ISO/IEC 15045-3-1

Edition 1.0 2024-12

INTERNATIONAL STANDARD

colour inside

Information technology – Home Electronic System (HES) gateway – Part 3-1: Privacy, security, and safety – Introduction

ISO/IEC 15045-3-1:2024-12(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

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

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

ISO/IEC 15045-3-1

Edition 1.0 2024-12

INTERNATIONAL STANDARD

colour inside

Information technology – Home Electronic System (HES) gateway – Part 3-1: Privacy, security, and safety – Introduction

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.200; 35.240.99

ISBN 978-2-8327-0002-0

CONTENTS

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 3-1: Privacy, security, and safety – Introduction

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.
3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this document.
7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
9) IEC and ISO draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC and ISO take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC and ISO had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch and www.iso.org/patents. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15045-3-1 has been prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
JTC1-SC25/3189/CDV	JTC1-SC25/3260/RVC

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, and the ISO/IEC Directives, JTC 1 Supplement available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

A list of all parts in the ISO/IEC 15045 series, published under the general title *Information technology – Home Electronic System (HES) gateway*, can be found on the IEC and ISO websites.

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

INTRODUCTION

0.1 Overview

The Home Electronic System (HES) is a set of standards that supports communications, control, and monitoring applications for homes and buildings. However, homes and buildings present a heterogeneous and evolving networked environment, where many of these networks and applications (including some that are based on HES standards) are not directly interoperable with each other. HES standards achieve interoperability through the ISO/IEC 15045 series, which relies on the ISO/IEC 18012 series to support functional interworking among the dissimilar home devices, applications, protocols, and networks found in this environment. The ISO/IEC 15045 series and ISO/IEC 18012 series were created to render all protocols interoperable.

The HES gateway enables an open and adaptable market for incompatible products by specifying a standardized modular system intended to provide interoperability among the diversity of networks found in homes and buildings. The HES interoperability process does not require modification of the various networks, applications, or protocols that use it. Appropriate interworking functions translate network messages through interface modules to a common lexicon expression that is then exchanged using a private internal network bus protocol. A protected application platform using a bus protocol supports an expanding array of services for both the application and the network.

In summary, the ISO/IEC 15045 series specifies a standardized modular dedicated private internal network system that includes:

– interfaces (i.e. interface modules) for communication and semantic translation among dissimilar home area networks (HANs), and between a HAN and external wide area networks (WANs),

– a platform for supporting a variety of application services (i.e. service modules), and

– a secure communication path among these modular elements with access restricted to the appropriate elements in order to protect data, safety and privacy.

0.2 Relation to existing work

ISO/IEC 15045-1 identifies a range of threats relating to privacy, security, and safety in general terms. ISO/IEC 15045-2 specifies the underlying architecture for the HES gateway. However, neither part provides specific privacy, security and safety requirements for HES gateway conformance. ISO/IEC 15045-3-1 (this document) introduces the privacy, security, and safety standards and requirements that are applicable to the HES gateway in order to protect the interest of consumers within the home and small office environments. This document also describes the inter-relationships among the overlapping topics of privacy, security, and safety.

This document anticipates and introduces the series of additional Part 3 subparts dealing with specific aspects of privacy (ISO/IEC 15045-3-2), security (ISO/IEC 15045-3-3), and safety (ISO/IEC 15045-3-4).

The purpose of the ISO/IEC 15045-3 series requirements is to specify methods for protecting home and building systems from both internal and external threats, intrusions, or unintended observation of data and unsafe conditions that can result from network functions. The ISO/IEC 15045-3 series specifies a set of basic and advanced requirements for gateway monitoring and control of both inbound and outbound traffic, including switching, routing, addressing, encryption, intrusion detection and prevention, and other "firewall" functions.

The ISO/IEC 15045-3 series requirements specify the following functions:

a) prevention of active inbound attacks and unsafe commands;

b) discovery and classification of outbound traffic;

c) management of privacy and security mechanisms;

d) blocking unauthorized HAN and WAN services and devices from communicating with internal networks and with each other;

e) enabling and managing authorized HAN and WAN services and devices including certification and other similar processes;

f) provision for a management and reporting dashboard for use by a non-technical end-user.

Devices or other entities communicating with each other but not on the same HAN use the HES gateway.

0.3 Relevant affected stakeholder categories

Manufacturers and vendors of smart home devices and other electrical or electronic products and appliances in the home and building systems market will be able to make and offer interoperable products with the benefit of a private, secure, and safe HES environment. Conformity with HES gateway interoperability, privacy, security, and safety requirements can create significant market synergy, expand the available range of applications, and serve the interests of consumers, manufacturers, vendors, and society as a whole. Specifically, this document, together with other parts in the ISO/IEC 15045-3 series, will ensure the privacy, security, and safety of personal and premises information in the emerging economy of devices connected to online services.

Figure 1 shows the core interoperability and HES gateway series of standards and where this document fits into the HES gateway series.

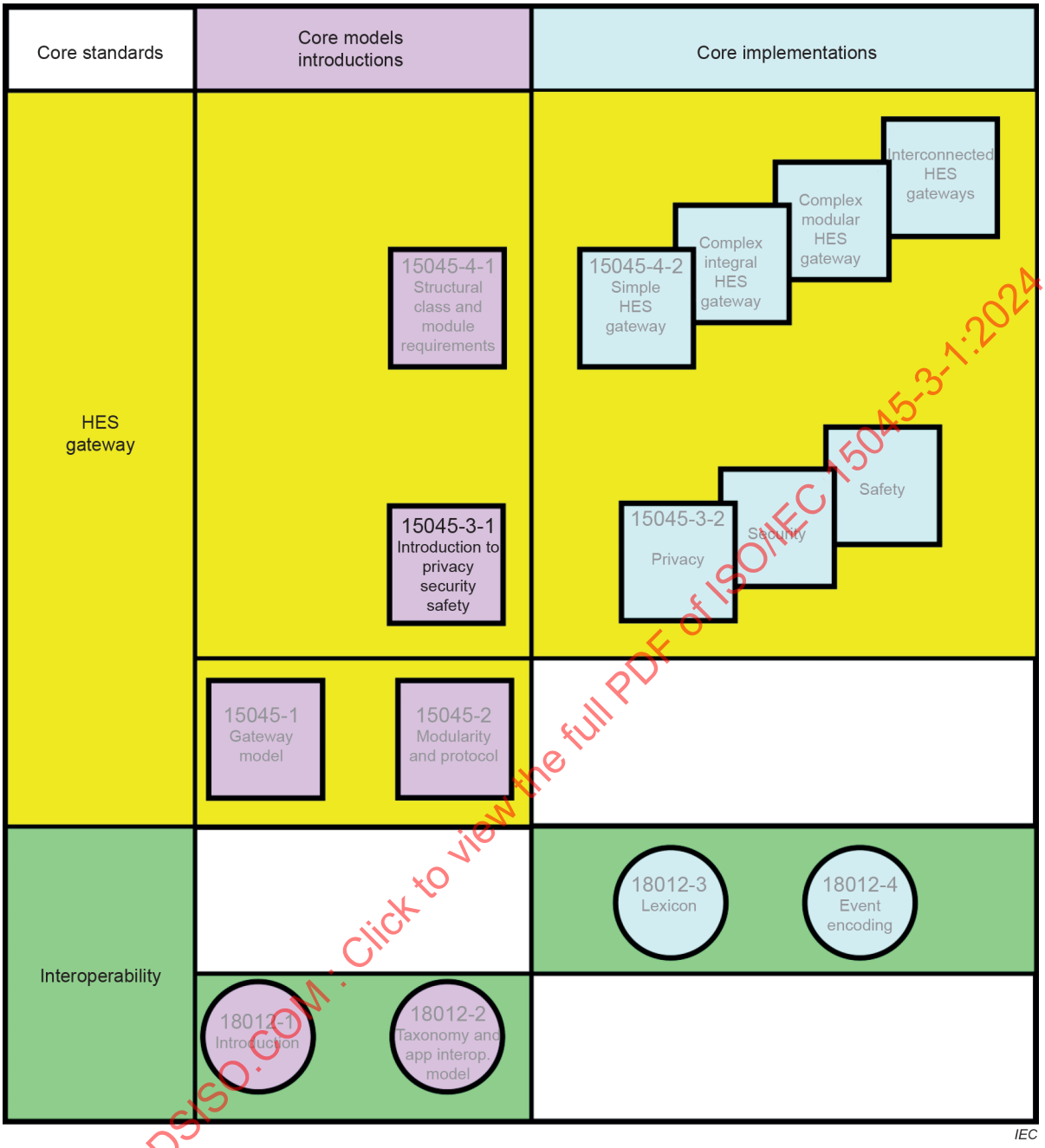

Figure 1 – ISO/IEC 15045-3-1 within the core interoperability and HES gateway standards

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 3-1: Privacy, security, and safety – Introduction

1 Scope

This document specifies the architectures for the HES gateway related to protection of privacy, security and safety of communications between different networks. It also offers guidelines for HES gateway implementations, interfaces, and application services regarding privacy, security and safety. Such HES gateway guidelines include suggested approaches, choices, or recommended practices. Further, it identifies some areas of vulnerability to be addressed and offers relevant categories or use cases.

