International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 26

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1111 – Supplement on security functional architecture for smart grid services using telecommunication networks

ITU-T X-series Recommendations – Supplement 26

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Supplement 26 to ITU-T X-series Recommendations

ITU-T X.1111 – Supplement on security functional architecture for smart grid services using telecommunication networks

Summary

Supplement 26 to the ITU-T X-series of Recommendations describes a security functional architecture for smart grid (SG) services using telecommunication networks. It identifies security risks and security requirements. Supplement 26 to Recommendation ITU-T X.1111 further defines a security functional architecture for smart grid services using telecommunication networks based on a general functional model.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 26	2016-03-23	17	11.1002/1000/12855

Keywords

Security functional architecture, smart grid.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 26 to ITU-T X-series Recommendations

ITU-T X.1111 – Supplement on security functional architecture for smart grid services using telecommunication networks

1 Scope

This Supplement defines a security functional architecture for smart grid (SG) services using telecommunication networks. The following issues are specified in this Supplement:

– security risks of smart grid services using telecommunication networks;

– security requirements for smart grid services using telecommunication networks;

– security functional architecture for smart grid services using telecommunication networks based on a smart grid functional model.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.3 privacy [b-ITU-T X.1252]: The right of individuals to control or influence what personal information related to them may be collected and managed, retained, accessed, and used or distributed.

3.1.4 advanced metering infrastructure (AMI) [b-ITU-T G.9902]: The primary means for utilities to interact with meters on customer sites. In addition to basic meter reading, AMI provides two-way communication which allows energy usage data to be collected and analysed and it enables the interaction with advanced devices such as electricity meters, gas meters, heat meters, and water meters, through various communications media.

3.1.5 home area network (HAN) [b-ITU-T G.9959]: A network capable of connecting devices in home premises.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 demand response (DR): A smart grid feature that allows consumers to reduce or change their electrical use patterns during peak demand, usually in exchange for a financial incentive. Demand response provides mechanisms and incentives for utility, business, industrial and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary to optimize the balance of power supply and demand.

3.2.2 distributed energy resources (DER): Energy generation and energy storage facilities located at the customer premises or at power transmission and distribution systems.

3.2.3 electric vehicle supply equipment (EVSE): Equipment that charges a vehicular electric battery by direct current or an alternating current power source.

3.2.4 energy management system (EMS): A computer system comprising a software platform providing basic support services and a set of applications providing the functionality needed for the effective operation of electrical generation and transmission facilities so as to ensure adequate security of the energy supply at a minimum cost.

3.2.5 intelligent electronic device (IED): A term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks.

3.2.6 regional transmission organization (RTO): An independent organization (profit or non-profit) established for the purpose of operating the transmission assets and providing wholesale transmission services within a defined (usually multi-state) geographic region. Typically, an RTO does not itself own the transmission facilities, but instead operates them on behalf of the transmission-owning utilities.

3.2.7 remote terminal unit (RTU): A microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or a supervisory control and data acquisition (SCADA) system by transmitting the telemetry data to the system or altering the state of connected objects based on control messages received from the system.

3.2.8 smart grid (SG): A two-way electric power delivery network connected to an information and control network through sensors and control devices. The smart grid supports the intelligent and efficient optimization of the power network.

3.2.9 smart meter: A device in the premises to monitor and control the electrical power usage of home devices based on demand response (see clause 3.2.1) information from home devices.

3.2.10 supervisory control and data acquisition (SCADA): A computer system that monitors an industrial, infrastructure or facility-based control process.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AMI Advanced Metering Infrastructure

CE Central Equipment

CEMS Customer Energy Management System

CIS Customer Information System

CPU Central Processing Unit

DAS Distributive on Automation System

DCU Data Collection Unit

DDoS Distributed Denial-of-Service

DER Distributed Energy Resources

DoS Denial-of-Service

DR Demand Response

DRAS Demand Response Automation System

DRMS Demand Response Management System

EMS Energy Management System

ESI	Energy Service Interface
ESS	Energy Storage System
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
GIS	Geographic Information System
GW	Gateway
HAN	Home Area Network
HSM	Hardware Security Module
HVAC	Heating, Ventilating and Air Conditioning
ICT	Information and Communication Technology
ID	Identity
IED	Intelligent Electronic Device
IP	Internet Protocol
ISO	Independent System Operator
MDMS	Metering Data Management System
OEM	Original Equipment Manufacturer
OMS	Outage Management System
PDC	Phasor Data Concentrator
PMU	Project Management Unit
RTO	Regional Transmission Organization
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SR	Security Requirement
WAMS	Wide Area Measurement System
WASA	Wide Area Situational Awareness
WMS	Work Management System

5 Conventions

In this Supplement, R indicates a risk. The digit on the right side of R is an indication of the security risk (e.g., R1). Thus, a security level (i.e., 1, 2, 3) refers to the classification in this Supplement. One of the notation examples in this Supplement is as follows: R1-2 indicates the security risk categorization of data disclosure for the moderate security level case.

In this Supplement, SR indicates a security requirement.

6 Reference architecture and smart grid services

This clause introduces the reference architecture of smart grids of clause 6.2 of [b-ITU-T Smart-O-33] and explains how smart grid services are treated in this Supplement. The relationship between the reference architecture of smart grids' and smart grid services is also discussed in this clause.

The reference architecture of smart grids is defined in [b-ITU-T Smart-O-33] and explained in Appendix I. The reference architecture of smart grids in [b-ITU-T Smart-O-33] is related to a domain perspective, whereas this Supplement focuses on a service perspective. The smart grid provides various services based on information and communication technology (ICT). These smart grid services cover common users of demand response (DR) and electric vehicles (EVs) as well as services for controlling the power grid, such as distribution grid management and wide-area power system monitoring. Such coverage is well beyond the services of the traditional power grid. The major service domains of the smart grid are specified in [b-NIST IR 7628] as described in clauses 6.1 to 6.6.

6.1 Smart meter infrastructure

Smart metering infrastructure is an advanced metering infrastructure (AMI) with bidirectional communications between provider and customer, which enables DR service and distributed energy resources service. It is called 'advanced metering infrastructure in [b-NIST IR 7628].

6.2 Demand response and consumer energy efficiency

Demand response (DR) is an active way of assessing electricity usage of a customer as a participant in the electricity market. Customers can control their own electricity usage. It is called customer premises in [b-NIST IR 7628].

