International Telecommunication Union

ITU-T X.1331

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Smart grid security

Security guidelines for home area network (HAN) devices in smart grid systems

Recommendation ITU-T X.1331

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.

Recommendation ITU-T X.1331

Security guidelines for home area network (HAN) devices in smart grid systems

Summary

A home area network (HAN) in smart grid systems is a premises network.. Unlike the traditional HAN, the HAN in smart grids includes smart grid devices, such as distributed energy resources (DERs), an electric vehicle (EV) charger, a home energy management system (HEMS) and a customer energy display (CED). Customer electricity loads and DERs are connected to the HAN, so that customers can turn the loads and DERs on or off based on the information from the utility in order to maximize the efficiency of electricity usage. A HAN is usually connected to the Internet, so attackers can easily access to a HAN and HAN devices. Thus, HAN devices should provide capabilities that prevent attackers from compromising the HAN and its devices. Recommendation ITU-T X.1331 provides threat analysis for a HAN in smart grid systems, security requirements and security functions. Since the role and functions of each HAN device are different, the security requirements and security functions by device are provided.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1331	2018-03-29	17	11.1002/1000/13405

Keywords

Home area network, security guidelines, security requirements, 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 Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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

Recommendation ITU-T X.1331

Security guidelines for home area network (HAN) devices in smart grid systems

1 Scope

This Recommendation provides security guidelines for home area network (HAN) devices in smart grid systems. This Recommendation covers:

– security risks to devices and communications in a HAN;

– security requirements for devices and communications in a HAN;

– security functions of devices and communications in a HAN.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 energy services interface (ESI) [b-ITU-T Y.2071]: A set of functions consisting of gateway functions and functions required for smart grid applications to control and manage the smart grid services in the customer premises.

3.1.2 energy storage system (ESS) [b-ITU-T L.1430]: The physical unit or component that has the capability to store or accumulate energy produced by an energy generator or energy captured from an energy consumer.

NOTE – An ESS provides storage functions for electricity using various types of battery. One example of use of energy storage is to respond effectively to a dynamic price mechanism from a utility network. Electrical energy is stored during a relatively low-cost period, while the stored electrical energy may replace higher-priced electrical power from a utility network.

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

3.1.4 home energy management system (HEMS) [b-ITU-T Y.4409]: 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 home equipment, such as home appliances and storage batteries, so as to assure adequate security of energy supply at minimum cost.

NOTE – A HEMS is designated by a HAN in a smart grid.

3.1.5 in-home display (IHD) [b-ITU-T Y.4409]: A user screen device to present home energy consumption information. Users can optionally control their home devices with its user interface.

NOTE – The control and usage information are transferred in a HAN communication system environment. A user screen device can also be a mobile or smart phone, (Internet protocol) television, internet video phone, personal computer, tablet or wall-pad.

3.1.6 wide area network (WAN) [b-ITU-T Y.4409]: An IP based communication network that covers a wide geographical area including the Internet and accommodates devices and local area networks.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 electric vehicle (EV): A motor vehicle that can be recharged from any external source of electricity and that can work as a power-providing system at the same time.

Examples include all-electric vehicles, battery EVs, plug-in hybrid EVs and plug-in conversions of hybrid EVs. A plug-in EV is sometimes referred to as a grid-enabled vehicle or an electrically chargeable vehicle.

3.2.2 neighbourhood area network (NAN): An access network that allows smart grid end-devices and home area networks (HANs) to connect to a wide area network (WAN).

NOTE – Adapted from [b-Smart-O-33].

3.2.3 smart meter: A device installed in premises to monitor and control the electrical power usage of smart home devices based on their demand response information.