2 Normative references

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

ISO/IEC 15944-8:2012, *Information technology – Business Operational View – Identification of privacy protection requirements as external constraints on business transactions*

ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
home area network
HAN
network serving nodes, devices, components and functions within a premises protected area

3.1.2
home electronic system
HES
control and sensing system for homes and buildings based on home electronic system (HES) ISO/IEC standards

Note 1 to entry: The referenced ISO/IEC standards normally include HES in the title of each standard.

3.1.3
HES gateway
electronic device that transfers messages among WANs and HANs providing interoperability, privacy, security and safety in accordance with the requirements of the ISO/IEC 15045 series and ISO/IEC 18012 series of standards

Note 1 to entry: For an HES gateway, a WAN is a network outside the protected area and a HAN is a network inside the protected area.

3.1.4
local
logically situated within the premises

3.1.5
privacy
freedom from being observed or disturbed

3.1.6
remote
logically situated outside the premises

3.1.7
risk
probability and magnitude of a harmful or damaging event or condition

3.1.8
safety
protection from, or unlikelihood of causing, danger or injury

3.1.9
security
freedom from danger or threat

Note 1 to entry: Security as used in this document is often referenced as "cybersecurity" to protect data.

3.1.10
user
natural person

3.1.11
vulnerability
weakness that can be exploited

3.1.12
wide area network
WAN
network that connects communication devices in the environment external to the premises protected area

3.2 Abbreviated terms

DSS	distributed secure systems
HAN	home area network
HES	home electronic system
HES-CLDPE	common language direct protocol data unit exchange
HES-CLIP	common language internal protocol
HES-CLME	common language message exchange protocol
ID	identifier
OS	operating system
WAN	wide area network

4 Conformance

An HES gateway system (including service modules and interface modules) conforming to this document shall implement those features (as appropriate to the services being implemented) required to cover the following clauses:

– 5.3.7 (internal communication bus concept); and
– 5.3.8 (DSS principle and practice); and
– 5.4 (operational protections); and
– 5.5 (risk management) requirements; and
– 5.6 (privacy, security, and safety guidelines and requirements); and
– Clause 6 (common services) requirements.

5 Protection of privacy, security, and safety

5.1 Privacy, security and safety concepts and principles in the HES gateway

The purpose of the HES gateway is to:

a) provide communications and interoperability among premises networks, services, and devices, and also between premises networks, services, devices, and wide area (external) networks and services,
b) provide a platform for management of premises network application services, and
c) provide protection for premises users, networks and devices from risks to privacy, security, and safety.

The HES gateway is a system with an internal architecture composed of a set of HES gateway modules as described in 5.2 and 5.3.

5.2 Structural protections provided by the HES gateway system

Figure 2 shows how the HES gateway system operates within the premises and shows the coverage of the HES gateway standards (ISO/IEC 15045 and ISO/IEC 18012 series).

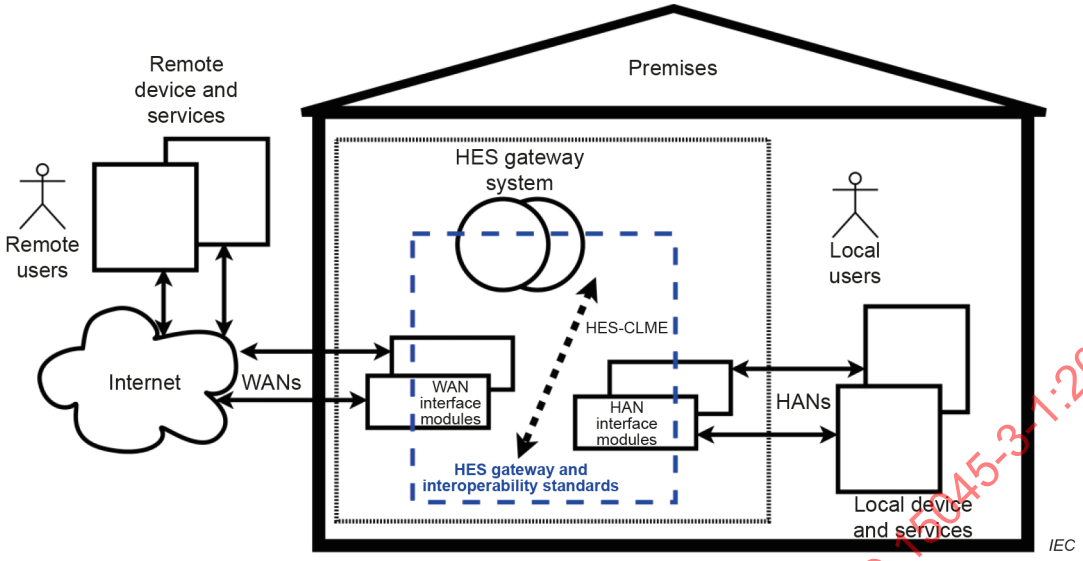

Figure 2 – HES gateway generalized architecture

HAN or WAN interface modules translate messages from or to their native HAN or WAN protocol from or to the HES gateway internal bus, called HES common language message exchange (HES-CLME). Within the gateway bus, HAN or WAN interface modules communicate with their appropriate service modules depending on the nature of the specific service they are intended to perform. HAN or WAN interface modules shall not communicate directly with other HAN or WAN interface modules, except through a service module. Service modules can communicate with appropriate interface modules or other service modules.

5.3 Interface and application services protections

5.3.1 Key concepts, principles and practices

5.3.2 to 5.3.8 describe the key HES gateway concepts, principles, and practices that shall be incorporated into the modular architecture and functionality of the HES gateway where relevant. These concepts, built upon ISO/IEC 15045-2, relate to privacy, security and safety.

5.3.2 HES concept

The Home Electronic System (HES) is a set of standards representing a specific coherent communication, control, and monitoring environment (standardizing networks, devices, applications, and a gateway) for homes and buildings.

5.3.3 HES gateway concept

A communications gateway is defined as an interface between dissimilar networks. The HES gateway is a specific standardized modular gateway for interfacing among multiple dissimilar networks or home area networks, and also providing an application platform. It anticipates and supports certification of conformance to a standard encouraging an open market in compatible and interoperable products.

5.3.4 Interface module concept

An interface module is defined as an interface between a specific external (to the premises) or in-premises network and the HES gateway internal network. In the context of the HES gateway, interface modules connect and translate between the internal HES-CLME (home electronic system common language message exchange protocol) network protocol and language, and the various networks external to the HES gateway that can either reside in the premises (i.e. home area networks (HANs)) or external to the home (i.e. wide area networks (WANs)) as users choose to install. This concept allows application services to operate on an expandable range of networks from different manufacturers without changes to each network. The translation and processing of HAN messaging to another HAN or WAN will be consistent from gateway to gateway regardless of the manufacturer.

5.3.5 Service module concept

A service module is defined as a software service agent residing within the HES gateway that supports specific gateway or application services via HES-CLME communications. Such service agents are essentially plug-ins for whatever service or application product the user chooses to have operating or installed in their home. Some service modules facilitate gateway system services (time, authorization and authentication, identification, etc.). Other service modules facilitate application-related services such as energy management, energy measurement, and audio.

5.3.6 Application platform concept

An application platform is defined as a set of software service agents residing within the HES gateway in the form of a type of service module called application service module that supports a specific user application service via HES-CLME communications. These service agents are essentially plug-ins for whatever applications and features users choose to have operating or installed in their homes, such as energy management, lighting control, etc.

5.3.7 Internal communication bus concept

The HES gateway employs an internal communication bus that enables interface modules to communicate with service modules in a consistent and interoperable manner. This internal communication bus utilizes the HES-CLME protocol (home electronic system common language message exchange protocol).

The internal bus shall be implemented with one of the following two techniques that results in the same overall operation:

a) HES-CLIP (common language internal protocol) uses Ethernet network technology functioning as a private Internet (local network), see IETF RFC 1918. This method can be supported by many manufacturers supplying independent and interoperable modular products.

b) HES-CLDPE (common language direct protocol data unit exchange) provides a family of protocols and signalling that supports operation between modular logical elements within a product, typically from one manufacturer.