6.3 Electric vehicle

An electric vehicle has a battery, electric motor, converter, inverter and battery management system as components. It is crucial for electric vehicles to connect with a charging infrastructure and smart grid. Electric vehicles can be used for energy storage and, with respect to DR, as backup power. It is called electric transportation in [b-NIST IR 7628].

6.4 Wide area situational awareness

Wide area situational awareness (WASA) is a technique for monitoring electrical grids. It can operate a power system safely using information technology.

6.5 Distributed energy resources and energy storage systems

A distributed energy resource (DER) is a small sized power system that is located near the customer side. One example is a solar panel for solar energy capture. Energy storage systems (ESSs) store overproduced electricity from power plants and temporarily transfer electrical power to areas where shortages occur. It is called electric storage in [b-NIST IR 7628].

6.6 Distribution grid management

Distributed grid management is mainly composed of functions, such as analysis in real time, self-recovery, information gathering and monitoring.

Table 6-1 shows the relationship between the reference architecture of smart grids in [b-ITU-T Smart-O-33] and this Supplement. The three columns on the left-hand side present the reference architecture of smart grids in [b-ITU-T Smart-O-33] and the right-hand column describes this Supplement. Appendix II explains in detail the relationship between the two. Among the five domains in the reference architecture of smart grids in [b-ITU-T Smart-O-33], communication network and smart metering are not listed in Table 6-1.

Table 6-1 – Relationship between reference architecture of smart grids and this Supplement

Reference architecture of smart grid (excluding communication network and smart metering) - Domain perspective			This Supplement - Service perspective
Service provider domain	Markets	Retailer/wholesaler	Smart meter infrastructure
		Aggregator	Smart meter infrastructure
		Energy market clearing house	Smart meter infrastructure
		Independent system operator/ regional transmission organization (ISO/RTO) participant	Smart meter infrastructure
	Operations	Energy management system (EMS)	Smart meter infrastructure
		Wide area measurement system (WAMS)	Wide area situational awareness (WASA)
		Applications/database management	Smart meter infrastructure
		Demand response (DR)	DR and consumer energy efficiency
		Supervisory control and data acquisition (SCADA)	Distribution grid management
		Metering system	Smart meter infrastructure
	Service providers	Customer information system (CIS)	Smart meter infrastructure
		Billing	Smart meter infrastructure
		Retail energy provider	Smart meter infrastructure
		Home/building manager provider	Smart meter infrastructure
		Common functionality platform provider	Smart meter infrastructure
		Aggregator	Smart meter infrastructure
		Others	Smart meter infrastructure
Grid domain	Bulk generation/ transmission/ distribution	Market services interface	Smart meter infrastructure
		Plant control system	Smart meter infrastructure
		Generators	Distributed energy resources (DERs) and energy storage systems (ESSs)
		Data collector	Smart meter infrastructure
		Field devices/sensors	Distribution grid management
		Electric storage	DERs and ESSs
		Substation devices	Distribution grid management
		Substation controller	Distribution grid management
		Distributed generation	DERs and ESSs

Table 6-1 – Relationship between reference architecture of smart grids and this Supplement

Reference architecture of smart grid (excluding communication network and smart metering) - Domain perspective		This Supplement - Service perspective
Customer domain	Gateway/energy service interface (GW/ESI)	Smart meter infrastructure
	Customer equipment, heating, ventilating and air conditioning (HVAC), smart appliances	Smart meter infrastructure
	Electric vehicle	Electric vehicle
	Customer EMS	Smart meter infrastructure
	Distributed generation	DERs and ESSs
	Electric storage	DERs and ESSs
NOTE 1 – A communication network is the communication infrastructure of the whole smart grid service. Therefore, communication network is not described in this table. NOTE 2 – As smart metering is the infrastructure of metering-related services (i.e., smart metering infrastructure, DR and DER), it is not described in this table.		

7 Security risks categorization of smart grid services

This clause categorizes the security risks in smart grids using telecommunication networks by security level. The categorized security risks are mapped with the entities in smart grid. The contents of this clause are mostly referenced from [b-SPS-SGSF1211-6197].

In [b-NIST FIPS 199], the security level is classified as low (limited adverse effect), moderate (serious adverse effect) and high (severe or catastrophic adverse effect). In this Supplement, security levels are categorized as 1 (i.e., low level), 2 (i.e., moderate level) and 3 (i.e., high level).

This Supplement identifies security risks of five entities in smart grids: device, system, protocol, service and data. The characteristics of five entities are explained in clauses 7.1 to 7.5.

7.1 Device

This entity consists of terminal devices with computing capability at a level that enables performing instrumentation data generation, transmission and monitoring in smart grid fields.

7.2 System

This entity is the server performing the functions of data analysis by collecting, storing, processing and utilizing data from equipment in smart grid fields.

7.3 Protocol

This entity is the communication covenant for communication, such as data exchange and control between smart grid equipment and the system.

7.4 Service

This entity is the application provided to participants through the smart grid infrastructure.

7.5 Data

These are numeric data and information generated, stored and exchanged on the smart grid infrastructure.

In [b-NIST IR 7628], the vulnerabilities and vulnerability classes of smart grids are identified. In addition, the potential impact on organizations and individuals is defined in [b-NIST FIPS 199] and that impact is an expected adverse effect caused by threat events. From these issues, the following security risks (R1 to R10) are identified for smart grid services in this Supplement. Each description of a security risk below can be also characterized by reference to potential events (security threats).

– **R1**: Disclosure of data stored in the devices and system

An attacker may physically access the devices or system from a remote location and obtain data from the memory of the devices or system. Once data is disclosed, the attacker can identify the content and such a situation impairs data confidentiality. Disclosure of data may cause damage to individuals, services and companies depending on the criticality of the data.

- **R1-1**: Not applicable
- **R1-2**: Disclosure of data of weak criticality

  Stored data of weak criticality and with no direct relevance to service-related information, such as device setup information and personal information, but allows an attacker to identify the functions and conditions of devices and system, network configuration and protocols employed, if disclosed. In such a case, the attacker may obtain information on the counterpart system and services or analyse the protocols; furthermore, the attacker may hack other systems based on the analysed information.
- **R1-3**: Disclosure of data of strong criticality

  Data of strong criticality may cause economic and social damage to individuals, services and institutions when an attacker succeeds in reading the data. Examples of such data include encryption keys, log-in information and information on power system operation.