NOTE – Adapted from [b-ITU-T Y.4409].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AMI Advanced Metering Infrastructure

CED Customer Energy Display

DER Distributed Electricity Resource

DG Distributed Generator

DoS Denial of Service

DTLS Datagram Transport Layer Security

ESI Energy Services Interface

ESS Energy Storage System

EV Electric Vehicle

G/W Gateway

HAN Home Area Network

HEMS Home Energy Management System

HMAC Hash-based Message Authentication Code

ID Identifier

IP Internet Protocol

IHD In-Home Display

NAN Neighbourhood Area Network

TLS Transport Layer Security

WAN Wide Area Network

WPA Wi-Fi Protected Access

5 Conventions

None.

6 General model of a home area network in a smart grid

A smart grid is an intelligent power grid equipped with information communication technologies. With a smart grid, electricity utilities can estimate electricity demand based on customer electricity usage information collected from smart meters. Consequently, utilities might then control the peak load situation based on the estimation. Before an electrical peak load occurs, a utility reduces customer usage or makes the customer switch to alternative sources generated by a distributed electricity resource (DER) in the customer premises, such as polar voltaic devices on the roof, electricity stores or electric vehicles (EVs). Moreover, the customer can delay or bring forward electricity usage based on peak load time information from the utility.

To exchange information between the utility and customer, the estimation or demand management system of the utility should be connected to devices in the customer premises, such as a home energy management system (HEMS) or customer energy display (CED). Figure 6-1 illustrates various networks in a smart grid environment. As shown in Figure 6-1, the connection can be made over several networks, such as a HAN, an access network [also known as a neighbourhood area network (NAN)] or a wide area network (WAN).

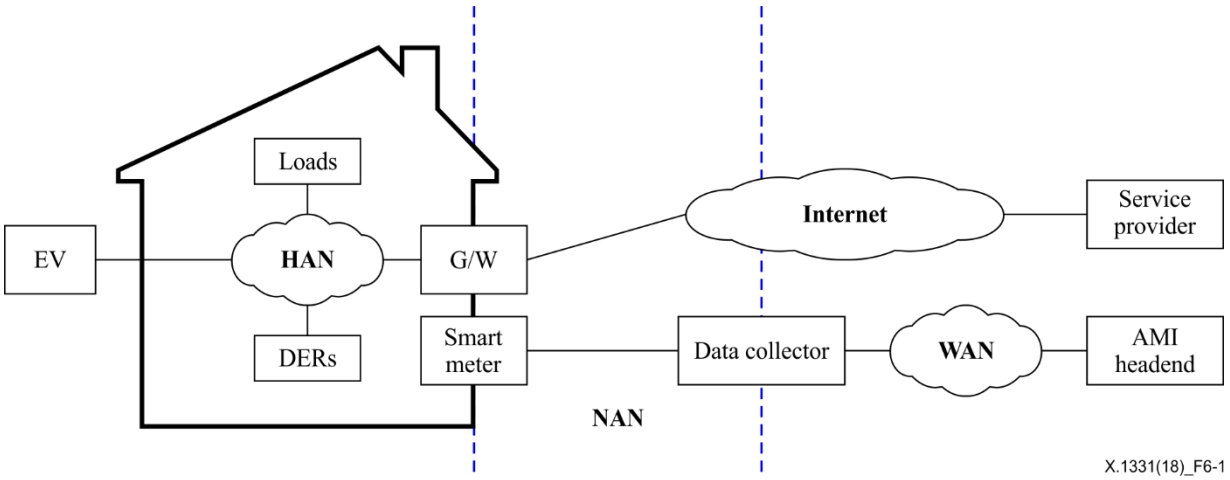

Figure 6-1 – Various types of networks in a smart grid

A HAN links electricity loads and electricity resources that are present in the customer premises. All information coming out of HAN devices should start its journey to a utility's backend system, such as an advanced metering infrastructure (AMI) headend, from the HAN, and all information from utilities should be delivered to customer devices via the HAN.

Since a HAN is usually connected to the Internet, a HAN is accessible from the Internet. Once a malicious user can access the HAN, HAN-connected devices can be compromised and information, such as electricity loads, can be changed intentionally by the attacker. In this situation, the attackers can control the HAN devices as they wish. Consequently, security measures should be considered in HAN-connected devices and their intercommunication.