5.3.8 DSS principle and practice

The HES gateway shall apply the DSS principle (distributed secure systems). The distributed modular HES gateway architecture provides structural separation isolating each interface and application so that information can only flow from one machine (i.e. processor, kernel, app) to another along known and constrained communication paths. The HES gateway is essentially a network of tiny computers talking to each other on a private wired communication bus. The main aspects that support this principle are as follows.

a) HES gateway elements: service module; interface module; internal gateway bus (HES-CLIP).

b) Communication is allowed only between service modules and interface modules; no communication is allowed directly between interface modules.

c) Service modules optionally include:

   1) application controller – determines the means and the purpose of the intended data processing service (e.g. setup and configuration);

   2) application processor – performs the relevant data manipulation and processing for the application (e.g. real time operation).

d) A single and mandatory identification service module shall be required for each HES gateway service (e.g. a distributed gateway is considered one gateway) to provide one place for identification:

   1) a unique public ID that is anonymous and publicly accessible;

   2) a "digital fingerprint" for internal uses that is not revealed.

5.4 Operational protections

The operation requirements of the HES gateway shall include the following structural and operational elements and principles that are important to privacy, security and safety:

– decentralized control (no single point of failure, no "gateway controller" or central operating system);

– interoperability of products achieved through translation into common internal language and protocol;

– separation and isolation of functional responsibility (allocation of operations to established and defined objects) by delegation to a service agent for each task or service (for example, operations dealing with authorization are handled by the authorization and authentication service, while operations dealing with identity of the HES gateway are handled by the identification service object);

– physical and logical partition or segmentation or functionality of elements, tasks, or risks.

5.5 Risk management

5.5.1 Overview

The risk management of an HES gateway system shall comprise two main aspects: risk assessment and risk treatment.

– Risk assessment estimates, identifies and prioritizes security risks.

– Risk treatment selects and implements measures to minimize risk.

5.5.2 Risk assessment

5.5.2.1 Overview of risk assessment

Risk assessment is performed for the HES gateway system using Figure 3. Manufacturers shall implement the standardized indicators as described within this risk assessment section. It the responsibility of system integrators to perform the risk assessment based upon these standardized indicators before releasing the operational HES gateway system to the customer.

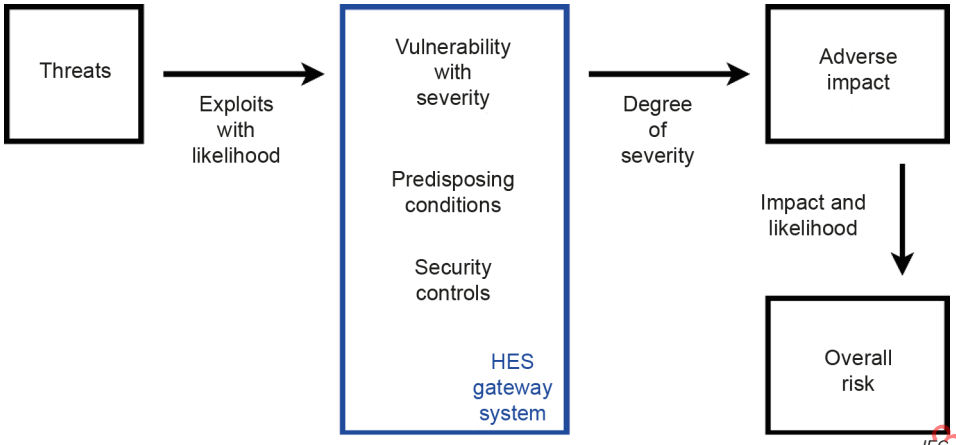

Figure 3 – Risk assessment diagram

Threats to the HES gateway system can originate from a range of sources, which can result in specific actions that affect the system. For example, some organizations or individuals outside the premises intentionally attempt to infiltrate the premises. Accidental threats such as power outages can inadvertently cause issues on the system or configuration. These threats are varied in the likelihood of occurring and varied in the likelihood of exploiting the vulnerabilities of the system.

Vulnerabilities of the system include potential hardware and software flaws in the individual modules that comprise the HES gateway system, and potential issues with the interconnection processes of the underlying HES-CLME messaging.

Predisposing conditions for the HES gateway system include the complex modular class in which different products are integrated together to form the complete operational system, and that can result in gaps or overlaps in the underlying system.

A range of security controls are included in the HES gateway system including extensive standardized risk data for all modules. Additional privacy, security and safety measures are implemented for WAN systems which are outside the protected on-premises.

The threats can have adverse impacts (i.e. unfavourable, but not necessarily damaging) on the system and on the local user with a degree of severity because of the vulnerabilities of the HES gateway system including the predisposing conditions, and the effect of the security controls.

The overall risk assessment is measured by the likelihood of the threats occurring and level of adverse impacts that result.

5.5.2.2 Threats

5.5.2.2.1 Overview of threats

Threats, a key part of risk assessment, are specific instances (threat events) caused by a variety of threat sources. These sources include the following types:

– adversarial (individual, group, organization, nation state);
– accidental;
– structural (e.g. equipment failure);
– environmental (e.g. disasters, telecommunications infrastructure outages or failures).

In 5.5.2.2.2 to 5.5.2.2.12 are some examples of specific threats, as described in ISO/IEC 15045-1, applicable to the HES gateway system[1]. Threats are frequently evolving with new previously unknown threats arising. For example, in recent years, fileless attacks[2] that occur in memory have emerged; such attacks can be introduced through malicious network packets and can be difficult to detect.

5.5.2.2.2 HAN masquerade and replay

Perhaps the most obvious threat to the home is unauthorized access to HAN devices or the HES gateway. As shown in Figure 4, a "masquerade user" arises when an impostor pretends to be a legitimate residential user, such as the homeowner.

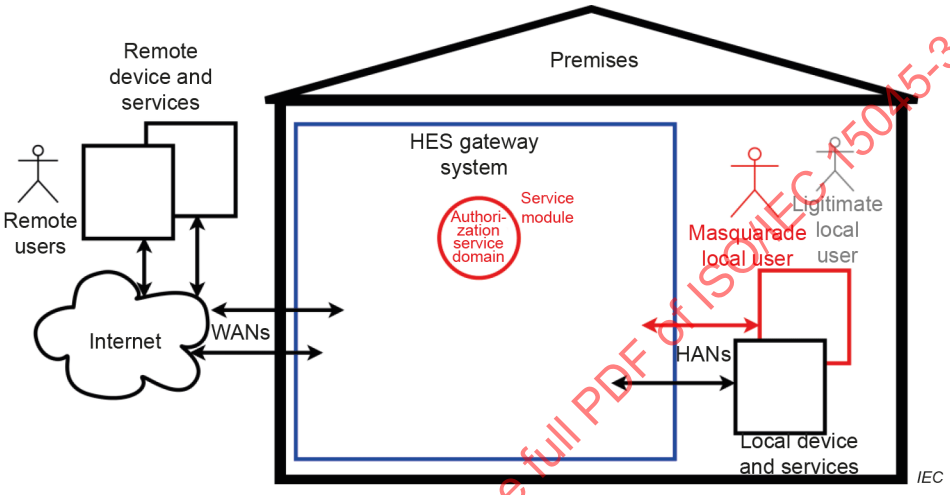

Figure 4 – HAN masquerade and replay

A masquerade can be effected by defeating the authentication mechanism, for example, guessing a password or stealing a token. Another way an impostor can trick the home network into assuming the impostor is an authorized user is for the impostor to capture a legitimate message, and to resend it at a later time. For example, if the impostor can intercept a message to the home's burglar alarm system, telling it to turn off, the same message can be replayed later to achieve the same result.

To minimize the risk, the HES gateway system shall implement several precautionary measures to contribute to the security controls as shown in Figure 3.

Local users shall be registered in a service module inside the HES gateway system supporting the authorization service domain. The objects in the authorization service domain contain the user name, level of authorization and password, all in protected memory and approved by the system owner. Only authorized users are allowed to access the configuration functions of the HES gateway.

The key operator shall be informed when any users are added, substituted or modified in any manner, so that this triggers a cautionary message when the masquerade user attempts to impose.

User access to system management functions within the premises via the HAN is protected. This limits the opportunity for masquerading.

---

1 Initial threats for the HES Gateway System are described in ISO/IEC 15045-1:2004, Annex C, Clause C.2.

2 Fileless attacks are written directly to RAM and difficult to find since they do not leave traditional traces of their existence in files on disks.

The HES gateway system supports a wide range of HANs that can have varying security features. The HES gateway system ensures that standardized information about the HANs is available to the user and system integrator so that more secure HANs can be identified and given preferential treatment. For example, some HANs use encryption techniques that further reduce the risk, and information about this strength will be available throughout the HES gateway system and can be used to inform the user, further encouraging the use of those higher quality HANs.

