 (for any kind of data flows except sample values) and IEC 61850-9-2 (for sample values) are used to support the selected set of High level use cases. IEC TR 61850-90-4 provides network engineering guidelines for communication inside a substation (automated Medium Voltage/Low Voltage MV/LV substations are not really covered yet). IEC 61850 mostly replaces the former IEC 60870-5-103, used for connecting protection relays. In the specific case of automated MV/LV substations, communications are more commonly based on industrial networks.

G_SGCG_Standards_Report_V3.1.pdf, 8.2.1 (Substation Automation System for Transmission and Distribution) describes related standards.

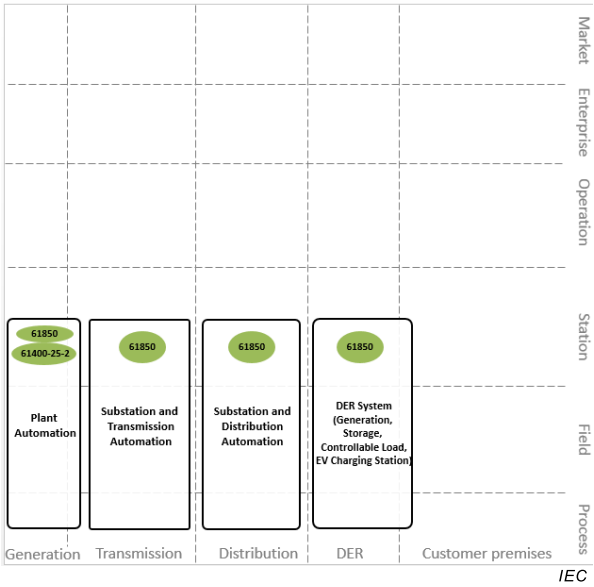


Figure 19 – Communication inside substation

6.4.3 Communication between substations

Horizontal communications may rely on IEC TR 61850-90-5 (full mapping over UDP) or IEC TR 61850-90-1 (tunnelling) or IEC TR 61850-90-12 (wide area network engineering guidelines) as described in Figure 20.

With existing and new applications in the field of the power system operation and protection, the requirement to exchange standardized information directly between substations increases.

IEC 61850 shall be the basis for this information exchange. IEC 61850 provides the basic features to be used for that information exchange, however, some extensions to IEC 61850 may be required.

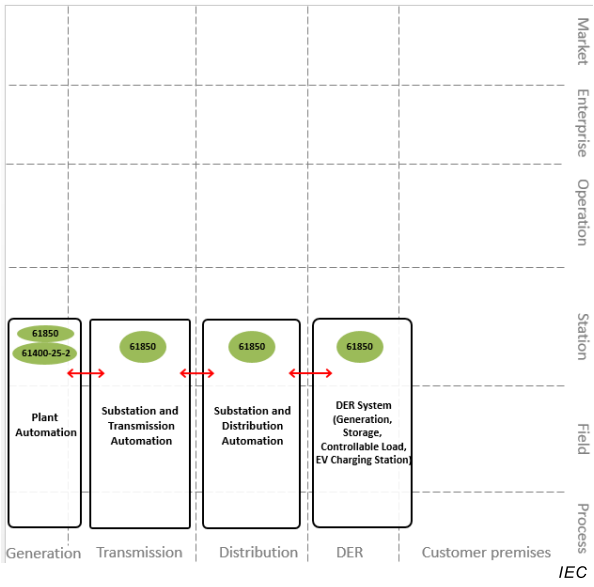


Figure 20 – Communication between substations

The use cases are:

- Distance line protection with permissive overreach tele-protection scheme
- Distance line protection with blocking tele-protection scheme
- Directional comparison protection
- Transfer/Direct tripping
- Interlocking
- Multi-phase auto-reclosing application for parallel line systems
- Current differential line protection
- Phase comparison protection

There are other applications of which the requirement for communication is almost the same as the requirement for current differential protection:

- Fault locator system (2, 3 terminals)
- System integrity protection schemes (SIPS)
- Real time predictive generator shedding
- Out-of-step detection
- Synchrophasors
- Remedial action schemes (RAS)

Refer to IEC 61850 indicated documents for other use cases.

6.4.4 Communication to support distributed automation along the feeder

Medium voltage feeders are largely impacted by the introduction of renewable and/or intermittent sources, especially in low voltage. This leads to many new requirements such as:

- Voltage management along the feeder (possibly down to LV)
- VAR management
- Anti-islanding automation
- (automatic or semi-automatic) Fault location, isolation and service restoration

This appears to be an increasing usage of IEC 61850; well suited to meet these requirements. The upcoming IEC TR 61850-90-6[10] will depict the possible usage of IEC 61850 in that field (associated to some proposed IEC 61850 data model extensions to fully support this application field)

6.4.5 Communication between substation and control centres and between control centres

6.4.5.1 General

Figure 21 describes the telecontrol and control standards used for equipment and systems:

10 Under preparation. Stage at the time of publication: IEC/PWI 61850-90-6:2016.

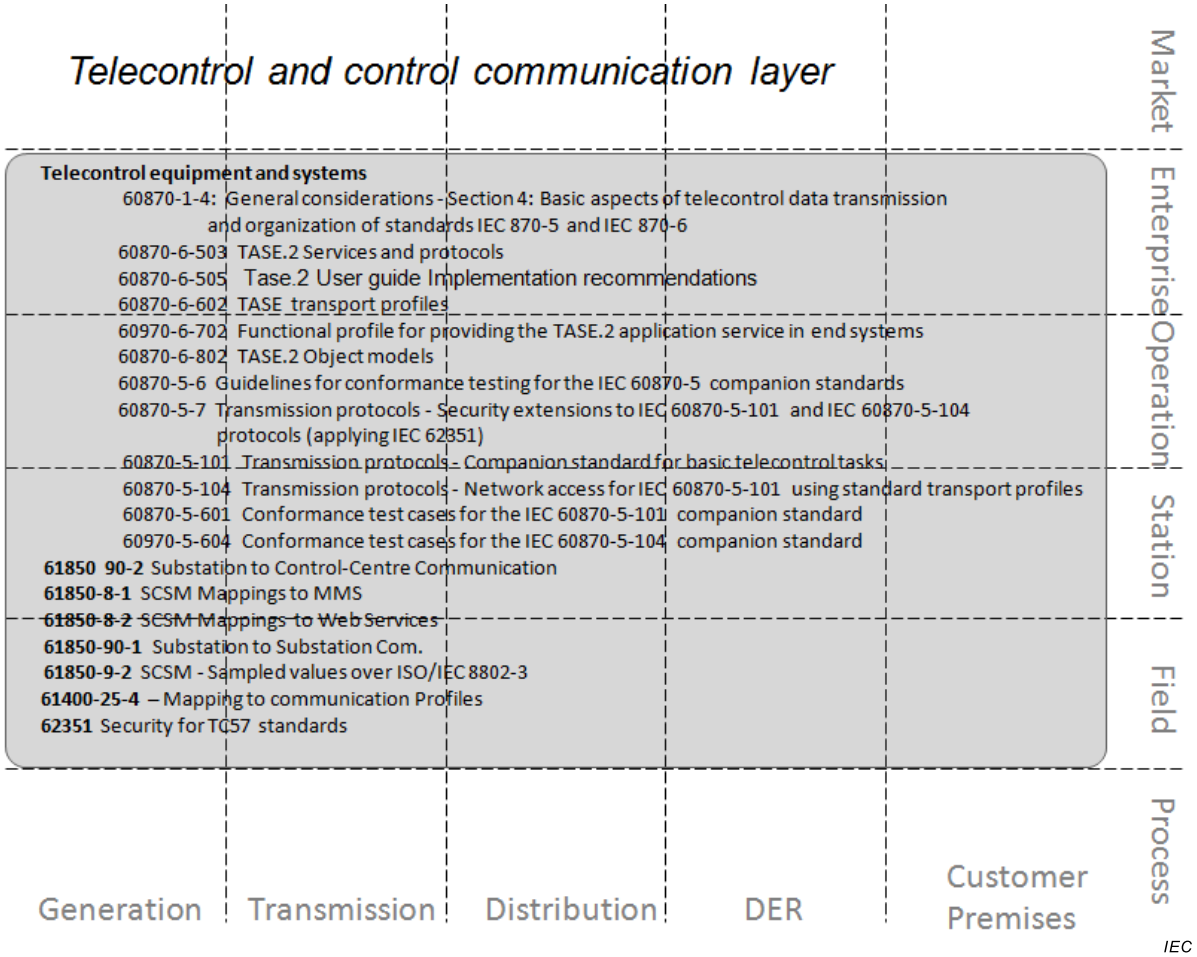


Figure 21 – IEC 61850 Telecontrol and control equipment and systems related standards

6.4.5.2 Communication between substation and control centres

Conventionally, vertical communications rely on IEC 60870-5-101 or IEC 60870-5-104 (see Figure 22).

Future vertical communication may rely on IEC TR 61850-90-2 (guideline for using IEC 61850 to control centres) to provide a seamless architecture, based on IEC 61850.

A new mapping of IEC 61850 over the web services technology (IEC 61850-8-2)[11] is under specification, in order to enlarge (in security) the scope of application of IEC 61850 outside the substation, while facilitating its deployment.

IEC TR 61850-90-12 (wide area network engineering guidelines) and associated use cases shall also be considered.

11 Under preparation. Stage at the time of publication: IEC/ACDV 61850-8-2:2016.

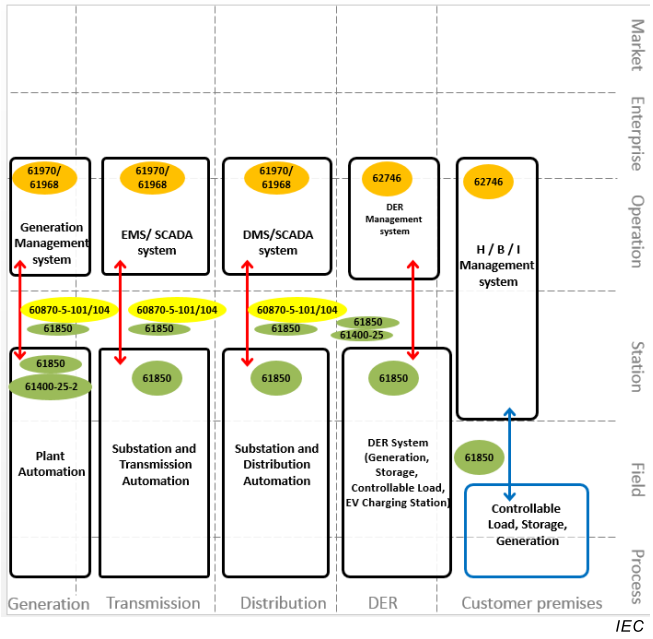


Figure 22 – Communication between substation and control centres

6.4.5.3 Communication between control centre

IEC TR 60870-6 Telecontrol Application Service Element TASE.2

G_SGCG_Standards_Report_V3.1.pdf, 8.2.3 (Energy Management System EMS SCADA System), 8.3.3 (Advanced Distribution Management System), 8.7.2 (Trading System) refers to IEC 60870-6-503 (see Figure 23).

IEC TR 61850-90-12 (wide area network engineering guidelines) and associated use cases shall also be considered.

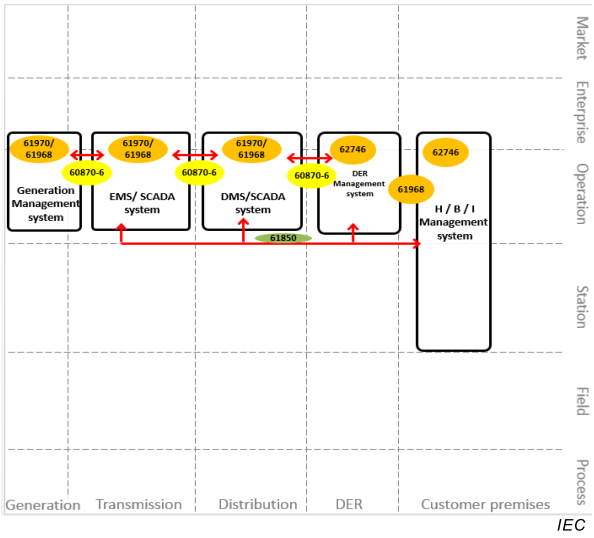


Figure 23 – Communication between control centre

6.4.6 Communication at the enterprise level

6.4.6.1 General

Figure 24 describes the communication standards used at the enterprise level:

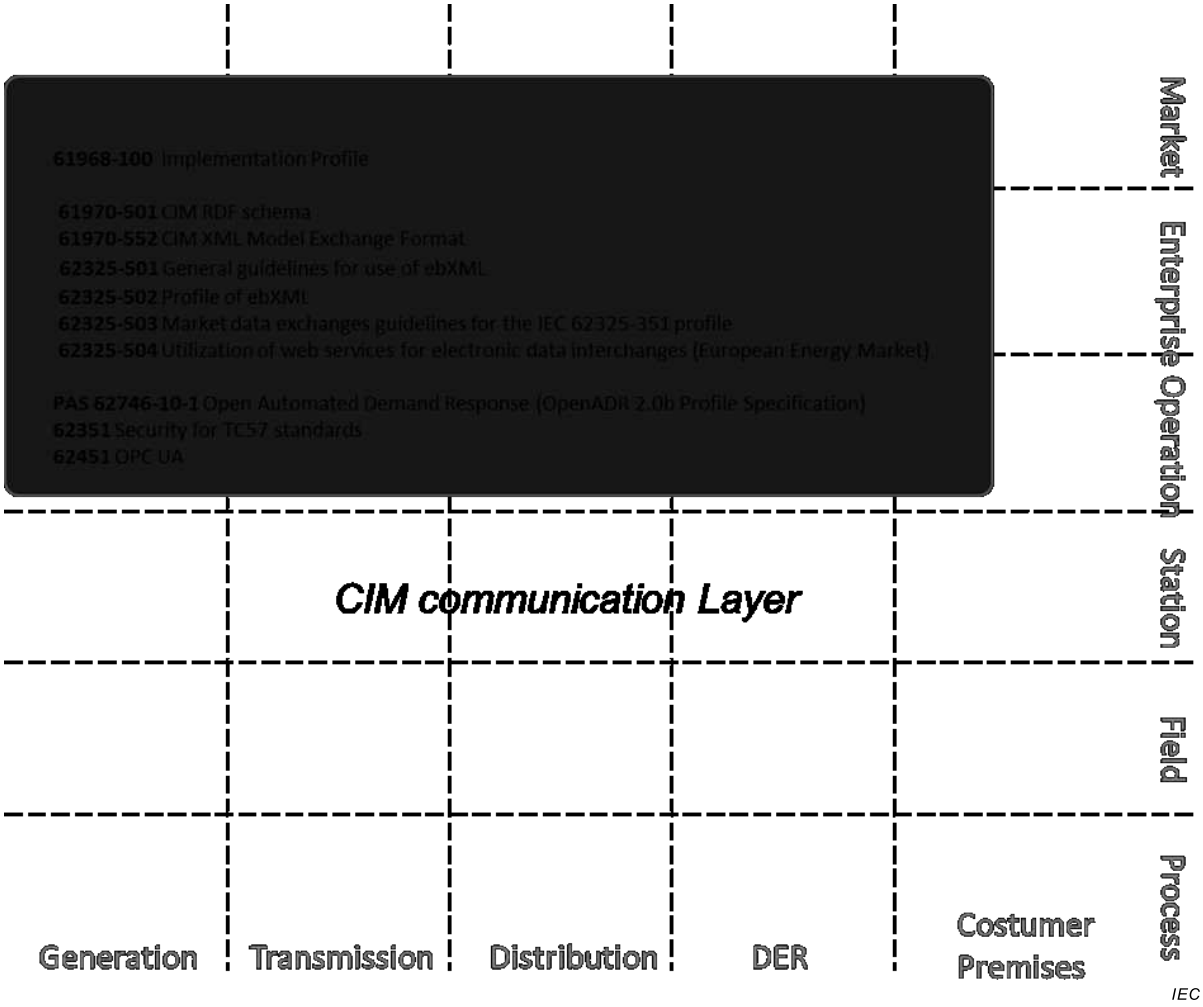


Figure 24 – CIM Communication layer standards

Other communication standards such as IEC 62541 can also be used.

6.4.6.2 Communication inside control centres (Distribution Management SystemDMS, EMS)

- IEC 61970 Transmission
- IEC 61968 Distribution
- IEC 62325 Market

This communication will leverage IEC 61968-100.

IEC 61968-100 specifies an implementation profile for the application of the other parts of IEC 61968 using common integration technologies, including JMS and web services. This International Standard also provides guidance with respect to the use of Enterprise Service Bus (ESB) technologies. This provides a means to derive interoperable implementations of IEC 61968-3 to IEC 61968-9. At the same time, this International Standard can be leveraged beyond information exchanges defined by IEC 61968, such as for the integration of market systems or general enterprise integration.

6.4.6.3 Communication from control centre / trading system to a market place

- IEC 62325

IEC TS 62325-503 is one of the IEC 62325 series which define protocols for deregulated energy market communications.

The principal objective of the IEC 62325 series of standards is to produce standards which facilitate the integration of market application software developed independently by different vendors into a market management system, between market management systems and market participant systems. This is accomplished by defining message exchanges to enable these applications or systems access to public data and exchange information independent of how such information is represented internally.

CIM specifies the basis for the semantics for the message exchange, as shown in Figure 25.

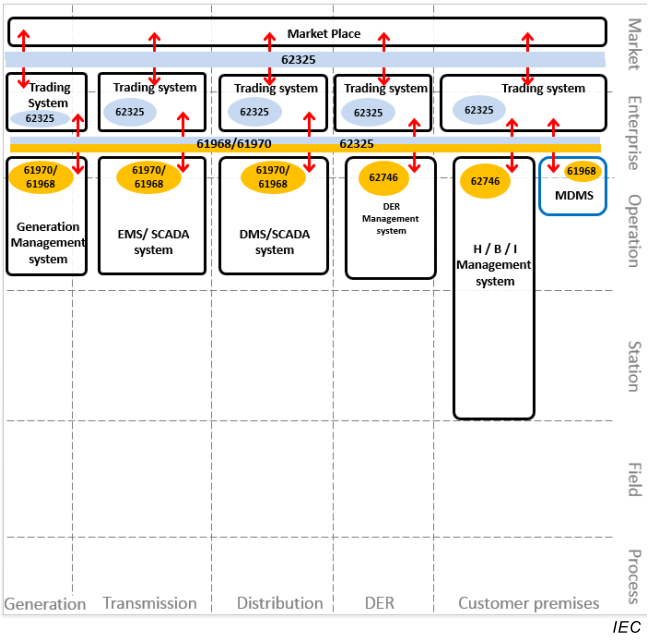


Figure 25 – Communication from control centre / trading system to a market place

6.4.7 Communication to connect DERs (see Figure 26)

- IEC 61850-7-420
- IEC 62746
- IEC 61400-25
- IEC TR 61850-90-15[12]

G_SGCG_Standard_Report_v3.1, 8.4 presents the DER Operation System and related standards.

12 Under preparation. Stage at the time of publication: IEC/PWI 61850:2016.

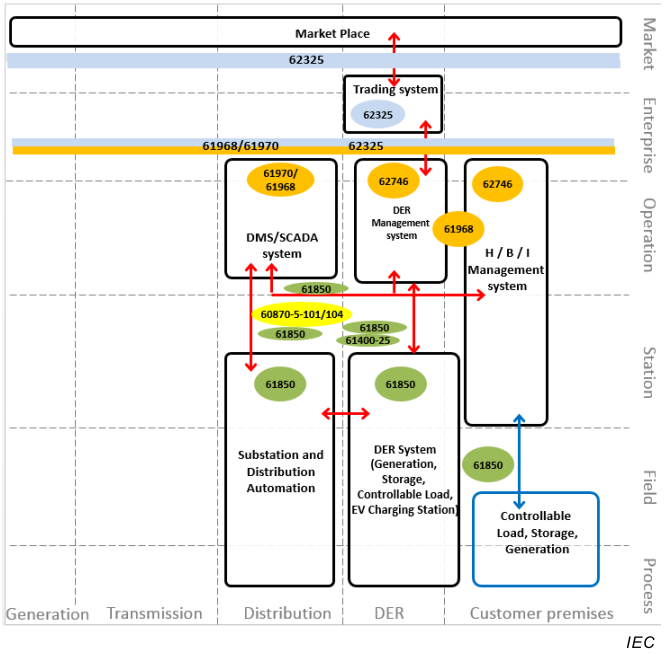


Figure 26 – Communication to connect DER

6.4.8 Communication to or within power plants (hydro, gas, thermal, wind) (see Figure 27)

- IEC 61850-7-410 and IEC TR 61850-7-510
- IEC 61970
- IEC 61400-25

Other relationships concepts are described in 7.1.3.

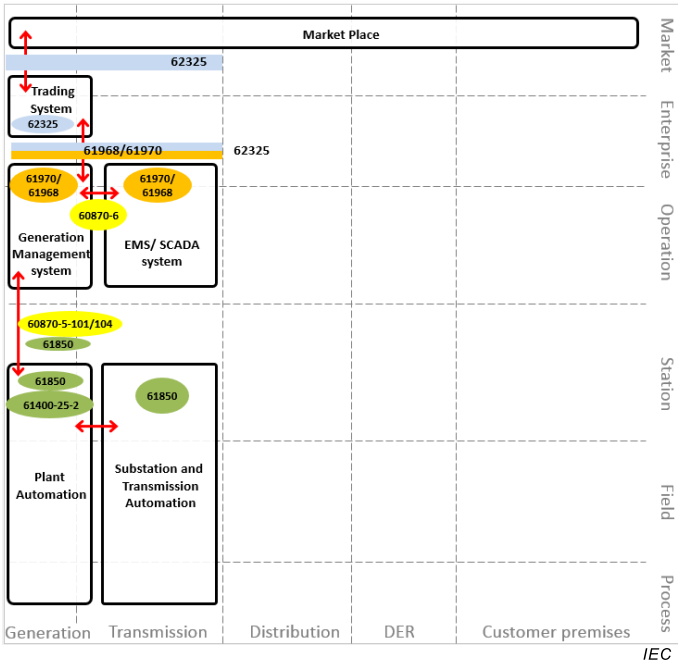


Figure 27 – Communication to/or within power plants

6.5 Security standard landscape for Reference Architecture

6.5.1 General

A security architecture provides a framework and guidance to support the reliable operation of power systems coping with technical, physical, and organizational security requirements appropriate for the target use case. It uses 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. Figure 28 provides an abstract view on the different facets of a generic security architecture.

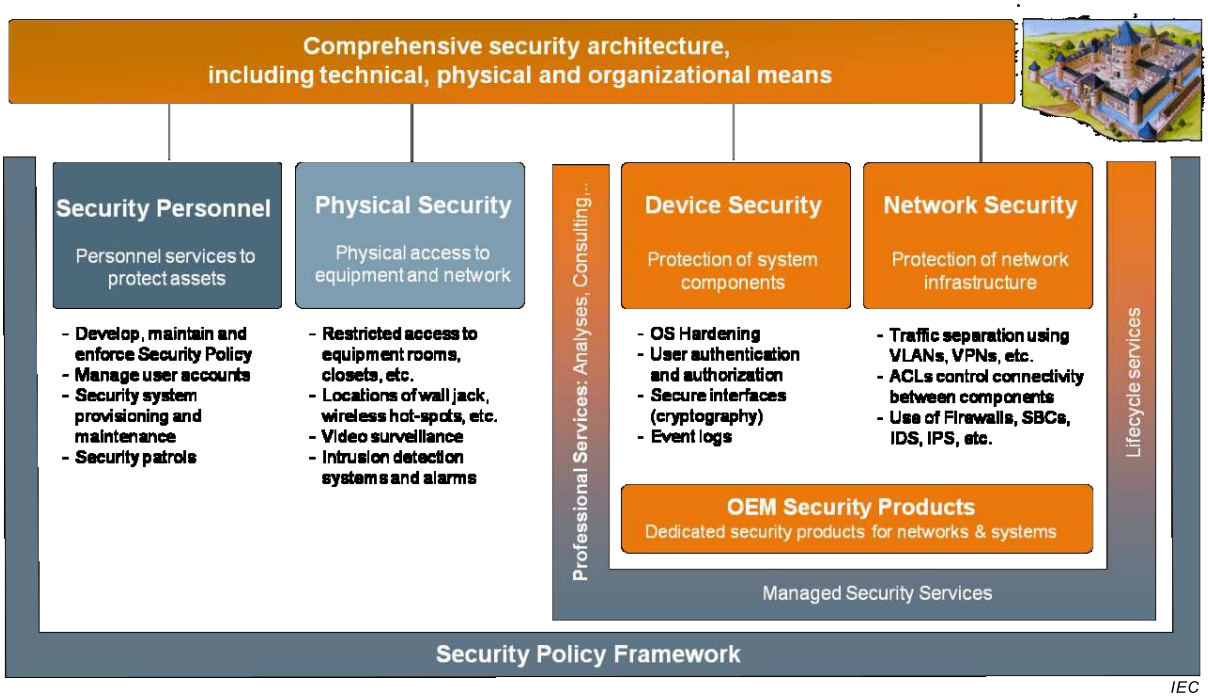


Figure 28 – Generic security architecture

As shown, a security architecture typically not only comprises technical means such as the application of dedicated security measures, 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. Most importantly cyber security must not interfere with the security of the power system.

Figure 29 maps the generic security architecture to a selection of security standards and guidelines which are applicable to power system management.

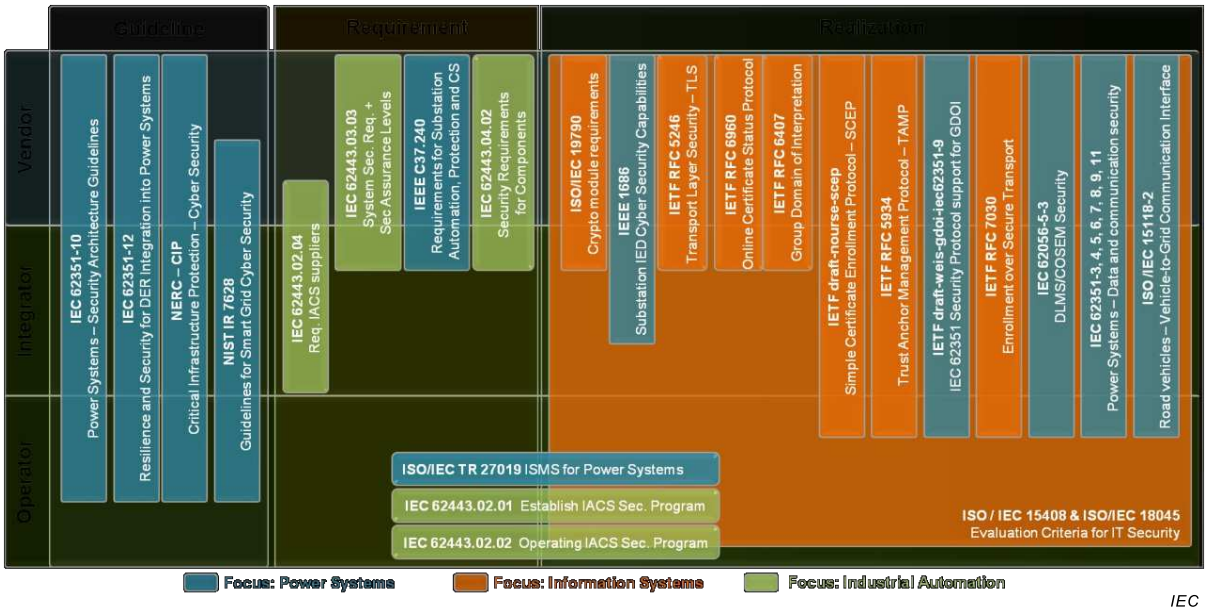


Figure 29 – Architecture of key power system management security standards and guidelines

The following notation is used in Figure 29:

- Guideline: Documents provide guidelines and best practice for security implementations. This may also comprise pre-requisites to be available for the implementation.
- Requirement: Documents contain generic requirements for products, solutions or processes. No implementation specified.
- Realization: Documents define implementation of security measures (specific realizations). Note if distinction possible, the level of detail of the document raises from left to right side of the column.
- Vendor: Documents address technical aspects relevant for products or components
- Integrator: Documents address integration aspects, which have implications on the technical design, are relevant for vendor processes (require certain features to be supported), or require product interoperability (e.g., protocol implementations).
- Operator: Documents address operational and/or procedural aspects, which are mainly focused on the service realization and provisioning on an operator site.