Before describing threats, requirements and security technologies, a general model of a HAN in a smart grid should be formulated. The general model should identify all entities and associated communication interfaces in order to clarify their interrelationships.

Figure 6-2 shows a general model of a HAN in a smart grid. In this HAN, there are many elements, such as an electricity load, a DER, a HEMS, a CED [also known as an in-home display (IHD)], an energy services interface (ESI) and a smart meter.

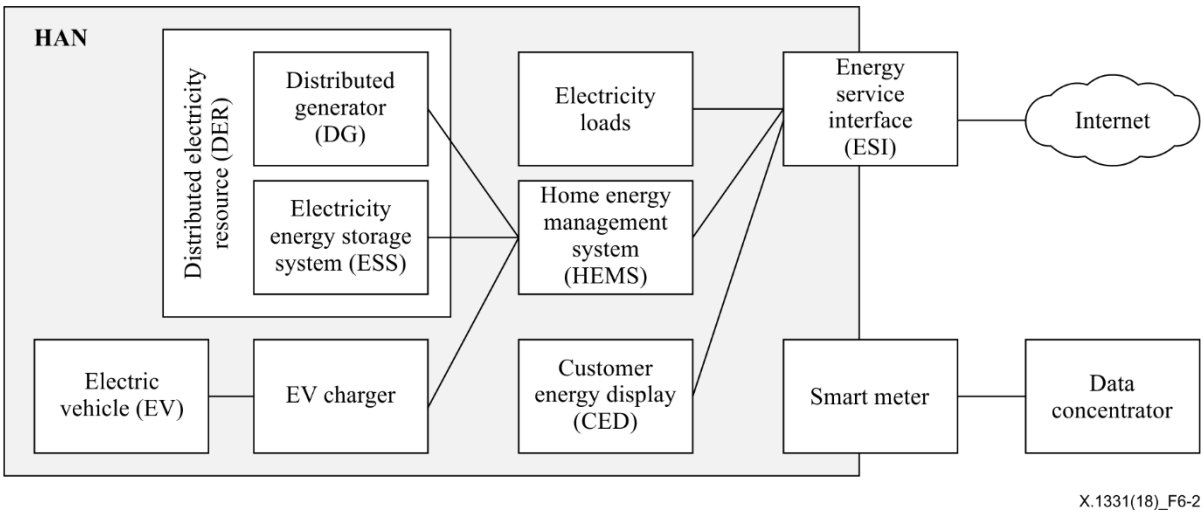

Figure 6-2 – General model of a home area network in a smart grid

- Electricity loads result from devices that consume electricity, such as domestic appliances, air conditioners and water pumps. The loads are generally of two types: smart and legacy. Smart loads include communicating and metering capabilities that are not present in legacy loads. Nonetheless, electricity consumption resulting from legacy loads can be controlled by a HEMS if the device is plugged into a socket via a smart plug, which has communication and switching capabilities. Thus, this Recommendation considers both smart loads and smart plugs as electricity loads.
- DERs, which include distributed generators (DGs) and electricity energy storage systems (ESSs), are devices that provide electricity for loads. Polar voltaic sources are widely used DGs in HANs.
- An EV can act as both a load and a DER. Charging an EV constitutes a load in a HAN, while as a DER it provides electricity for home appliances.
- A HEMS controls the capabilities of the loads and the DERs based on either the customer-registered schedule or pre-defined conditions. The main criteria of the conditions are the price of electricity and the demand response signal.
- A CED shows current electrical usage statistics and price information, so that customers can reduce their electricity consumption or shift their electricity-consuming activity plan.

7 Security threats against home area networks

This clause lists major security threats to a HAN. Note that this clause does not intend to define the taxonomy of the threats, but to share the threats HAN operators need to minimally consider.

7.1 Data leakage

Disclosure of stored or communicated data is a widely identified threat against networks and devices. An attacker can actively eavesdrop on transmitted data or physically access a device to obtain data from its memory. If the data are not protected, the attacker can disclose it.