– **R2**: Exposure of communication data

An attacker may obtain messages forwarded via communication media during communication between systems and the data contained in the message may be disclosed. Once data is disclosed, the attacker can identify the content and such a situation impairs data confidentiality. Disclosure of data may cause damage to individuals, services and companies depending on the criticality of data.

- **R2-1**: Not applicable
- **R2-2**: Disclosure of communication data of weak criticality

  Disclosure of data of weak criticality may cause damage to individuals or one or part of the system or devices. Data of weak criticality includes power consumption data.
- **R2-3**: Disclosure of communication data of strong criticality

  Data of strong criticality may cause economic and social damage to multiple individuals, services and institutions when an attacker succeeds in reading the data. Examples of such data include control commands and information on power system operation.

– **R3**: Deletion of data stored in the devices and system

The deletion of data stored in the devices and system disrupts normal operations and the timely supply of the required information. This situation impairs availability. For example, deletion of communication setup information of devices may disable the connection of devices to the communication channel. Disclosure of data may cause damage to individuals, services and companies depending on the criticality of information.

- **R3-1**: Not applicable

- **R3-2**: Deletion of data of weak criticality stored in the devices and system

  Stored data of weak criticality and with no direct relevance to service-related information, such as device setup information and personal information, affects the functions of devices and system, if deleted. An example of such a case includes failure to forward measured data because of change of sensor setup.

- **R3-3**: Deletion of data of strong criticality stored in the devices and system

  Data of strong criticality may disrupt services or expose personal information, causing damage to individuals, if deleted. An example of such a case includes the deletion of the billing information stored in the metering data management system (MDMS). Then, billing is not possible, causing huge damage to the electricity service provider.

– **R4**: Alteration of data stored in the devices and system

An attacker alters the data stored in the devices and system to cause the users of the stored data to make an incorrect decision due to misleading information. This situation impairs data integrity. For example, alteration of power consumption information stored in the system may lead to incorrect decisions with regard to real-time power charge or prediction of power demands. Alteration of encryption key information stored in the system disrupts communication with other systems or devices.

- **R4-1**: Not applicable
- **R4-2**: Alteration of data of weak criticality

  Alteration of stored data that may cause damage to a single device, system and individual; alteration of setup information of a device causes damage to the device in question only; alteration of the individual's power consumption information may cause billing errors, i.e., higher charge.

- **R4-3**: Alteration of data of strong criticality

  Alteration of stored data that may affect regional or nationwide areas; e.g., alteration of data stored in MDMS may cause billing errors throughout the country and errors in nationwide demand prediction may result in catastrophic power system operations.

– **R5**: Alteration of communication data

An attacker alters the message forwarded through communication media during the communication between systems and transfers the altered message to the final destination so that the recipient would get misleading information. This situation may impair information integrity and availability of the devices, system and service owing to such damage.

- **R5-1**: Not applicable
- **R5-2**: Alteration of communication data of weak criticality

  This data includes data measured by sensors. Damage from the transfer of the altered information is limited to the modification of a part of that data; whole statistics are not changed. Therefore, the damage is negligible.

- **R5-3**: Alteration of communication data of strong criticality

  Control command altered during transmission may cause serious damage. For example, a converted switch ON/OFF command may cause the destruction of devices or blackout.

– **R6**: Forgery of communication data

An attacker forges data through communication media during the communication between systems and causes the transfer of forged data to a specific system. This situation may impair data integrity and availability of the devices, system and service as a consequence of the attack. If the forged data involves command control or a malicious code, the attacked system may malfunction or it may be controlled by the malicious code.

- **R6-1**: Not applicable

- **R6-2**: Forgery of communication data of weak criticality

  This data includes data measured by sensors. Damage from the transfer of forged information is limited to the modification of a part of that data; whole statistics are not changed. Therefore, the damage is negligible.

- **R6-3**: Forgery of communication data of strong criticality

  A control command that is forged, transferred and executed may cause serious damage. For example, the transfer of a forced command for power shutdown may lead to catastrophic consequences, such as blackout.

– **R7**: Device manipulation through physical access

A field device installed outside a direct control area (e.g., smart meter, data collection unit (DCU) and remote terminal unit (RTU)) is easy to access for an attacker. The attacker may use functions of the device to access the network or use various pieces of information acquired from the device to install a false device disguised as a normal device. This situation may impair the integrity and availability of device.

- **R7-1**: Physical access to device with weak vulnerability to physical attack

  Systems installed in restricted zones are protected by various physical security measures and are hard to access physically.

- **R7-2**: Physical access to device strongly vulnerable to physical attack, with weak propagation effects

  If an attacker attempts direct access to a device installed in the field without a particular protection device and which regularly transmits measured data, damage is limited to the device, such as destruction of the device or acquisition of data from the device.

- **R7-3**: Physical access to device strongly vulnerable to physical attack, with strong propagation effects

  A device without particular protection devices is installed in the field, notifying the superordinate device of major events, while the control of the power system is executed by communication between devices. If unauthorized access to a device capable of inducing change of conditions of the power grid – by controlling the superordinate system – is allowed, the attacker uses this feature to attempt change of conditions of the power grid without the command of the superordinate system. This situation may lead to large-scale damage, such as blackout.

– **R8**: Unauthorized access to the network of devices and computing systems

An attacker may connect devices and computing systems to the smart grid network. The devices and computing system of the attacker play the role of normal devices to acquire information from the devices or cause malfunction of the devices. This risk may impair the integrity of the network.

- **R8-1**: Not applicable

- **R8-2**: Unauthorized access to the field network

  If an attacker's attempt at unauthorized access to the field network is successful, the attacker may disguise him- or herself as the sensor, the devices or the control systems. In such a case, the attacker may attempt an attack aimed at damaging the operation system or collect information for an attack. Note, however, that unauthorized access to the field network itself does not cause direct social or economic damage.

- **R8-3**: Unauthorized access to the operation network

  An attacker succeeding in connecting his/her devices and computing system to the network where the operation system resides may analyse the vulnerability of the operation system for an attack. In such a case, the attacker may become capable of

controlling every system linked to the operation system, causing regional or nationwide damage.

– **R9**: Denial of action

Actions performed by the user, devices, system or process – such as data transmission and data storage – may be denied. For example, the AMI operation server may deny the transmission of a power shutdown message to the smart meter and the smart meter claims that the value it transmitted differs from the power metering value. In such a case, it is difficult to do cause analysis due to incorrect information and commands. It may cause billing disputes. This situation impairs the integrity of the service operation.