Table 2 includes key standards, specifications, and guidelines from ISO/IEC, IETF, NIST, and NERC which are important for developing security for power system management:

Table 2 – Standards Guidelines

Base Standard / Guideline	Description
IEC 62351	Power systems management and associated information exchange – Data and communications security, further details below
IEC 62443	Industrial communication networks – Network and system security, here mainly Part 3-3 and Part 4-2 are referenced, which define security levels and appropriate security measures for the different security levels on system and component levels.
IEC 62056	Electricity metering – Data exchange for meter reading, tariff and load control, contains also security measures on application layer to protect the confidentiality of communicated data
ISO/IEC 27002	Information Technology — Security techniques — Code of practice for information security management addresses the application of the ISMS
ISO/IEC 27019	Information Technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
ISO/IEC 19790	Information technology – Security techniques – Security requirements for cryptographic modules describes specific requirements for the implementation of cryptography, which may be used for certification
ISO/IEC 15408	Information technology – Security techniques – Evaluation criteria for IT security to be used in the context of common criteria certification
ISO/IEC 18045	Information technology – Security techniques – Evaluation criteria for IT security to be used in the context of common criteria certification
IEEE 1686	Intelligent Electronic Devices Cyber Security Capabilities describes security capabilities to be supported in field devices utilized in Energy Automation
IETF RFC 5246	The Transport Layer Security (TLS) Protocol describes a security protocol above TCP/IP building the base for many protection options in IEC 62351
IETF RFC 5934	Trust Anchor Management Protocol – TAMP describes a protocol for the management of trust anchors like root certificates (lists) on IEDs
IETF RFC 6407	The Group Domain of Interpretation describes a group based key management protocol providing cryptographic key material in multicast communication
IETF RFC 6960	Online Certificate Status Protocol – OCSP supports the query of the revocation state of specific X.509 certificates
IETF RFC 7030	Enrolment over Secure Transport is a protocol used to apply for and distribute certificates
draft-nurse-scep	Simple Certificate Enrolment Protocol – SCEP is a protocol used to apply for and distribute RSA certificates Note that the current draft is historic and there are attempts to provide a historic RFC for SCEP to be able to reference this protocol from other standards. This work targeting the historic RFC is done as new draft “draft-gutmann-scep-00.txt”.
draft-weis-gdoi-iec62351-9	IEC 62351 Security Protocol support for GDOI provides necessary enhancements to the group based key management in the context of energy automation.
NIST IR 7628	Guidelines for Smart Grids Cyber Security
NERC – CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
CIGRE – TB 427	The Impact of Implementing Cyber Security Requirements using IEC 61850
CIGRE WG D2.31 615	Security architecture principles for digital systems in Electric Power Utilities
CIGRE JWG B5/D2.46 603	APPLICATION AND MANAGEMENT OF CYBERSECURITY MEASURES FOR PROTECTION AND CONTROL SYSTEMS

6.5.2 Evolving security requirements for power system management

In addition, the traditional methods of operating the power system have changed significantly over the last decades. The energy market has imposed new threats as stolen information on competitors can financially benefit market participants and possibly disrupt power system operations. The fluctuations caused by renewable energy sources require more precise

forecasting and coordination of generation across wider territories. DER are owned and operated by non-utility parties whose primary interests may not be reliable and efficient grid operations, and yet these DER systems must still be monitored and coordinated through widespread Information and Communication Technologies ICT facilities. Terrorism for political gain and infrastructure destruction is also a greater threat. Some of these threats and attack vectors are illustrated in Figure 30.

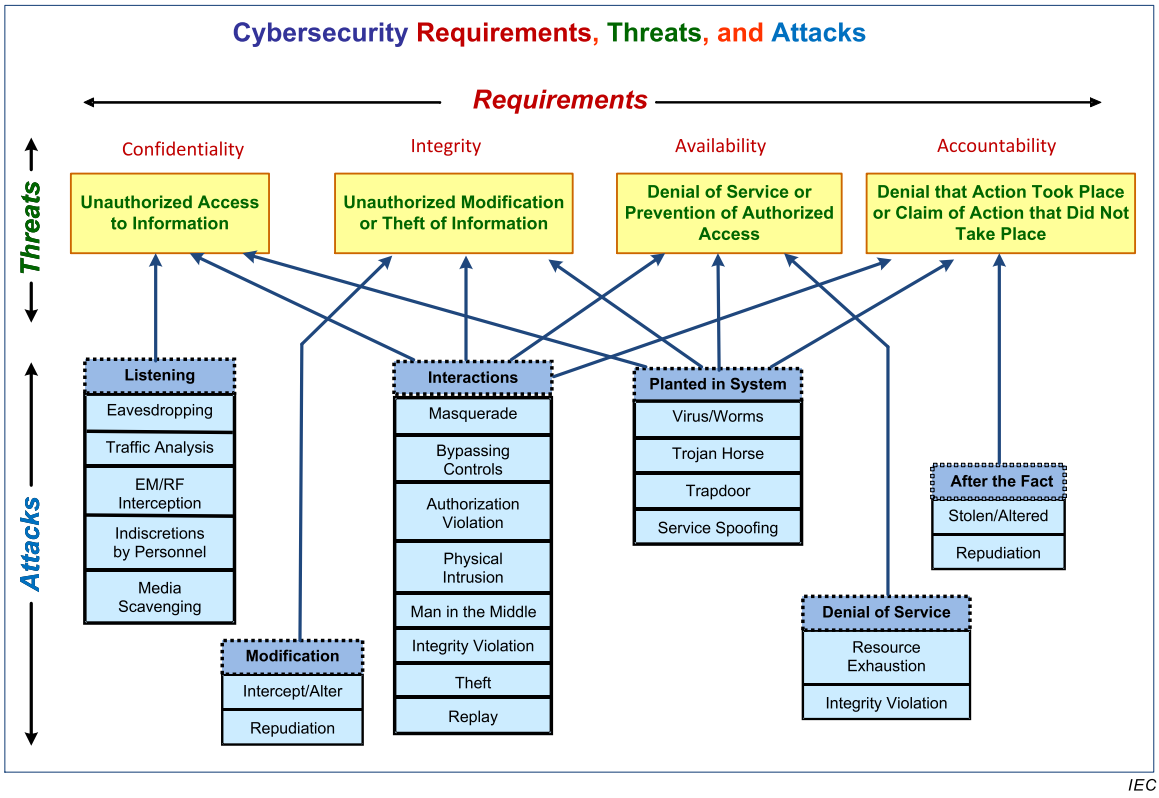


Figure 30 – Typical cyber security requirements, threats, and possible attack techniques

At the same time, cyber security attackers are becoming increasingly sophisticated in their abilities to infiltrate networks and gain access to sensitive systems. Prime examples of recent cyber security attacks are the Stuxnet infiltration of Iranian uranium centrifuge systems, and the cyber security malware named “Dragonfly” which infected many power plants worldwide, allowing the power plant operational data to be monitored by the attackers, with the possibility that the attackers might have issued control commands as well.

6.5.3 Resilience and security measures for power system operations

Because power system operations must be 24h/7days and involve widely dispersed users and equipment, resilience is the ultimate security requirement. Resiliency implies that the power system critical infrastructure is designed not only to prevent malicious cyber and physical attacks and inadvertent failures, but also to cope with and recover from such attacks and failures in a timely manner. Therefore, traditional cyber security techniques are not always directly applicable. For example, the requirements for Confidentiality, Integrity, and Availability (CIA) are typically applied to enterprise information systems with confidentiality the most important. Heavy-duty encryption and verification techniques may cause long delays in exchanging information, while breaches of security usually are countered by shutting down the systems. These security approaches must be replaced with more appropriate methods for power system operations.

Resilience requires a combination of cyber security and power system engineering design and procedures. The cyber security requirements for Authentication, Authorization, and Accountability (the 3 As) along with Integrity are usually more critical than the traditional CIA requirements. Authentication ensures that both the sender and the receiver of data can verify

each other. Authorization, often utilizing role-based access control (RBAC), identifies what privileges are assigned to each user (human or software application). Accountability (also called non-repudiation) assures that the receiver of data cannot deny receiving that data, or conversely, cannot claim to have received data that they did not receive. Integrity ensures that the data received is the same as the data sent, or is flagged as not the same. Although not as critical to most power system operations, confidentiality may be required for sensitive data such as financial or private information. Availability is more likely to be provided by power system engineering strategies and operations than by cyber means (e.g. through equipment redundancy, autonomous device operations, interoperable radio and communications technologies, and properly trained users).

Defence-in-depth is critical because of the large variety of communication methods and performance characteristics that can affect security methods, as well as because no single security measure can counter all types of threats. 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).

Defence-in-depth also may entail the interleaving of cyber technologies and engineering designs. For instance, cyber security measures may prevent some but not all attacks or failures, so power system engineering should design the systems to cope with “successful” attacks. As an example, cyber security integrity technologies may ensure that the data is not changed between sender and receiver, but cannot protect against invalid data being sent: therefore, the receiver should also verify that the received data is at least “reasonable” and not dangerous.

Some of the threats that are seen as more likely in typical information technology systems are less critical for power system operations, while others are more critical. Although importance of specific threats can vary greatly depending upon the assets being secured, some of the more critical threats are:

- Indiscretions by personnel – employees stick their passwords on their computer monitors or leave doors unlocked.
- Bypass controls – employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so does not authenticate its actions.
- Authorization violation – someone undertakes actions for which they are not authorized, sometimes because of careless enforcement of authorization rules, or due to masquerade, theft, or other illegal means.
- Man-in-the-middle – a gateway, data server, communications channel, or other non-end equipment is compromised, so the data which is supposed to flow through this middle equipment is read or modified before it is sent on its way.
- Resource exhaustion – equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Or a certificate expires and prevents access to equipment. This denial of service can seriously impact a power system operator trying to control the power system.
- Replay – an authenticated control command is copied when it is sent by an operator to a field device, such as breaker trip. At some later time, this presumably authenticated but copied command is sent again, thus causing an undesired action at that time.

6.5.4 Overview and correlations of IEC 62351 security standards

The IEC 62351 series of security standards addresses specific security requirements in specific parts of the IEC Reference Architecture. The current IEC 62351 framework consists of the standards and guidelines shown in Table 3:

Table 3 – Overview of IEC 62351 standards

Part	Scope
IEC TS 62351-1:2007	*Introduction*
IEC TS 62351-2:2008	*Glossary of terms*
IEC 62351-3:2014	*Security for profiles including TCP/IP* provides a profiling of TLS
IEC TS 62351-4:2007	*Security for profiles including MMS* provides security for profiles that include the Manufacturing Message Specification (MMS) (ISO 9506), including TASE.2 (ICCP) and IEC 61850 for transport level security (T-profile) and application level security (A-Profile) by utilizing IEC 62351-3 for the T-Profile NOTE This TS is currently being updated
IEC TS 62351-5 ed.2: 2013	*Security for IEC 60870-5 and derivatives* provides different solutions for the serial version (primarily IEC 60870-5-101, as well as parts 102 and 103) and for the networked versions (IEC 60870-5-104 and DNP 3) by utilizing IEC 62351-3 for the T-Profile when using TCP transport
IEC TS 62351-6:2007	*Security for IEC 61850 profiles*, profile that includes the MMS protocol running over TCP/IP uses IEC 62351-3 and IEC TS 62351-4. Additional IEC 61850 profiles that run over TCP/IP (web services or other future profiles) will use IEC 62351-3 plus possible additional security measures developed by the communications industry for application-layer security (out-of-scope for this set of standards).
IEC TS 62351-7:2010	*Objects for Network Management*, Edition 1 of IEC 62351-7 developed sets of abstract NSM data objects, but did not map these to any protocol, suggesting that later work would undertake mappings to the IETF's Simple Network Management Protocol (SNMP) and IEC 61850. This will be replaced by Edition 2 (first edition is currently at CCDV stage). NOTE This TS is currently being transformed to International Standard status
IEC TS 62351-8:2011	*Role-Based Access Control (with: IEC TR 62351-90-1: Guidelines for Using Part 8 Roles)*, specifies a format for transmitting role information for Role-based Access Control (RBAC) in X.509 public key and attribute certificates and software tokens as well as a mechanism to fetch this information, e.g., from LDAP servers. Additionally, IEC TR 62351-90-1 will address the definition of custom roles and the distribution of the role-to-right mapping information.
IEC 62351-9 (target)	*Key Management,* specifies how to generate, distribute, revoke and handle digital certificates, cryptographic keys to protect digital data and communication. It also addresses the handling of asymmetric keys (private keys and X.509 certificates), as well as symmetric keys (pre-shared keys and session keys). NOTE Under preparation. Stage at the time of publication: IEC/CCDV 62351-9:2016.
IEC TR 62351-10: 2012	*Security Architecture*, provides security architecture guidelines for power systems based on essential security controls
IEC 62351-11 (target)	*Security for XML Files,* provides a mechanism to authenticate the source of the XML files like CIM or SCL files. Also provided is a mechanism for tamper detection.
IEC TR 62351-12:2016	*Resilience and Security Recommendations for Power Systems with DER*, provides resiliency recommendations that recognize the need for integrating both cyber security techniques with engineering/operational strategies in order for power systems with Distributed Energy Resources (DER) systems to achieve equal or greater resilience to attacks, failures, and natural disasters.
IEC TR 62351-13:2016	*Guidelines on What Security Topics Should Be Covered in Standards and Specifications*, provides guidelines to support the developers of standards and specifications with addressing cyber security at the appropriate level for their standard.
IEC 62351-14 (target)	*Cyber security event logging and reporting.* Specifies technical requirements for logging security events: transport, log data and semantics, such as how to send and receive security events securely, reliably, how to forward security events or logs, how to query logs, etc. Target protocol is syslog. NOTE This document is being considered

Part	Scope
IEC TR 62351-90-1 (target)	*Guideline for RBAC*, targets specifically the definition of custom roles and associated rights as well as the distribution of this information between the involved entities. NOTE This document is being considered
IEC TR 62351-90-2 (target)	*Deep Packet Inspection*: Investigation of currently available techniques to evaluate their applicability, with detailed threat analysis regarding traffic injection issues and the cost of implementation in the overall architecture NOTE This document is being considered
IEC TR 62351-100-1 (target)	Compliance testing for IEC TS 60870-5-7 (IEC 62351-3 and -5))

There is not a one-to-one correlation between the IEC communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers. These interrelationships between the IEC communication standards and the IEC 62351 security standards are illustrated in Figure 31.

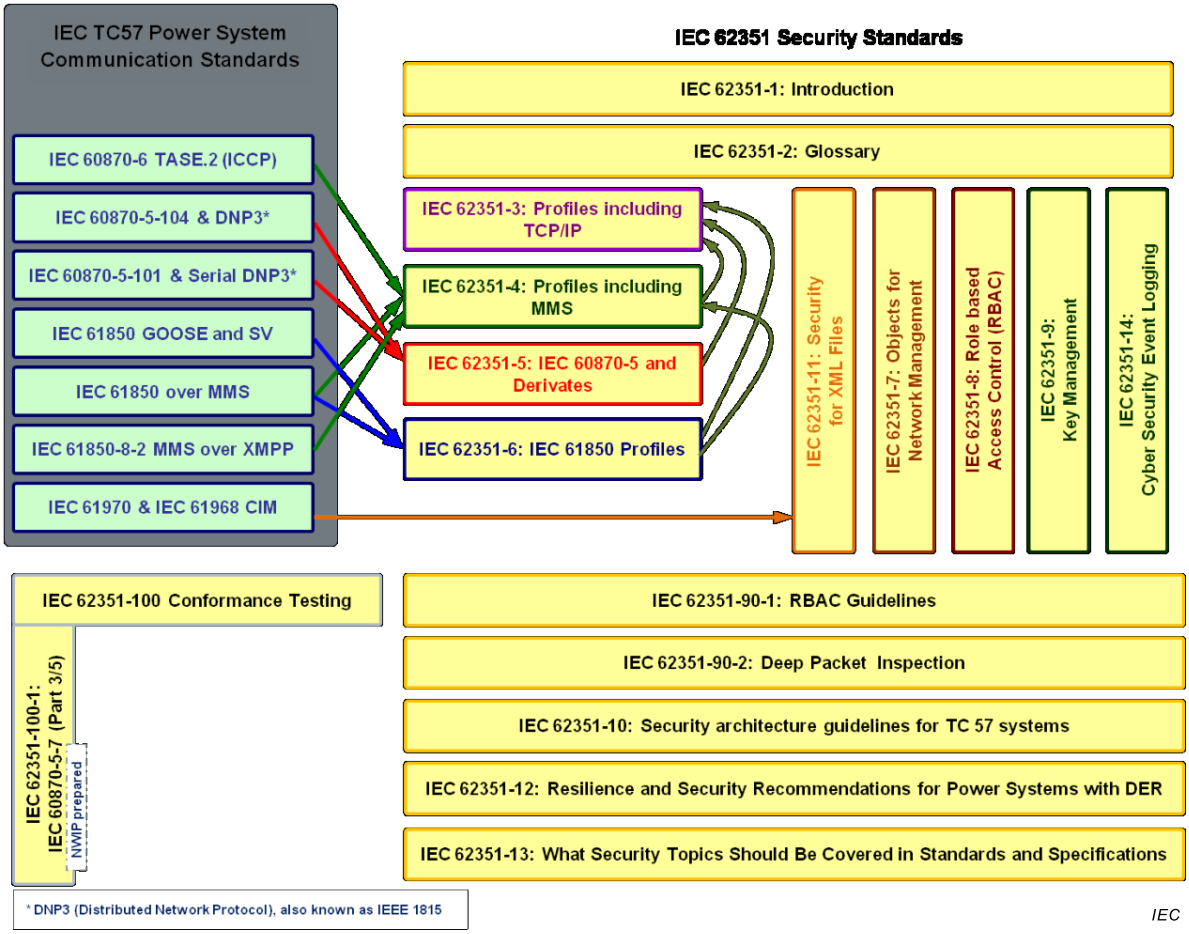


Figure 31 – Interrelationships between IEC communication standards and IEC 62351 security standards

More detailed information about the different parts of IEC 62351 is provided in D.5.2.

6.6 Relationships applied to telecommunication

6.6.1 General

A secure, reliable and economic power supply is closely linked to fast, efficient and dependable telecommunications services.

A telecommunications service is any service provided by a telecommunications network through a telecommunications system. A telecommunications system is a collection of individual telecommunications networks and telecommunication end points capable of interconnection and interoperation to form an integrated whole.

The planning and implementation of telecommunications systems, needed to support the expected services mentioned above, requires the same care as the installation of the power supply system themselves.

One way to categorize the different types of telecommunications networks is by means of transmission:

- Wireless: communication through the air
- Wire line: communication through cable dedicated to telecommunications services
- Powerline: communication through cable designed for electric power transmission, but used for carrying data too.

Wireless communications may have to comply with local or regional regulations (such as the Telecommunication Directive 99/05/CE for Europe and FERC in USA).

For Smart Grids communication architecture/technology, products based on specifications from industry consortia (e.g. the IETF, IEEE, World Wide Web Consortium W3C) have been deployed widely, notably in the area of IP protocols and web services. In the below section, the list of standards/specifications takes into account the ones which fulfil market requirements.

Depending on the Smart Grids target applications, different types of telecommunications networks and also collections of telecommunications networks using different transmission technologies may be selected in order to transmit and deliver Smart Grids data.

The following network types could be defined for the Smart Grids:

- (A) Industrial Fieldbus Area Network

  network that interconnects process control equipment mainly in power generation (bulk or distributed) in the scope of Smart Grids.

- (B) Subscriber Access Network

  network that provides general broadband access (including but not limited to the internet) for the customer premises (homes, building, facilities). They are usually not part of the utility infrastructure and provided by communication service providers, but can be used to provide communication service for Smart Grids systems covering the customer premises like Smart Metering and Aggregated prosumers management.

- (C) Home and Building integration bus Network

  network that interconnects home/building communicating components and sub-systems to form a home or building management sub-system or system

- (D) Neighbourhood network

  network at the distribution level between distribution substations and end users. It is composed of any number of purpose-built networks that operate at what is often viewed as the “last mile” or Neighbourhood Network level. These networks may service metering, distribution automation, and public infrastructure for electric vehicle charging, for example.

- (E) Multi-services backhaul Network

  network at the distribution level upper tier, which is a multi-services tier that integrates the various sub layer networks and provides backhaul connectivity in two ways: directly back to control centres or directly to primary substations to facilitate substation level distributed intelligence. It also provides peer-to-peer connectivity or hub and spoke connectivity for distributed intelligence in the distribution level. This network may serve Advanced Metering or Distribution Automation types of services.

- (F) Low-end intra-substation network

  network inside secondary substations or MV/LV transformer station. It usually connects Remote Terminal Unit RTUs, circuit breakers and different power quality sensors.

- (G) Intra-substation network

  network inside a primary distribution substation or inside a transmission substation. It is involved in low latency critical functions such as tele-protection. Internally to the substation, the networks may comprise from one to three buses (system bus, process bus, and multi-services bus).

- (H) Inter-substation network

  network that interconnects substations with each other and with control centres. These networks are wide area networks and the high end performance requirements for them can be stringent in terms of latency and burst response. In addition, these networks require very flexible scalability and due to geographic challenges they can require mixed physical media and multiple aggregation topologies. System control tier networks provide networking for SCADA, SIPS, event messaging, and remote asset monitoring telemetry traffic, as well as peer-to-peer connectivity for tele-protection and substation-level distributed intelligence.

- (I) Intra-Control Centre / Intra-Data Centre network

  network inside two different types of facilities in the utility: utility data centres and utility control centres. They are at the same logical tier level, but they are not the same networks, as control centres have very different requirements for connection to real time systems and for security, as compared to enterprise data centres, which do not connect to real time systems. Each type provides connectivity for systems inside the facility and connections to external networks, such as system control and utility tier networks.

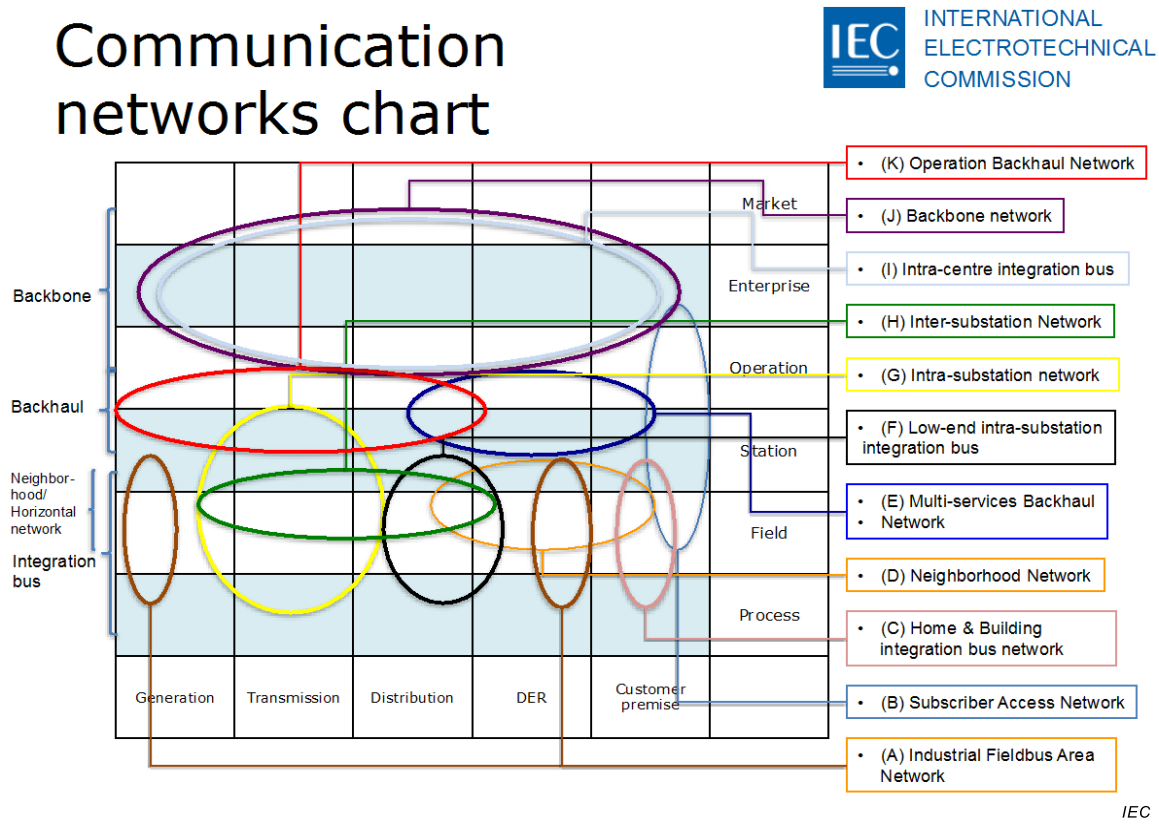
- (J) Backbone Network

  inter-enterprise or campus networks, including backbone Internet network, as well as inter-control centre networks..

- (K) Operation Backhaul Network

  networks that can use public or private infrastructures, mostly to support remote operation. They usually inter-connect network devices and/or subsystems to the “Operation level” over a wide area (region or country).

Figure 32 provides a mapping of the different Smart Grids networks to the SGAM model. Where a circle is tangent to a zone, this means that the corresponding network type can support the interface with the tangent zone.



NOTE 1 These areas are a mapping example and cannot be normative to all business models.

NOTE 2 It is assumed that sub-networks depicted in Figure 32 are interconnected (where needed) to provide end-to-end connectivity to applications they support. VPNs, Gateways and firewalls could provide means to ensure network security or virtualization. These security measures are determined based on a threat and risk analysis (see 7.6.2).

Figure 32 – Mapping of communication networks on SGAM

6.6.2 Applicability statement of communication technologies to the Smart Grids sub-networks

Table 4 provides an applicability statement indicating the standardised communication technologies to the Smart Grids sub-networks depicted in the 6.6.1. The choice of a technology for a sub-network is left to implementations, which need to take into account a variety of deployment constraints.

Extracted from the M.490 Methodology Working Group WG (in 2012) and the CENELEC Set of Standards WG (in 2014), Table 4 provides this information:

1) From each SDO, a certain list of technologies are introduced;
2) The available SGAM Communications sub-networks are listed;
3) The green rectangle indicates what is currently mostly used (dark green rectangle), potentially used (light green rectangle) and not used (white rectangle).

The choice of a technology for a sub-network is left to implementations, which need to take into account a variety of deployment constraints.