Since wireless communication is widely used in a HAN, eavesdropping inside or outside the HAN can be easily launched. Moreover, since the entities in a HAN are connected to the Internet in many cases, a remote entity can access them. Accordingly, both communicated and stored data can be accessed by an unauthorized attacker in a HAN environment.

In a HAN, various types of privacy-related data, such as electricity consumption information, billing information and electricity usage plan, are stored in a HEMS, CED or smart meter. This private data can be transferred from or to a HEMS and CED via an ESI. Disclosure of data can have a serious

adverse effect on a customer's privacy. The attacker would then know the customer's daily life pattern.

In addition, commands controlling the operation of loads, DERs or EV chargers can be transferred from a HEMS and CED over the communication network. With access to the data, an attacker can identify how to control the loads and DERs in a HAN. This knowledge can cause another threat, such as the injection of malicious data described in clause 7.2.

7.2 Falsification of data or injection of malicious data

An unauthorized attacker can insert, change or delete information that is transmitted between entities in a HAN or stored in a HAN entity. The attacker can be a person, a program or a HAN entity. Once this kind of threat occurs, data integrity can be damaged. In addition, damage to data integrity can result in device malfunction.

Since a wireless communication network can be accessed by any anonymous entity, an anonymous entity can send malicious data to HAN entities. In addition, an attacker can add data to an existing connection with the intent of hijacking the connection or maliciously sending data. Moreover, an attacker can access the memory of the HAN entity such as a HEMS and change stored data or insert malicious data into the memory.

If the signal for electricity price has been changed upwards, a HEMS can reduce electricity consumption against the customer's wishes. Furthermore, the attacker can send a control message that results in the discharging of an EV or an ESS. Other examples include sending vast numbers of requests to an entity, resulting in denial of service (DoS) to the entity, changing values in a data file or altering a program so that a HAN entity performs differently.

7.3 Interruption of communication

One interruption of communication is jamming, which occurs when an intentional or unintentional interference overpowers the sender or receiver of a communication link, thereby effectively rendering the communication link useless. Another interruption example is the overconsumption of communication bandwidth by sending extremely large amounts of data.

In a HAN, a HEMS should gather information on the status of the loads and the DERs related to electricity usage, as well as receiving price and control signals from the electricity utility or service provider, in order to respond to adjustment demands requested of them. Thus, so that a HAN functions properly, its communication capabilities should be well maintained.

7.4 Unauthorized access

Unauthorized access can occur when an attacker gains access to entities, such as DERs, HEMSs or CEDs, by masquerading as a real user. Once an attempt at unauthorized access succeeds, the attacker can also access other devices.

To do so, an attacker must be identified and authenticated. For this, an attacker can launch a port scanning attack, which is performed to check which vulnerable ports of the HAN device are open. If there are open vulnerable ports, an attacker can exploit the HAN device's vulnerability. In addition, an attacker can gain unauthorized access to the "invulnerable" service by launching a password guessing attack.

Malware is another principal threat. Malware can infect a HAN device, such as a CED, via email or web service, and it could then propagate to other devices in a HAN. Once malware is installed on a HAN device, it can gain unauthorized access to the device's resources, possibly resulting in malfunction of, damage to or disruption of the device.

7.5 Repudiation

This threat can occur when the attacker, a sender or receiver, denies the fact of having transmitted or received a message. This does not result in any damage to or malfunction of HAN devices, but a conflict can arise when this happens. According to the nature of the conflict, it is possible that the cause of the fault or malfunction of service is not identified correctly.

7.6 Relationship between security threats and a home area network

The security threats described in clauses 7.1 to 7.5 appear in a particular entity or communication in the general HAN model. The relationships between security threats and HAN entities are shown in Table 7-1, in which an open circle in a cell indicates that a particular threat exists for a specific entity.