- **R9-1**: Not applicable
- **R9-2**: Denial of action that causes damage to individuals and metering system

  In the case of a power cut (outage) caused by a control command, such as remote power shut-off issued to devices like smart meters for individuals, conflict may arise between individuals and smart grid businesses if the smart grid business denies sending the control command. If transmission of the information collected from the metering system is denied, it is hard to perform audit functions fully because of the difficulty in tracking the source of the incorrect data.
- **R9-3**: Denial of action that causes damage to groups, industries and countries

  It is hard to perform full audit functions for actions causing large-scale damage, such as power shutdown due to an incorrect generation control command, including the identification of the cause of the damage.

– **R10**: Excessive consumption of resources

Excessive consumption of network bandwidth and computing resources may cause inoperability of the network or shutdown of the system or devices. Distributed denial-of-service (DDoS) attacks may also cause inoperability of the network or shutdown of the system or devices. This situation impairs the availability of the system, devices and network.

- **R10-1**: Not applicable
- **R10-2**: Excessive consumption of general system resources

  Excessive consumption of resources, such as the central processing unit (CPU), memory and network interface, of a single system or devices may disrupt normal services of the system or devices.
- **R10-3**: Excessive consumption of network resources or major system resources

  Wasting resources, such as network bandwidth and systems for network operation, may disrupt the services of the network. On the other hand, excessive consumption of major resources, such as that of an AMI server, may lead to regional or nationwide shutdown of services.

The security risks are mapped with the entities of smart grid services in Table 7-1. The risk level is assigned by the magnitude of the expected adverse effects caused by threats, which is provided in [b-NIST FIPS 199].

Table 7-1 – Mapping of security risks and entities

Side	Risk level	Device	System	Protocol	Service	Data
Confidentiality	Low	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
	Moderate	R1-2	R1-2	R2-2	R2-2	R1-2 R2-2
	High	R1-3	R1-3	R2-3	R1-3 R2-3	R1-3 R2-3
Integrity	Low	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
	Moderate	R3-2 R4-2	R3-2 R4-2	R5-2 R6-2 R8-2	R3-2 R4-2 R5-2 R6-2 R8-2 R9-2	R4-2 R5-2 R6-2 R8-2 R9-2
	High	R3-3 R4-3	R3-3 R4-3	R5-3 R6-3 R8-3	R3-3 R4-3 R5-3 R6-3 R8-3 R9-3	R4-3 R5-3 R6-3 R8-3 R9-3
Availability	Low	R7-1	R7-1	Not applicable	Not applicable	Not applicable
	Moderate	R10-2	R10-2	R10-2	R3-2 R10-2	R3-2 R10-2
	High	R3-1 R7-1 R10-3	R3-1 R7-1 R10-3	R10-3	R3-3 R10-3	R3-3 R10-3

8 Security requirements of smart grid services

There are 15 types (SR1 to SR12) of SRs in smart grid services. Each of the SRs is explained in the clause 8.1.

– **SR1**: Secure local and remote access methods are considered when a system administrator or interface user accesses devices. Unauthorized access to the network of devices and computing systems can be prevented by making use of accounts capable of certifying users and secure log-in functions when attempting local or remote access to control and to set smart grid devices.

  - **SR1-1**: Not applicable
  - **SR1-2**: Function of setting accounts for local and remote access. Functions for setting identity (ID) and password are installed for user access.
  - **SR1-3**: Function of setting accounts for local and remote access, encrypted communication for radio and remote log-in. Functions of encrypted communication are installed to prevent the disclosure of ID and password for user access.

– **SR2**: Depending on the conditions, setting user access by authorities is considered. Unauthorized access to device and computing systems and use of unauthorized technologies

by staff, device and processes can be prevented by operating functions that limit users attempting to access the resources of smart grid device (e.g., directory or folder, file and process).

- **SR2-1**: Not applicable
- **SR2-2**: Function of setting access authority to All or Nothing level. A function related to access authority is installed to block unauthorized users.
- **SR2-3**: Function of setting user access authority depending on the level of device resources and execution of security setting. A function for setting access authority – by installation of classifying the device resources to access

– **SR3**: Measures for preventing the disclosure of stored personal information and power operation information are considered. There is a need to consider the installation of an encryption function to prevent hacking of personal information or disclosure of information, which causes failure of power operation, particularly in case of disclosure of information stored in smart grid devices or systems. The types of personal information and power operation information are limited for a smart grid device; note, however, that various types of information can be stored in the systems. Therefore, utilizing these types of information can prevent the disclosure of data stored in the devices and systems.

- **SR3-1**: Not applicable
- **SR3-2**: Not applicable
- **SR3-3**: Function of encryption of important information. The encryption algorithm is applied to important information causing damage to one or more individuals, systems and devices, if disclosed, to prevent the disclosure of information.

– **SR4**: Measures for preventing the disclosure of important information from the standpoint of encryption are considered. Installing a hardware security module (HSM) is considered from the standpoint of encryption to prevent the disclosure of important information stored in smart grid devices and systems. Operating an HSM allows the protection of a series of procedures related to encryption (encoding, decoding and digital signature) and securely creating and storing important information. An HSM can prevent the disclosure of data stored in devices and systems. A digital signature prevents denial of action.

- **SR4-1**: Not applicable
- **SR4-2**: Not applicable
- **SR4-3**: Using a validated software security module or HSM to perform a series of actions related to encryption, and creating and storing important information related to encryption

– **SR5**: There is a need to consider measures for checking important information stored in devices and systems for alteration. Installing a function to check the alteration of important information stored in smart grid devices and systems – when reusing the information – is considered. For example, when transmitting, upon request, metering information stored in a smart meter to be collected by a DCU, the correct metering information is forwarded only after having checked the metering information for alteration. These conditions protect data stored in devices and systems from alteration or deletion.

- **SR5-1**: Not applicable
- **SR5-2**: Not applicable
- **SR5-3**: Function for checking the stored data for alteration or deletion by making use of the hash algorithm.

– **SR6**: Measures for creating, storing and transmitting logs are considered for the analysis of the accident (i.e., caused by cyber attack). A log is a data recording of the actions taken on the device; logs are utilized as core evidentiary data for analysis when a security intrusion

accident takes place. Important log data includes system events, audit records, significant operational actions and account information. Log records allow the checking of data stored in devices and systems for disclosure, deletion or alteration, device manipulation by physical access, unauthorized access to networks of device and computing systems, use of unauthorized technologies by staff, devices or processes and excessive consumption of resources.