Table 4 – Technologies covered by SDOs in function of SGAM Communications Sub-Networks

		Process/ Field Area Network	Substation Access Network	Home and Building/ Integration Bus Network	Neighborhood network	Multi-service backbone Network	Local and Intra-substation network	Intra-substation network	Inter substation network	Intra-Control Centre / Intra-Data Centre network	Backbone Network	Operation Backbone Network
		A	B	C	D	E	F	G	H	I	J	K
IEEE protocols (MAC-PHY)												
	IEEE 1901.2 Narrow band PLC			■	■							
	IEEE 1901 Broad band PLC		■	■	■							
	IEEE 802.15.4 wireless Low Power		▒	■	■							
	IEEE 802.11 (WIFI)	▒	▒	■	■	■	■	■	▒			
	IEEE 802.3/1 (Ethernet)	▒		■			■	■		■	▒	
	IEEE 802.16 (Wimax)		■	▒	■	■						
IETF protocols (layer 3, 4 and above)												
	IPv4	▒	■	■	■	■	■	■	■	■	■	■
	IPv6	▒	■	■	■	■	■	■	■	■	■	■
	6LPL / 6LowPan			■	■							
	IP MPLS / MPLS TP					■			■	■	■	■
	XMPP			■	■	■			■			■
ITU Protocols												
	SDH/OTN		▒	▒	▒	■	■	▒	■	■	■	■
	DSL/PON		■		■	■			▒	■	■	
	DWDM		▒	▒	▒	■	■	■	■	■	■	■
	Narrow band PLC (Medium & Low voltage)			■	■							
	Narrow band PLC (High & very High voltage)							▒	■			
	Broadband PLC		■	■	■							
ANSI standards												
	SONET / SONET NG		▒	▒	▒	■	■	■	■	■	■	■
ETSI / 3GPP Protocols												
	ETSI TS 102 887 Wireless (IEEE 802.15.4g)		▒	■	■							
	GSM / GPRS / EDGE		▒		■	▒						
	3G / WCDMA / UMTS / HSPA		■		■	■					▒	▒
	4G LTE/LTE-A		■		■	■			■		■	▒
EN standards												
	EN 14908	■		▒	▒	▒						
	EN 50090			■	■	▒						
	EN 13757	■		▒	▒							
IEC standards												
	IEC 61158	■										
	IEC 61850				▒	▒	■	■	■			
	IEC 60870-5											■
Higher layer comm protocol			■	■	■	■			■	■	■	■

Legend

■ Mostly used

▒ May be used

Communication layer profiles

Generally a profile defines a subset of an entity (e.g. standard, specification or a suite of standards/specifications). Profiles enable interoperability and therefore can be used to reduce the complexity of a given integration task by:

- Selecting or restricting standards to the essentially required content, e.g. removing options that are not used in the context of the profile
- By setting specific values to defined parameters (frequency bands, metrics, etc.)

A standard profile for communications standards may contain a selection of communication capabilities applicable for specific deployment architecture. Furthermore a profile may define instances (e.g. specific device types) and procedures (e.g. programmable logics, message sequences) in order to support interoperability.

It may also provide a set of engineering guidelines to ease the deployment of new technologies.

6.7 Interoperability

The Smart Grids as a system cannot be engineered from the ground up. Instead, Smart Grids development is most likely to follow transformation processes. This means that business models as well as roles on one hand, and technical components and architectural structures on the other hand, are to be transformed from the current “legacy” state into the “Smart Grids”. Due to the scale of the system and its economic importance, failures in operation and especially architectural and functional planning of the system, potentially induce high costs. In order to enable a well-structured migration process, the requirements for the Smart Grids and the current system have to be decomposed using an appropriate model. Although the majority of Smart Grids equipment is based on (inter)national or regional standards, this has not resulted in an interoperable Smart Grids infrastructure yet. This is partly due to misunderstanding of what interoperability means, what can be expected from it and what should be done to realize it. Key to reaching Smart Grids system interoperability is through detailed specifications, use of standards and testing.

Therefore, as more and more ICT components are being connected to the physical electrical infrastructure, interoperability is a key requirement for a robust, reliable and secure Smart Grids infrastructure. The way to achieve Smart Grids system interoperability is through system specifications, through use of standards, and through testing under applications of profiles.

7 Use of Reference Architecture

7.1 General

The Reference Architecture for power system information exchanges provides a guideline for users (regulators, utility, vendor, integrator, standardization experts) and can assist in designing individual solutions and concepts based on specific requirements.

7.2 Development of Enterprise Architecture

7.2.1 General

The IEC Reference Architecture is aligned with the Model Driven Architecture approach as defined by the Object Management Group.

7.2.2 Model Driven Architecture

The MDA defines an approach to IT system specifications that separates the specifications of system functionality from the specifications of the implementation of that functionality on a specific technology platform. To this end, the MDA defines an architecture for models that provides a set of guidelines for structuring specifications expressed as models.

The MDA approach and the standards that support it allow the same model specifying system functionality to be realized on multiple platforms through auxiliary mapping standards, or through point mappings to specific platforms, and allow different applications to be integrated by explicitly relating their models, enabling integration and interoperability and supporting system evolution as platform technologies come and go.

As explained in MDA Guide rev. 2.0, “MDA provides an approach for deriving value from models and architecture in support of the full life cycle of physical, organizational and I.T. systems"[13]. The MDA approach represents and supports everything from requirements to business modelling to technology implementations. By using MDA models, ability to better deal with the complexity of large systems and the interaction and collaboration between organizations, people, hardware, software is given.

The primary feature of MDA which enables us to deal with complexity and derive value from models and modelling is defining the structure, semantics, and notations of models using industry standards – models conforming to these standards are “MDA Models. MDA models can then be used for the production of documentation, acquisition specifications, system specifications, technology artefacts (e.g. “source code”) and executable systems.”

7.2.3 The Open Group Architecture Framework

The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture which provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture. TOGAF is a high level approach to design. It is typically modelled at four levels: Business, Application, Data, and Technology.

TOGAF is based on the Architecture Development Method (ADM) shown Figure 33.

---

13 A “System”, in this context, is any arrangement of parts and their interrelationships, working together as a whole. This is inclusive of designs at all levels such as an entire enterprise, a process, information structures or IT systems.

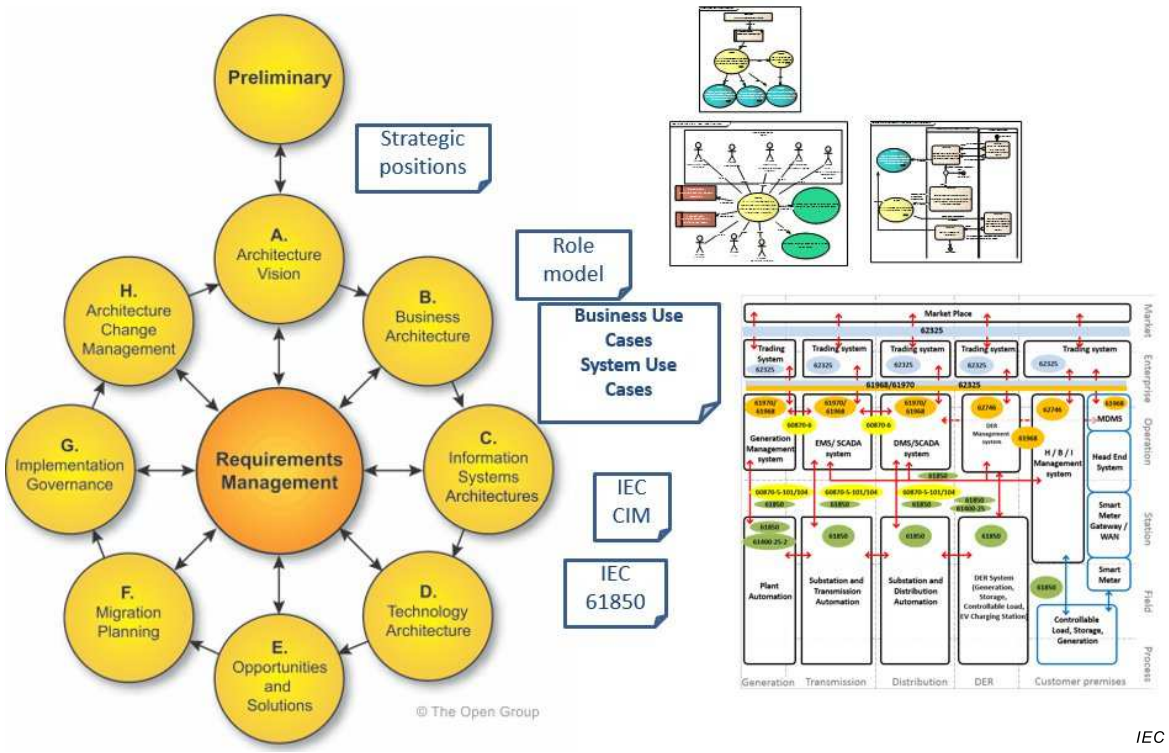


Figure 33 – Use of Reference Architecture in TOGAF

7.3 How to evolve from a Present User Architecture to Reference Architecture

The Reference Architecture for power system information exchanges can assist users (regulators, vendor, utility, and integrator, standardization experts) in evolving from their current architecture to their target architecture. It can assist in identifying differences between the current state and the target state and help to identify migration steps.

In the TOGAF Architecture Development Method the activities that the Reference Architecture for power system information exchanges can assist with are:

Phase A – Architecture Vision. Adopt an architecture principle that indicates the all projects must use standards.

Phase B – Business Architecture. Develop Business Use Cases

Phase C – Information systems architecture. Projects can use the Reference Architecture for power system information exchanges to identify which standards to use in their information systems. Develop System Use Cases associated to Business Use Cases.

Phase D – Technology architecture Projects can use the Reference Architecture for power system information exchanges to identifies which standards to use in their technology architecture

7.4 Example: how to map a use case using Reference Architecture

7.4.1.1 General

A common use case which is to control and monitor a circuit breaker within a SCADA System using CIM is presented hereafter.

7.4.1.2 CIM circuit breaker application view

A CIM application will be able to model the Electrical Network using CIM information model. A circuit breaker model is illustrated in Figure 34:

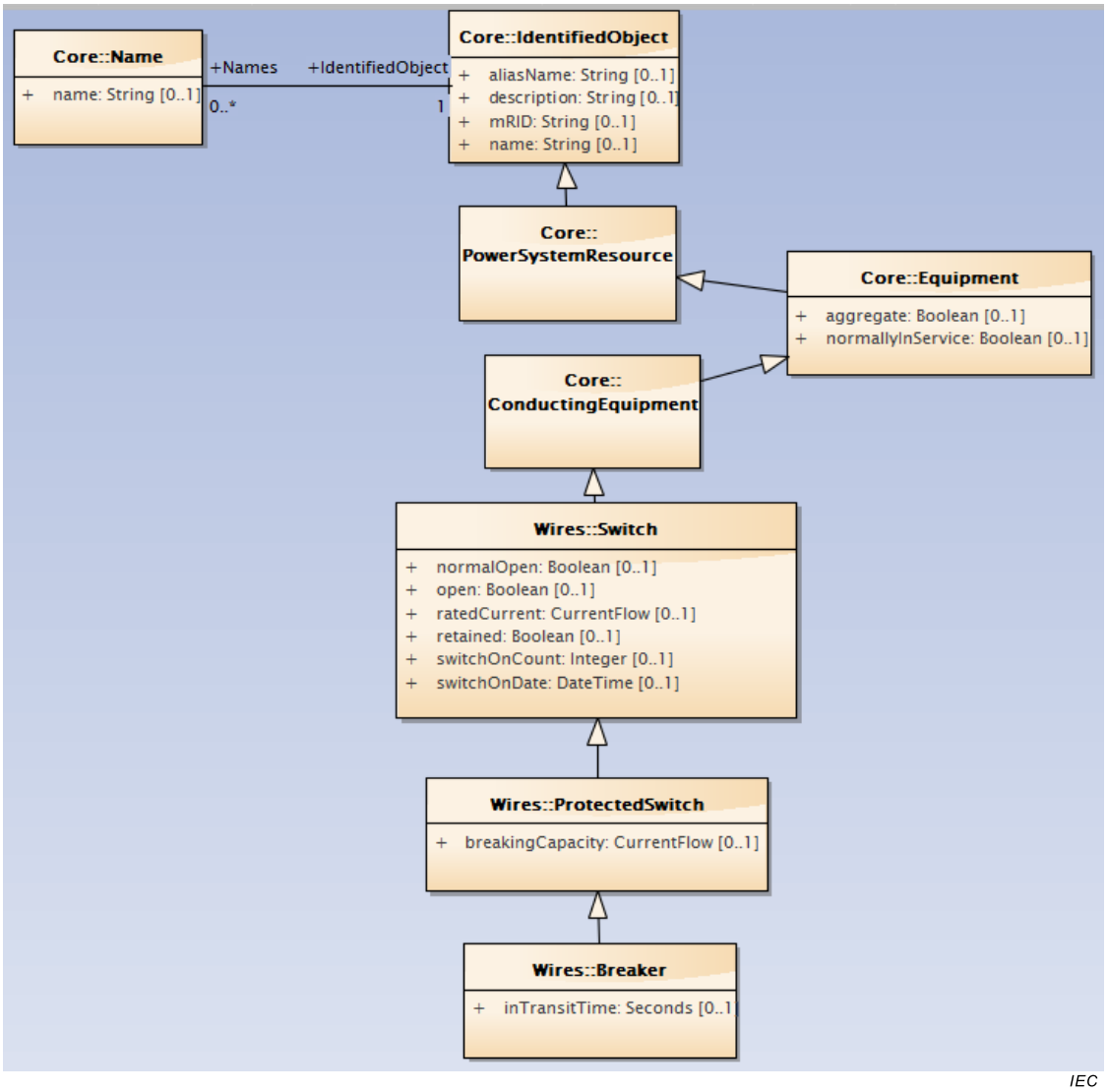


Figure 34 – CIM circuit breaker application view

According to definition IRM NO-NMON (Network Operation, Network Monitoring) system provides the means for supervising main substation topology (breaker and switch state) and NO-CTL provides the mean to control equipment status. Two of its abstract components, "Network state supervision“ and “Switching action supervision”, allow the monitoring and operation of a circuit breaker.

Two typical message types will be exchanged between abstract components such as the one shown in Table 5:

Table 5 – Message types

NO-NMON	NO-CTL	Create Control	Request for SCADA-commanded operation of switches for execution of switching plan. Payload – Switch ID (PSR mRID) – Affected Phases – Switch Action (open or close)
NO-CTL	NO-FLT	Created DiscreteMeasurement	Notification of device status change due to execution of switching operations. Payload: – Device ID – Status of Device (phases on) – Time of Operation – Person who performed operation (crew member or operator)

The Control Message type allows changing the Switch position whereas the DiscreteMeasurement message allows notifying the status of the switch.

At the Enterprise level the application will communicate these message types according to 61968-100.

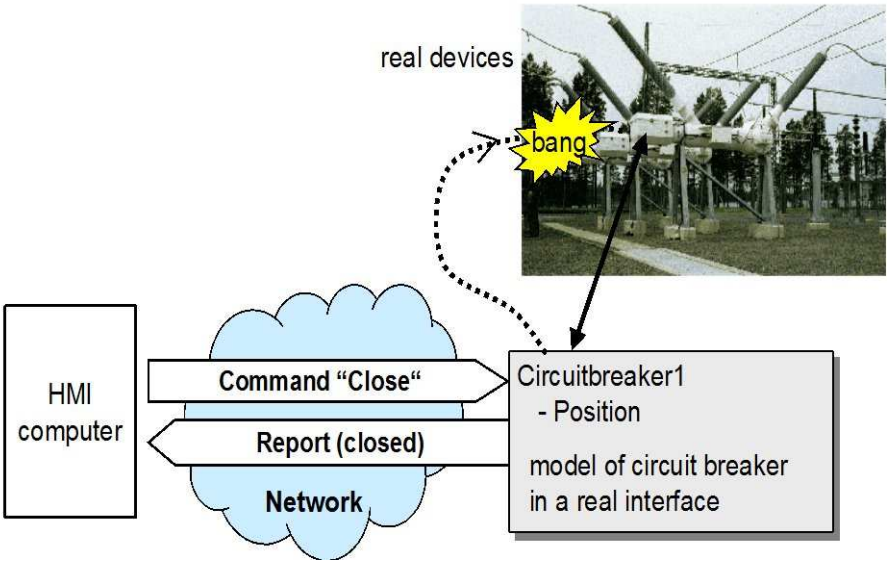
At the Network Operation level, the NO-NMON Network state supervision /NO-CTL Switching action supervision abstract components will interoperate with a real device which will be modelled using IEC 61850 modelling concepts as described in 7.4.1.3.

The NO-MON/NO-CTL abstract components (equivalent of SCADA System) will interoperate with the Switching device using a communication protocol. See 6.4.5.2.

7.4.1.3 Circuit breaker within substation with IEC 61850

A sample operation, illustrated in Figure 35, is to switch a circuit breaker. An operator at a remote Human Machine Interfaces (HMI) wants to remotely switch the circuit breaker. The HMI computer and the circuit breaker have to operate together (interoperate). First, the computer needs to know what information it has to transmit to the IED representing the circuit breaker (normally called the “process interface”). Secondly, it has also to know the name of this IED (for example “Circuitbreaker1”) and how to address the IED. Both the HMI computer on the left side and the IED “Circuitbreaker1” on the right side are connected to a common communication network. The HMI sends a control command to the “Circuitbreaker1” to switch the position of the breaker (close the breaker). After switching is completed, the interfaces IED may (if configured) send a report to the HMI computer indicating that the switch position has changed.

Different users may name the circuit breaker differently: one may use “Circuitbreaker1”, another may choose “CBK-2”. IEC 61850-7-4, based on the approach described in IEC 61850-5, standardises many abbreviated names for substation functions and related equipment. The standardised name for a circuit breaker is XCBR. This name may be accompanied by a suffix and a prefix: "Q1XCBR1" (for naming conventions, see IEC 61850-7-2).



IEC

Figure 35 – Real world devices

The relations between parts of the IEC 61850 series to operate a circuit breaker are shown in Figure 36:

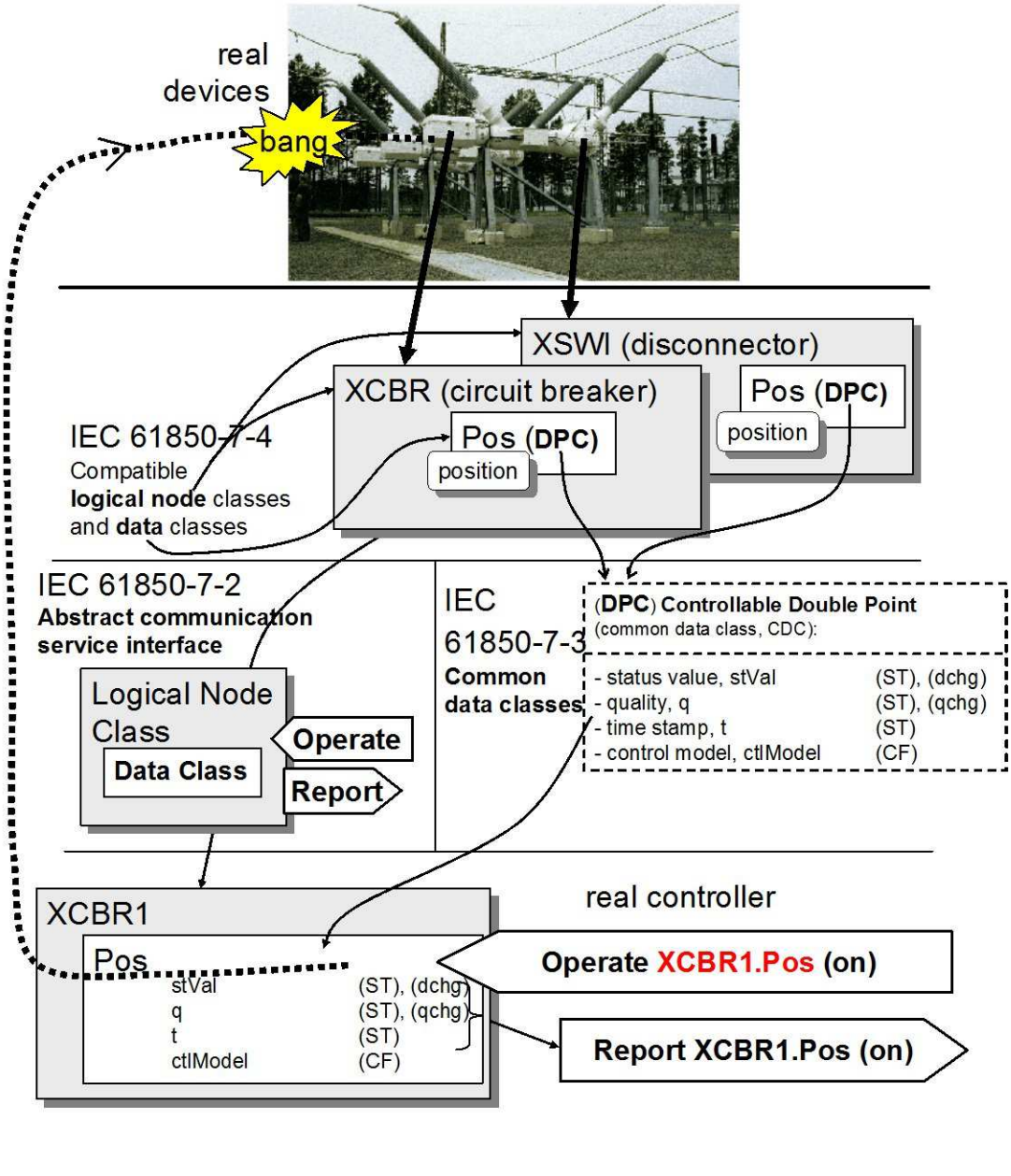


Figure 36 – Operate a circuit breaker with IEC 61850

7.4.1.4 IEC 61850 Profiling

Figure 37 shows the logical node class XCBR as it is defined in IEC 61850-7-4. There are several data items defined as being mandatory (M) other data are defined as being optional (O).

A logical node (XCBR) of a device model is specified with a SCL file. By definition, all mandatory data defined in the class defined in IEC 61850-7-4 are used by the logical node in the device model.

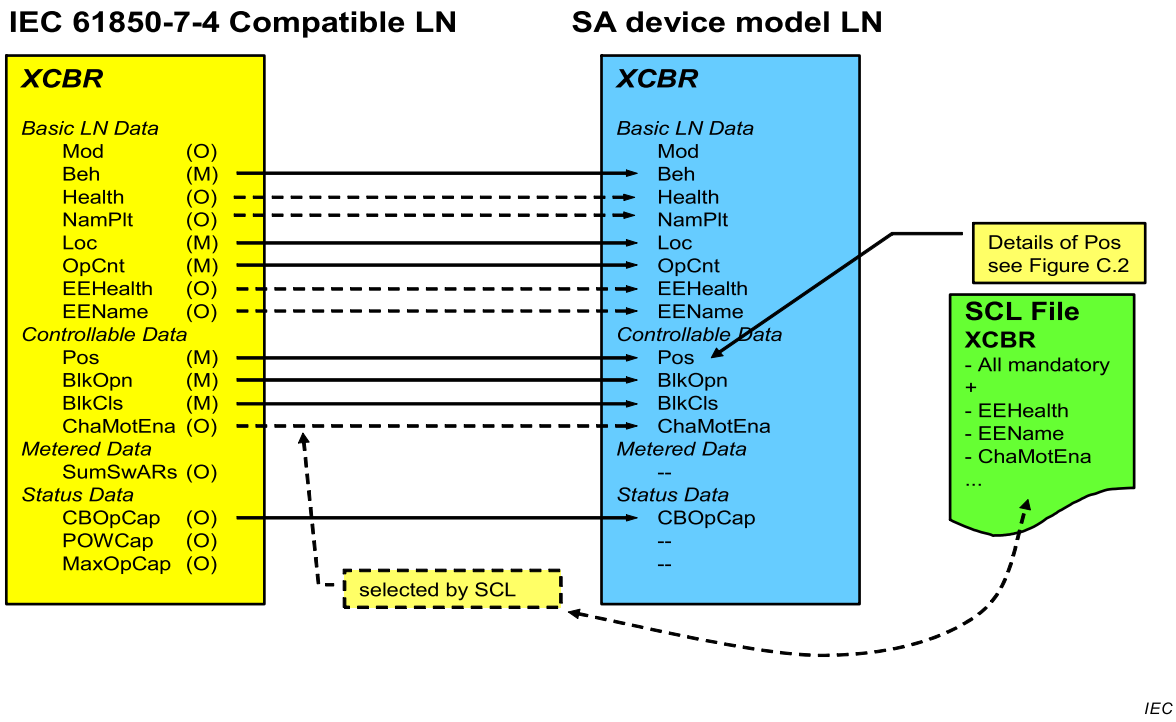


Figure 37 – SCL for LNs

The SCL needs to list all data to be used in the device model. Three optional data items are selected in the example (EEHealth, EEName, and ChaMotEna).

The SCL also needs to list the optional data attributes of each data selected.

At the logical node level, the SCL shall list the names of the mandatory and optional data. The SCL for the data requires the list of mandatory and optional data attributes as well as the initialisation (configuration) values for several data attributes.

The SCL file in Figure 38 shows which “Pos” optional data attributes are selected. In addition, the SCL file assigns values to three data attributes.

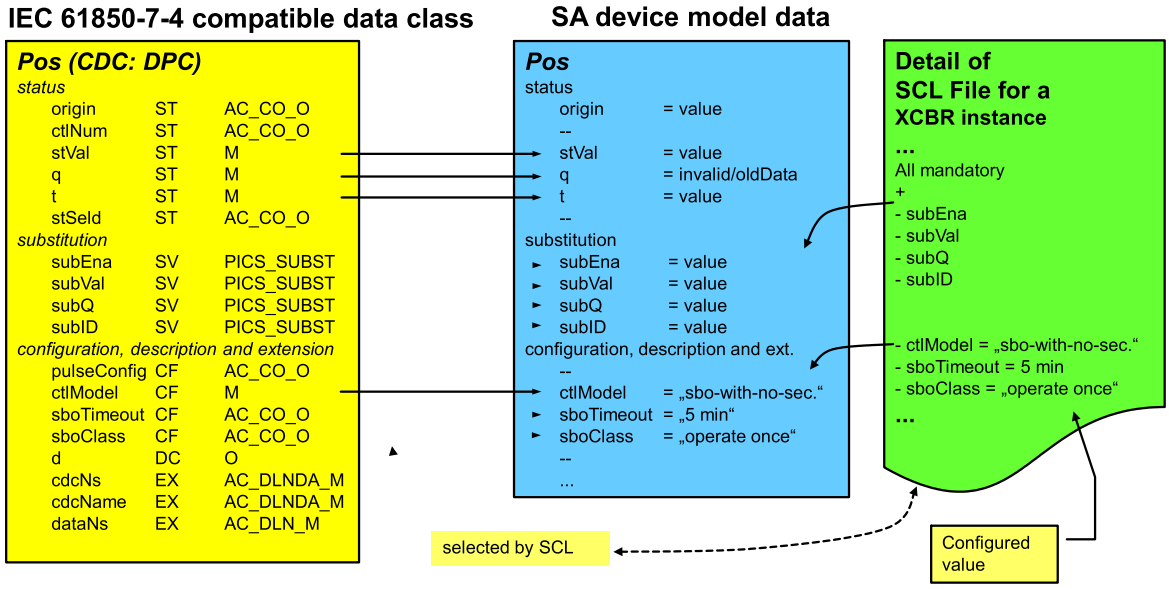


Figure 38 – SCL POS attribute

The configured values for ctlModel, sboTimeout, and sboClass become effective as soon as the real device has been configured. The values may be overwritten (if the device allow overwriting these values at all) by a service request from a specific client.