Table 7-1 – Relationships between security threats and home area networks

Entities	Disclosure		Modification/ injection		Interruption	Unauthorized access	Repudiation
	Stored data	Comm. data	Stored data	Comm. data			
Load		○		○	○		
DER		○		○	○	○	○
EV charger		○		○	○		○
HEMS	○	○	○	○	○	○	○
CED	○	○	○	○	○	○	○
ESI					○	○	
Communication		○		○	○		

8 Home area network security requirements

This clause describes high-level security requirements from the standpoints of four major security aspects, i.e., availability, confidentiality, integrity, and non-repudiation.

8.1 Availability

Availability ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. In other words, if an entity in a HAN wants to get information on another device with permission, the entity should be able to access to the device immediately.

A HAN in a smart grid should control the usage of the loads, generation or storage of electricity by DERs according to the demands of the grids. When utilities estimate that there is peak demand, a consumption reduction request or newly decided price signal should be transferred to the HEMS or CED, so that they can manage the electricity demands of customer devices. Whether the request is accepted can be determined based on conditions registered by the customer.

For the scenario, primarily, the availability of the network and HAN entities' functionality must be ensured. If the HAN network is not available when peak demand occurs, it is possible that the HEMS does not receive any signal from the utility, resulting in higher cost to the customer.

8.2 Confidentiality

Confidentiality ensures that data content cannot be read by unauthorized entities. Even in incidences where some of data have been intercepted by eavesdropping wireless communication, its confidentiality can be ensured, unless the attacker cannot reveal it.

Confidentiality is required for entities and sensitive communication data, whether for storage or transmission. Sensitive data in a HAN include electricity usage metering information, command messages controlling the operation of loads and DERs, price signals or demand adjustment requests from the utility and personally identifiable information stored in the CED.

8.3 Integrity

Integrity ensures that data, once transferred, does not differ from that at the source. Recently the meaning of integrity has been expanded to include the state of a system or device, which is required not to change from the baseline configuration. Likewise, original stored data are required not to change after authorized manipulation.

The integrity of control command and status information transferred between a HEMS and other entities, which are loads and DERs, should be ensured. In addition, the integrity of data transmitted from or to a CED should be protected. Moreover, to ensure functionality, the integrity of the list of programs installed on each HAN device, as well as that of the programs themselves, should be protected.

8.4 Non-repudiation

Non-repudiation prevents an individual or entity denying having performed a particular action related to data, by making available digital proof of the action.

In a HAN, the actions potentially giving rise to conflict can include controlling DERs and loads, receiving price signals and demand adjustment requests, as well as registering the electricity usage schedule via a CED. Thus, the entities of a HAN related to these actions should satisfy the non-repudiation requirement. In the case of loads, however, non-repudiation may not be possible due to the performance of the loads. For example, a smart plug is a constrained device that does not have enough memory and computing power.

8.5 Relationship between security requirements and home area networks

The relationship between security requirements and security threats is shown in Table 8-1, in which an open circle in a cell indicates that a particular security requirement should be satisfied in order to remove or mitigate a specific threat.

Table 8-1 – Relationship between security requirements and threats

			Security threats						
			Disclosure		**Modification/ injection**		**Interruption**	**Unauthorized access**	**Repudiation**
			Stored data	**Comm. data**	**Stored data**	**Comm. data**			
Security requirements	Confidentiality	Stored data	○						
		Comm. data		○					
	Integrity	Stored data			○			○	
		Comm. data				○		○	
	Availability						○		
	Non-repudiation								○

Since the threats for each entity in a HAN are listed in Table 7-1 and the requirements for each threat are listed in Table 8-1, the security requirements for each entity in a HAN can be provided by correlating these two tables. The allocation of security requirements to entities in a HAN is shown in Table 8-2, in which an open circle in a cell indicates that a particular security requirement should be satisfied by each entity in order to remove or mitigate a specific threat.