- **SR6-1**: Storing logs for 1 month or longer in a device or transmitting the logs in real time to the log server from the device. Logs may be stored for 1 month or longer in the device or transmitted to the log server to save device capacity.
- **SR6-2**: Storing logs for 3 months or longer in a device or transmitting the logs in real time to the log server from the device.
- **SR6-3**: Storing logs for 6 months or longer in a device or transmitting the logs in real time to the log server from the device.

– **SR7**: Measures for certifying communication objects are considered. Certification mechanisms are required to provide object certification services, which are classified into public key mode and private key mode. Certification of a public key mode is used when a digital signature function is required to provide non-repudiation services, whereas a public key or private key mode is applied when exchanging a private key for data integrity and confidentiality depending on the environments of the application. Communication object certification is considered when providing security services to prevent data disclosure and forgery or alteration, unauthorized access to the network of devices and computing systems, and denials of action.

- **SR7-1**: Not applicable
- **SR7-2**: Unidirectional certification function. Unidirectional certification is a mode wherein a certain subject demands its counterpart to provide its ID, and the latter proves it to the former. There is a need to determine the objects to be certified (client or server), depending on the environments of the application for unidirectional certification.
- **SR7-3**: Mutual certification function. In mutual certification mode, all of the objects participate in communication demand certification from each other and every subject of the communication proves its ID.

– **SR8**: There is a need to consider the provision of the end-to-end integrity function when transferring information on the application hierarchical service layer, depending on the network structure and nature of service data. The end-to-end data integrity function in the data transmission section is provided when transmitting data of the application hierarchical service layer to prevent forgery or alteration of data. The end-to-end integrity function prevents the forgery or alteration of communication data.

- **SR8-1**: Not applicable
- **SR8-2**: If the end-to-end integrity is provided by a hop-by-hop approach, the entire zone of data transmission is divided into sections, and data integrity is verified and regenerated at the intermediate point between sections.
- **SR8-3**: If the end-to-end integrity is provided by an end-to-end approach, data integrity value is created at the first data transmission point over the entire data transmission zone; the value is verified at the final data reception point to provide the integrity function.

– **SR9**: There is a need to consider the provision of end-to-end confidentiality when transferring information on the application hierarchical service layer depending on the nature of service data. The end-to-end data confidentiality function in the data transmission section is provided when transmitting data of the application hierarchical service layer to prevent the disclosure of data. The end-to-end confidentiality function prevents the disclosure of communication data.

- **SR9-1**: Not applicable
- **SR9-2**: If the end-to-end confidentiality is provided by a hop-by-hop approach, the entire zone of data transmission is divided into sections, and the encoded data is decoded and then encoded again at the intermediate point between sections.
- **SR9-3**: If the end-to end confidentiality is provided by an end-to-end approach, data is encoded at the first data transmission point over the entire data transmission zone and decoded at the final data reception point to provide the confidentiality function.

– **SR10**: There is a need to consider the provision of the non-repudiation function when transferring information on the application hierarchical service layer depending on the nature of service data. Thenon-repudiation service of the application hierarchical services is provided by making use of the digital signature function for services subject to conflict in messages exchanged between communication participants, such as price information. The non-repudiation service can prevent denial of action. If embedded devices have only very small resources to compute, consider the use of an access control function that relies on a faster encryption procedure, like the selective encryption procedure. This encryption procedure can be applied where certain data fields within a communication packet are sensitive, but others are not. In this case, selective encryption procedure selects and encrypts only data stored in sensitive data fields.

- **SR10-1**: Not applicable
- **SR10-2**: Digital signature function for providing non-repudiation services during the transmission of service data on a regular basis.
- **SR10-3**: Digital signature function for providing non-repudiation services during the transmission of service data.

– **SR11**: There is a need to consider measures for mitigating or limiting the effects of a DoS/DDoS attack. If a DDoS attack on devices and systems is successful, the availability of devices and systems is seriously impaired; hence the need to consider measures for blocking unauthorized traffic or detecting and preventing abnormal wastage of system resources to minimize damage from a DDoS attack. These measures prevent the excessive consumption of resources. A DoS attack is more crucial in comparison with other functions. However, this Supplement mainly considers the security properties of confidentiality, data integrity and availability. Therefore, in this Supplement, security requirements that are related to the three security properties are listed before the DoS attack case.

- **SR11-1**: Not applicable
- **SR11-2**: Function of detecting and blocking unauthorized or abnormal traffic. A method for detecting rapid increase in specific traffic or abnormal traffic exchanged between devices and systems and for blocking traffic to ensure normal service.
- **SR11-3**: Design of a communication protocol by taking DDoS attacks into account. The nature of DDoS attacks is considered for the design of communication protocols for detecting and defending against DDoS attacks.

– **SR12**: There is a need to consider measures for selecting and using a secure cryptographic algorithm to ensure object certification, and integrity and confidentiality of data. A secure cryptography algorithm – which has been validated by taking into account the application environment and security services – is selected. Some of the conventional standards for the security of smart grid define the cryptography algorithm with a security strength of 128 bits or lower. Note, however, that selecting and using an algorithm with a security strength exceeding 128 bits is also considered. Disclosure of data stored in devices and systems and communication data can be prevented by making use of a cryptography algorithm.

- **SR12-1**: Not applicable
- **SR12-2**: Not applicable

- **SR12-3**: Using a cryptographic algorithm with a security strength exceeding 128 bits for symmetrical key and cryptographic algorithm with security strength exceeding 112 bits for public key.

SR12 is about the cryptographic algorithm in smart grid and it is considered for the cryptographic algorithm in SR12.

9 Security functional architecture of smart grid services

This clause provides security functional architecture for smart grid services using telecommunication networks. The security functional architecture is the mapping of security risks and security requirements for the six smart grid services. Among the six smart grid services, three of the smart grid services (i.e., smart metering infrastructure, DR and DER) in clause 6 are combined with one service in clause 9.

9.1 Smart metering infrastructure, DR and DER

The security risks of the communication interface for smart metering infrastructure, DR and DER are mapped with the security requirements in Table 9-1.