7.4.1.5 Communicating in IEC 61850 with an IEC 61850 Circuit breaker, and within a substation

The ACSI (Abstract communication service interface) defines common utility services for substation devices. The Operate service from Control Service Model will be used to operate the Circuit Breaker. The ACSI provides access to the real data and real devices through a virtual image as depicted in Figure 39. A virtual image that represents the real data of devices is made visible and accessible through ACSI services. A computer may request services, for example, get data values, or may receive spontaneously reported values from the controller.

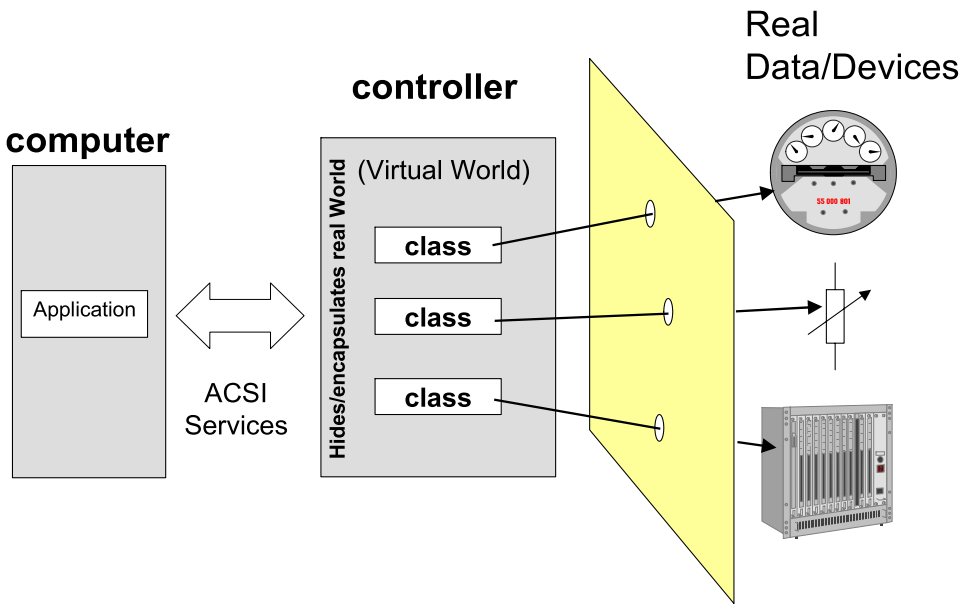


Figure 39 – ACSI service example

The mapping of ACSI services to specific application layer messages is beyond the scope of IEC 61850-7-2; this mapping is specified by a specific communication service mapping (SCSM) in the IEC 61850-8-x and the IEC 61850-9-x series.

IEC 61850-7-4, IEC 61850-7-3, and IEC 61850-7-2 define abstract information and service models for the application domain substation. Even so, the IEC 61850 series in general allows discrete devices to share data and services. For this to occur, the devices must agree on the concrete form of the services and data that will be exchanged.

The form of the service and data is of no consequence to the transport, network, and media protocols, i.e. to the lower layers of the communication stack and they are invariant to it. Conversely, the application that is sending and receiving data has no real procedure describing how this is achieved and it is therefore largely invariant of the mechanisms used.

This separation of roles is important as it allows many different technologies to be employed in a relatively transparent manner. As consequence, these lower layers may be exchanged, for example,

- networks with different types of physical media may be used;
- more than one application layer protocol may exist and use the same physical network and protocols.

Standardised mappings of the abstract services to different communication stacks are defined in the IEC 61850-8-x and IEC 61850-9-x series, so that common utility functions will be performed consistently across all field devices independently of the underlying communication systems.

The mapping of ACSI services to specific application layer messages is described in Figure 40.

EXAMPLE The ACSI service “GetDataSetValues” may have different mappings for different application layers (AL). For example, a specific AL may support this service directly while another AL provides “Get of single data” only. In the last case the mapping has to issue several “Get of single data”.

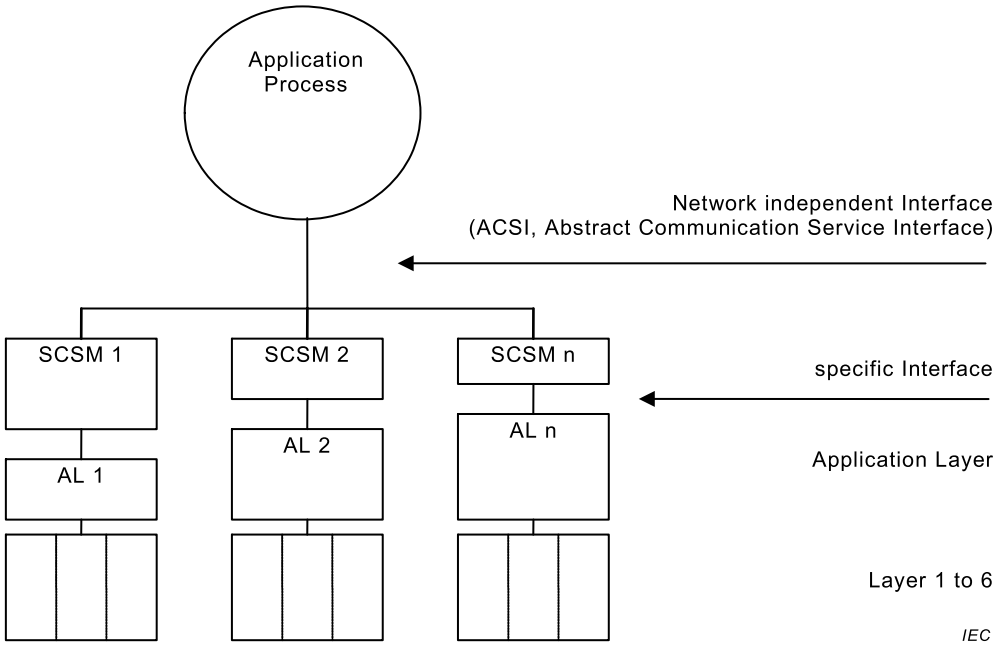


Figure 40 – Mapping of an ACSI service

Figure 41 illustrates a model excerpt of XCBR1 representing a real device. The complete hierarchical model may be mapped, for example, to MMS applying the SCSM according to IEC 61850-8-1. As a result, many MMS named variables have to be implemented in a real server. The services of the ACSI are mapped to MMS services.

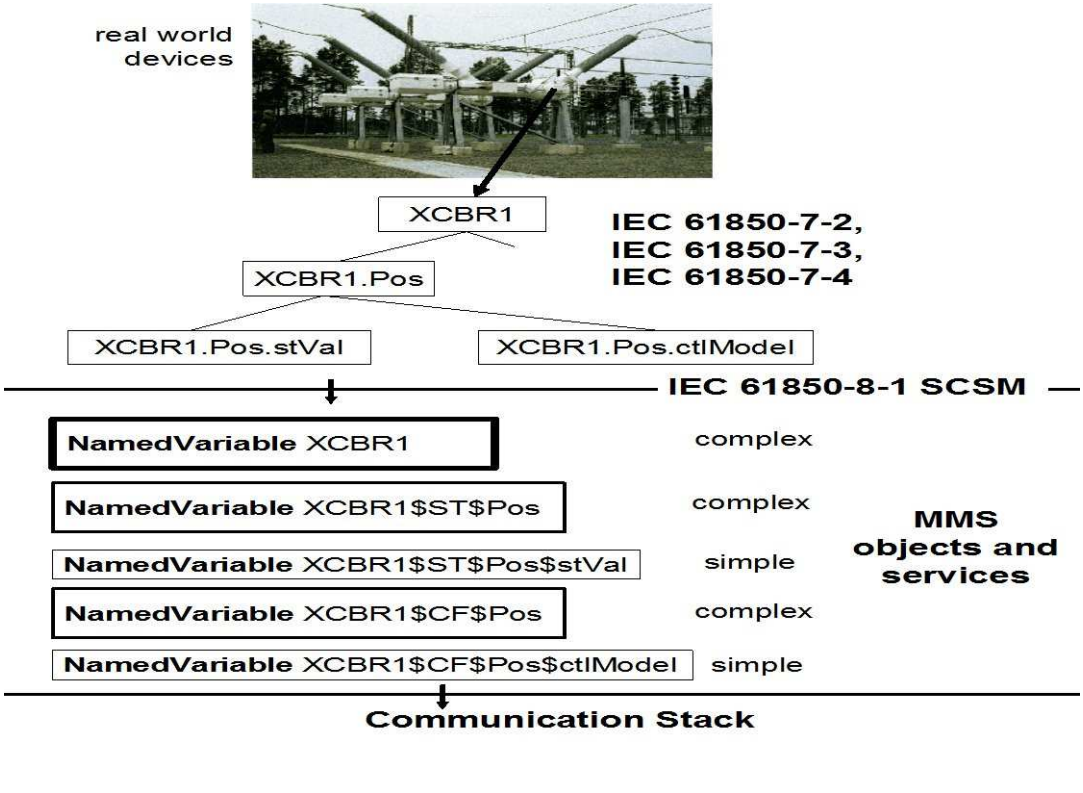


Figure 41 – Hierarchical model for a circuit breaker

7.5 Development of information exchange specification

This methodology is used when two parties identify the need for the specification of an interface to enable information exchange among their business areas to support a function, as illustrated by Figure 42 (extracted from M490).

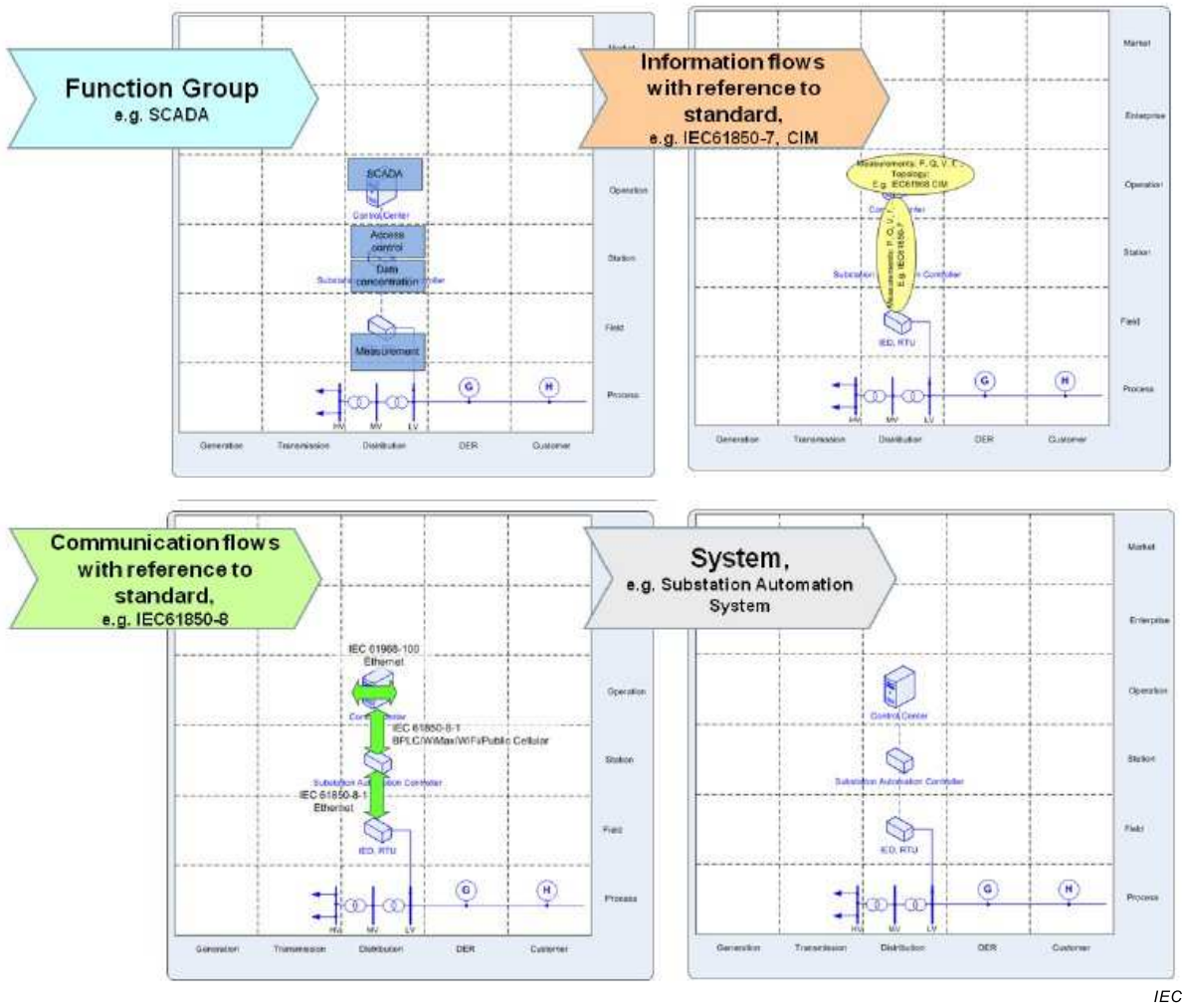


Figure 42 – SGAM analysis for the function "Monitoring inside the distribution grid"

The complete methodology, based on the use case methodology, involve identifying actors and step by step analysis. Exchange requirements should be identified (information, performances, security, reliability, etc.). If an IEC use case already exists, the information exchange specification could reuse the use case description and adapt it to its context for a better function description.

In order to help IEC standard users, IEC has provided a tool. The Mapping Tool allows to easily and instantly identify the standards that are needed for any part of the Smart Grids – there is no need to be a standards expert.

It provides reliable and reproducible results – every time – now and in the future. It is cost-effective and fast – no need to wade through thousands of pages of standards documents.

With this tool users are able to identify any given standard in relation to its role within the Smart Grids.

This document is a Reference Architecture document which has been considered as a basis to feed this tool.

Figure 43 describes the Mapping Tool layout:

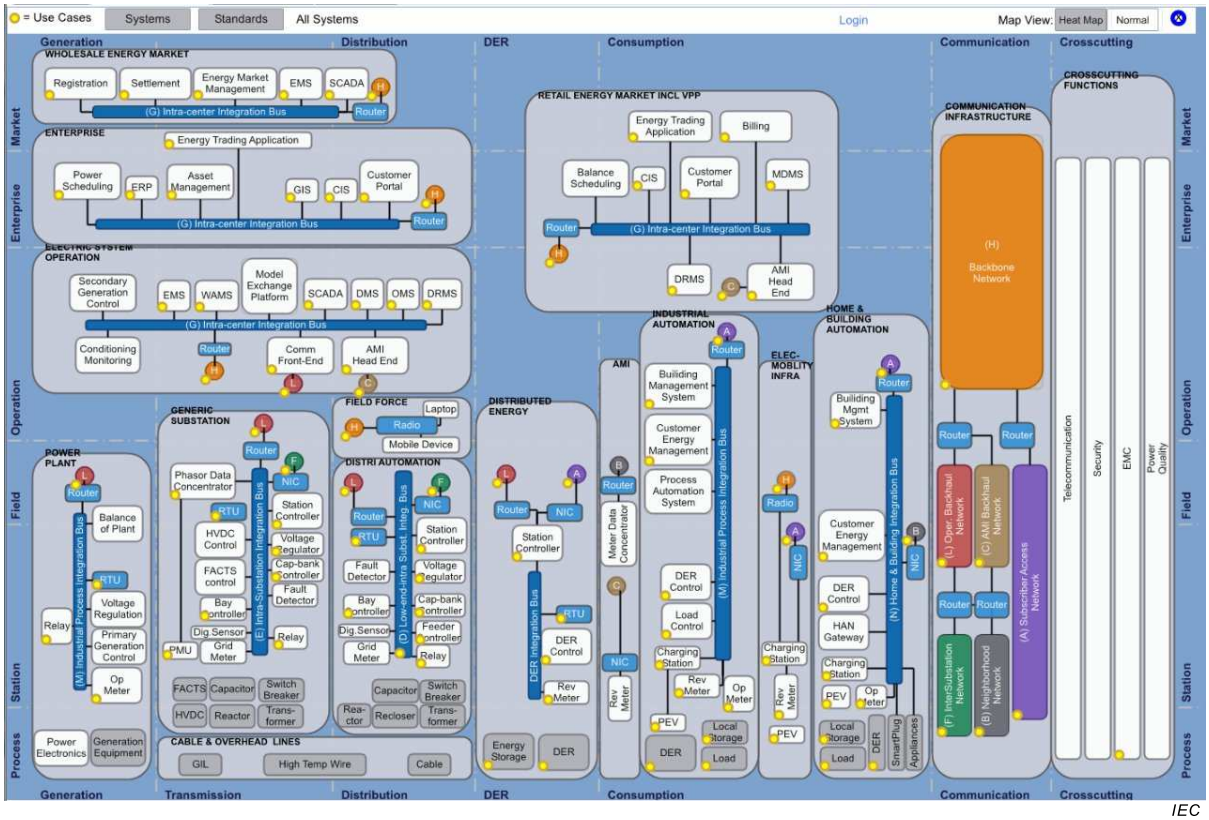


Figure 43 – IEC mapping tool

7.6 Integrating security in Reference Architecture

7.6.1 General

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. It typically not only comprises technical means such as the application of dedicated security measures, 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.

Hence, security in the Reference Architecture addresses both with a different level of detail, either as part of the IEC 62351 series or as contribution to other standards, e.g., ISO/IEC TR 27019 for example for a power system-specific Information Security Management Standard.

6.5.4 described the scope and target of the different parts of the IEC 62351 series. Two parts are emphasized here explicitly, as they target guidelines for defining a secure system architecture:

- IEC TR 62351-10:2012 targets the description of security architecture guidelines for power systems based on essential security controls. Note that the approach described in Part 10 closely aligns to the NIST IR 7628 defined categories and domains.

- IEC TR 62351-12: provides resilience recommendations for engineering/operational strategies and cyber security techniques that are applied to DER systems.

The definition of a security architecture is typically specific to a set of target use cases and follows a risk based approach. The risk based approach targets the identification and definition of security requirements. These in turn build the base to define security counter measures, which are then used to directly address the identified security requirements.

Subclause 7.6.2 aims to provide an overview of the approach for defining security architecture as well a list of selected security controls.

7.6.2 Identification of security requirements

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 or security levels 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. Depending on the availability of existing systems this approach may not only target a conceptual assessment but also a practical assessment, both approaches leading to distinct security requirements as shown in Figure 44.

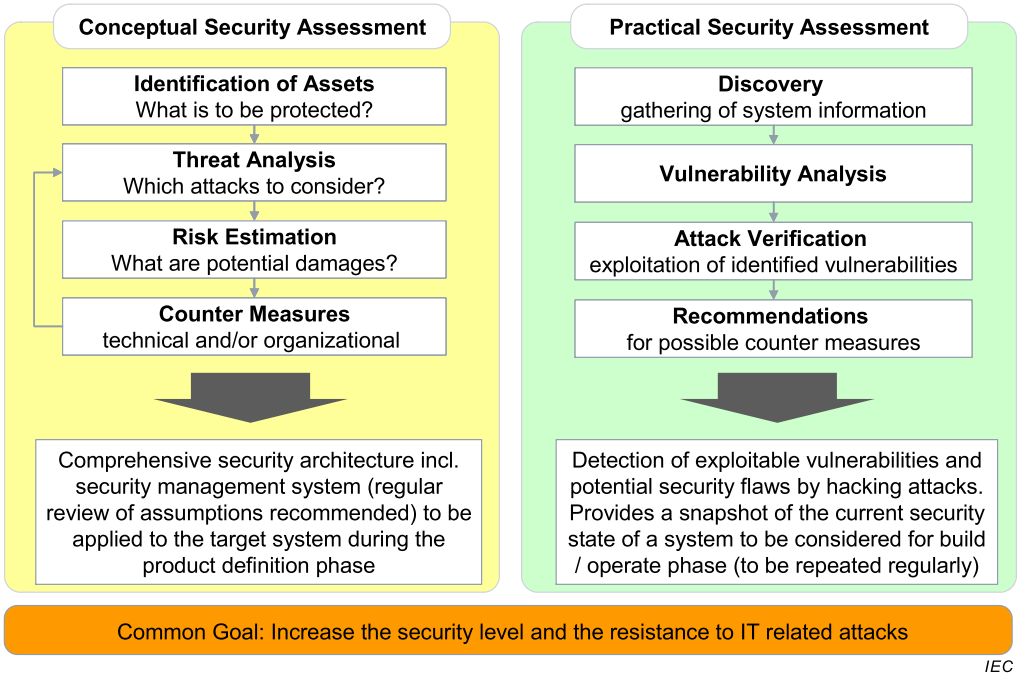


Figure 44 – Security assessment types supporting Security Architecture design

The first step is the identification of information assets and their relation to the system security based on a given set of use cases. Based on the use cases the data and information flow is analysed, providing a view on, which components communicates with which other components and what is the influence of the communicated content to the operation of the overall power system. Example data to be analysed is provided in Table 6.

Table 6 – Information assets and their relation to system security

Information asset	Description, potential content	Security relation
Customer ID and location data	Customer name, identification number, schedule information, location data	Effects on customer privacy
Meter Data	Meter readings that allow calculation of the quantity of electricity consumed or supplied over a time period and may be used for controlling energy loads but also for interactions with an electricity market.	Effects on system control and billing
Control Commands	Actions requested by one component of other components via control commands. These commands may also include Inquiries, Alarms, Events, and Notifications.	Effects on system stability and reliability and also safety
Configuration Data	Configuration data (system operational settings and security credentials but also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behaviour of a component and may need to be updated remotely.	Effects on system stability and reliability and also safety
Time, Clock Setting	Time is used in records sent to other entities. Phasor measurement directly relates to system control actions. Moreover, time is also needed to use tariff information optimally. It may also be used in certain security protocols.	Effects on system control (stability and reliability and also safety) and billing
Access Control Policies	Components need to determine whether a communication partner is entitled to send and receive commands and data. Such policies may consist of lists of permitted communication partners, their credentials, and their roles.	Effects on system control and influences system stability, reliability, and also safety
Firmware, Software, and Drivers	Software packages installed in components may be updated remotely. Updates may be provided by the utility (e.g., for charge spot firmware), the car manufacturer, or another OEM. Their correctness is critical for the functioning of these components.	Effects on system stability and reliability and also safety
Tariff Data	Utilities or other energy providers may inform consumers of new or temporary tariffs as a basis for purchase decisions.	Effects on customer privacy and also competition

The identification of assets is done based on a use case description, which uses SGAM. The assets to be protected can be identified based on the considered SGAM layer. The assets listed in the table above are related to the information layer, which in turn utilizes protocols defined in the IEC.

7.6.3 Mapping of security to power system domains

IEC 62351-10 contains a mapping of the security domains to the power system domains. Meanwhile, through the adoption of the SGAM, this definition is split into layers, domains, and zones as discussed in 6.1.3. Using SGAM, security requirements and tasks targeting technical or organizational means can be easily mapped to the SGAM layers, as shown in Figure 45.

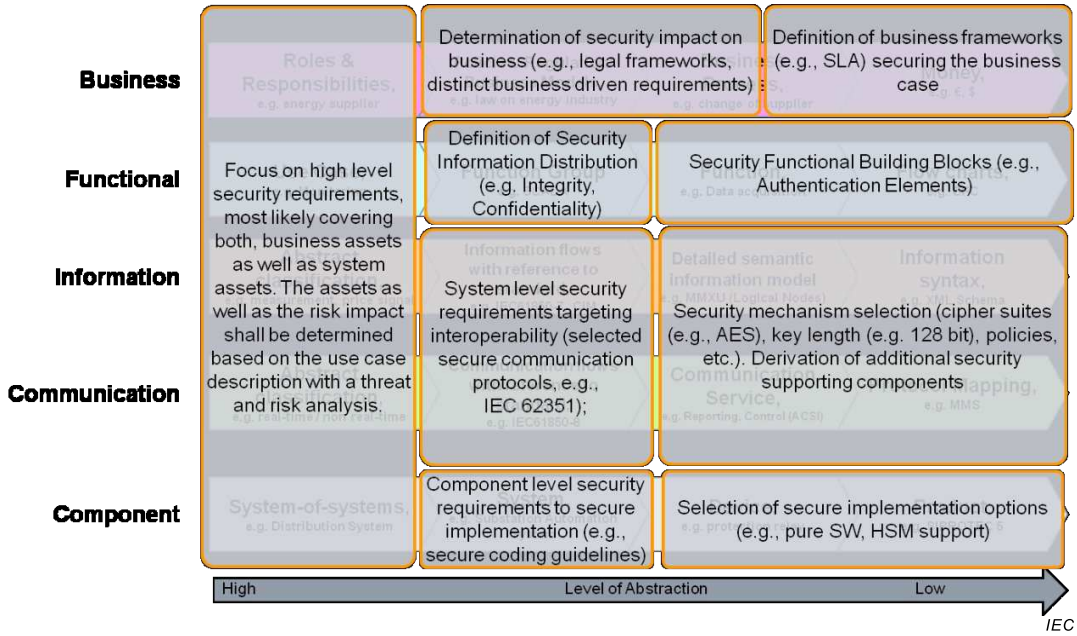


Figure 45 – Security requirements and tasks per SGAM Layer depending on the abstraction layer

As shown, security means are easily distinguished on the different SGAM layers. The diversion into zones and domains will rather lead to specific realizations of the security requirements, e.g., depending on the utilized processes or protocols. The different IEC 62351 parts (3, 4, 5, 6, 7, 8, 9, 11) target explicit technical means for security with the goal to achieve an interoperable solution.

7.6.4 Security controls

Security controls describe specific security counter measures to avoid, counteract or minimize security risks. Following the definition in IEC 62351-10 they 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.
- operational security controls like state analysis or contingency analysis;
- legal and regulatory or compliance controls e.g. privacy laws, policies and clauses.

Figures 46 and 47 provide examples for each of the categories.

