

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 26
Corrigendum 1
(03/2018)

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
Corrigendum 1

ITU-T X-series Recommendations –
Supplement 26 (2016) – Corrigendum 1

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
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

Corrigendum 1

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.

Corrigendum 1 corrects the following three problems;

- starting a new clause without clause title in clause 7.6;
- incorrect total number of security requirements specified in the first sentence of clause 8; and
- incorrect mention regarding starting position of detailed security requirements in the second sentence of clause 8.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 26	2016-03-23	17	11.1002/1000/12855
1.1	ITU-T X Suppl. 26 (2016) Cor. 1	2018-03-29	17	11.1002/1000/13592

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/11.1002/1000/1830-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/>.

© ITU 2018

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	1
4	Abbreviations and acronyms	2
5	Conventions	3
6	Reference architecture and smart grid services	4
	6.1 Smart meter infrastructure	4
	6.2 Demand response and consumer energy efficiency	4
	6.3 Electric vehicle	4
	6.4 Wide area situational awareness.....	4
	6.5 Distributed energy resources and energy storage systems	4
	6.6 Distribution grid management	4
7	Security risks categorization of smart grid services	6
	7.1 Device	6
	7.2 System	6
	7.3 Protocol.....	6
	7.4 Service	6
	7.5 Data.....	7
	7.6 Security risks of the entities	7
8	Security requirements of smart grid services.....	11
9	Security functional architecture of smart grid services	15
	9.1 Smart metering infrastructure, DR and DER	15
	9.2 Electric vehicle	17
	9.3 Wide area situational awareness.....	18
	9.4 Distribution grid management	19
	Appendix I – Reference architecture of smart grid.....	21
	Appendix II – Relationship between reference architecture of smart grids and smart grid services in this Supplement	25
	Bibliography.....	26

Supplement 26 to ITU-T X-series Recommendations

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

Corrigendum 1

Editorial note: This is a complete-text publication. Modifications introduced by this corrigendum are shown in revision marks relative to ITU-T X. Supplement 26 (2016).

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



Documents

Document Sharing Hub

X series – Supplement 26 (2016)/Cor.1 (03/2018)

1

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