Table 8-2 – Allocation of security requirements to entities in home area networks

		Security requirements					
		Availability	Confidentiality		Integrity		Non-repudiation
			Stored data	Comm. data	Stored data	Comm. data	
Entities	Load	○		○		○	
	DER	○		○		○	○
	EV charger	○		○		○	○
	CED	○	○	○	○	○	○
	HEMS	○	○	○	○	○	○
	ESI	○				○	
	Communication	○		○		○	

9 Relationship between security requirements and security functions

To satisfy the security requirements for a HAN and its devices, security functions should be applied. These security functions include encryption or decryption, digital signature, message authentication, entity authentication, authorization, access control, an anti-DoS attack measure, audit and physical security. Table 9-1 describes how security requirements can be satisfied with security functions. An open circle in a cell indicates that a particular security function can be adopted to satisfy specific security requirements. Note that the description of each of the security functions listed in Table 9-1 are provided in clause 10.

Table 9-1 – Relationship between security requirements and security functions

			Security functions							
			Enc./ Dec.	Digital Sign.	Authentication		Access control	Anti-DoS	Audit	Physical security
					Msg.	Entity				
Security requirements	Confidentiality	Stored data	○							
		Comm. data	○							
	Integrity	Stored data		○	○		○			
		Comm. data		○	○		○			
	Availability					○		○	○	○
	Non-repudiation			○					○	○

10 Security guidelines for home area network devices in smart grid systems

10.1 Security functions for loads

Table 10-1 lists the security functions for the loads in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-1 – Security functions for the loads in a home area network

Security requirements	Security functions	Description
Availability	Anti-DoS measure	The capability to detect and mitigate the DoS attack should be considered.
	Physical security	The capability to prevent unauthorized physical access should be considered in order to prohibit unauthorized users from manipulating or configuring the loads.
Integrity	Message authentication	The capability to generate and verify cryptographic integrity data should be considered in order to ensure the integrity of report and control command messages. Cryptographic integrity data can be generated by a hash-based message authentication code (HMAC) mechanism.
Confidentiality	Encryption or decryption	The capability to decrypt the encrypted command message from the HEMS should be considered.

10.2 Security functions for distributed energy resources

Table 10-2 lists the security functions of the DERs in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-2 – Security functions for the distributed energy resources in a home area network

Security requirements	Security functions	Description
Availability	Anti-DoS measure	The capability to detect and mitigate the DoS attack should be considered.
	Physical security	The capability to prevent unauthorized physical access should be considered in order to prohibit unauthorized users from manipulating or configuring the DERs.
Integrity	Message authentication	The capability to generate and verify cryptographic integrity data should be considered in order to ensure the integrity of report and command messages. Cryptographic integrity data can be generated by an HMAC or digital signature mechanism.
	Entity authentication	• The capability to authenticate remote terminals, which send control command messages should be considered. Verification of a cryptographic credential or certificate can be considered as an authentication method. • The capability to authenticate users trying to configure or manipulate the DERs should be considered. Password verification is a typical way of user authentication. Biometrics, such as fingerprints, can be an alternative.

Table 10-2 – Security functions for the distributed energy resources in a home area network

Security requirements	Security functions	Description
	Access control	The capability to allow only authorized users to change the configuration of a DER and manipulate it should be considered.
Confidentiality	Encryption or decryption	The capability to decrypt the encrypted command message from the HEMS should be considered.
Non-repudiation	Digital signature	The capability to verify the digital signature included in a control command message should be considered.
	Audit	The capability to create and maintain audit trails should be considered in order to ensure accountability. Charging and discharging of the ESS can be an important action that should be recorded.