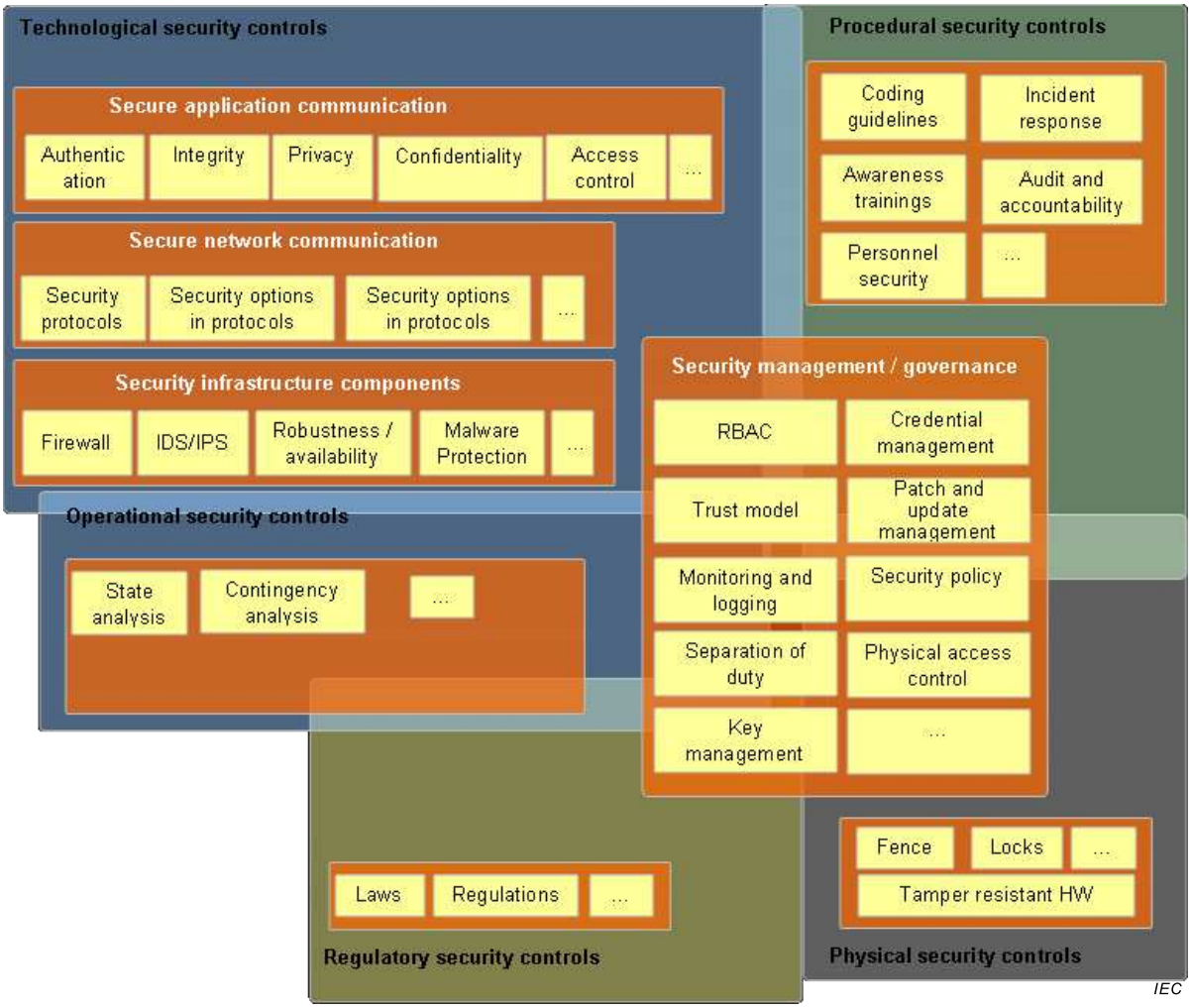


Figure 46 – Security Controls

As stated above, the determination of security controls is done by their capability to address identified security requirements. This also needs to take into account that there are different security levels and that these security levels may result in different strength of a security control. With IEC 62443-3-3 there exists a standard providing a relation between the strength of a security measure and an achievable security level. Four security levels are defined relating to different strength of security means, as shown in Figure 47 on the example of user authentication.

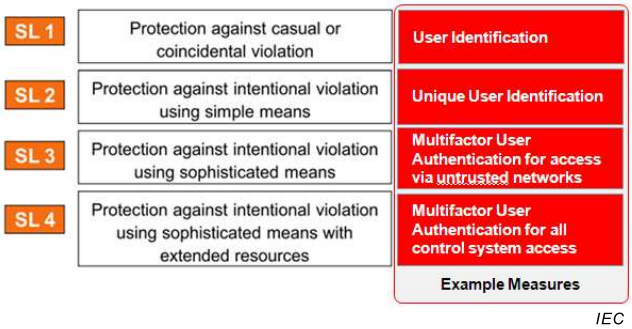


Figure 47 – Addressing security requirements with security means of different strength

The application of this approach requires typically a two stage process, the determination of the actual security needs expressed by a target security level. In a second step the selection

of appropriate security controls coping with the target security level. Here, mechanisms defined in IEC 62351 can be directly applied as security controls.

Refer also to the bibliography.

8 Main areas of future standardisation work

8.1 General

The Power System Reference Architecture has evolved on a regular basis as described in Figure 48:

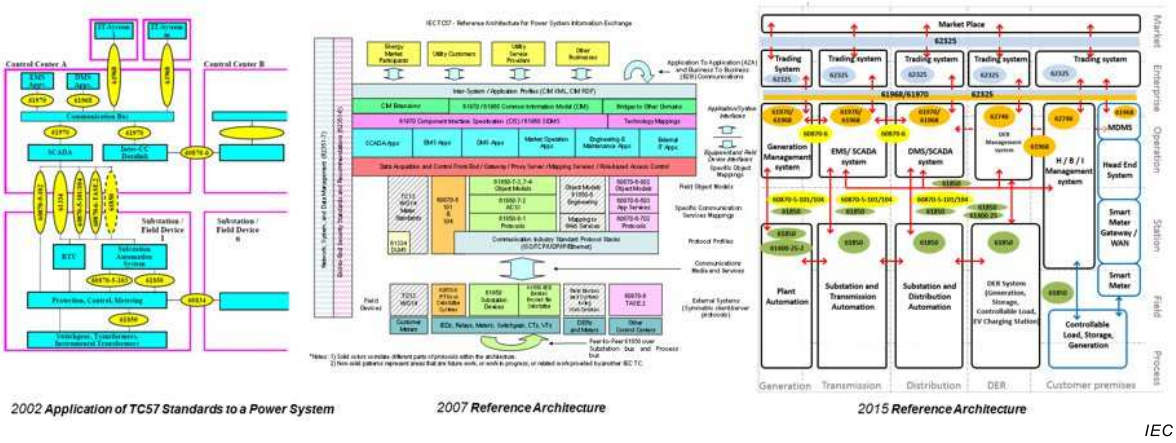


Figure 48 – RA through time

In 2002, the focus was Substation Automation and Control Centers.

In 2007, the focus was extended to Entreprise Integration.

In 2016, the security and telecommunication aspects are part of the Reference Architecture, and a strong emphasis is given to the methodology approach, using the SGAM interoperability layers, from use case requirements down to profile definitions.

8.2 Increase standard usage efficiency through digitalisation

It is believed that standard usage will increase through digitalisation. A model-driven engineering approach has been taken: from UML CIM and IEC 61850 models, IEC standards are derived (profiles, documentation, etc.), which insure more consistency. Use cases, which can also be formalized in UML, are managed by Use Case managers, CIM and IEC 61850 UML models are managed by Model Managers.

From models, software artefacts can be generated which facilitate the development process.

8.3 Harmonise data modelling

Harmonised data modelling is already taking place at the IEC level, and CIM and IEC 61850 are following an harmonisation process (see D.9, WG 19 roadmap).

CIM and IEC 61850 are one of the main assets of IEC for the considered area and they fit well the requirements of their respective markets

The vision is to reinforce the relevancy of each on its own domain to better support the drivers defined in introduction such as:

- Preserve backward compatibility
- Facilitate their usage, have seamless processes to manage the different phases of the lifecycle
- Extend the scope base market requirements
- Offers bridging capabilities while reducing the distance between both

8.4 Other future topics

In the future it is also expected to:

- Extend standard application coverage
- Extend protocol support by use of on the shelves communication technology
- Reinforce and harmonise cyber security everywhere

9 Conclusion

A new Reference Architecture for power system information exchange is proposed to provide a framework for future standards development and for resolution of differences in object models within standards currently under development.

It is hoped that by providing an overview and more concrete framework for standards development, more insight will be available to all contributors for the harmonization of power system object models. This will in turn lead to greater acceptance of IEC standards in new product development and fewer incompatibilities requiring custom adapters and gateways for implementing new computer systems and network for power system control.

Furthermore, now IEC standards, especially the CIM (IEC 61968 / IEC 61970 / IEC 62325 / IEC 62746) and IEC 61850 standards, have been recognized as pillars for realization of the Smart Grid objectives of interoperability and device management, it is imperative that a correct understanding of these standards and their application be made available to the key stakeholders and all other interested parties involved in implementing the Smart Grid.

The Reference Architecture for power system information exchange is constantly evolving as new standards are developed and existing standards are modified. As a result, this report should be treated as a living document, wherein future editions of this document will be needed to reflect the latest new developments as well the results of harmonization efforts.

Annex A
(informative)

SGAM Layer description

Figure A.1 shows a SGAM layer description.

Layer	Description
Business	The business layer represents the business view on the information exchange related to smart grids. SGAM can be used to map regulatory and economic (market) structures (using harmonized roles and responsibilities) and policies, business models and use cases, business portfolios (products & services) of market parties involved. Also business capabilities, use cases and business processes can be represented in this layer.
Function	The function layer describes system use cases, functions and services including their relationships from an architectural viewpoint. The functions are represented independent from actors and physical implementations in applications, systems and components. The functions are derived by extracting the use case functionality that is independent from actors.
Information	The information layer describes the information that is being used and exchanged between functions, services and components. It contains information objects and the underlying canonical data models. These information objects and canonical data models represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means.
Communication	The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.
Component	The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system & device actors, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers.

IEC

Figure A.1 – SGAM layer description

Annex B
(informative)

Elements examples

B.1 Example of control centre distribution systems

Figure B.1 represents typical network operation systems, and their relationships with other typical distribution systems:

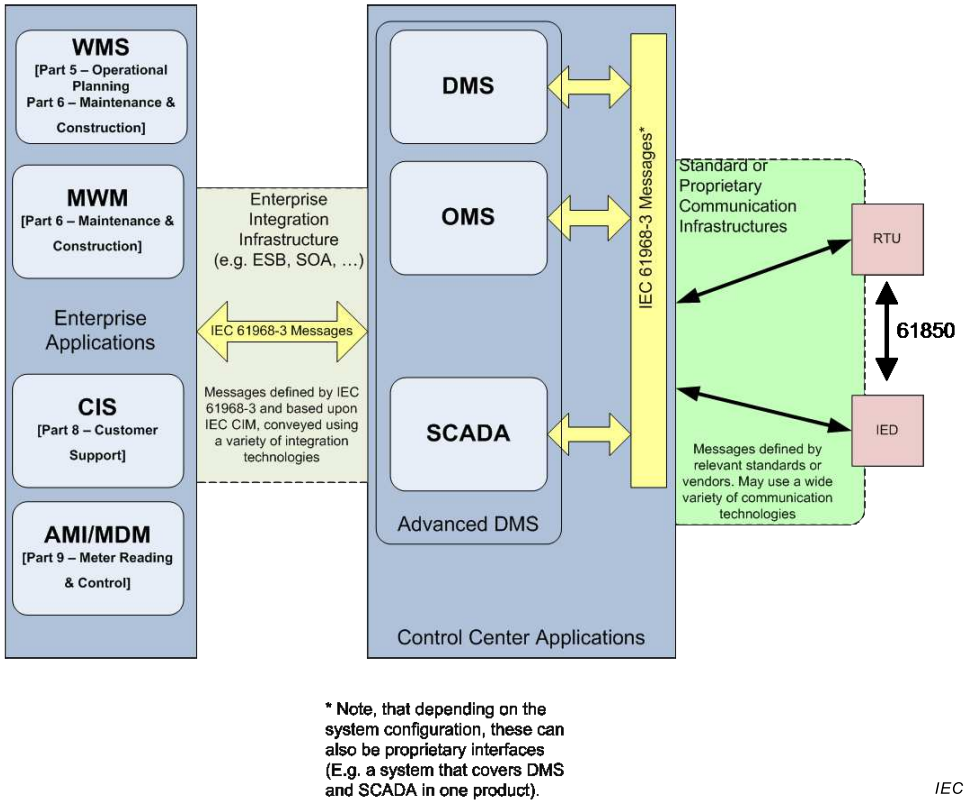


Figure B.1 – Example of control centre distribution system and relationships with other typical distribution systems

The Smart Grids component, the ADMS system, is based on DMS, OMS, and SCADA as abstract components. These abstract components are grouped by the business functions and sub-functions of the IRM and support one or more interfaces defined in CIM-based standards.

B.2 Example of a system, the case of network model management system

The term ‘network model management’ (NMM), refers to all data management activities for all types of analysis that require network models (power flow, state estimator, contingency analysis, short circuit, dynamics, transients, etc.) and all situations that require network analysis (operations, operations planning, long-term planning).

Figure B.2 illustrates this kind of system and how NMM is expected to relate to other systems involved in network model management:

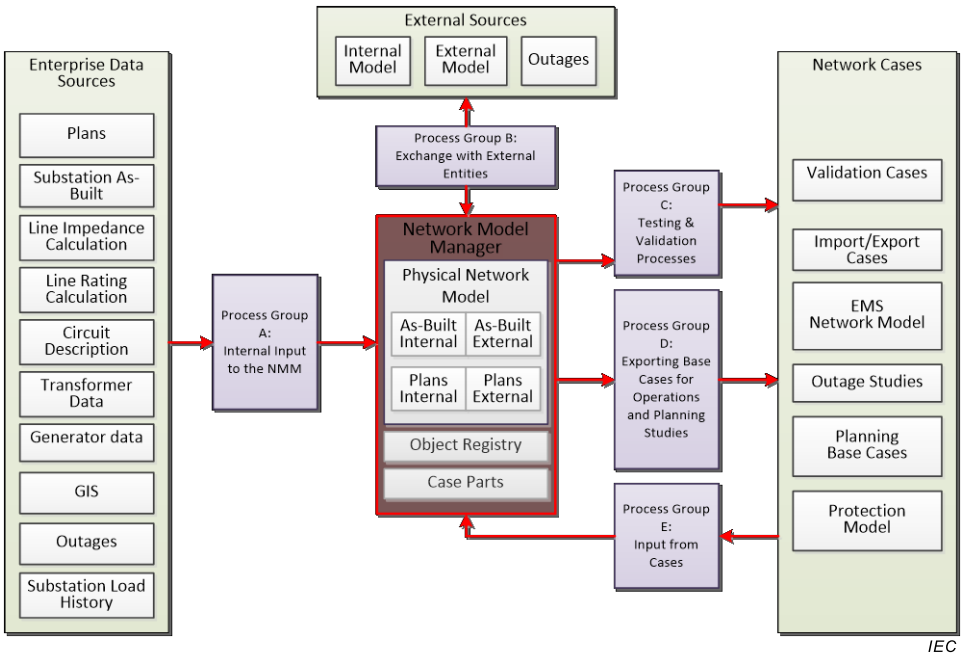


Figure B.2 – Network Model Management and other involved systems

The NMM In this diagram, the light green shaded boxes identify existing sources of and destinations for network model information:

- Enterprise data sources represent information from host system operator systems that are the original source for parts of the data required in network models.
- External sources represent information in systems outside the host system operator, such as other system operators or neighbouring utilities, from which the system operator can get models of neighbouring grid territory and to which the system operator must supply models of itself.
- Network cases are analytical cases managed within network analysis systems such as EMS or planning or protection applications.

B.3 Example of a power flow component

There are two basic aspects of input to any power flow study: the first is the physical network model (the configuration of equipment and connectivity) and the second is a steady-state (or operating) hypothesis for the study (the operating condition to be studied). The output is a set of values for the network variables (primarily flows and voltages) that satisfy the laws of physics at one instant in time. Together, the input and output make up a case – where a 'case' is defined as being the data (input and optionally output) associated with a power flow or state estimator for one instant in time.

Figure B.3 shows the specific components that make up a case, as defined by CIM standards. In the diagram, rounded-corner rectangles are used to represent sets of data and square-corner rectangles are used for processes.

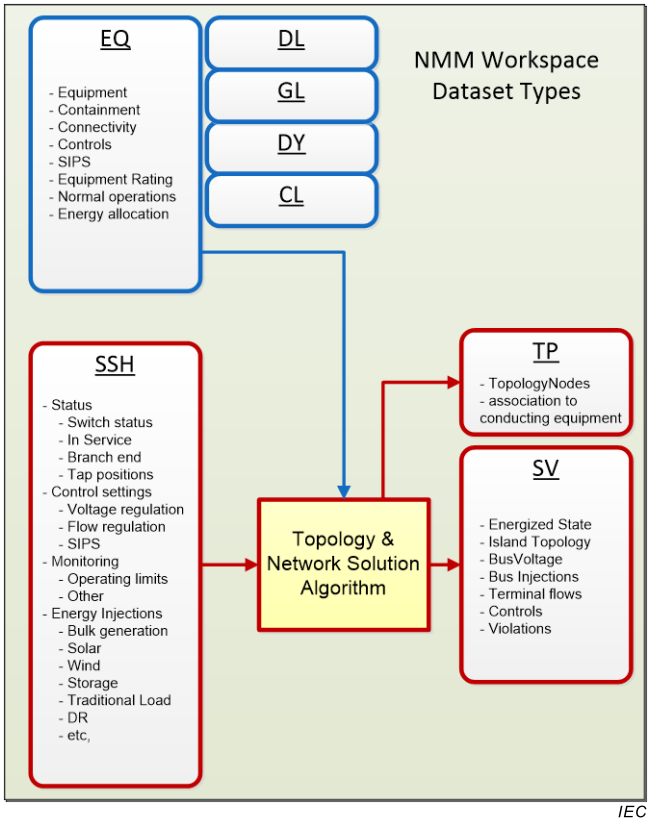


Figure B.3 – Parts of a CIM network case

The components outlined in blue contain the physical network model data. They include the following kinds of network model parts:

- EQ (IEC 61970-452 CIM static transmission network model profile, IEC 61968-13 CIM static distribution network model profile) – Describes the steady-state electrical characteristics of the equipment and describes how the equipment is connected together (connectivity).
- DL (IEC 61970-453 Diagram layout profile) – Describes any diagram layouts that are used. (Optional)
- GL (subset of IEC 61968-4) – Describes any geographic location data. (Optional)
- DY (IEC 61970-457[14] Dynamic profiles) – Describes dynamic modelling. (Required only if the case is going to be used for dynamic analysis.)
- CL – Describes contingency list. (Required only if the case is going to be used for contingency analysis.)

The components outlined in red describe the operating condition under study. This includes:

- SSH – Describes the input data that defines the steady-state hypothesis. This includes device status, load and generation, control settings, operating limits, etc.
- TP (subset of IEC 61970-452) – Describes the topology that results from processing closed switching devices into traditional power flow ‘buses’.
- SV (IEC 61970-456 Solved power state profiles) – Describes the state variables that are produced by the network analysis solution algorithm.

14 Under preparation. Stage at the time of publication: IEC/PWI 61970-457:2016.

Annex C
(informative)

Relationship examples

C.1 General

Reference Architecture relationships allow communication between elements.

C.2 Data transformation via gateways and adapters

Figure C.1 illustrates the relevant interfaces and the transformations required when these standards are applied today. SCADA data received via IEC 60870-6 TASE.2 links from either another control center or from a SCADA master in a substation is transformed in the TASE.2 Adapter to be compliant with the IEC 61970 CIM. More specifically, it is transformed to comply with the SCADA interface defined as part of the EMS-API standards. This data is then exposed to the integration bus via one of the standard interfaces. In a similar fashion, SCADA data received via IEC 61850 ACSI links from either substation or field devices is transformed in the ACSI Adapter to be compliant with the CIM and the same service interface. SCADA data from an existing SCADA system that uses the IEC 60870-5 standards, IEEE 1815, DNP3, or some proprietary RTU protocol is transformed by a custom SCADA System Adapter to be CIM-compliant.

The effect of the use of adapters is that all SCADA data, regardless of the protocols/services and data representation used to obtain the data from the field or from other control centers, has the same representation on the integration bus. This means that any applications that operate on SCADA data, including data repositories or historical information systems, need to be designed to support only a single interface, the IEC 61970 EMS-API SCADA interface, to be able to be integrated into a system framework.

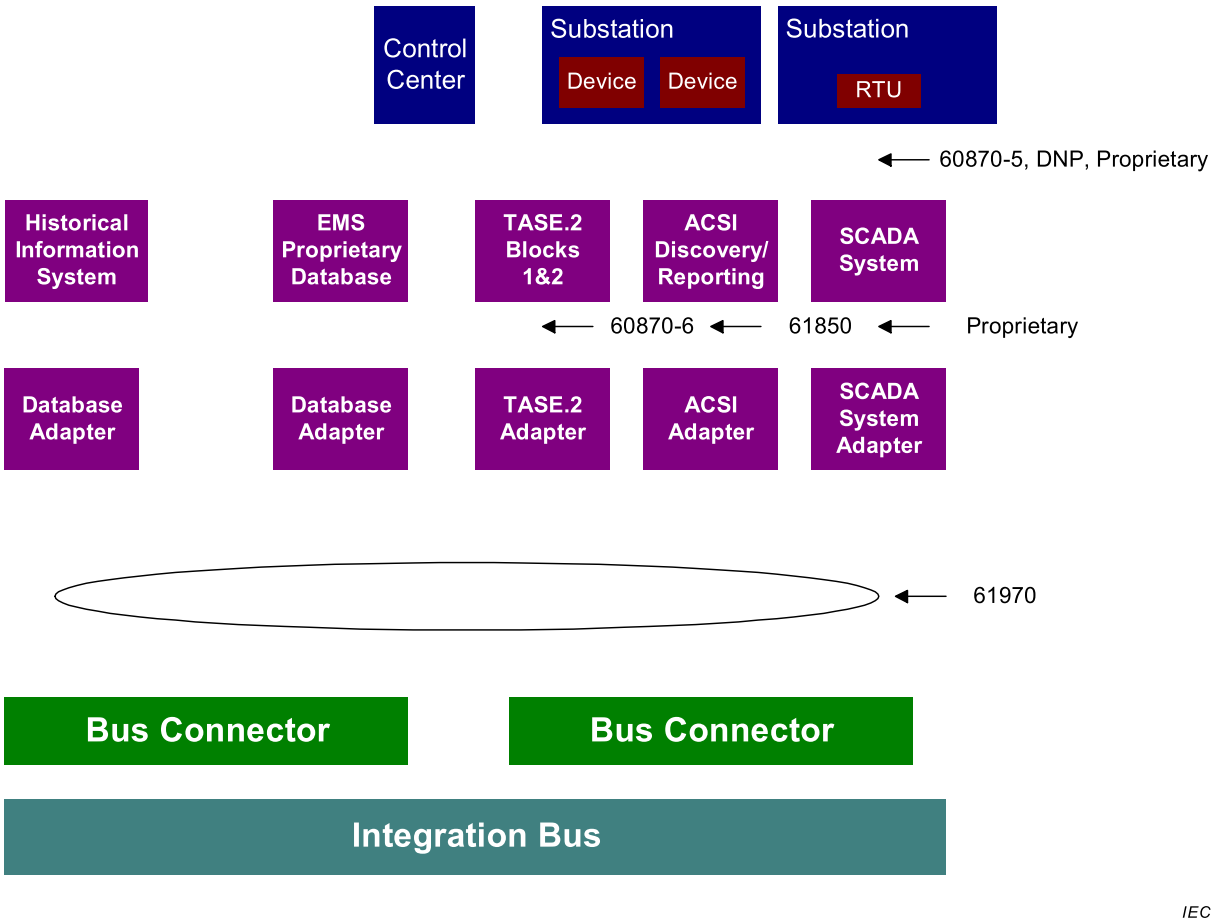


Figure C.1 – SCADA data interfaces

Figure C.1 also illustrates the use of database adapters to transform data from proprietary representations in an EMS database or from industry standard representations in a Historical Information System to the CIM representation for access via the integration bus.

C.3 Example of a Message Exchange

Figure C.2 attempts to provide an overview of the IEC 61968-100 scope, where IEC 61968 compliant messages are conveyed using web services or JMS. Through the use of an ESB integration layer, the initiator of an information exchange could use web services, where the receiver could use JMS, and vice versa. The integration layer also provides support for one to many information exchanges using publish/subscribe integration patterns and key functionality such as delivery guarantees.

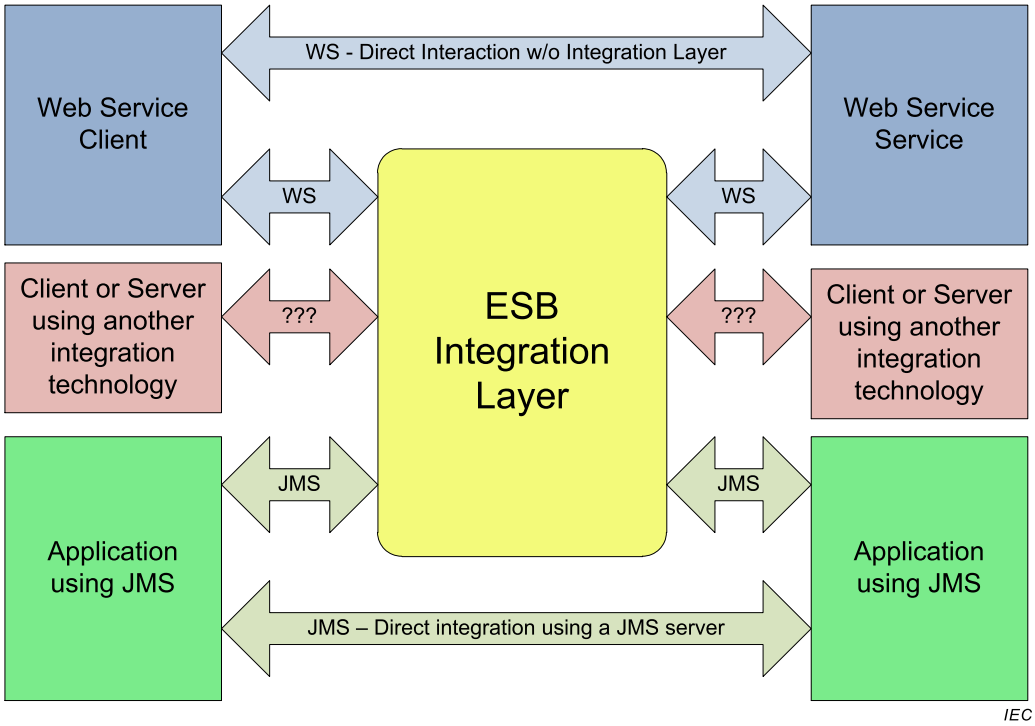


Figure C.2 – IEC 61968 associated communication technologies

At the Enterprise domain level, several use cases related to the interactions between components within a set of systems cooperating to support a set of business processes can be described. It is important to note that the use cases can be described from the perspective of the integration of systems, or be end use application-level use cases. In the context of integration of systems, the actors for the use cases include the following: Client, Server, ESB, Adapter, Subscriber (an Event Listener). End use application level use cases use IRM system actors.

IEC 61968-100 will be extended to take into account Extensible Messaging and Presence Protocol (XMPP), which is used for real time communication of XML data. This standard was formalized by the IETF in 2004. Figure C.3 represents an XMPP architecture, where clients connect to XMPP servers.