Insecure HANs are highlighted and caution provided to the key operator that such HANs can be susceptible to masquerading.

The standardized HAN information can also be used for the development of specialized application services focused on supporting enhanced security.

5.5.2.2.3 WAN masquerade and replay

Another obvious threat to the home is unauthorized access through the WAN connections to HES gateway system. As shown in Figure 5, a "masquerade remote user" arises when an impostor pretends to be a legitimate remote user or service.

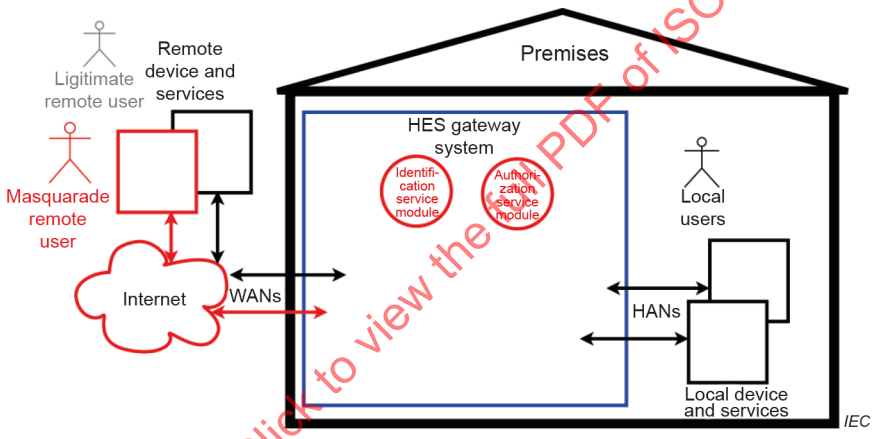

Figure 5 – WAN masquerade and replay

A masquerade can be effected by defeating the authentication mechanism, for example, guessing a password or stealing a token. Another way an impostor can trick the HES gateway into thinking it is an authorized remote user or remote service is for the impostor to capture a legitimate external message, and to resend it at a later time. For example, if the impostor can intercept a message to the home, the same message can be replayed later to achieve the same result.

To minimize the risk, the HES gateway system implements several additional precautionary WAN measures to contribute to the security controls as shown in Figure 3.

Remote users are registered in the authorization service module inside the HES gateway system. Each HES gateway system has a unique hidden identification code held within its identification service module, called "digitalFingerprint". This code is used in the initial setup of authorizing remote users to form an encrypted one-to-one link to remote users and services that cannot easily be duplicated.

The authorization service module contains the remote user name, level of authorization and password, all in protected memory and approved by the key operator. Only authorized remote users are allowed to access the certain authorized functions of the HES gateway.

The system owner is informed when any remote users are added, substituted or modified in any manner, so that this triggers a cautionary message when the masquerade remote user attempts to impose.

The HES gateway system supports a wide range of WANs that can have varying security features. The system ensures that standardized information about the WANs is available to the user and system integrator so that more secure WANs can be identified and given preferential treatment. For example, some WANs use encryption techniques that further reduce the risk, and information about this strength will be available throughout the HES gateway system and can be used to inform the user, further encouraging the use of those higher quality WANs.

Insecure WANs are highlighted and caution provided to the key operator that such WANs can be susceptible to masquerading.

The standardized WAN information can also be used for the development of specialized application services focused on supporting enhanced security.

5.5.2.2.4 HAN interception: eavesdropping and modification

A HAN interception occurs when an unauthorized party gains access to a message passing over a HAN between the HES gateway and a local user, service or device, as shown in Figure 6.

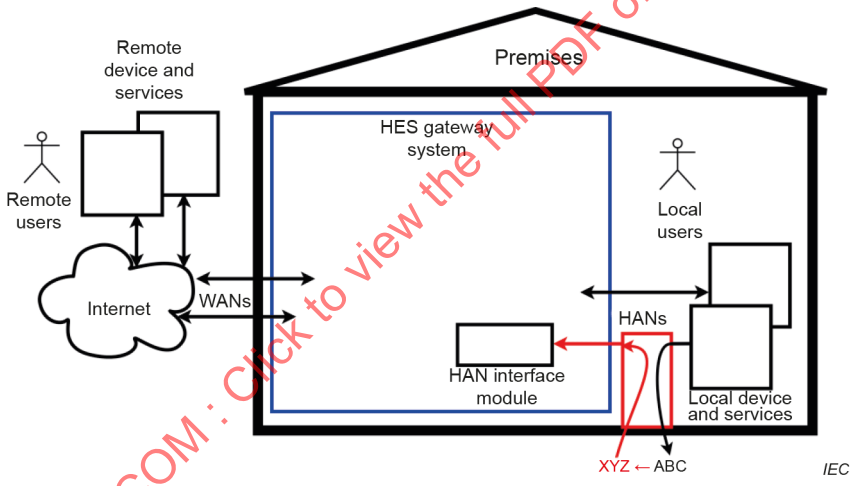

Figure 6 – HAN interception: eavesdropping and modification

The intruder can be an automated system that is programmed to search for vulnerable messages, or it can be a person who has wiretapped or otherwise violated the integrity of the communications channel.

The interception can be passive or active; a passive interception amounts to eavesdropping – in effect, reading someone else's traffic. An active interception can involve changing the contents of the message, deleting or rearranging part of the communication, or changing its protocol control information, particularly the header (including the destination or source address).

The key defence for an interception attack is to implement integrity and confidentiality services. Authentication can also be used to thwart modification attacks.

Even if all communications employ integrity and confidentiality services, an eavesdropper can learn a great deal about the home network by monitoring source and destination information and the time of each message. This practice is called traffic analysis.

Even if transmission is encrypted, the attacker is able to learn a great deal by simply noting which devices are active and in communication partnerships. This is especially important with wireless communications since the eavesdropper can operate from a considerable distance. This type of monitoring can be used to determine occupancy and the type of activity being performed.

To minimize the risk, the HES gateway system shall implement several precautionary measures to contribute to the security controls as shown in Figure 3.

The HES gateway system manages and controls communications to HANs to provide protection, which limits the opportunity for interception.

The HES gateway system supports a wide range of HANs that can have varying capabilities for detecting eavesdropping and preventing modification of packets. The HES gateway system ensures that standardized information about the HANs is available to the user and system integrator so that these risks can be identified and appropriate systems given preferential treatment.

One key element for determining the ease of eavesdropping relates to the type of media used in the HAN. For example, eavesdropping is normally easier for wireless systems in which a receiver can be placed anywhere, whereas a wired system, in most cases, requires access to the cable itself, or at least proximity to it. In contrast, a fibre optic system is fairly immune to eavesdropping. The HAN interface module shall be manufactured with a standardized characteristic, "mediaType", indicating the media of the attached HAN.

Some network systems are designed for point-to-point operation in which the addition of unwanted receivers can be easily detected. Other network systems are based on a bus-type network where an extra tap cannot be detected.

Another element to consider is a transmission technique, in which spreading of the signal (called spread spectrum communications) can help mask traffic by using more than a single frequency. The spreading algorithm uses a key known only to the sender and the receiver.

Some HANs use sophisticated error detection and correction techniques that will reduce the chances of data modification in transit.

The HAN interface service module shall include retrievable status information relating to the susceptibility to eavesdropping and data modification. This is accomplished through the use of standardized "eavesDrop", "dataModification" and "hanFailure" characteristics of the HAN interface module.

The standardized HAN information can be used for the development of specialized application services focused on reducing susceptibility for eavesdropping and modification of data.

5.5.2.2.5 WAN interception: eavesdropping and modification

A WAN interception occurs when an unauthorized party gains access to a message passing between the HES gateway and an external user, as shown in Figure 7.

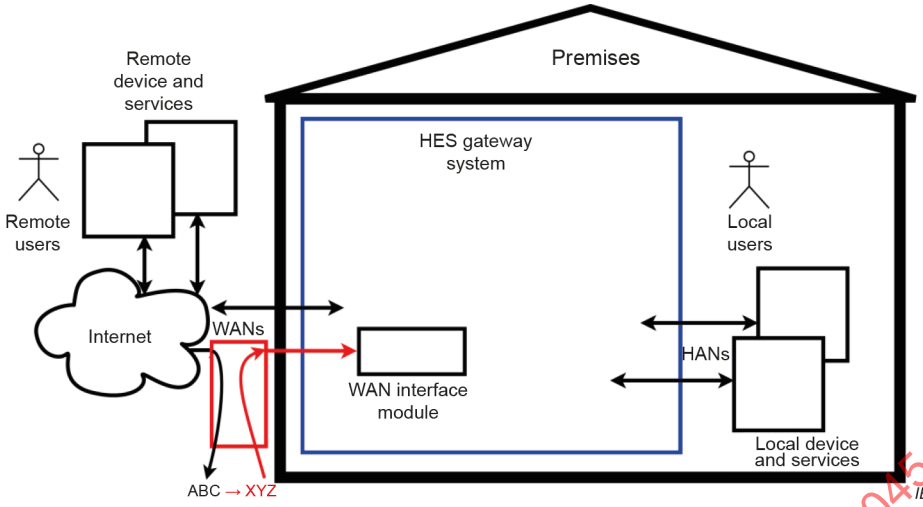

Figure 7 – WAN interception: eavesdropping and modification

The intruder can be an automated system that is programmed to search for vulnerable messages, or it can be a person who has wiretapped or otherwise violated the integrity of the communications channel.