10.3 Security functions for electric vehicle chargers

Table 10-3 lists the security functions of the EV chargers in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-3 – Security functions for the electric vehicle chargers in a home area network

Security requirements	Security functions	Description
Availability	Anti-DoS measure	The capability to detect and mitigate the DoS attack should be considered.
	Physical security	The capability to prevent unauthorized physical access should be considered in order to prohibit unauthorized users from manipulating or configuring the chargers.
Integrity	Message authentication	The capability to generate and verify cryptographic integrity data should be considered in order to ensure the integrity of report and control messages. Cryptographic integrity data can be generated by an HMAC or digital signature mechanism.
	Entity authentication	• The capability to authenticate remote terminals sending control command messages should be considered. Verification of a cryptographic credential or certificate can be considered as an authentication method. • The capability to authenticate users trying to configure or use the chargers should be considered. Password verification is a typical way of user authentication. Biometrics, such as fingerprints, can be an alternative.
	Access control	The capability to allow only authorized users to change the configuration of the charger or manipulate it should be considered.
Confidentiality	Encryption or decryption	The capability to decrypt the encrypted command messages from the HEMS should be considered.

Table 10-3 – Security functions for the electric vehicle chargers in a home area network

Security requirements	Security functions	Description
Non-repudiation	Digital signature	The capability to verify the digital signature included in a control command should be considered.
	Audit	The capability to create and maintain audit trails should be considered in order to ensure accountability. Start or stop charging can be an important action that should be recorded.

10.4 Security functions for customer energy displays

Table 10-4 lists the security functions of the CEDs in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-4 – Security functions for the customer energy displays in a home area network

Security requirements	Security functions	Description
Availability	Physical security	The capability to prevent unauthorized physical access should be considered in order to prohibit unauthorized users from using CEDs.
Integrity	Message authentication	The capability to generate and verify cryptographic integrity data should be considered in order to ensure the integrity of status information coming from a HEMS and control command sending to a HEMS. Cryptographic integrity data can be generated by an HMAC or digital signature mechanism.
	Entity authentication	• The capability to authenticate a HEMS should be considered. Verification of a certificate can be considered as an authentication method. • The capability to authenticate users trying to use CEDs is considered. Password verification is a typical way of user authentication. Biometrics, such as fingerprints, can be an alternative.
	Access control	The capability to allow only authorized users to change the configuration of a CED or use its functions should be considered.
	Application integrity	The capability to ensure application integrity should be considered in order to detect applications infected by malware or modified by attackers. The executable files or libraries may be changed or deleted intentionally by attackers, which will cause the application to be unstable. With this capability, the HAN devices can identify whether the application is not changed. An example method for this capability can be verifying the cryptographic integrity code for an application, which is generated when the application is installed or updated.
Confidentiality	Encryption or decryption	The capability to encrypt or decrypt messages from or to a HEMS should be considered in order to protect command messages and messages including personally identifiable information. The capability to encrypt or decrypt stored data in a CED should be considered in order to protect personally identifiable information in the CED.

Table 10-4 – Security functions for the customer energy displays in a home area network

Security requirements	Security functions	Description
Non-repudiation	Digital signature	The capability to verify the digital signature included in a control command should be considered.
	Audit	The capability to create and maintain audit trails should be considered in order to ensure accountability.

10.5 Security functions for a home energy management system

Table 10-5 lists the security functions of a HEMS in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-5 – Security functions for a home energy management system in a home area network

Security requirements	Security functions	Description
Availability	Anti-DoS measure	The capability to detect and mitigate the DoS attack should be considered. In particular, a service that is used by customers to control loads and DERs should be protected against DoS attack.
	Physical security	The capability to prevent unauthorized physical access should be considered in order to prohibit unauthorized users from using a HEMS.
Integrity	Message authentication	The capability to generate and verify cryptographic integrity data should be considered in order to ensure the integrity of status information coming from other devices (loads, DERs and EV chargers) and control command sending to other devices (loads, DERs and EV chargers). Cryptographic integrity data can be generated by an HMAC or digital signature mechanism.
	Entity authentication	• The capability to authenticate remote terminals should be considered. Verification of a certificate can be considered as an authentication method. For loads having low computing power, authentication can be achieved by verifying a credential that is generated based on a pre-shared secret. • The capability to authenticate users trying to use a HEMS should be considered. Password verification is a typical way of user authentication. Biometrics and quick response code can be alternatives.
	Access control	The capability to allow only authorized users to change the configuration of a HEMS and use its functions. Accounts for administrators and general users should be separated Separate accounts for different purpose should be created and used, so that attackers will have limited access to sensitive information, functions and other accounts if one account is compromised.
	Application integrity	The capability to ensure application integrity should be considered in order to detect applications infected by malware or modified by attackers. The executable files or libraries may be changed or deleted intentionally by attackers, which will cause the application to be unstable. With this capability, the HAN devices can identify