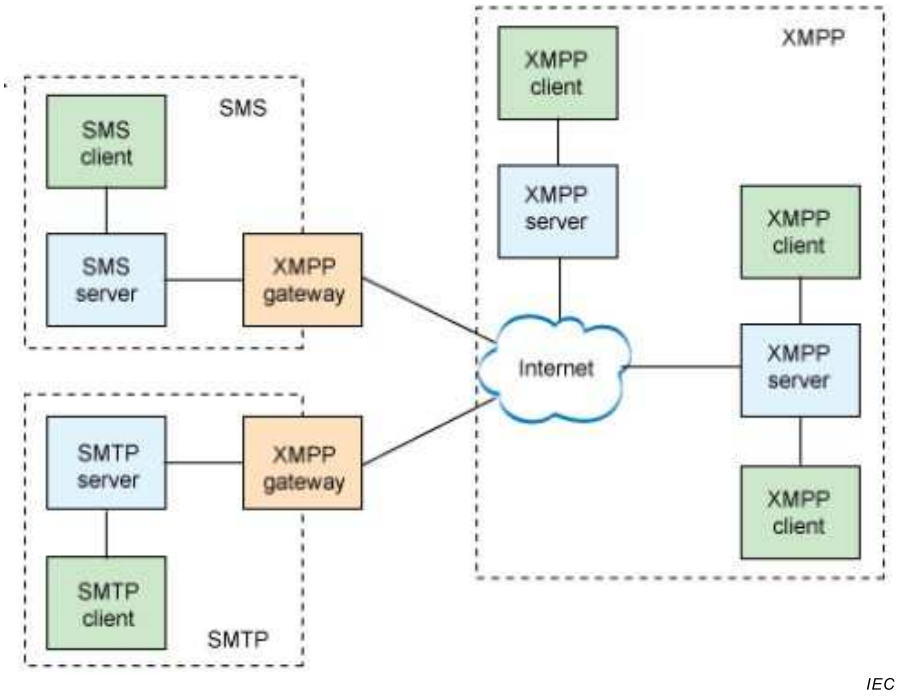


Figure C.3 – XMPP architecture concept

In the context of SmartGrid, XMPP can be used as transport for communication between market operators, grid operators, utilities, service providers and resources as illustrated in Figure C.4:

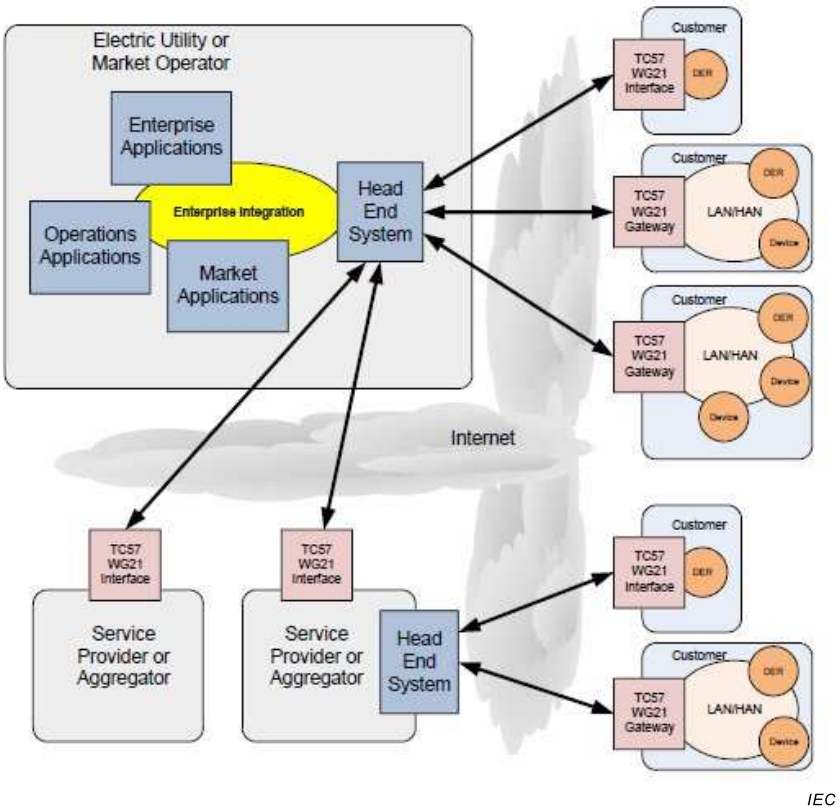


Figure C.4 – Use of XMPP example

Annex D
(informative)

TC 57 standards descriptions and roadmaps

D.1 TC 57 Working Group 03

<table>
<tr><th colspan="3">WG 03 – Telecontrol protocols</th></tr>
<tr><th colspan="2">Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td colspan="2">• The task of WG 03 is to standardize telecontrol protocols with high integrity, high reliability and appropriate security
• Telecontrol protocols defined by WG 03 apply to telecontrol equipment and systems controlling widespread processes using wide area communication networks (serial, IP-based)</td><td>• Maintenance cycle of IEC 60870-5 companion standards and conformance test cases accepted by NCs (57/1473/DC, 57/1491/INF)
• Amendment 1 for IEC 60870-5-101 Ed.2 and IEC TS 60870-5-601 Ed.2 published
• Amendment 1 for IEC 60870-5-104 Ed.2 and IEC TS 60870-5-604 Ed.2 published</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016</th></tr>
<tr><td>Release:
• IEC 60870-5-101/-104 Ed.2
IEC 60870-5-601/-604 Ed.1

Correction of Ambiguities between
IEC 60870-5-101/-104 Ed.2 and
IEC TS 60870-5-601/-604 Ed.1

CDV of Amendments

CDTS of
IEC TS 60870-5-601 Ed. 2 and
IEC TS 60870-5-604 Ed. 2</td><td>Release:
• IEC TS 60870-5-601/-604 Ed.2

FDIS of Amendments

IEC TS 60870-5-601/-604 Ed.2

• IEC 60870-6-503
• IEC 60870-6-702
• IEC 60870-6-802</td><td></td></tr>
</table>

D.2 TC 57 Working Group 10

D.2.1 General

<table>
<tr><th colspan="3">WG 10 – Power system IED communication and associated data models</th></tr>
<tr><th colspan="2">Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td colspan="2">• WG 10 is developing standards and technical reports related to the communication and data models of Power System IEDs
• WG 10 is responsible for the generic aspects of IEC 61850 and coordinates with other WGs that are developing domain specific data models</td><td>• Improve and extend IEC 61850 for the usage in substation automation
• Support other domains using IEC 61850 by improving and extending the basic concepts as needed
• Improve the standard to facilitate easy integration of multivendor systems based on the standardized data models and the engineering language</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016</th></tr>
<tr><td>Data Models in UML/XML
• For maintenance
• Web based access
• For tools
Ed 2.1 auto-generated
Technical reports
• Condition monitoring (DTR)
• WAN Engineering guidelines (DTR)</td><td>Technical reports / specifications
• Guidelines for modelling applications (DTR)
• Logic modelling
• Commissioning testing (DTR)
• FACTS (DTR)
• Mapping DLMS</td><td>Technical reports / specifications
• Alarm handling
• Standardized Function / Sub function names for SCL
System management
• Mapping Modbus</td></tr>
</table>

D.2.2 IEC 61850 standard overview

Figure D.1 describes the IEC 61850 standard series:

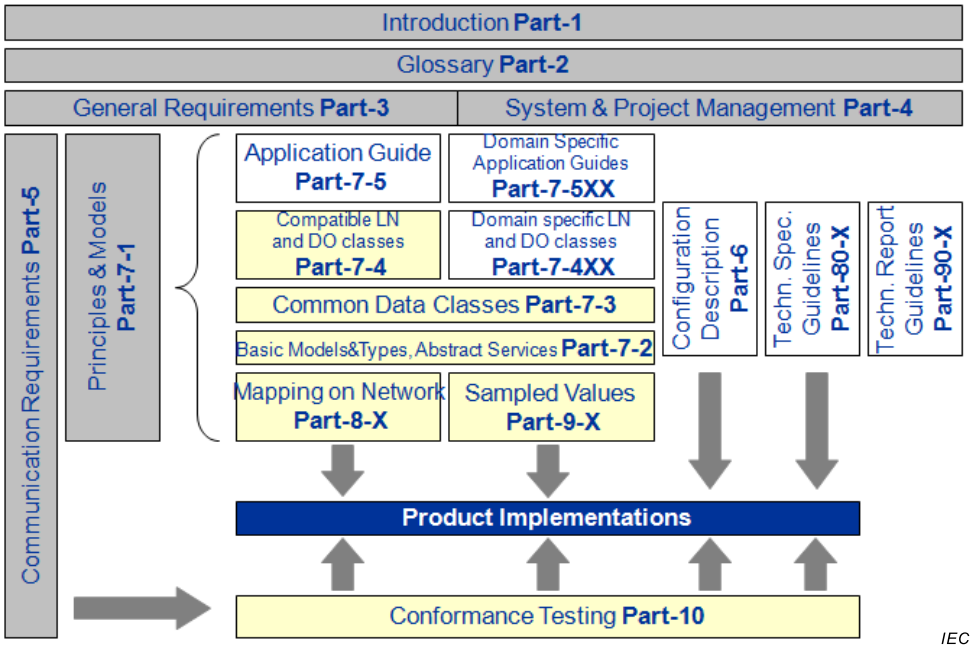


Figure D.1 – IEC 61850 standard series

- IEC TR 61850-1 gives an introduction and overview of the IEC 61850 standard series,

- IEC TS 61850-2 contains the glossary of specific terminology and definitions used in the context of power utility automation systems within the various parts of the standard,
- IEC 61850-3 specifies the general requirements of the communication network with regard to the quality requirements, environmental conditions and auxiliary services,
- IEC 61850-4 pertain to the system and project management with respect to the engineering process, the life cycle of the SAS and the quality assurance from the development stage to the discontinuation and decommissioning of the SAS,
- IEC 61850-5 specifies the communication requirements of the functions being performed in systems for power utility automation and to device models. All known functions and their communication requirements are identified,
- IEC 61850-6 specifies a file format for describing communication related IED configurations and IED parameters, communication system configurations, switchyard (function) structures, and the relations between them. The main purpose of the format is to exchange IED capability descriptions, and system level descriptions between engineering tools of different manufacturers in a compatible way. The defined language is SCL Mapping specific extensions or usage rules may be required in the appropriate parts,
- IEC 61850-7-1 defines the basic principles and modelling methods,
- IEC 61850-7-2 provides the services to exchange information for the different kinds of functions (for example, control, report, get and set, etc.) – how to exchange information,
- IEC 61850-7-3 has a list of commonly used information (for example, for double point control, 3-phase measure and value, etc.) – what the common basic information is,

  IEC 61850-7-4 defines specific information models for substation automation functions (for example, breaker with status of breaker position, settings for a protection function, etc.) – what is modelled and could be exchanged. Other domain specific information models within the scope of IEC technical committee 57 are defined in the IED 61850-7-4xx series,
- IEC TR 61850-7-5 defines the usage of information models for substation automation applications. It gives clear examples on how to apply LNs and data defined in IEC 61850-7-4 for different substation applications. The examples cover applications from monitoring function to protection blocking schemes. Other domain-specific application guides which are within the scope of IEC technical committee 57 are defined in the IEC 61850-7-5xx series[15]. Examples are Hydropower and Distributed Energy Resources domains,
- IEC 61850-8-1 defines the concrete means to communicate the information between IEDs (for example, the application layer, the encoding, etc.) – how to serialise the information during the exchange,
- IEC 61850-9-2, and particularly the subset 9-2LE described in the “Implementation Guideline for Digital Interface to Instrument Transformers using IEC 618509-2” by the UCAIug, defines the concrete means to communicate sampled values between sensors and IEDs.

15 E.g. IEC 61850-7-500, IEC TR 61850-7-510, IEC 61850-7-520, and so on.

D.3 TC 57 Working Group 13

D.3.1 General

<table>
<tr><th colspan="4">WG 13 – Energy Management Systems Application Program Interfaces (EMS API)</th></tr>
<tr><th colspan="2">Mission & Scope</th><th colspan="2">Organization & major activities</th></tr>
<tr><td colspan="2"></td><td colspan="2">• CIM UML issue resolution
• NWIPs: IEC 61970-302 and -457 Dynamic Model Exchange and -451 – SCADA Data Exchange
• IEC 61970-301 – CIM Base, sixth edition finalized based on CIM16
• IEC 61970-452 – CPSM, edition 2 and Edition 3 CDV in preparation for CIM15 and CIM16 respectively
• IEC 61970-456 – Solved power system state profiles: Amendment 1 to Ed. 1 published
• IEC 61970-555 – CIM/E: published
• IEC 61970-556 – CIM/G: published
• IEC 61968-13 Ed. 2 Common Distribution Power System Profiles [16]
• CIM Users Group
• liaison with ENTSO-E</td></tr>
<tr><th colspan="4">Roadmap</th></tr>
<tr><th colspan="2">2014</th><th>2015</th><th>2016</th></tr>
<tr><td colspan="2">Published
• IEC 61970-301 – CIM base, Ed 5 based on CIM15
• IEC 61970-452 – CIM static transmission network model profiles, Ed 1
• IEC 61970-453 – CIM diagram layout profile, Ed. 2
• IEC 61970-456 – Solved power system state profiles, Ed. 1
• IEC 61970-552 – CIM XML Model Exchange Format, Ed. 1
• Includes file header specification</td><td></td><td>IEC 61968-13 Ed 2</td></tr>
</table>

D.3.2 IEC 61970 standard overview

Figure D.2 describes the IEC 61970 (Working Group 13) series:

16 61968-13:− is managed by Working Group 13.

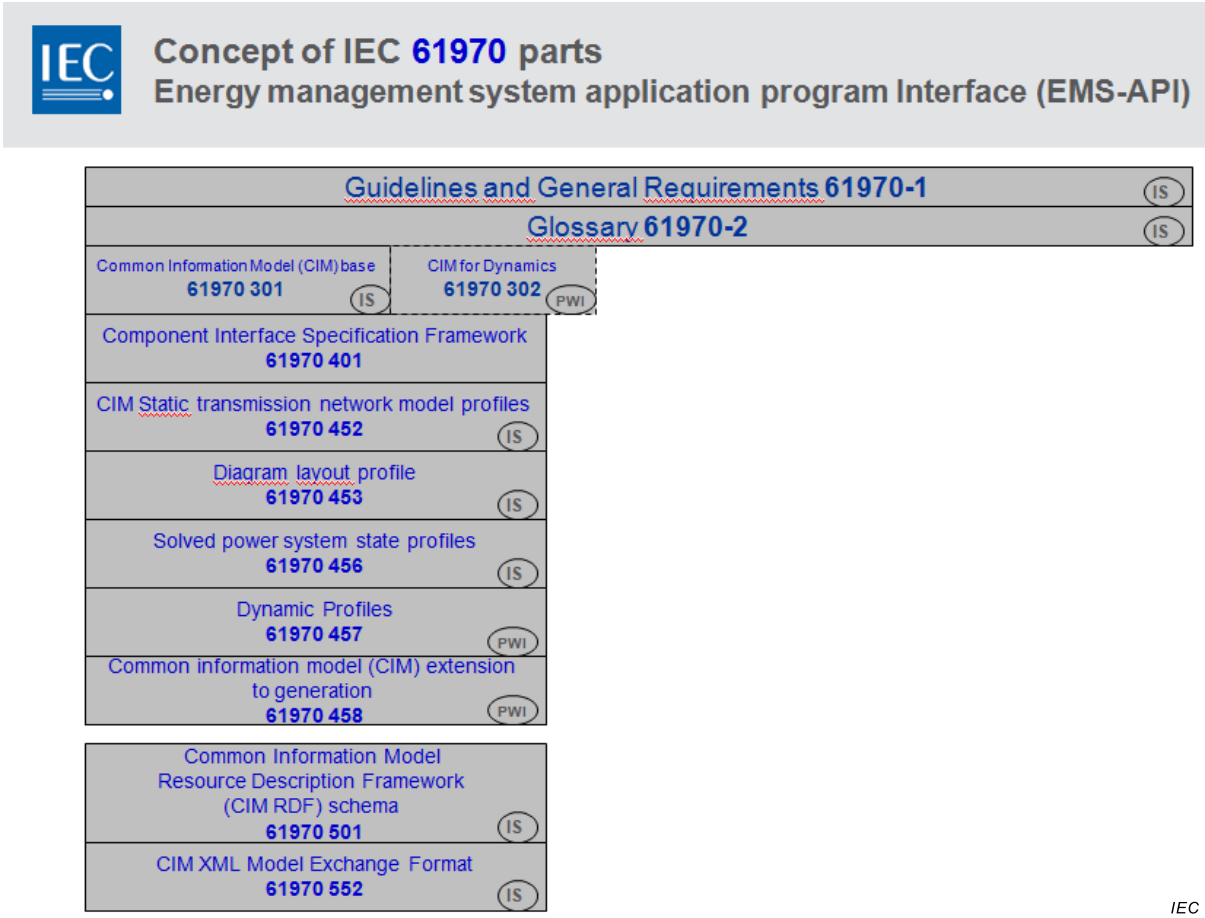


Figure D.2 – IEC 61970 standard series

D.4 TC 57 Working Group 14

D.4.1 General

<table>
<tr><th colspan="3">WG 14 – System Interfaces or Distribution Management</th></tr>
<tr><th>Mission & Scope</th><th colspan="2">Organization & major activities</th></tr>
<tr><td>• The IEC 61968 series is intended to facilitate inter-application integration of the various distributed software application systems supporting the management of utility electrical distribution networks within a utility's enterprise systems environment.
• The IEC 61968 series of standards supports this integration by:
– developing information exchange standards using the Common Information Model (CIM), normative message structures, additional normative parameters, informative recommendations and examples.</td><td colspan="2">WG 14 Organizes Its Work Around the IEC 61968-1 Interface Reference Model (IRM)
WG 14 Teams:
• IEC 61968-1 Architecture and General Requirements
• IEC 61968-2 Glossary
• IEC 61968-3 Network Operations
• IEC 61968-4 Records and Asset Management
• IEC 61968-5 Operational Planning and Optimization
• IEC 61968-6 Maintenance and Construction
• IEC 61968-7 Network Extension Planning
• IEC 61968-8 Customer Support
• IEC 61968-9 Meter Reading and Control
• IEC 61968-11 CIM Extensions for Distribution
• IEC 61968-13 Ed. 1 CIM RDF Model Exchange Format for Distribution
• IEC 61968-14 MultiSpeak – CIM Harmonization
• IEC 61968-100 Implementation Profiles
• IEC 61968-102 EXI for IEC 61968 XML Messages
• IEC 61968-103 Working Practices Style Guide
• IEC 61968-900 Guidance for implementation of IEC 61968-9
• Use Cases Ongoing Collaboration</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016</th></tr>
<tr><td>Submitted:
• IEC 61968-8 Customer Support
• FDIS
• IEC 61968-14 MultiSpeak – CIM Harmonization
• IEC 61968-900 Guidance for implementation of IEC 61968-9</td><td>To be submitted to IEC:
• IEC 61968-2 Glossary 3rd edition MCR
• IEC 61968-3 Network Operations CDV 2nd edition
• IEC 61968-5 Operational Planning and Optimization NWIP/CD
• IEC 61968-102 EXI for IEC 61968 XML Messages
• IEC 61968-103 61968 Working Practices Style Guide</td><td>To be reviewed by WG 14:
• IEC 61968-4 Records and Asset Management 2nd edition
• IEC 61968-13 CIM RDF Model Exchange Format for Distribution</td></tr>
</table>

D.4.2 IEC 61968 standard overview

Figure D.3 describes the IEC 61968 (Working Group 14) series:

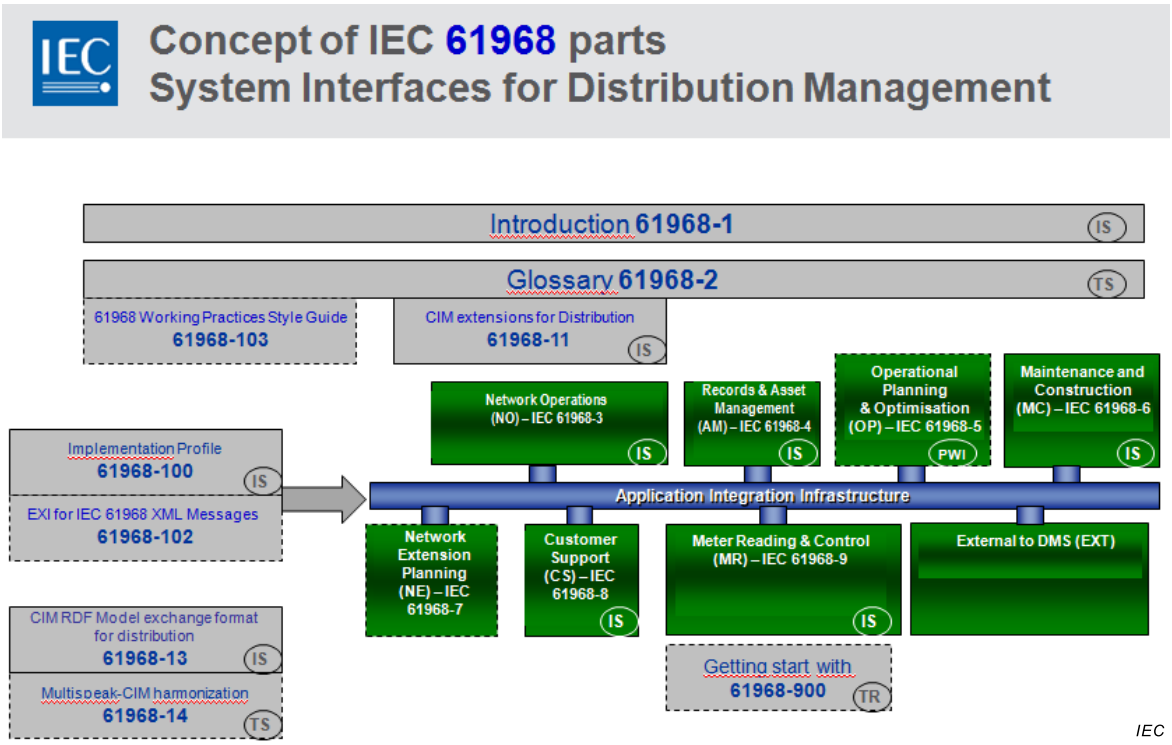


Figure D.3 – IEC 61968 standard series

D.5 TC 57 Working Group 15

D.5.1 General

<table>
<tr><th colspan="2">WG 15 – Data and Communication Security Status & Roadmap</th></tr>
<tr><th>Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td>• Undertake the development of standards for security of the communication protocols defined by IEC TC 57
– Specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series.
– Review and advise on cyber security of TC 57 standards
• Undertake the development of standards and/or technical reports on end-to-end security issues.</td><td>• IEC 62351
• Liaisons with Other Security Activities (ISO JTC 1 / SC 27 IT Security, M/490 SGIS, IEEE PES PSCC Security Subcommittee…)
• Coordination with Security Groups (NIST, NERC, CIGRE…)</td></tr>
<tr><th colspan="2">Roadmap</th></tr>
<tr><th>2014</th><th>2015+</th></tr>
<tr><td>Complete work for IEC 62351:
• Parts 1, 2, 3, 4, 5, 6, 7, 8, and 10 – finalized as TR or TS documents (Ed. 1)
• Part 5 as TS Ed. 2</td><td>• IEC 62351-2 Glossary: update pending
• IEC 62351-3 Security using TLS: published
• IEC 62351-4 Security for MMS: Ed. 2 started
• IEC 62351-5 Security for IEC 60870-5 and Derivatives: Amendment or Corrigendum
• IEC 62351-6 on IEC 61850: develop RR for updates to equivalent to IEC TR 61850-90-5
• IEC 62351-7 Network and system management: update process to Ed. 2 started in 2013
• IEC 62351-8 developing IEC TR 62351-90-1 as Guidelines for using RBAC
• IEC 62351-9 Key management: 2nd CD to be issued
• IEC 62351-11 Security for XML Files: published
• IEC 62351-12 Resilience and security for power systems with DER: published
• IEC 62351-13 What security topics should be covered in standards and specifications
• IEC 62351-14 Cyber security event logging
• IEC 62351-90-1 RBAC guidelines
• IEC 62351-90-2 Deep packet inspection
• IEC 62351-100-1 Conformity assessment of IEC 60870-5-7 (targeting IEC 62351-3/5)</td></tr>
</table>

D.5.2 IEC 62351 standard overview

IEC TC 57 Working Group 15 was formed in 1999 to develop security standards for the IEC TC 57 protocols and to address other cyber security issues for the power industry. The WG 15 title is “Power system control and associated communications – Data and communication security” and its scope and purpose are to:

“Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues.”

The justification for the formation of WG 15 was that safety, security, and reliability have always been important issues in the design and operation of systems in the power industry,

and cyber security is becoming more important in this industry as power system operations rely increasingly on information and communications technologies (ICT).

- IEC TS 62351-1: Introduction

This first part of the standard covers the background on security for power system operations, and introductory information on the series of IEC 62351 security standards.

- IEC TS 62351-2: Glossary of Terms

This part includes the definition of terms and acronyms used in the IEC 62351 standards. These definitions are based on existing security and communications industry standard definitions as much as possible, given that security terms are widely used in other industries as well as in the power system industry.

The terms in this glossary are provided for free access on the IEC web site at http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2

- IEC 62351-3: Security for Profiles That Include TCP/IP

IEC 62351-3 provides security for any profile that includes TCP/IP, including IEC 60870-6 TASE.2, IEC 61850 ACSI over TCP/IP, and IEC 60870-5-104.

Rather than reinventing the wheel, it specifies the use of TLS (Transport Level Security) which is commonly used over the Internet for secure interactions, covering authentication, confidentiality, and integrity. This part describes the parameters and settings for TLS that should be used for utility operations. Specifically, IEC 62351-3 protects against eavesdropping through TLS encryption, man-in-the-middle security risk through message authentication, spoofing through Security Certificates (Node Authentication), and replay, again through TLS encryption. However, TLS does not protect against denial of service. This security attack should be guarded against through implementation-specific measures.

- IEC TS 62351-4: Security for profiles that include MMS and similar payloads

IEC TS 62351-4 provides security for profiles that include the Manufacturing Message Specification (MMS) (ISO 9506) and similar payloads, such as IEC 60870-6 (TASE.2 (ICCP)), IEC 61850-8-1 (MMS-based), and IEC 61850-8-2 (XML/XSDs over XMPP).

The communication security provided by this standard include:

- Transport profile (layers 1-4 of the OSI Reference Model): this document specifies how to use Transport Layer Security (TLS) and the securing of IETF RFC 1006, requiring compliance with IEC 62351-3.
- Application profiles: An application profile defines the sets of protocols and requirements for layers 5-7 of the OSI Reference Model.

There are two T-profiles and four application profiles identified within the TC 57 context. This specification shall specify security extensions for all of the identified profiles except for the OSI T-profile.

- IEC TS 62351-5: Security for IEC 60870-5 and derivatives (i.e. DNP 3)

IEC TS 62351-5 provides different solutions for the serial version (primarily IEC 60870-5-101, as well as Parts 102 and 103) and for the networked versions (IEC 60870-5-104 and DNP 3).

Specifically, the networked versions that run over TCP/IP can utilize the security measures described in IEC 62351-3, which includes confidentiality and integrity provided by TLS encryption. Therefore, the only additional requirement covered in this standard is authentication.

The serial version is usually used with communications media that can only support low bit rates or with field equipment that is compute-constrained. In these situations, TLS would be too compute-intense and/or communications-intense. Therefore, the only security measures provided for the serial version include certain authentication mechanisms which address spoofing, replay, modification, and some denial of service attacks, but do not attempt to address eavesdropping, traffic analysis, or repudiation that require encryption. These encryption-based security measures could be provided by alternate methods, such as VPNs or “bump-in-the-wire” technologies, depending upon the capabilities of the communications and equipment involved.

- IEC TS 62351-6: Security for IEC 61850 peer-to-peer profiles (e.g. GOOSE)

The IEC 61850 profile that includes the MMS protocol running over TCP/IP uses IEC 62351-3 and IEC TS 62351-4. Additional IEC 61850 profiles that run over TCP/IP (web services or other future profiles) will use IEC 62351-3 plus possible additional security measures developed by the communications industry for application-layer security (out-of-scope for this set of standards).

IEC 61850 contains three protocols that are peer-to-peer multicast datagrams on a substation LAN and are not routable. The main protocol, GOOSE, is designed for protective relaying where the messages need to be transmitted within 4 milliseconds peer-to-peer between intelligent controllers. Given these stringent performance requirements, encryption or other security measures which may significantly affect transmission rates are not acceptable. Therefore, authentication is the only security measure included as a requirement, so IEC TS 62351-6 provides a mechanism that involves minimal compute requirements for these profiles to digitally sign the messages.

- IEC TS 62351-7: Security through network and system management

The information infrastructure in power operations is not typically treated as a coherent infrastructure, but is viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols. Often SCADA systems perform some minimal communications monitoring, such as whether communications are available to their RTUs, and then they flag data as “unavailable” if communications are lost. However, it is up to the maintenance personnel to track down what the problem is, what equipment is affected, where the equipment is located, and what should be done to fix the problem. All of this is a lengthy and often ad hoc process. In the meantime, the power system is not being adequately monitored, and some control actions may be impossible. As the analysis of the August 14, 2003 blackout in the US showed, the primary reason behind the blackout itself was the lack of critical information made available to the right user at the right time.