The interception can be passive or active; a passive interception amounts to eavesdropping – in effect, reading someone else's traffic. An active interception can involve changing the contents of the message, deleting or rearranging part of the communication, or changing its protocol control information, particularly the header (including the destination or source address).

The key defence for an interception attack is to implement integrity and confidentiality services. Authentication can also be used to thwart modification attacks.

Even if all communications employ integrity and confidentiality services, an eavesdropper can learn a great deal about messages to and from the HES gateway system through the external links by monitoring source and destination information and the time of each message. This practice is called traffic analysis.

Communications outside the HES gateway system can be hidden by anonymizer services.

To minimize the risk, the HES gateway system shall implement several precautionary measures to contribute to the security controls as shown in Figure 3.

The HES gateway system supports a wide range of WANs that can have varying degrees of detecting eavesdropping and preventing modification of packets. The HES gateway system ensures that standardized information about the WANs is available to the user and system integrator so that these risks can be identified and appropriate systems given preferential treatment.

One key element for determining the ease of eavesdropping relates to the type of media used in the WAN. For example, eavesdropping is normally easier for wireless systems in which a receiver can be placed anywhere. In contrast, a fibre optic system is fairly immune to eavesdropping. Other possible media types include powerline, wired, and satellite. The WAN interface module shall be manufactured with a standardized characteristic, "mediaType", indicating the media of the attached WAN.

Another element to consider is a transmission technique in which spreading of the signal can help mask traffic by using more than a single frequency. The spreading algorithm uses a key known only to the sender and receiver.

Some WANs use sophisticated error detection and correction techniques that will reduce the chances of data modification in transit.

The WAN interface service module shall include retrievable status information relating to the susceptibility to eavesdropping and data modification. This is accomplished through the use of standardized "eavesDrop", "dataModification" and "wanFailure" characteristics of the WAN interface module.

The standardized WAN information can be used for the development of specialized application services focused on reducing susceptibility for eavesdropping and modification of data.

5.5.2.2.6 HAN denial-of-service and resource-exhaustion attack

An HAN denial-of-service (DoS) attack is effected by flooding one of the internal HANs connected to the HES gateway system with traffic, thus preventing legitimate messages from reaching the HES gateway system or the HANs as shown in Figure 8.

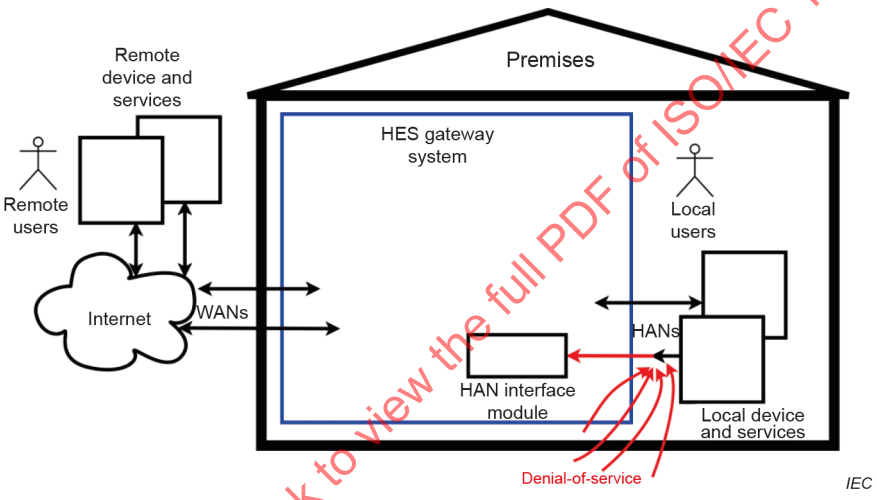

Figure 8 – HAN denial-of-service and resource-exhaustion attack

Denial-of-service attacks are almost impossible to defend against in real time. In fact, security mechanisms alone cannot be effective against denial-of-service attacks, as it is trivially easy to overwhelm any defence by sending additional bogus messages.

Careful design and implementation of the protocol and access device can mitigate resource exhaustion, whereby the flooding ties up only certain parts of the home network or access device.

To minimize the risk, the HES gateway system shall implement several precautionary measures to contribute to the security controls as shown in Figure 3.

All internal (to the premises) network connections (HANs) to the HES gateway system connect to HAN interface modules. This module is responsible for ensuring that traffic coming from outside the HES gateway system (but within the premises) does not overwhelm the internal HES-CLME network bus and isolates the flooding from affecting other modules in the system, including other internal HANs and associated devices, and other modules in the HES gateway.

The HAN interface service module includes limits on the rate of incoming packets and number of incoming connections. This is accomplished through the use of standardized "maxIncomingPacketRate" and "maxIncomingConnections" characteristics of the HAN interface module. If these limits are exceeded, the module ignores additional incoming requests, and an alarm shall be initiated by setting the appropriate value in the "hanFailure" characteristic of the HAN interface module. It can give priority to messages in the output queues originating in the home.

To ensure the home network does not become an unwitting participant in a DoS attack, measures are taken to ensure corrupt software is not installed, see Figure 8. Access control devices implement ingress filtering. This prevents the use of spoofed IP addresses; it has no effect if the attacker uses valid network addresses. Ingress filtering makes tracking down the source of the attack much easier because the packet source address is the source of the traffic. To perform ingress filtering, the access devices block any packets with source addresses that do not originate within the home network.

5.5.2.2.7 WAN denial-of-service and resource-exhaustion attack

A WAN denial-of-service (DoS) attack is effected by flooding the external access network to the HES gateway with traffic, thus preventing legitimate messages from reaching HES gateway or the HANs within the premises as shown in Figure 9.

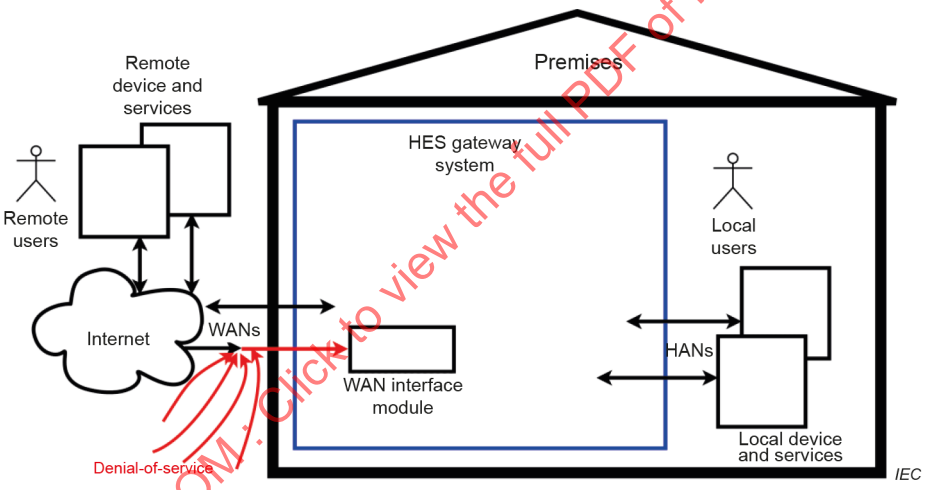

Figure 9 – WAN denial-of-service and resource-exhaustion attack

Denial-of-service attacks are almost impossible to defend against in real time. In fact, security mechanisms alone cannot be effective against denial-of-service attacks, as it is trivially easy to overwhelm any defence by sending additional bogus messages.

Careful design and implementation of the system and access device can mitigate resource exhaustion, whereby the flooding ties up only certain parts of the network or access device.

To minimize the risk, the HES gateway system shall implement several precautionary measures to contribute to the security controls as shown in Figure 3.

All external network connections to the HES gateway system connect to WAN interface modules. This module is responsible for ensuring that external traffic does not overwhelm the internal HES-CLME network bus and isolates the flooding from affecting other modules in the system, including the internal HANs and associated devices, and other modules in the HES gateway.