Table 9-1 – Mapping of the security risks and the security requirements in smart metering infrastructure, DR and DER

Communication interface		Security risks	Security requirements
Component A	**Component B**		
Appliance	HAN display device	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2 SR10-2, SR12-3
HAN display device	Energy service interface/customer energy management system (ESI/CEMS)	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2 SR10-2, SR12-3
ESI/CEMS	AMI meter	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2 SR10-2, SR12-3
ESI/CEMS	Customer DER-EMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-2, SR12-3
ESI/CEMS	Demand response management system (DRMS)	R2-3, R5-3, R6-3	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2, SR10-2, SR11-3, SR12-3
ESI/CEMS	Demand response automation system (DRAS) client	R2-3, R5-3, R6-3	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2 SR7-2, SR8-2, SR9-2 SR10-2, SR12-3
ESI/CEMS	Billing system	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3 SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3

Table 9-1 – Mapping of the security risks and the security requirements in smart metering infrastructure, DR and DER

Communication interface		Security risks	Security requirements
Component A	**Component B**		
AMI meter	DCU	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-2, SR12-3
Customer DER-EMS	DER	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
Customer DER-EMS	ESS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3 SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
DCU	AMI head- end	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-2, SR12-3
AMI head- end	Outage management system (OMS)	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
AMI head- end	MDMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
OMS	Distribution SCADA	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
CIS	MDMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
DRMS	Distribution SCADA	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
MDMS	Billing system	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
DMS	Distribution SCADA	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
DRAS server	DRAS client	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2 SR10-2, SR11-3, SR12-3

Table 9-1 – Mapping of the security risks and the security requirements in smart metering infrastructure, DR and DER

Communication interface		Security risks	Security requirements
Component A	**Component B**		
DRAS server	DRMS	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2 SR10-2, SR11-3, SR12-3
Distribution SCADA	Distribution DER-EMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
Distribution DER-EMS	Distribution DER	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
Distribution DER-EMS	Distribution ESS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3

9.2 Electric vehicle

The components for electric vehicle charging are classified into several groups: electric vehicle, electric vehicle supply equipment, power grid operation centre at the back-end stack (e.g., distribution SCADA and metering system) and EV-related service provider. Table 9-2 lists the security risks of the communication interface in an electric vehicle and the security risks are mapped with the security requirements.

Table 9-2 – Mapping of the security risks and the security requirements in electric vehicle

Communication interface		Security risks	Security requirements
Component A	**Component B**		
EV	EVSE	R2-2, R2-3, R5-2, R5-3, R6-2, R6-3, R8-2, R10-2	SR1-2, SR1-3, SR2-2, SR2-3, SR3-3, SR4-3, SR5-3, SR6-2, SR6-3, SR7-2, SR7-3, SR8-2, SR8-3, SR9-2, SR9-3, SR10-2, SR10-3, SR11-2, SR12-3
EV	Home ESI	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR6-3, SR7-2, SR8-2, SR9-2, SR10-2, SR12-3
EVSE	EV operator	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3

Table 9-2 – Mapping of the security risks and the security requirements in electric vehicle

Communication interface		Security risks	Security requirements
Component A	**Component B**		
EVSE	EVSE operator	R2-2, R2-3, R5-2, R5-3, R6-2, R6-3, R8-2, R10-2	SR1-2, SR1-3, SR2-2, SR2-3, SR3-3, SR4-3, SR5-3, SR6-2, SR6-3, SR7-2, SR7-3, SR8-2, SR8-3, SR9-2, SR9-3, SR10-2, SR10-3, SR11-2 SR11-3, SR12-3
EVSE	Billing	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
EVSE	Vehicle service	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR6_3, SR7-2, SR8-2, SR9-2, SR10-2, SR11-3, SR12-3
EVSE	Bank/Card	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
EVSE	Original equipment manufacturer (OEM)	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
EVSE	Metering system	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3

9.3 Wide area situational awareness

When monitoring all smart grid services by making use of applicable solutions, there may be critical effects on the security of all smart grid services when incorrect analysis results are transferred to the management system. Therefore, there is a need to analyse the security risk factors to WASA services including the connection with other service domains. In a wide area situational awareness system, the security risks of the communication interface are mapped with the security requirements as presented in Table 9-3.

Table 9-3 – Mapping of the security risks and the security requirements in wide area situational awareness system

Communication interface		Security risks	Security requirements
Component A	**Component B**		
Database	Super phasor data concentrator (PDC)	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2 SR7-2, SR8-2, SR9-2 SR10-2, SR12-3
Central equipment (CE)	Database	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2 SR7-2, SR8-2, SR9-2 SR10-2, SR12-3
CE	Super PDC	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3 SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
PDC	Project management unit (PMU)	R2-2, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2 SR7-2, SR8-2, SR9-2 SR10-2, SR11-3, SR12-3
Super PDC	PDC	R2-2, R5-2, R6-2, R2-3, R5-3, R6-3	SR1-2, SR1-3, SR2-2, SR2-3, SR3-3, SR4-3, SR5-3, SR6-2, SR6-3, SR7-2, SR7-3, SR8-2, SR8-3, SR9-2, SR9-3, SR10-2, SR10-3, SR11-3, SR12-3
PDC	IED	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3 SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3

9.4 Distribution grid management

Information from the network is analysed and processed based on information received from outside environments, such as an IED and substations. Receiving incorrect information may lead to erroneous analysis of all situations of the network. In addition, there are a number of connections with other domains, and this may cause troubles in areas of other domains as well. Security risk analysis is required for all internal services, such as blackout control, and services related to outside domains linked with DR. Table 9-4 provides the security risks of communication interface in distribution grid management and the security risks are also mapped with the security requirements.

Table 9-4 – Mapping of the security risks and the security requirements in distribution grid management

Communication interface		Security risks	Security requirements
Component A	**Component B**		
IED	IED	R2-2, R5-2, R6-2, R10-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2, SR10-2, SR11-2, SR12-3
IED	Distributive on automation system (DAS) server	R2-2, R5-2, R6-2, R10-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2, SR10-2, SR11-2, SR12-3
Substation	DAS Server	R2-2, R5-2, R6-2, R10-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR7-2, SR8-2, SR9-2, SR10-2, SR11-2, SR12-3
Distribution SCADA	DAS server	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
Distribution SCADA	OMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
Distribution SCADA	Work management system (WMS)	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
Distribution SCADA	DMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
OMS	WMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
OMS	Geographic information system (GIS)	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR12-3
WMS	Asset management	R2-3, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR6-3, SR7-2, SR7-3, SR8-2, SR9-3, SR10-2, SR12-3
Asset management	DMS	R2-3, R5-2, R6-2	SR1-2, SR2-2, SR3-3, SR4-3, SR5-3, SR6-2, SR6-3, SR7-2, SR7-3, SR8-2, SR9-3, SR10-2, SR12-3
DMS	GIS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
Distribution SCADA	Distribution DER-EMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
DRMS	DMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
AMI Head-end	DMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3
DMS	EMS	R2-3, R5-3, R6-3	SR1-3, SR2-3, SR3-3, SR4-3, SR5-3, SR6-3, SR7-3, SR8-3, SR9-3, SR10-3, SR11-3, SR12-3

Appendix I

Reference architecture of smart grid

ITU-T established the Focus Group on Smart Grid (FG Smart) in February 2010 and FG Smart concluded in December 2012. FG Smart developed five deliverables:

– use case for smart grid;

– requirements of communication for smart grid;

– smart grid architecture;

– smart grid overview;

– terminology.