Table 10-5 – Security functions for a home energy management system in a home area network

Security requirements	Security functions	Description
		whether the application is not changed. An example method for this capability can be verifying the cryptographic integrity code for an application, which is generated when the application is installed or updated.
Confidentiality	Encryption or decryption	• The capability to encrypt or decrypt messages from or to another entity in a HAN should be considered in order to protect control command messages and messages including personally identifiable information. • The capability to encrypt or decrypt stored data in a HEMS should be considered in order to protect personally identifiable information in a HEMS if it is needed.
Non-repudiation	Digital signature	The capability to verify the digital signature included in a control command should be considered.
	Audit	The capability to create and maintain audit trails should be considered in order to ensure accountability.

10.6 Security functions for an energy services interface

Table 10-6 lists the security functions of an ESI in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-6 – Security functions for the energy services interface in a home area network

Security requirements	Security functions	Description
Availability	Physical security	The capability to prevent unauthorized physical access is considered in order to prohibit unauthorized users from using the ESI.
Integrity	Access control	• The capability to allow only authorized local devices to access the HAN should be considered. For the Wi-Fi access point, Wi-Fi protected access (WPA) II should be applied, and its password should be complicated in order to hinder password guessing attacks. In addition, the service set identifier (ID) broadcast function should be turned off. For the Zigbee or Bluetooth access point, security features in the specification of each protocol should be fully applied in order to meet security requirements. • The capability to block unauthorized traffic based on unique IDs should be considered. The media access control (MAC) address or Internet protocol (IP) address of the device can be used as a unique ID.
	Application integrity	The capability to ensure application integrity should be considered in order to detect applications infected by malware or modified by attackers. The executable files or libraries may be changed or deleted intentionally by attackers, which will cause the application to be unstable. With this capability, the HAN devices can identify whether the application is not changed. An example method for this capability can be verifying the cryptographic integrity code for an application, which is generated when the application is installed or updated.

10.7 Security functions for communication

Table 10-7 lists the security functions of the communication in a HAN. It shows the mapping of security requirements and security functions, as well as describing the details of capabilities in order to implement the security functions.

Table 10-7 – Security functions for communication in a home area network

Security requirements	Security functions	Description
Availability	Anti-DoS measure	The capability to detect and mitigate the DoS attack should be considered.
Integrity	Message/entity authentication	The capability of mutual authentication of the communication entities and of the messages should be considered in order to ensure the integrity of communication data. An appropriate option for this can be transport layer security (TLS) or datagram transport layer security (DTLS) using certificates. A secure cryptographic algorithm should be selected for TLS or DTLS.
	Access control	• The capability to allow only authorized local devices to access the HAN should be considered. • The capability to block unauthorized traffic based on unique IDs should be considered. The MAC address or IP address of the device can be used as a unique ID.
Confidentiality	Encryption or decryption	The capability to encrypt or decrypt stored data in a HEMS should be considered in order to protect personally identifiable information in a HEMS, if it is needed.

Bibliography

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

[b-ITU-T L.1430] Recommendation ITU-T L.1430 (2013), *Methodology for assessment of the environmental impact of information and communication technology greenhouse gas and energy projects*.

[b-ITU-T Y.2071] Recommendation ITU-T Y.2071 (2015), *Framework of a micro energy grid*.

[b-ITU-T Y.4409] Recommendation ITU-T Y.4409/Y.2070 (2015), *Requirements and architecture of the home energy management system and home network services*.

[b-ITU-T Smart-O-33] ITU-T FG-Smart Grid: Smart-O-33Rev.6 (2011), *Smart grid architecture*; http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018