The WAN interface service module shall include limits on rate of incoming packets and number of incoming connections. This is accomplished through the use of standardized "maxIncomingPacketRate" and "maxIncomingConnections" characteristics of the WAN interface module. If these limits are exceeded, it ignores additional incoming requests, and an alarm is set by setting the appropriate value in the "wanFailure" characteristic of the WAN interface module.

5.5.2.2.8 Software and configuration security: Trojan horses, worms, viruses

A range of HAN devices, HAN interface modules and WAN interface modules allow for software and firmware updating of features, including enhanced security features. While useful, this re-programmability also allows the products to be exposed to other threats, such as worms, viruses and Trojan horses, as shown in Figure 10.

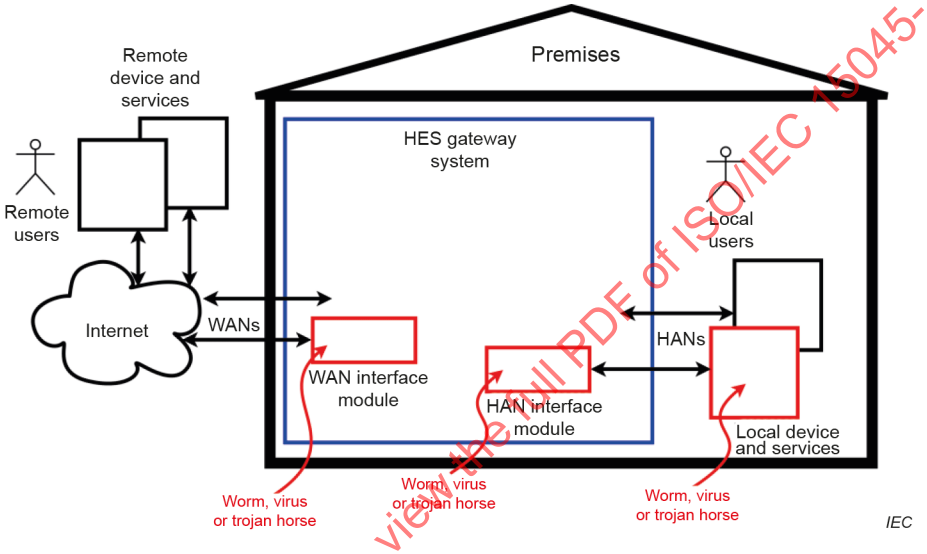

Figure 10 – Worm, virus or Trojan horse

A Trojan horse is an unauthorized program that enters the home hidden in a legitimate message. Once in the home, the Trojan horse can reside in a processor in any networked device. For example, a Trojan horse can be inserted into an intercepted MPEG data stream and take up residence in the processor of the digital television (DTV). The Trojan horse can then use the resources of the television's processor and the digital home network to compromise the security of the internal network.

Worms and viruses have received considerable publicity in both the technical and popular press.

A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm can be activated to replicate and propagate again. In addition, the worm usually performs some unwanted function. A worm that invades the home network can thus spread across the network to multiple devices. If the worm performs harmful activities, such as wiping out the non-volatile memory of the device, the homeowner can find that multiple appliances, from DTVs to toasters, no longer work properly.

A virus is code embedded within a program that causes a copy of itself to be inserted in one or more other programs, as well as performing some unauthorized function on the host machine. Unlike a worm, a virus will not actively try to spread itself to other processors on the home network, so its damage will be confined to a single appliance. However, such an appliance can function in unpredictable and undesired ways and can cause widespread problems if this appliance is essential to the operation of the home network.

To minimize the risk, the HES gateway system implements several precautionary measures to contribute to the security controls as shown in Figure 3.

HAN and WAN interface modules that have re-programmability features shall provide the re-programming with sufficient authorization and authentication.

All HAN and WAN interface modules shall include retrievable status information to indicate whether or not the HES gateway modules have on-line software update or operating system update features. This is accomplished through the use of standardized "interfaceModuleUpdating" and "interfaceModuleOSUpdating" characteristics of the HAN interface module object.

All HAN interface modules shall include retrievable status information to indicate whether or not the HAN networks to which they are attached have on-line software update or operating system update features. This is accomplished through the use of standardized "hanUpdating" and "hanOSUpdating" characteristics of the HAN interface module object.

If a worm, virus or Trojan horse is suspected to have occurred on an attached HAN, an alarm is set by setting the appropriate value in the "hanFailure" characteristic of the HAN interface module.

5.5.2.2.9 Spyware and data leakage

Software, purposely installed, can constitute a threat to privacy and the integrity of the HAN. Spyware is often included in commercial software packages. Spyware is commonly used to embed advertising messages in shrink-wrapped applications. It constantly refreshes the advertising message. Diagnostic and usage utilities are used to gather information and report back to the software vendor. Because these are legitimately installed applications they have the ability to access almost any system information they are running. They can also search the HAN for additional information.

Personal firewalls or other access control mechanisms can be installed on terminal devices and in the HES gateway to control access rights. Control of this type of activity is very difficult because the applications and destination can be used for other purposes approved by the user.

5.5.2.2.10 Risks of commerce over the Internet

With the rapid increase of commerce over the Internet, any payment from a home can be questioned in retrospect and possibly be repudiated. Payments can be made by appliances on behalf of the resident (for instance pay per view on TV or pay per wash by the washing machine or automatic re-ordering by the refrigerator). Goods and services can be ordered by the resident or family. Therefore, it becomes vital to the service provider that there be a verifiable audit trail of the transaction including the identity and authenticity of the purchaser and that the goods were received with due regard for any contract between the service provider and the buyer.

EXAMPLE If it is possible for the cat to trigger supplies of caviar, clearly the process of authentication and authorization would be dysfunctional, and the service provider would have no way of proving the provenance of the purchase.

Many devices on a HAN use owner-authorized automatic or owner controlled purchase or micro payment for goods and services. It is particularly important for application service providers and content providers in particular that the home owner is assured of the integrity of financial transactions and that there are secure routes for funds to reach the service provider.

5.5.2.2.11 Unintentional network to network interconnect

The deployment of virtual private networks (VPNs) allows HAN hosts to be directly connected via a secure tunnel to another network. This enables employees to have full access to corporate resources from home. VPNs create two potential problems: address conflict and message relaying.

If two or more networks using private addresses are interconnected, the same host address can occur in both networks. The benefit of private addresses is the lack of global administrative control resulting in a potential address ambiguity making it impossible to access both devices. In the IP world this is likely to occur if network address translation (NAT) is used to expand a limited range of addresses available to the HES gateway.

The other risk is that a compromised device will relay traffic from one domain to another. If a VPN workstation is compromised, the attacker is able to use the workstation to relay traffic from the attacker's system, through the workstation, to the remote network.

The first case is an addressing issue. If the HES gateway is responsible for address allocation, it shall have a flexible address assignment mechanism to move the HAN to a different block of addresses if a conflict occurs.

The address conflict is not confined to remote access to a corporate VPN. It is also a problem when providing VPN access into the HAN. This is likely to occur when the HAN is accessed from other HANs via a VPN.

Anti-virus and anti-Trojan horse programs minimize the risk that a device on the HAN becomes compromised.

5.5.2.2.12 Communications internal to the HES gateway (HES-CLIP)

The threats discussed so far in 5.5.2.2 deal with threats to the HES gateway system as a whole, complete entity. There are also possible threats to the internal communications (HES-CLIP) of a modular gateway system.

HES-CLIP is run on an internal network (inside the HES gateway) so it is protected and managed within the premises. This limits the opportunity for threats.

Besides the principles discussed throughout this document, there is support to enhance privacy and security through flexible encryption techniques between devices running on HES-CLIP.

5.5.2.3 Vulnerabilities, conditions and controls

As shown in Figure 3, vulnerabilities, predisposing conditions and security controls of the HES gateway system are also key considerations for risk assessment.

To support the identification of vulnerabilities, HAN interface modules shall include retrievable status information to indicate the level of vulnerability. This is accomplished through the use of standardized "vulnerability" characteristics for data within user objects. The HAN interface modules are required to support information with higher numbers indicating increased vulnerability. The units and setting of values are determined by the system integrator of the HES gateway system.

For example, HANs containing devices that can be updated on-line without rigorous security protection would be placed at a higher level (more vulnerable) than HANs containing only devices that cannot be updated on-line. As noted earlier, one key predisposing condition is to ensure that different manufacturers' products can be integrated together using the modular concept while ensuring privacy, security, safety and interoperability. This condition is handled through the document structure of the standards with detailed specifications of each module starting from one common standard, ISO/IEC 15045-4-1.

As noted earlier, one key element of strong security controls for the HES gateway is the use of extensive standardized risk data for all modules. These data provide a strong foundation for effective security controls to be implemented. For example, if a HAN is found to be less secure, the system can ensure that less sensitive data or commands be exchanged via that HAN. Or a poorly behaving HAN can be improved by reducing the incoming packet rate.