Especially, the deliverable on smart grid architecture [b-ITU-T Smart-O-33] defines a reference architecture of smart grids. [b-ITU-T Smart-O-33] shows the smart grid domain model, which is based on the consideration from the ICT perspective. The model consists of five domains which are viewed in three different areas: smart grid service or applications, communication and physical equipment; each covering one or more of the five domains:

– grid domain (bulk generation, distribution and transmission);

– customer domain [smart appliances, electric vehicles, premises networks (home/ building/industrial area network)];

– communication network;

– service provider domain (markets, operators and service providers).

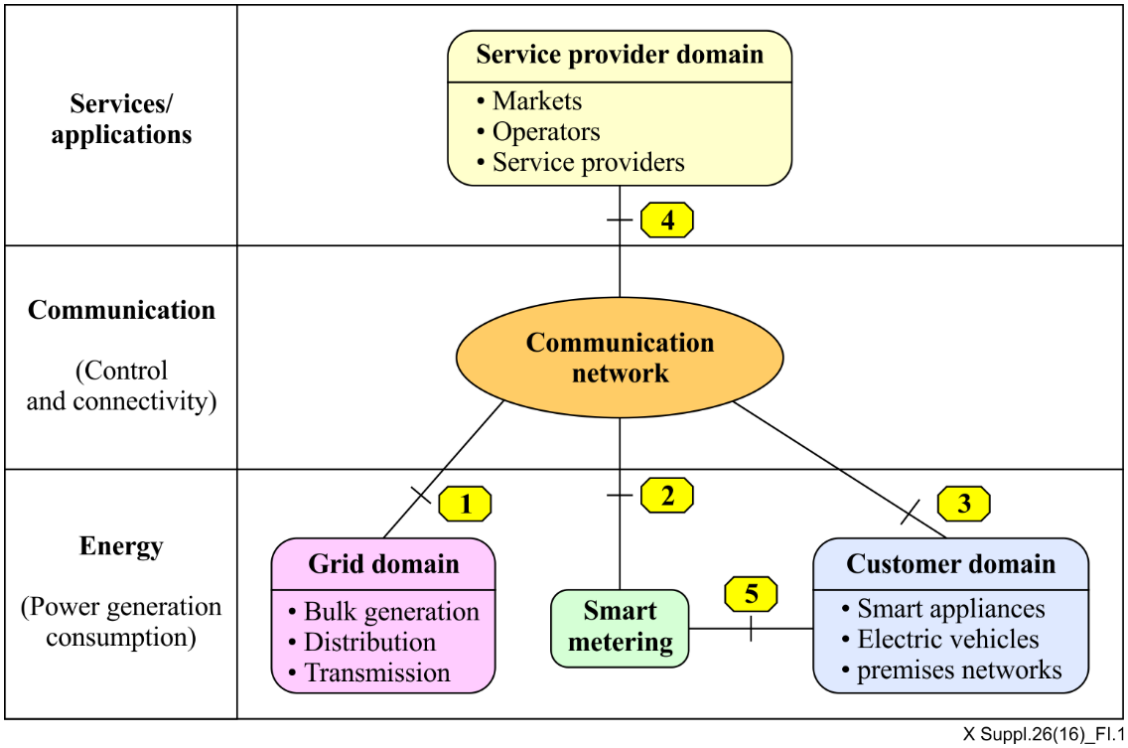

Figure I.1 – Simplified smart grid domain model from the ICT perspective

Figure I.1 also shows five interfaces between domains, marked with numbers in circles. These are places where communications and exchange of information between the communication network and

the other four domains, and between the smart metering domain and the customer domain, take place. Sample functions at each of reference points are listed below:

– **Reference point 1** – This is a reference point between the grid domain and the communication network. It enables the exchange of information and control signals between devices in the grid domain and the service provider domain. Examples of supervisory control and data acquisition (SCADA) and other operations are listed below:
  - a remote terminal unit (RTU) in transmission systems to enable SCADA operations;
  - intelligent electronic devices (IEDs) in transmission systems to interact with SCADA operations in the service provider domain;
  - a plant control system interacts with SCADA and energy management system (EMS) in the service provider domain;
  - a plant control system interacts with regional transmission organizations (RTOs)/ independent system operators (ISOs) wholesale market in market operations (e.g., the control signals of monitoring, reporting and telephony between bulk storage domain and markets to enable wholesale market operations control, hence optimizing portfolios of sources);
  - information and control signals and power generation information between the grid domain (e.g., bulk generation) and the service provider domain (e.g., control and operations);
  - the grid domain (e.g., transmission sensors and measurement devices) provides information from the transmission line to the service provider domain (e.g., transmission operation, protection and control) for transmission line maintenance information, monitoring, reporting and SCADA;
  - information exchange and coordination between the grid domain (e.g., power generation) and the service provider domain (e.g., power transmission operation and control);
  – distribution sensors and measurement devices provide distribution system information for use by the distributed energy resources (DERs).

– **Reference point 2** – This is a reference point between the smart metering domain and the communication network. It enables the exchange of metering information and interactions through operators and service providers in the service provider domain towards customers in the customer domain. Some examples are listed below:
  - management of meters, retrieval of aggregated meter readings from AMI head-end or controller in operations and the service provider in the service provider domain;
  - interacting with customer EMS to exchange pricing, data related to DR, including load-shedding information and relevant information enabling automation of tasks involved in a better use of energy;
  - billing in the service provider domain that interacts with the meters in the customer domain;
  - smart meters interact with billing in the service provider domain;
  - smart meters form a metering infrastructure to ensure reliable communication to the meter head-end through this reference point.