IEC TS 62351-7 focuses on Network and System Management (NSM) of the information infrastructure. Power systems operations are increasingly reliant on information infrastructures, including communication networks, intelligent electronic devices (IEDs), and self-defining communication protocols. Therefore, management of the information infrastructure is crucial to providing the necessary high levels of security and reliability in power system operations.

Edition 1 of IEC TS 62351-7 (2010) developed sets of abstract NSM data objects (see Figure D4) but did not map these to any protocol, suggesting that later work would undertake mappings to the IETF’s Simple Network Management Protocol (SNMP) and IEC 61850. In SNMP, Management Information Base (MIB) data is used to monitor the health of networks and systems, but each vendor must develop their own set of MIBs for their equipment. For power system operations, SNMP MIBs are only available for common networking devices, such as routers. Therefore Edition 1 of IEC 62351-7[17] defines the abstract NSM objects in UML, and then maps these UML objects to SNMP MIBs.

17 Under preparation. Stage at the time of publication: IEC/ADIS 62351-7:2016.

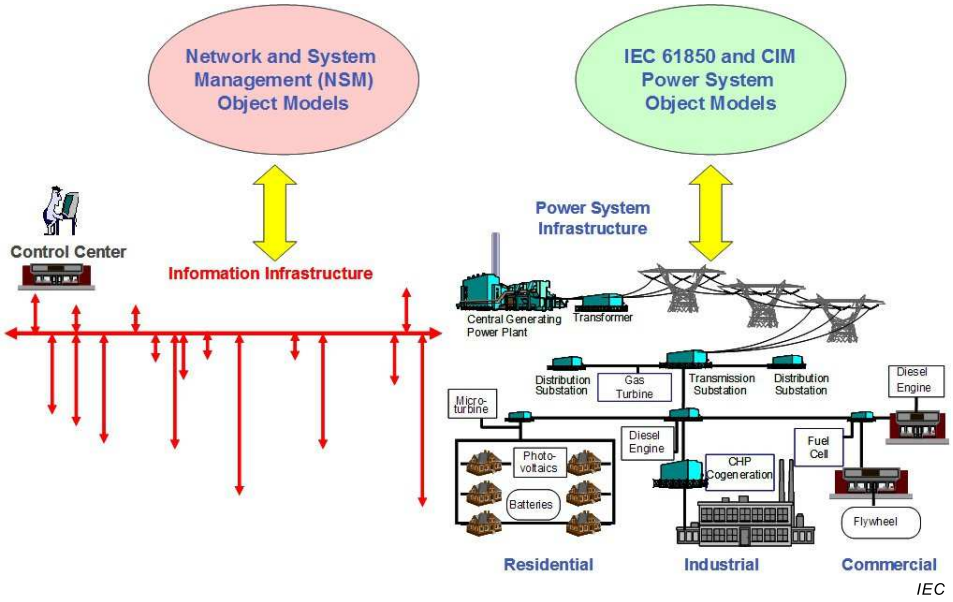


Figure D.4 – NSM object models

NSM object models are the Information Infrastructure equivalent to the CIM and IEC 61850 object models of the Power System Infrastructure

- IEC TS 62351-8: Role-based access control for power system management

The scope of this technical specification is the access control of users and automated agents to data object in power systems by means of role-based access control (RBAC). RBAC is not a new concept; in fact, it is used by many operating systems to control access to system resources. However, many power system devices treat all users alike – if the user has the device's password (and often the same password is used on many different devices), then they have complete access to all data and applications.

RBAC is an alternative to this all-or-nothing super-user model. RBAC is in keeping with the security principle of least permission, which states that no user should be given more privileges than necessary for performing that person's job. RBAC enables an organization to separate super-user capabilities and package them into special user accounts termed *roles* for assignment to specific individuals according to their job needs. RBAC is not confined to human users; it applies equally well to automated computer agents, i.e., software parts operating independent of user interactions.

Role-based access control is a technology that has the potential to reduce the complexity and cost of security administration in networks with large numbers of intelligent devices. Under RBAC, security administration is simplified through the use of roles and constraints to organize subject access levels. RBAC reduces costs within an organization primarily because it accepts that employees change roles and responsibilities more frequently than the rights within roles and responsibilities have to be changed. As in many aspects of security, RBAC is not just a technology; it is a way of running a business. RBAC provides a means of reallocating system controls, but it is the organization that decides the implementation.

The RBAC concepts developed in IEC TS 62351-8 are shown in Figure D.5.

The purpose of this document is therefore:

- Firstly, to introduce "subjects-roles-rights" as authorization concept (in ANSI INCITS 359-2004, referred to as "users-roles-permissions");
- Secondly, to promote role-based access control for the entire pyramid in power system management; and

- Thirdly, to enable interoperability in the multi-vendor environment of the power industry.

To achieve these goals, this part of IEC 62351 specifies the following items:

- Format of credentials, including subject name for logging;
- Mandatory security roles and permissions for administration, audit, and maintenance;
- Transmission of roles for TCP/IP and serial communications;
- Extensions in data models of power systems necessary to implement RBAC; and
- Verification of credentials in the target system to ensure secure access control.

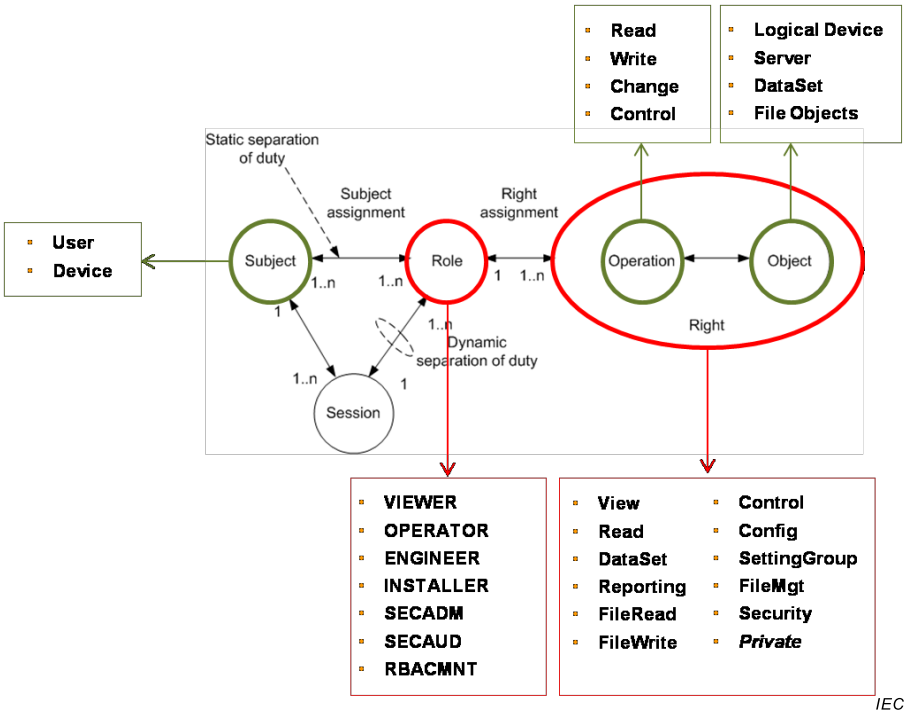


Figure D.5 – RBAC concepts in IEC TS 62351-8

Only a subset of possible roles is identified in this standard. Therefore additional work is on-going to develop categories and subcategories of roles and their privileges in IEC 62351-90-.

- IEC 62351-9: Key management

This part of IEC 62351 specifies how to generate, distribute, revoke, and handle digital certificates and cryptographic keys to protect digital data and its communication. Included in the scope is the handling of asymmetric keys (e.g. private keys and X.509 certificates), as well as symmetric keys (e.g. session keys).

This part assumes that other standards have already chosen the type of keys and cryptography that will be utilized, since the cryptography algorithms and key materials chosen will be typically mandated by an organization's own local security policies and by the need to be compliant with other international standards. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures. The objective is to define requirements and technologies to achieve interoperability of key management.

Cryptographic keys used with selected cryptographic functions can be used to secure the messages being sent between different entities, such as users, systems, software applications, communication nodes, and the potentially large numbers of devices that are often located at remote and often untrusted sites.

These cryptographic keys should be managed so that they can effectively and securely be provided to the entities that require secure exchanges of data. This key management must take into account many issues, ranging from the capabilities of entities, to the varied types of locations of these entities, to the timing for providing and revoking keys, and to protecting the key management processes itself from attacks.

For instance, many smaller devices are limited in computational power and memory capacity, while the communication networks may also be limited in available bandwidth. Therefore some of the key management techniques used in traditional enterprise information technology system environments are not well suited to power system automation and communication environments.

To address these constraints, this part specifies different key management techniques that should be used for different requirements. Specifically it specifies how to manage keys for each of the cryptographic functions specified in the other IEC 62351 parts.

- IEC TR 62351-10: Security architecture

IEC TR 62351-10 provides 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 guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards. It includes the Architecture of TC 57 protocols shown in Figure D.6:

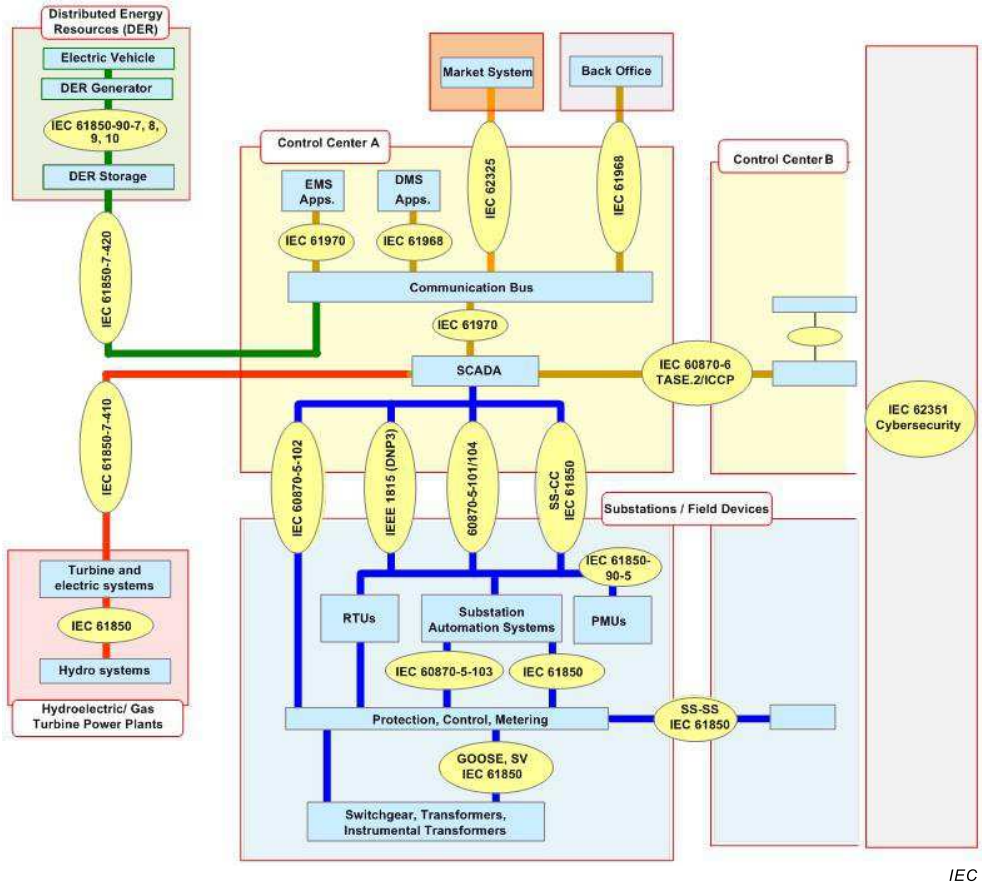


Figure D.6 – Architecture of IEC information exchange standards

- IEC 62351-11: Security for XML files

Within the industry and the IEC, the use of XML to exchange information is becoming more prevalent. Within the scope of the IEC, exchanges of XML-based documents are used for IEC 61970 as well as for some types of information exchanges in IEC 61850. XML-based information exchanges are also utilized within other standards, such as IEEE 1815 (DNP3) and IEEE C37.111 (COMTRADE). For these standards and other XML-based documents, the information contained in the document may:

- Be sensitive to inadvertant or malicious modifications of its contents that could result in mis-operation/misinterpretation if the exchanged information is used (e.g. a tamper security vulnerability).
- Contain confidential or private data.
- Contain subsets of information that may be considered sensitive by the document creation entity.

This part of IEC 62351 proposes to standardize mechanisms to protect the document contents from tampering/disclosure when the document is being exchanged (e.g. in transit). Additionally, this part proposes to standardize a mechanism to aid in the protection of the information when in transit across multiple parties with different trust relationships (e.g. entity A trusts entity B; B trusts A and C, and A needs to exchange information with C. but A does not know of or trust C). As an example, a utility (A) may trust an aggregator (B). The aggregator trusts the utility and a DER facility (C). The utility therefore sends an XML-based document with both sensitive and general information to the aggregator and “trusts” that the aggregator will only send the non-sensitive information on to the DER facility. This part provides a mechanism to identify the sensitive information so that the middle entity (B) can determine not to send it on.

Although this document is intended to secure XML documents used within the scope of the IEC, the mechanism/methodologies specified within this document can be applied to any XML document.

- IEC TR 62351-12: Resilience for power systems with DER systems

This document provides resiliency recommendations that recognize the need for integrating both cyber security techniques with engineering/operational strategies in order for power systems with Distributed Energy Resources (DER) systems achieve equal or greater resilience to attacks, failures, and natural disasters. It covers the resilience requirements for the many different stakeholders of these dispersed cyber-physical generation and storage devices, with the goal of enhancing the safety, reliability, power quality, and other operational aspects of power systems, particularly those with high penetrations of DER systems.

While recognizing that the resilience of the power system to anomalous conditions has many components and extends far beyond the impacts of DER systems, the focus of this document is the role of DER systems in grid resiliency, including:

- DER system resilience: The cyber security and engineering strategies for designing and installing DER systems to provide DER resilience to anomalous power system events and cyber-attacks.
- Grid resilience for grid planning with significant numbers of DER interconnections: The cyber security and engineering strategies for promoting grid resilience by studying the impact of and planning for interconnecting DER systems with the grid to promote grid resilience.
- Grid resilience for grid operations with significant capacity of DER generation and storage: The cyber security and engineering strategies for operating the grid with significantly large numbers and capacities of DER systems that can impact grid reliability and security.

Figure D.7 illustrates the types of communications required between the various stakeholders involved in operating power systems with interconnected DER systems.

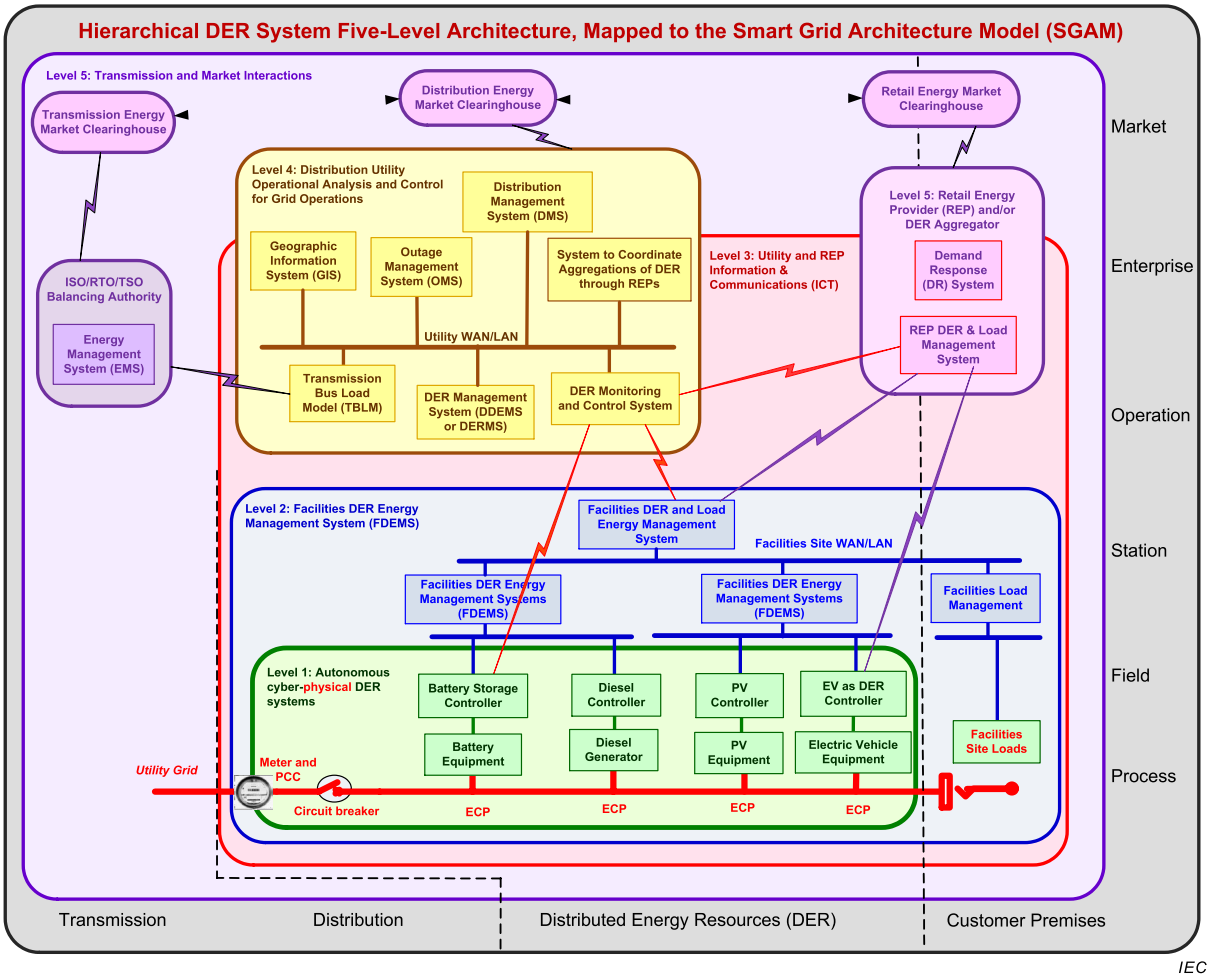


Figure D.7 – Hierarchical architecture of DER system operations

- IEC TR 62351-13: Guidelines on what security topics should be covered in standards and specifications

The IEC has developed guidelines to support the developers of standards and specifications with addressing cyber security at the appropriate level for their standard. These guidelines provide suggestions on what security topics should be covered in standards and specifications that are to be used in the power industry. These suggestions cannot be prescriptive for every standard, since individual standards and specifications may legitimately have very different focuses, but it should be expected that the combination of such standards and specifications used in any implementation should cover these security topics. These suggestions could therefore be used as a checklist for the combination of standards and specifications used in implementations of systems.

- IEC 62351-14: Cyber security event logging and reporting (under consideration)

Part 14 specifies technical requirements for logging security events: transport, log data and semantics, such as how to send and receive security events securely, reliably, how to forward security events or logs, how to query logs, etc. Besides the specification of the logging events, also the transport is being defined. Specifically, as syslog has become the de-facto standard to log system events, a mapping to syslog is targeted.

- IEC 62351-90-1: RBAC guidelines (under consideration)

This document enhances the role based access control specification in power systems defined in IEC TS 62351-8 with best practise guidelines for the distribution of role-to-right information enabling the definition of custom roles. More specifically it focuses on means to describe custom roles, the management of new roles and associated rights, which are

typically administered in a management tool and enforced in the endpoints. By defining categories, the workflow for defining new roles and associated rights besides the already predefined roles in IEC TS 62351-8 as well as the assignment to subjects shall be eased. Consequently the information exchange necessary to distribute the RBAC information is also target of this report to ensure interoperability between different vendor's products. This is achieved by utilizing the already existing standard XACML. In addition to IEC TS 62351-8 further constraints of role execution are considered. These constraints are bound to the execution environment rather than the access token carrying the role information itself. It is intended to include the technical enhancements into the revision of IEC TS 62351-8.

- IEC 62351-90-2: Deep Packet inspection (under consideration)

This technical report analyses the impact of encrypted communication channels in power systems introduced with IEC 62351. As defined in IEC 62351 an encrypted channel can be employed when communicating with IEDs and encryption can be adopted at message level as well. For example, the use of encrypting TLS setups according to IEC 62351-3 introduces some issues when Deep Packet Inspection (DPI) is needed to inspect the communication channel for monitoring, auditing and validation needs. Also, the new application layer security profiles, currently being specified as part of the revision of IEC 62351-4, provide optional encryption. The report illustrates the state-of-the art of DPI techniques that can be applied to the various kinds of channels, highlighting the possible security risks and implementation costs. Additional, beyond state-of-the-art proposals are also described in order to cope with the main limits of existing solutions.

- IEC 62351-100-1: Cyber security conformance testing (under consideration)

This 100-x series in IEC targets the specification of common available procedures for conformance testing of the different specification parts of IEC 62351.

The scope of this technical specification is to specify common available procedures and definitions for conformance and/or interoperability testing of IEC TS 62351-5, IEC TS 60870-5-7 and their recommendations over IEC 62351-3. These are the security extensions for IEC 60870-5 and derivatives.

IEC TC 57 WG 3 has developed a document for conformance testing of IEC 60870-5-101 and IEC 60870-5-104, respectively IEC TS 60870-5-601 and IEC TS 60870-5-604.

The same arguments for defining this proposed document are also valid for IEC TS 62351-5 and IEC 62351-3 applied to the IEC 60870-5 series through IEC TS 60870-5-7 for secure data exchange. The widespread use of IEC 60870-5 and the increasing use of its data communication security through IEC 62351 around the world justify the definition of test procedures for IEC TS 62351-5, IEC TS 60870-5-7, and their recommendations over IEC 62351-3 for profiles including TCP/IP.

D.6 TC 57 Working Group 16

D.6.1 General

<table>
<tr><th colspan="3">WG 16 – Deregulated Market Communications</th></tr>
<tr><th colspan="2">Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td colspan="2">• Develop Standards for Electricity Market Communications
– Market Participants to Market Operator
– Intra Market Operator
• Use of TC 57 Common Information Model (CIM)</td><td>Organized in two team
– European markets
– North American markets
Standardization as IEC 62325</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016</th></tr>
<tr><td>Planned TS:
• Market data exchanges guidelines for the IEC 62325-351 profiles, ed 1
• Planned IS:
• Common Dynamic Data Structures for DAM, RTM, CRR
• Problem statement and status request business process, contextual and assembly models for European markets, ed 1
• Settlement and reconciliation process, contextual and reconciliation process for European Markets
• Transmission capacity allocation business process (explicit or implicit auction) and contextual models for European market, ed 1
• Scheduling business process and contextual model for CIM European markets, ed 1
• Common information model (CIM) extensions for markets, ed 1</td><td>Planned TS:
• Utilization of web services for electronic data interchanges on the European energy market for electricity, ed 1</td><td>Planned IS:
• Profiles for Day Ahead Market
• Profiles for Real Time Market
• Profiles for Financial Transmission Rights
• Dynamic structures for DAM, RTM, FTR
• Common information model (CIM) extensions for markets, ed 2
• CIM European market model exchange profile, ed 2</td></tr>
</table>

D.6.2 IEC 62325 standard overview

D.6.2.1 IEC 62325 European style market overview

Figure D.8 represents European market related standards.

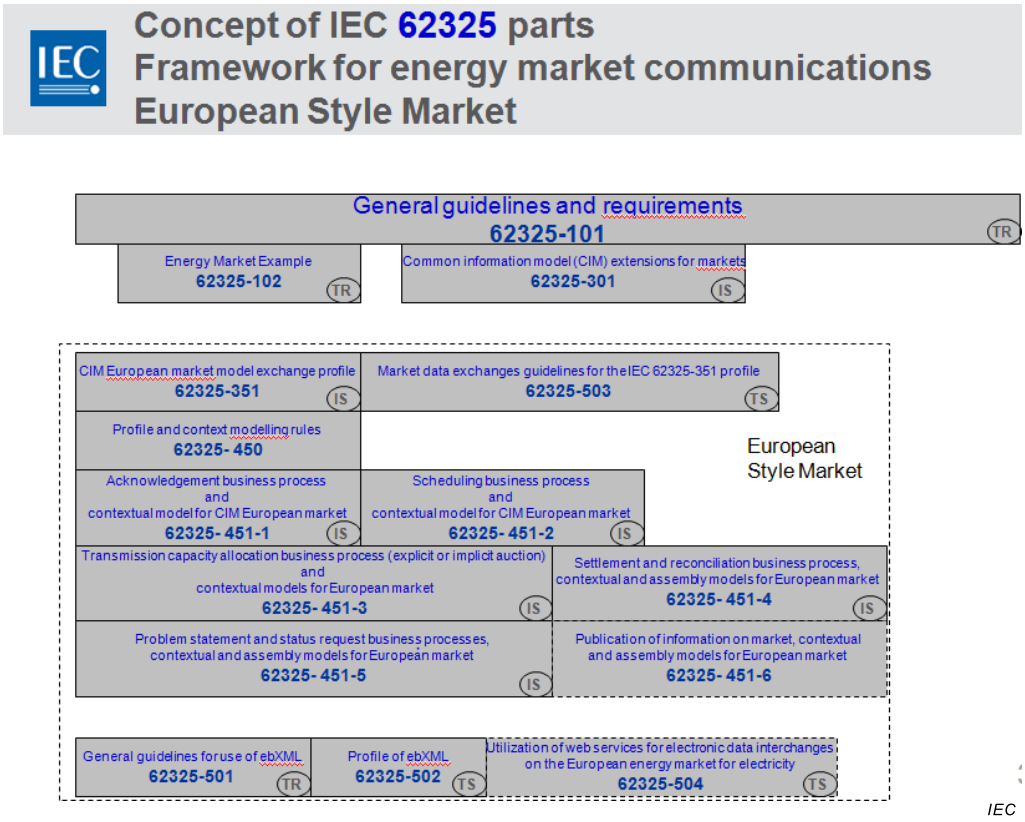


Figure D.8 – IEC 62325 standard series

The European style market profile specifications that support the European style design electricity markets is defined in IEC 62325-351. These electricity markets are based on the European regulations, and on the concepts of third party access and zonal market. The IEC 62325-451-n series specifies the content of the messages exchanged.

The purpose of IEC TS 62325-503 is to provide the guidelines to exchange the above mentioned messages. A European market participant (trader, distribution utilities, etc.) could benefit from a single, common, harmonized and secure platform for message exchange with the European TSOs; thus reducing the cost of building different IT platforms to interface with all the parties involved.

This document specifies a standard for a communication platform which every Transmission System Operator (TSO) in Europe may use to reliably and securely exchange documents. Consequently a European market participant (trader, distribution utilities, etc.) could benefit from a single, common, harmonized and secure platform for message exchange with the different TSOs; thus reducing the cost of building different IT platforms to interface with all the parties involved. This also represents an important step in facilitating parties entering into markets other than their national ones.

From now on the acronym “MADES” will be used to designate these Technical Specifications. MADES is a specification for a decentralized common communication platform based on international IT protocol standards:

- From a business application (BA) perspective, MADES specifies software interfaces to exchange electronic documents with other BAs. Such interfaces mainly provide means to send and receive documents using a so-called “MADES network”. Every step of the delivery process is acknowledged, and the sender can request about the delivery status of a document. This is done through acknowledgement, which are messages returned back to the sender. This makes MADES network usable for exchanging documents in business processes requiring reliable delivery.

- MADES also specifies all services for the business application (BA); the complexities of recipient localisation, recipient connection status, message routing and security are hidden from the connecting BA. MADES services include directory, authentication, encryption, signing, message tracking, message logging and temporary message storage.