5.5.2.4 Risk levels; HAN, WAN, data

The overall risk is a combination of the adverse impact and the likelihood. The HES gateway provides quantifiable values that can be used to compare the relative adverse impact, likelihood or risk for HAN networks and their devices. Using the retrievable status information provided in 5.5 and 5.6, system integrators can develop formulas to determine risk levels, threats, and assessment scales. Actual value ranges are determined by the systems integrator.

Manufacturers shall ensure that the adverse-impact level values are accessible through the standardized "adverseImpactLevel" characteristic of the objects. Similarly, the likelihood level values shall be accessible through the standardized "likelihoodLevel" characteristic.

The risk level values, (calculated through a formula based upon the adverse impact and likelihood, shall also be accessible through the standardized "riskLevel" characteristic. Low risk values mean that the adverse effects are negligible, while high risk values mean the adverse effects can be catastrophic.

With manufacturers ensuring that all objects contain these characteristics, system integrators can then update these standardized characteristics and can supply advanced risk-related features for the user, including enabling the display of the information to the user.

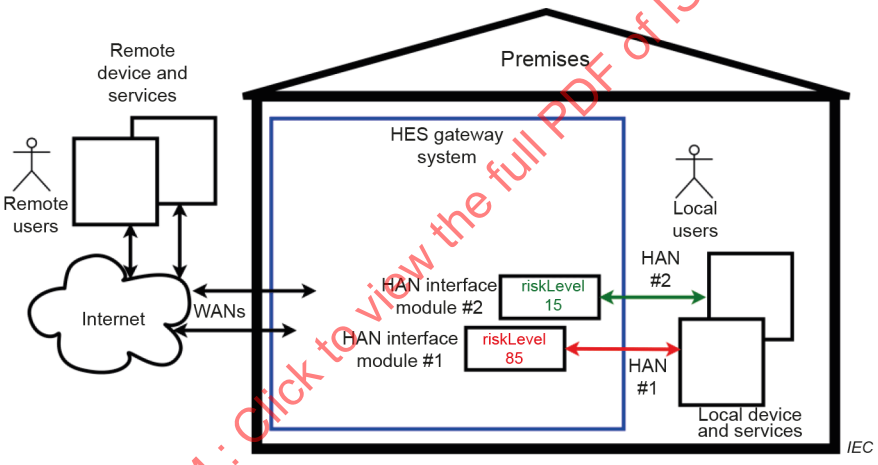

Figure 11 – Risk level for HAN: example

An example for using the HAN risk level is shown in Figure 11. An HES gateway system has two HAN networks: HAN 1 and HAN 2. The systems integrator decided to use a numbering scheme similar to the NIST values up to 100[3]. Through analysis of the retrievable status information from the HAN interface module 1, the system integrator has calculated the riskLevel of HAN 1 to be 85, or high risk. Calculations for HAN 2 resulted in a riskLevel of 15, or low risk (e.g. fibre optics). Based upon this analysis, the system integrator decided that it would be appropriate to turn lights on and off through either HAN, but it would only use HAN 2, the lower risk network, to control setpoint in the premises.

A similar process for the riskLevel characteristic is done for the WAN services, which can have different algorithms and ranges than for HANs.

The riskLevel characteristic for data in user objects does not have the support of underlying status information to rely upon as HANs and WANs do but is still available for system integrators to quantify for their system requirements. The risk level values are placed in the standardized "riskLevel" characteristic of the appropriate user object.

---

3 National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST SP 800-30, Rev 1, Appendix D, Table I-3

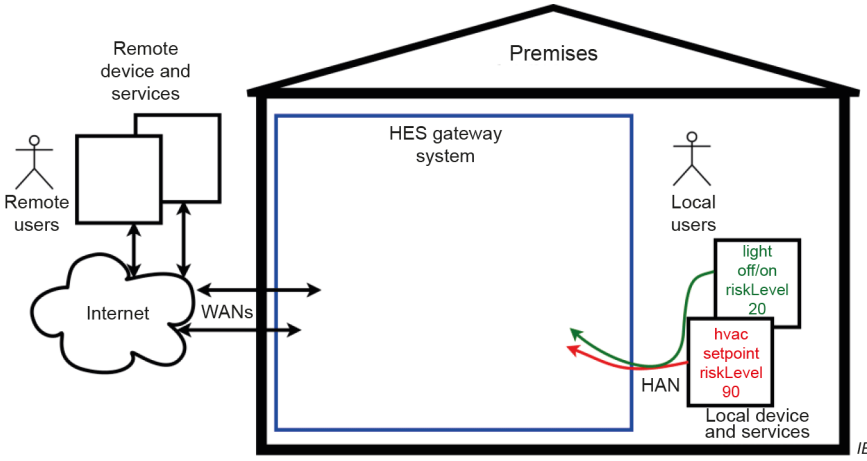

Figure 12 – Risk level of data inside user objects: example

An example for using the risk level of data inside user objects is shown in Figure 12. An HES gateway system has a HAN network with a light controller ("on/off" actuator) and an HVAC thermostat with a temperature setpoint. The systems integrator determines that the risk to controlling the light is low (e.g. value of 20) as turning off or on the light inadvertently has little consequence. For the thermostat setpoint, on the other hand, the risk is high (e.g. value of 80), as inadvertently setting the setpoint too high or too low can cause uncomfortable conditions, or in some cases, unsafe conditions. Other risks include loss of private information, some of which can be more important than others.

Similar functionality can be performed using the adverse impact or likelihood level data instead of the risk level.

5.5.3 Risk treatment

A key part of risk treatment is the identification of alternatives, or other solutions or ways of gaining the benefits or reducing the risk. The HES gateway system ensures that manufacturers provide the underlying information and that it is available for system integrators to treat the risk to the rigour that they consider appropriate.

After implementing the alternatives, the risk levels and subsequent benefits can be compared, and an evaluation performed to decide on the best approach as shown in Figure 13.

For example, assume a HAN is poorly behaving through an overload of incoming packets. The likelihood of adverse impacts increases the overall risk. One of the selected measures can be to limit the incoming packet rate for a HAN. With the decrease in packet rate, the behaviour of the HAN can be re-evaluated. If the HAN continues to be an issue, the packet rate can be completely shut-down.

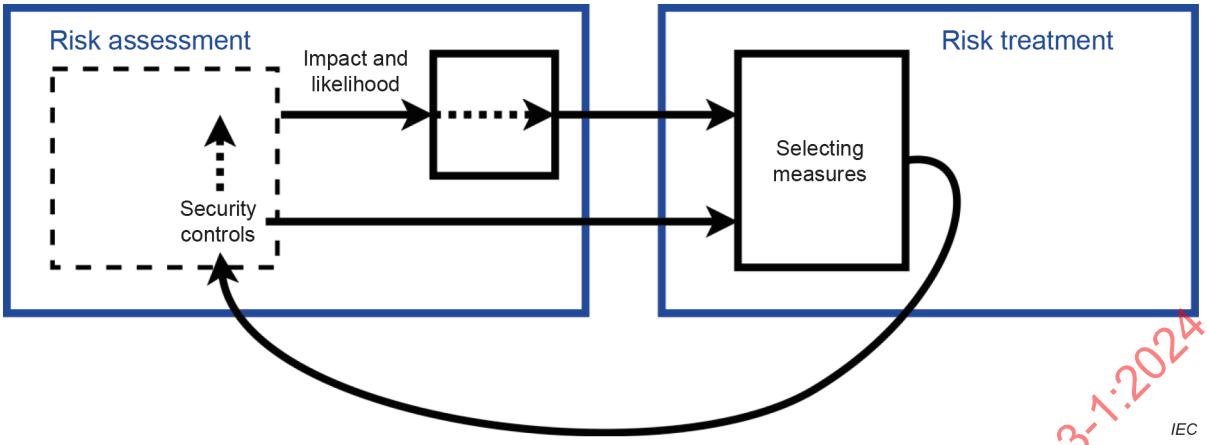

Figure 13 – Risk treatment and risk assessment flow

5.6 Privacy, security, and safety guidelines and requirements

5.6.1 Privacy-by-design approach

5.6 provides general privacy, security and safety guidance and requirements on how developers approach the design of their interface and application service modules for the HES gateway environment. Because the HES gateway applies the privacy-by-design approach, all related hardware and software design begins from this perspective. Additional guidance is provided in Annex B.

To further support the privacy-by-design approach within the modular and interoperable structure of the HES gateway, manufacturers of HES gateway modules shall support standardized status information relating to the principles of privacy, security and safety as specified in the HES gateway lexicon. This status information, which can be presented to installers or users, provides a consistent standardized foundation for system integrators to enhance the privacy, security and safety principles in their implementations. It also encourages developers to further enhance their products to support these principles.