– **Reference point 3** – This is a reference point between the customer domain and the communication network domain. It enables interactions between operators and service providers in the service provider domain and devices in the customer domain. Some examples are listed below:
  - HAN communicates over this reference point either through a secure energy service gateway or through a public network (e.g., the Internet);

- an ESI/HAN gateway interacts with the metering, billing and utility back office in the service provider domain (operations);
- ESI/HAN gateway interacts with the load management system or demand response management system in the service provider domain (operations);
- customer EMS interacts with the energy service provider in the service provider domain;
- billing in the service provider domain interacts with customers in the customer domain;
- customer EMS interacts with the distribution management system in the grid domain;
- customer EMS interacts with an aggregator or retail energy provider in the service provider domain;
- monitoring and controlling the information exchange for distributed generation and DER in the customer domain.

– **Reference point 4** – This is a reference point between the service provider domain and the communication network domain. It enables communications between services and applications in the service provider domain to actors in other domains to perform all smart grid functions illustrated above.

– **Reference point 5** – This is a reference point between the smart metering and the customer domain; it conducts services through ESI. Some examples are listed below:
  - smart meter interacts with devices, including customer EMS, ESI in home, customer appliances and equipment;
  - devices in the customer domain, including customer EMS, ESI in home, customer appliances and equipment interact with smart meters.

In addition, [b-ITU-T Smart-O-33] defines the functional model of smart grids. The following functions are addressed in each domain:

– grid domain: power grid functions;

– smart metering: smart metering functions;

– customer domain: end-user functions;

– communication network: telecommunication, including internet protocol-based (IP-based), network functions;

– service provider domain: application functions.

Moreover, management or security functions are required for all domains.

The deliverable describes management/security function as follows:

– *Management functions*: This function group consists of functions for the management of systems in all function blocks. This function group interacts with all other function groups and covers various types of system management, including application management, device management and network management, which are described below:
  - *Application management function*: This function provides the functions to help the operator to manage the key aspects of applications. It monitors various applications and helps application providers to ensure that their applications meet end-users' expectations.
  - *Device management function*: This function enables the communication with a vast array of devices in the field and substations, whether heterogeneous or homogeneous. The device management provides an efficient way to normalize and transmit data to and from these devices.
  - *Network management function*: This function enables the diagnostics solution of network issues before the system actors are affected. It ensures that the network is available and runs as expected, so that the desired network service performance can be achieved.

Network management function is also responsible for keeping track of network resources and how they are assigned, configuring resources in the network to support a given service and adjusting configuration parameters in the network for better quality. Data for network management is collected through a real-time two-way communication between the network management function and other functional groups.

– *Security functions*: This function group interacts with all other function groups in terms of physical security, system security and operation security. This function group covers various security aspects and examples of applications are described below:

  - *Authentication and identification function*: This function is the process of verifying the ID of a user, process or a device, as a prerequisite for granting access to resources in a smart grid system.
  - *Accountability and audit function*: This function enables the review and the examination of the information record and activities related to smart grid to determine the adequacy of security requirements and to ensure compliance with the established security policy and procedures.
  - *Access control function*: This function ensures that only authorized personnel or users have access to use various utilities and services in the grid system.
  - *Data integrity function*: The function is responsible for data integrity in smart grid via cryptography and validation mechanisms.
  - *Privacy preserving function*: This function is designed to provide the privacy considerations with respect to the smart grid, including the examination of the rights, values and interests of individuals, the related characteristics, descriptive information and labels, activities, opinions of individuals and others.

Appendix II

Relationship between reference architecture of smart grids and smart grid services in this Supplement

The main components of the reference architecture of Smart Grids in [b-ITU-T Smart-O-33] are related to smart grid services in this Supplement as follows. While the reference architecture of Smart Grids in [b-ITU-T Smart-O-33] is viewed from the domain perspective, smart grid services in this Supplement are mainly seen from the components viewpoint. Therefore, smart grid services in this Supplement examine the detailed view of the reference architecture of Smart Grids in [b-ITU-T Smart-O-33] with a component view in an ICT context. The representative parts are explained as follows. The reference architecture of smart grids in [b-ITU-T Smart-O-33] shows the components (e.g., demand response, SCADA, market services interface, plant control system and customer EMS). Additionally, [b-NIST IR 7628] specifies smart grid services, such as smart meter infrastructure, demand response (DR) and consumer energy efficiency, electric vehicle, wide area situational awareness (WASA), distributed energy resources (DERs) and energy storage systems (ESSs), and distribution grid management.

– Service provider domain

  The components of the markets box can be mapped into the smart meter infrastructure in this Supplement. The demand response (DR) component in the operations box can be mapped into the DR and consumer energy efficiency in this Supplement and the SCADA in the operations box can be mapped into the distribution grid management in this Supplement. Then, the components of the service providers box can be mapped into the smart meter infrastructure in this Supplement.

– Grid domain

  The grid domain provides the bulk generation, transmission and distribution. For instance, the market services interface, the plant control system and the data collector can be mapped into the smart meter infrastructure. On the other hand, the field devices/sensors, the substation devices and the substation controller can be mapped into the distribution grid management.

– Customer domain

  In the customer domain, the GW/ESI, the customer equipment, the HVAC, smart appliances and the customer EMS are related to the smart meter infrastructure in this Supplement. The component electric vehicle can be mapped into the electric vehicle.

Bibliography

[b-ITU-T G.9902] Recommendation ITU-T G.9902 (2012), *Narrowband orthogonal frequency division multiplexing power line communication transceivers for ITU-T G.hnem networks.*

[b-ITU-T G.9959] Recommendation ITU-T G.9959 (2015), *Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T Smart-O-33] ITU-T FG-Smart Deliverable, *Smart grid architecture* (2011). http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc.

[b-NIST IR 7628] NIST IR 7628 Revision 1 (2014), *Guidelines for smart grid cyber security:*
Vol. 1 – *Smart grid cybersecurity strategy, architecture, and high-level requirements;*
Vol. 2 – *Privacy and the smart grid;*
Vol. 3 – *Supportive analyses and references*.

[b-NIST FIPS 199] NIST FIPS Publication 199 (2004), *Standards for security categorization of federal information and information systems*.

[b-SPS-SGSF1211-6197] SPS-SGSF1211-6197 (2014), *Requirements for ensuring security of smart grid standards.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016