The purpose of MADES is to create a data exchange standard comprised of standard protocols and utilizing IT best practices to create a mechanism for exchanging data over any TCP/IP communication network, in order to facilitate business to business information exchanges.

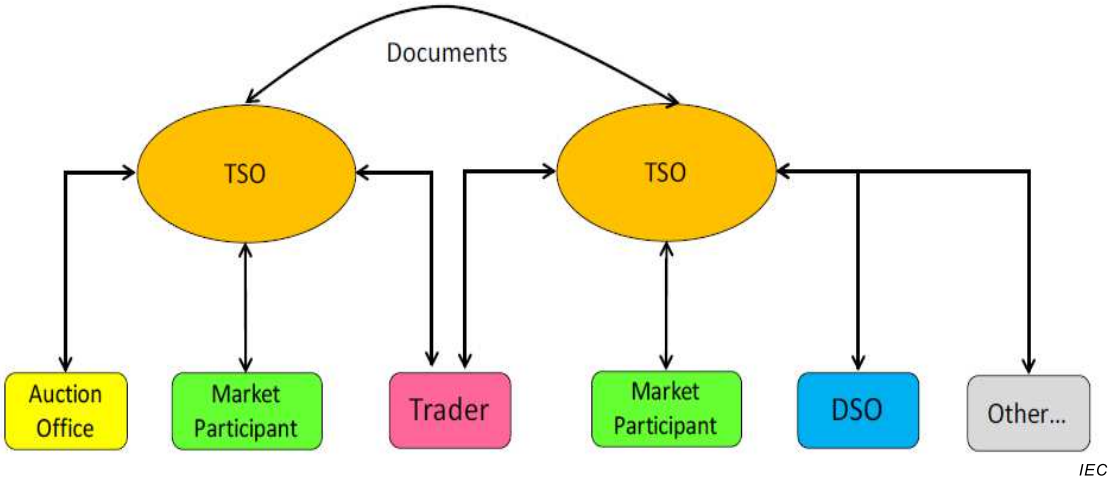


Figure D.9 – MADES overview

The MADES scope is provided by Figure D.10:

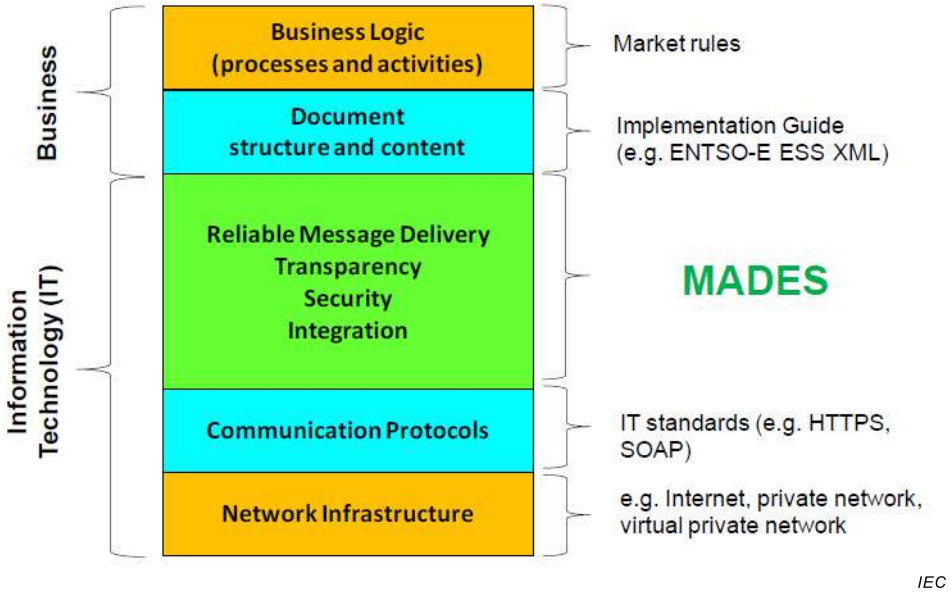


Figure D.10 – MADES scope

G_SGCG_Standard_Report_v3.1, 8.7.2 presents Trading Systems and related standards.

D.6.2.2 IEC 62325 North American style market overview

The following list represents an overview of the North American part of the standard, showing existing and future documents (under consideration).

IEC 62325-301	Common information model—extensions for markets ed 2
IEC 62325-352[18]	Profiles for North American style markets
IEC 62325-450	Modeling and Messaging Methodology
IEC 62325-452-1	Profiles for day ahead markets
IEC 62325-452-2[22]	Profiles for real time markets
IEC 62325-452-3[22]	Profiles for financial transmission rights
IEC 62325-550-2	Common dynamic structures for DAM. RTM, and FTR markets
IEC 62325-552-1	Dynamic data structures for DAM
IEC 62325-552-2[22]	Dynamic data structures for RTM
IEC 62325-552-3[22]	Dynamic data structures for FTR

North American style market overview

The North American style markets are characterized by central unit commitment and dispatch by a market operator. Merchant generators provide offers to sell electrical products, wholesale load serving entities provide bids to buy electrical energy at the wholesale level. The system operator provides requirements for ancillary services for reliable operations. The market is cleared using a security constrained unit commitment that determines awards to generators with successful offers and computes locational marginal prices that are used in billing and settlement. These wholesale markets operate in two time frames. In the day ahead time frame, the commitment of units with long start up times is determined, and the market is cleared to provide bid-in load. In the Intraday time frame, commitment of units with short start up times and dispatch are determined to meet short term forecasts for loads. The power system network is used in the market clearing optimization as a set of constraints that represent base case and contingency case operations.

Figure D.11 shows the Interface Reference Model for the North American style ISO/RTO market operations. Key software systems are briefly described along with their major interfaces.

18 Under consideration.

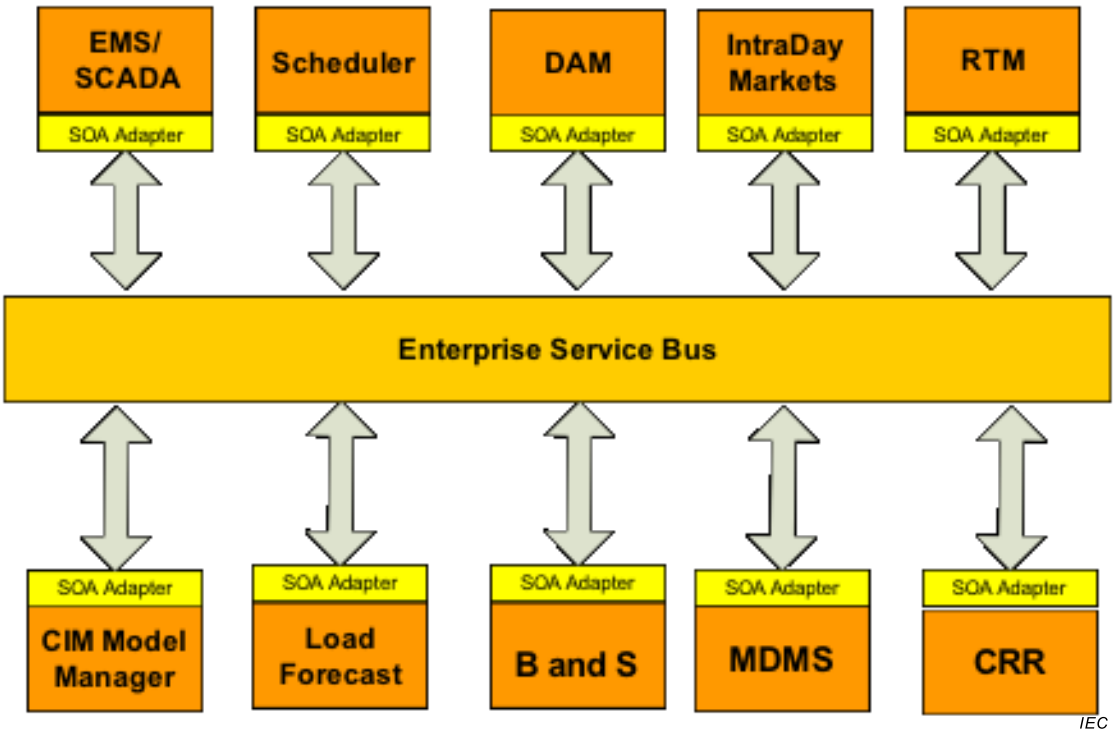


Figure D.11 – Interface Reference Model or the North American Style ISO/RTO market operations

CIM Model Manager: This system is used for maintaining the power system network model and supplemental market data such as the definition of market resources, pricing nodes, and market constraints. Power system network models are provided in the exchange format of the standards maintained by WG 13. Supplemental market data is provided in standards maintained by WG 16.

Load Forecast: This system is used to predict system and nodal loads for use in the part of the day ahead market clearing that determines reliability unit commitment.

EMS/SCADA systems: These systems provide the results of a state estimator that is used as the initial point for market clearing optimization.

Scheduler: This is system provides bilateral interchange schedules between market participants within the ISO/RTO footprint and entities outside of the footprint.

DAM: The Day Ahead Market System clears the market for the following operating day(s). It provides awards requiring the commitment of units and financially binding schedules.

Intraday Markets: This system provides awards requiring the commitment of fast start units and advisory dispatch schedules.

RTM: The Real Time Market provides clears the real time market and provides dispatch instructions to generation (and demand response) resources within a short term dispatch horizon.

B and S: The Billing and Settlement system reconciles awards with metered data and provides bills for energy and ancillary services.

MDMS: Meter data management systems validates meter reading, and may provide error correction, editing, and estimation functionality.

CRR: Congestion Revenue Rights (also known as Financial Transmission Rights) provides functionality that allows the market operator to allocate these instruments by conducting an auction. Results of the auction are provided to Billing and Settlement for the allocation of congestion charges and revenues.

D.7 TC 57 Working Group 17

<table>
<tr><th colspan="3">WG 17 – Communication Systems for Distributed Energy Resources (DER)</th></tr>
<tr><th colspan="2">Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td colspan="2">• WG 17 extends the IEC 61850 object models and services required for information exchanges, covering
– Distributed energy resources (DER), comprising generation, load and storage;
– Distribution feeder and network equipment, to support automation of power distribution systems;
• Management systems required for their operation and integration with electric power systems.</td><td>•</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016+</th></tr>
<tr><td>• IEC TR 61850-80-3 Mapping to Web Services – Requirement Analysis and Technology Assessment
• IEC TR 61850-90-8 Object Models for Electrical Mobility
• IEC TR 61850-90-10 Object Models for Scheduling</td><td>• IEC 61850-8-2 Specific communication service mapping (SCSM) – Mappings to Web Services
• IEC TR 61850-90-6 Use of IEC 61850 for Distribution Automation System
• IEC TR 61850-90-9 Use of IEC 61850 for Electrical Storage Systems
• IEC TR 61850-90-15 Hierarchical architecture of a DER system</td><td>• IEC 61850-7-420 Ed. 2 Basic communication structure – Distributed energy resources logical nodes
• IEC 61850-7-520 Distributed Energy Resources – modelling concepts and guidelines</td></tr>
</table>

D.8 TC 57 Working Group 18

<table>
<tr><th colspan="3">WG 18 – Hydroelectric power plants – Communication for monitoring and control</th></tr>
<tr><th colspan="2">Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td colspan="2">To develop communication standards for power plants – by defining additional structures and components for IEC 61850 models, to allow the use of this standard in hydropower, larger steam and gas turbine production plants.</td><td></td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016</th></tr>
<tr><td>• CDV for IEC 61850-7-410 Amd. 1
• CD for IEC TS 61850-10-210</td><td>• IEC TS 61850-10-21 for interoperability testing
• IEC TS 61850-90-410 Communication network in hydropower plants</td><td>• IEC 61850-7-410 Ed.3
• IEC 61850-7-510 Ed.2
• CD for IEC TS 61850-10-210
• In 2018, IEC 61850-7-510 Ed.2 and -7-410 Ed.3.</td></tr>
</table>

D.9 TC 57 Working Group 19

D.9.1 General

<table>
<tr><th colspan="3">WG 19 – Reference Architecture for Power System Information Exchange</th></tr>
<tr><th>Mission & Scope</th><th colspan="2">Organization & major activities</th></tr>
<tr><td>Interoperability within TC 57 in the long term.

WG 19 includes all of TC 57 scope. WG 19 will support all other working groups, but will not perform the work of the other working groups (no compete). WG 19's focus is on topics that cross multiple working groups, and how TC 57 technically fits externally to TC 57.

WG 19 conceptually is the technical architecture board of TC 57.</td><td colspan="2">Vision: All new TC 57 standards should use/extend the CIM as the common semantics for their configuration/engineering modeling, and IEC 61850 for [SCADA oriented / IED / field] communications. Other existing standards would likely take a mapping approach. Services could also be addressed (IEC 61850 services, Web Services, security, operations, SOA and GID services could be harmonized).

Mainstream Information Technologies shall be evaluated prior to creating new equivalent approaches.

Approach: Document Interoperability approaches via the IEC 62357 (reference architecture), IEC 62361 (interoperability in the long term) series of documents.</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2014</th><th>2015</th><th>2016</th></tr>
<tr><td>• IEC 62361-2, End-to-end quality codes for supervisory control and data acquisition (SCADA)

• IEC 62361-100, CIM Profiles to XML schema mapping (CDV)

• IEC 62361-101, Common Information Model Profiles (under consideration)</td><td>• IEC TS 62361-102, CIM-IEC 61850 Harmonization (CD)

• IEC TR 62357-1 Ed 2, Power System Management and Information exchanges reference architecture (DTR)

• IEC TR 62357-200, Guidelines for migration from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6)</td><td>• IEC TR 62357-2, Power System Management Use Cases (DTR)</td></tr>
</table>

D.9.2 IEC 62357 and IEC 62361 related standard overview

Figure D.12 describes WG 19 standards and their IEC status.

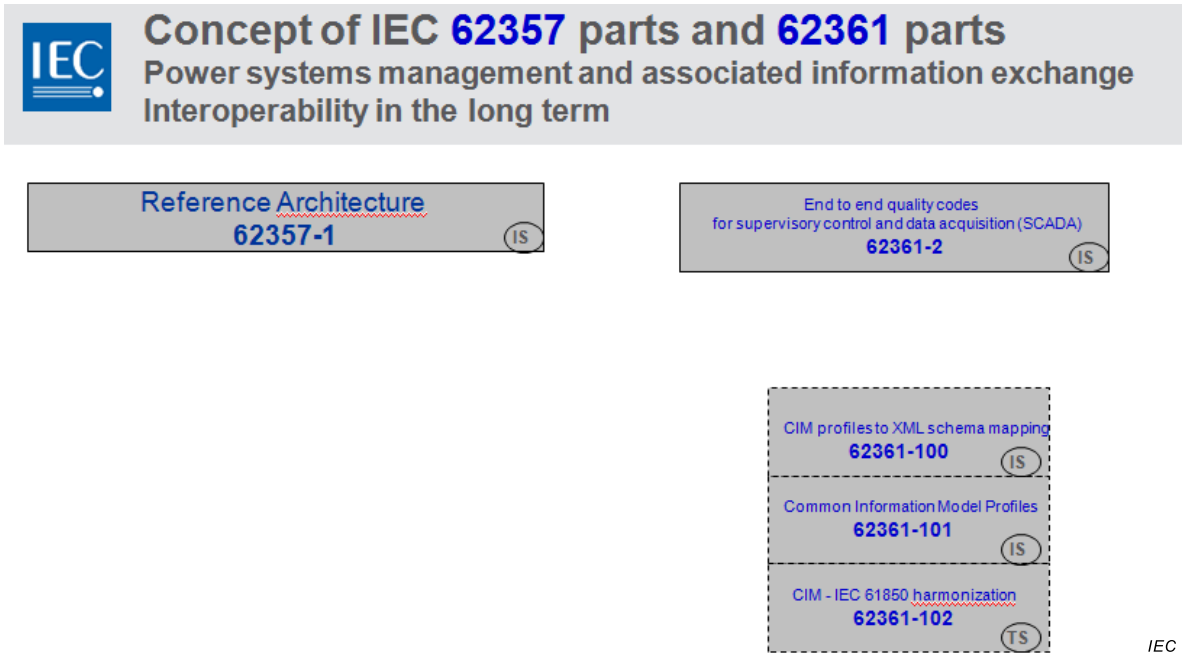


Figure D.12 – IEC 62361, IEC 62357 standard series

D.10 TC 57 Working Group 20

WG 20 – Power system IED communication and associated data models	
Mission & Scope	**Organization & major activities**
• Planning of Analogue and Digital Power Line Carrier Systems Operating operating over EHV/HV/MV Electricity Grids	The IEC 62488 series of standards consists of the following parts under the general title:Power line Systems for Power Utility Applications • Part 1: Planning of Analogue and Digital Power Line Carrier Systems Operating over EHV/HV/MV Electricity Grids • Part 2: Analogue Power Line Terminals:2014 • Part 3: Digital Power Line Carrier Terminals:2015 • Part 4: Broadband Power Line Systems:2016
Roadmap	
2014	**2015+**
• CD 62488-2 Analogue Interfaces circulated September 2014 to National committees	• IEC 62488-2, IEC Analogue Power Line Terminals • IEC 62488-3, Digital Power Line Terminals • IEC 62488-4, Broadband Power Line Terminals • Discussion with ITU-T:power line Carrier systems operating in the low and broadband frequency ranges • Electromagnetic Interference of communication systems in Utility systems • Interference from local communication networks on utility communications

D.11 TC 57 Working Group 21

D.11.1 General

<table>
<tr><th colspan="3">WG 21 – Interfaces and protocol profiles relevant to systems connected to the electrical grid</th></tr>
<tr><th colspan="2">Mission & Scope</th><th>Organization & major activities</th></tr>
<tr><td colspan="2">• Mission: Define interface between the Smart Grids and residential and commercial building and industrial energy management systems.
• Scope: Identification of use cases which involve systems connected to the electrical grid. The focus is on interaction between power system management (TC 57 standards) and H/B/I energy management systems.
Development of requirements and international standards for system interfaces, communication protocols and profiles in consideration of
– Interconnecting a large number of geographically distributed systems
– Domain specific protocols for industrial, home and building automation
– State-of-the-art wireless and wired communication
– Efficient installation, commissioning and maintenance</td><td>Structure of standard developed:
• IEC 62746 Ed.1: Systems Interface between Customer Energy Management System and the Power Management System
• IEC TR 62746-2: Use Cases and Requirements
• IEC TS 62746-3: Architecture
• IEC 62746-4: Data Model
• IEC 62746-5: Service interface to customer system
• IEC 62746-10-1 Ed.1: Systems interface between customer energy management system and the power management system – Part 10-1: Open automated demand response[a]
• IEC PAS 62746-10-1 PAS OpenADR 2.0b[a]
• IEC 62746-10-2 CIM compliant Mapping to XMPP</td></tr>
<tr><th colspan="3">Roadmap</th></tr>
<tr><th>2015</th><th>2016</th><th>2017+</th></tr>
<tr><td>• Use Cases and requirements for virtual resources in customer premises
• Architecture</td><td>• Data models
• Message content and exchange patterns
• Message transport and services
• Security</td><td>• Availability, redundancy
• Engineering
• Service interface to customer system
• Profiles, Interoperability
• Conformance Testing</td></tr>
<tr><td colspan="3">[a] Projects/publications under the responsibility of Project Committee 118.</td></tr>
</table>

D.11.2 IEC 62746 related standard overview

Figure D.13 represents WG 21 standards and their IEC status.

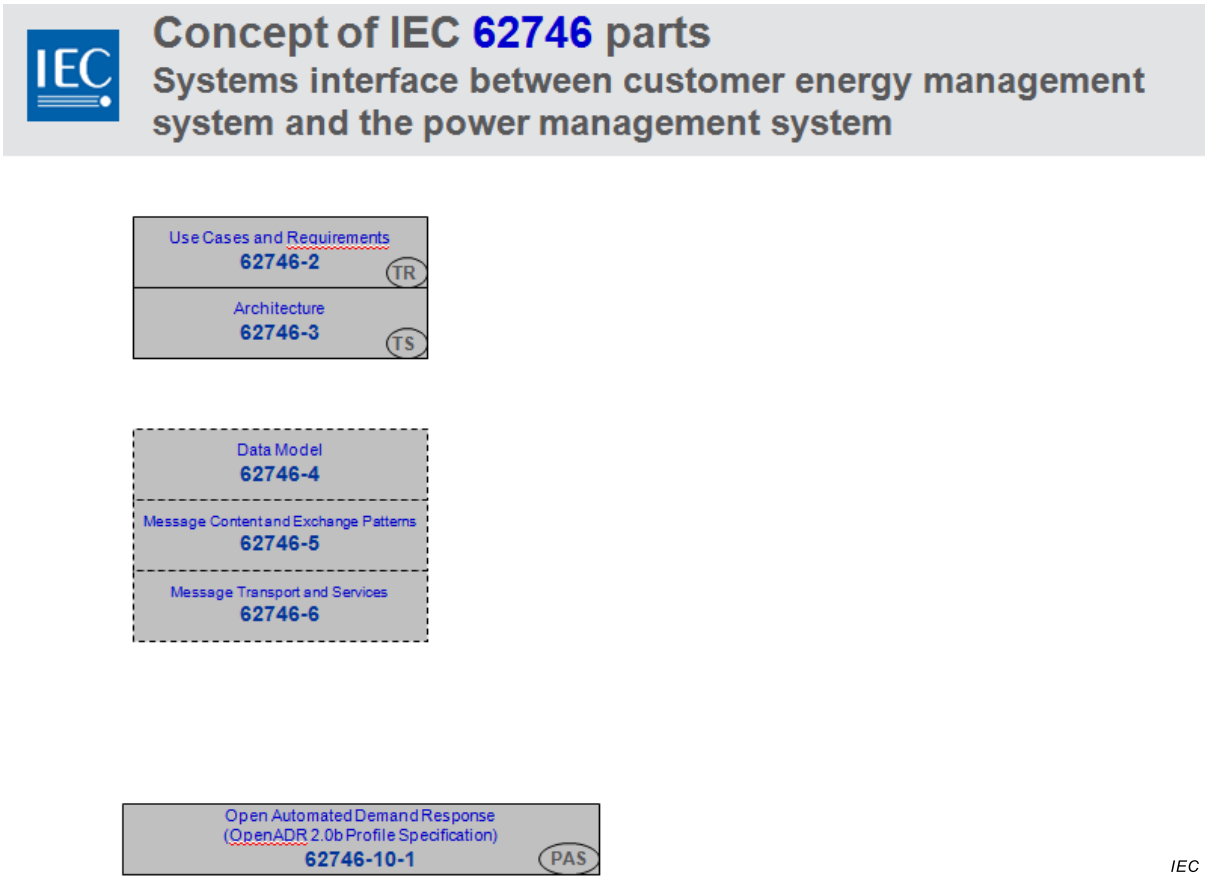


Figure D.13 – IEC 62746 standard series

D.12 Supplemental standards developed by the IEC and other bodies

Some other standards have been developed which can complete those presented in the Reference Architecture illustrated by Figure D.13.

The following list is not complete, and illustrates these complementary standards:

IEC 62541 is standardized by TC 65, Industrial-process measurement, control and automation

ISO/IEC 15118 is standardized by TC 69, Electric road vehicles and electric industrial trucks

IEC 62056 is standardized by TC 13, Electrical energy measurement and control

IEC 61334 is standardized by TC 57, Power systems management and associated information exchange

IEC 62394 Service Diagnostic Interface for Consumer electronics products and networks Echonet implementation is standardized by TC 100, Audio, Video and Multimedia systems and equipment

IEC 62746 System interface between industrial facilities and the Smart Grid

IEC technical committees and subcommittees and other bodies in charge of developing these standards could map their standards on the SGAM layers as they have been made for IEC TC 57 standards.

Bibliography

IEC Smart Grids Standardization Roadmap, IEC Smart Grids Strategy Group (SG3), 2010

IEC 62559-1[19], *Use case methodology – Part 1: Use case approach in standardization – Motivation and processes*

IEC 62559-2:2015, *Use case methodology – Part 2: Definition of use case template, actor list and requirement list*

IEC 62559-3[20], *Use case methodology – Part 3: Definition of use case template artefacts into an XML serialized format*

IEC TR 62939;2014, *Smart grid user interface*

IEC TS 62913-1[21], *Specific application of Method & Tools for defining Generic Smart Grids Requirements*

IEC TS 62913-2[22], *Generic Smart Grids Requirements*, itself composed of 5 sub parts which refer to the clusters which regroup several domains and further categorise the scope of Smart Grids:

Part 2-1: *Grid related domains* (DCT1, DCT2a, and DCT2b)

Part 2-2: *Market related domain* (DCT11)

Part 2-3: *Resources connected to the grid domains* (DCT4, DCT6, DCT7, and DCT10)

Part 2-4: *Electric transportation domain* (DCT8)

Part 2-5: *Support functions domains* (DCT3, DCT5, DCT9)

IEC 61968, *Application integration at electric utilities – System interfaces for distribution management*

M490 and CEN/ European Committee for Electrotechnical Standardization CENELEC/ European Telecommunications Standards Institute (ETSI)

Documents published in 2012

[SG-CG/F] SG-CG/M490/A_ Framework Document

[SG-CG/F] SG-CG/M490/B_ First Set of Standards

[SG-CG/F] SG-CG/M490/C_ Smart Grids Reference Architecture

[SG-CG/F] SG-CG/M490/D_ Smart Grids Information Security

[SG-CG/F] SG-CG/M490/E_ Sustainable Processes

Documents published in 2014

[SG-CG/F] SG-CG/M490/B_ Set of Standards 28 August 2014

[SG-CG/F] SG-CG/M490/F_ Overview of SG-CG Methodologies

[SG-CG/G] SG-CG/M490/G_ Smart Grids Set of standards

---

19 Under preparation. Stage at the time of publication: IEC/ACDV 62559-1:2016.

20 Under preparation. Stage at the time of publication: IEC/APUB 62559-3:2016.

21 Under preparation. Stage at the time of publication: IEC/CDM 62913-1:2016.

22 Under preparation. Stage at the time of publication: IEC/CDM 62913-2:2016.

[SG-CG/H] SG-CG/M490/H_ Smart Grids Information Security

[SG-CG/I] SG-CG/M490/I_ Smart Grids Interoperability

[SG-CG/J] SG-CG/M490/J_ Conceptual model – market models

[SG-CG/K] SG-CG/M490/K_ SGAM usage and examples

[SG-CG/L] SG-CG/M490/L_ Flexibility Management

NIST Framework Release 3 and Smart Grids Interoperability Panel SGIP (Smart Grids Architecture Committee SGAC and Smart Grids Testings & Certification Committee SGTCC)

NIST Framework and Roadmap for Smart Grids Interoperability Standards, Release 3.0, 2014-10

Conseil International des Grands Réseaux Electriques CIGRE D2.24

SC D2-24 Information systems and telecommunications – EMS architectures for the 21st century

Other references:

ENTSO-E, EFET & EBIX, The Harmonised Electricity Market Role Model, 2014-01

EURELECTRIC, Deploying publicly accessible charging infrastructure for electric vehicles: how to organise the market? July 2013

EPRI Intelligrid Common Information Model Primer Second Edition 2013 Technical Report

EPRI Using the Common Information Model for Network Analysis Data Management – 2014 [3002002587]

Booth, D., et al, Web Service Architecture, Wide Web Consortium, 2004-02-11; http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/

Technology Roadmap Smart Grids 2011 AIEA, https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf

IBIS Issue 1 (6), 2011 21 Standardized Smart Grids Semantics using OPC UA for Communication

Documents supporting Subclause 7.6.4:

IEC TR 62351-10, *Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines*

IEC TR 62351-12, *Power systems management and associated information exchange – Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems*

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

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