5.6.2 External services non-reliance principle and practice

Critical premises systems should not rely on external services (e.g. "cloud" services) including WANs, wireless networks, or other media that are beyond the physical control of the premises. External services should be regarded as adjunct services. The products and system should be able to provide and maintain basic functionality without external communication, known as "islanding" capability.

To support this principle, HAN interface modules shall include retrievable status information that indicates the ability of the attached HAN system to setup or configure without external services and its islanding capability. This is accomplished through the use of standardized "externalSetupConfiguring" and "islandingCapability" characteristics of the HAN interface module object.

5.6.3 Use of wireless or shared media principle and practice

Critical premises (HAN) network traffic for basic or critical internal functions should not rely on communications employing wireless or other shared media that can be jammed or impaired, e.g. subject to DoS attack or to electromagnetic interference (EMI).

To support this principle, HAN interface modules shall include retrievable status information to indicate the type of media used for the HAN. This is accomplished through the use of standardized "mediaType" characteristic of the HAN interface module object.

5.6.4 Privacy best practice

The best way to make sure that data are kept secure or private is to not collect them.

To support this principle, HAN interface modules shall include retrievable status information to indicate whether data are collected or not. This is accomplished through the use of standardized "collectedDataType" characteristic for data within user objects.

5.6.5 Privacy next best practice

The next best way to make sure that data are kept secure or private is to delete and dispose of (make impossible to recover) the data immediately after they have been used for the intended purpose.

To support this principle, HAN interface modules shall include retrievable status information to indicate how and when data are erased. This is accomplished through the use of standardized "collectedDataType" and "collectedDataParameter" characteristics for data within user objects.

5.6.6 Online update vulnerability principle

On-line software update features are a potential vulnerability and are regarded as risky.

To support this principle, HAN interface modules shall include retrievable status information to indicate whether or not the HES gateway modules or the HAN networks to which they are attached have on-line software update features. This is accomplished through the use of standardized "interfaceModuleUpdating" and "hanUpdating" characteristics of the HAN interface module object.

5.6.7 Online OS update vulnerability principle

On-line OS updates are especially vulnerable and can circumvent all other safeguards.

To support this principle, HAN interface modules shall include retrievable status information to indicate whether or not the modules or the HAN networks to which they are attached have on-line operating system update features. This is accomplished through the use of standardized "interfaceModuleOSUpdating" and "hanOSUpdating" characteristics of the HAN interface module object.

5.6.8 "Social engineering" vulnerability principle

It is recognized that one of the most common and successful security and privacy attacks is "social engineering", which can circumvent all other safeguards. Social engineering involves psychological manipulation to convince the user to take actions that can be detrimental. Any technology including the HES gateway is limited in the ability to protect the user from deliberate actions that the user chooses, even if potentially harmful.

5.6.9 Privacy-by-design principle and practice

The principle of privacy by design[4] is imperative, requiring that security, privacy, and safety be considered in the design of products at all stages from the beginning.

5.6.10 User priority principle

The purpose of the HES gateway is first to serve the interests and integrity of the premises and its users before the interests of external parties.

---

4 See reference to Ann Cavoukian's work in the Bibliography. Also relevant strategies: security by design and safety by design.

5.6.11 Fail-safe principle

Apply the fail-safe principle for privacy, security, and safety. Product failure modes shall not result in an unsafe event or condition, or in a risk to privacy or security. If a failure mode does occur, an indication of that failure should be accessible.

To support this principle, HAN interface modules shall include retrievable status information to indicate failure modes in the HES gateway modules and the HAN networks to which they are attached. This is accomplished through the use of standardized "imFailure" and "hanFailure" characteristics of the HAN interface module object.

5.6.12 Precautionary principle

Apply the precautionary principle for privacy, security, and safety. In a case of uncertain risk, the default assumption shall be in favour of the lowest risk alternative.

This document standardizes crucial status information that manufacturers, developers, and system integrators can use to develop mechanisms to choose the lowest risk alternatives.

5.6.13 Normal accident principle

Apply the normal accident principle for privacy, security, and safety. Design choices should recognize that the greater the complexity, coupling, and interdependencies in a system, the greater the likelihood of inevitable systemic failure (i.e. simpler or smaller is better).

A significant aspect of complexity is related to the number of modules within the HES gateway and HES gateway class type. To support this principle, the identification service module shall include retrievable status information of the number of modules and class of the HES gateway. This is accomplished through the use of standardized module number counts and "classHESGateway" characteristics of the identification service module.

5.6.14 Privacy principles

The privacy principles of ISO/IEC 29100, which are modified for HES in ISO/IEC 15045-3-2, shall be applied. ISO/IEC 15944-8:2012; Clause 5 also applies.

5.6.15 Watchdog practice

Utilize process "watchdogs" (i.e. timers used to detect and recover from module malfunctions) at the module level.

– Apply watchdog timers for module implementations to prevent a crash condition.
– Monitor process watchdogs for unintended or anomalous system behaviours.

5.6.16 Redundancy principle

Apply the redundancy principle, i.e. plan on or expect sensor and actuator failures and reduce dependencies and unnecessary coupling.

6 Common services

6.1 Common services

The following services are or can be shared among all services that deal with privacy, security or safety considerations.

6.2 Binding map

The binding map service provides the key directing role of messages from one interface module to another within the HES gateway using HES-CLME. It also translates standardized HES gateway lexicon information from one application to another.

To support the privacy, security and safety features of the HES gateway, the binding map has strict rules in which it operates, such as limiting the data used in real-time processing, providing distinct, interoperable objects for all binding maps, and ensuring that interface modules do not communicate directly to each other (they shall go through binding maps).

For further information, refer to the binding map service module as specified in ISO/IEC 18012-3 and ISO/IEC 15045-4-1.

6.3 HES gateway unique ID service module

A global ID service module shall be used for HES gateways that are connected to external services so that masquerade gateways cannot pretend to be legitimate gateways. This ID defines the unique system for all premises products that utilize a specific HES gateway environment. This ID module derives a 256-bit true random number (see NIST SP 800-90A) that is used to establish:

a) a unique ID that is publicly accessible, yet anonymous, where information relating to the gateway cannot be derived from the ID (e.g. location, generation date);

b) a secret internal random code or "digital fingerprint" that is not revealed and is used for encryption techniques.

This method does not rely on any other external services such as DNS look-up, which can be inconsistent and typically requires duplicates.

Each specific HES gateway instance requires its own global identifier because it represents a specific unique set of networks and functions or applications that can overlap or co-occupy physical or logical space that includes another such gateway instance, or possibly even multiple such gateway instances. A unique identifier is also needed to establish a link to an external service, independently of IP addresses or other network addresses, which can be temporarily assigned. The identifier is used for access and differentiation purposes. For data analysis purposes, further randomization and potentially other cryptographic techniques should be used to protect the privacy of the user and premises' contents.

6.4 Cryptographic services

A cryptographic service module provides encryption services to support all other service modules within the HES gateway system via HES-CLIP communications or to support secure communications with external services. This service module also provides cryptographically protected storage, management and validation for credentials such as passwords and certificates (including ISO/IEC 9594-8 | Rec. ITU-T X.509 public key infrastructure (PKI) certificates), true random generation, cryptographic calculations, and trusted mechanisms (e.g. root of trust, keys).

6.5 Authorization and authentication service

An authorization service module provides authorization and authentication services to support all other service modules within the HES gateway system via HES-CLIP communications or to support authorization and authentication with external services. All operations within the HES gateway shall have appropriate authorization before being allowed to proceed and are linked to the binding map. Different levels of authorization allow for focused restricted network operations for certain classes of user (such as for parents versus children), or for privacy considerations of certain premises or personal data. Key operator authorization ensures that system-wide management functions are appropriately restricted.

6.6 Time service

A time service module provides time information for a wide range of applications in the HES gateway. The source of time can originate from network time via external services or from locally generated time sources. Time can be used for application operations (e.g. for scheduling events or datalogging), for HES gateway operations (e.g. time stamping of events) and for cryptographic operations such as certificates that restrict their validity after certain dates or times.

Annex A
(informative)

Privacy protection principles and sources

A.1 Privacy protection principles

Eleven basic privacy protection principles are identified and described in ISO/IEC 15944-8:2012, 5.2:

1) preventing harm
2) accountability
3) identifying purposes
4) informed consent
5) limiting collection
6) limiting use, disclosure, and retention
7) accuracy
8) safeguards
9) openness
10) individual access
11) challenging compliance

These privacy principles serve as a basis for this document.

A.2 Sources

The sources of the above privacy protection principles relied on and specified in this document are summarized in Figure A.1.