INTERNATIONAL STANDARD

ISO/IEC 15045-1

First edition
2004-01

Information technology –
Home electronic system (HES) gateway –

Part 1:
A residential gateway model for HES

Reference number
ISO/IEC 15045-1:2004(E)

INTERNATIONAL STANDARD

ISO/IEC 15045-1

First edition
2004-01

Information technology – Home electronic system (HES) gateway –

Part 1: A residential gateway model for HES

PRICE CODE P

For price, see current catalogue

CONTENTS

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 1: A residential gateway model for HES

FOREWORD

1) ISO (International Organization for Standardization) and IEC (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) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

3) All users should ensure that they have the latest edition of this publication.

4) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

5) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 15045-1 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INTRODUCTION

The residential gateway (RG) is a device of the Home Electronic System (HES) that connects home network domains to network domains outside the house, as shown in Figure 1. It supports communications among devices within the premises and systems, service providers, operators and users outside the premises.

The RG enables service and content providers to deliver services such as entertainment, video and broadband digital streams, monitoring for health care, security and occupancy, home appliance control and preventive maintenance, remote metering, and energy management. The RG specified by this standard does not imply the use of any particular protocol such as IP and it is recognised that many forms of the RG will exist using many types of data such as analogue video and broadband digital streams.

The safe and effective delivery of these services places many demands on the facilities of the RG. These include the integrity and security of communications, the delivery of commands to devices in the home from external sources, the blocking of selected commands that may create unsafe conditions, the protection of the home from the risks inherent in a connection to the internet, and facilitating micro-payments. There may be many different configurations of RG. Regardless of the RG configuration, this standard ensures the interoperability of home devices with external services. Also, this standard specifies features to enhance the safety and security of network devices and consumer transactions via the network.

The RG connects the remote user and the internet with the people, equipment, appliances or services in the home. These devices or systems are usually objects or nodes on a particular Home Area Network (HAN).

Residential gateway

Some of the potential interfaces and supported networks of a residential gateway are shown in Figure 1. In all cases the gateway provides the mechanism whereby Wide Area Networks (WANs) communicate with Home Area Networks. The gateway may be a standalone gateway; it may be embedded in another device; or more than one gateway unit may be used. A number of distributed gateway units may display the behaviour of a single gateway.

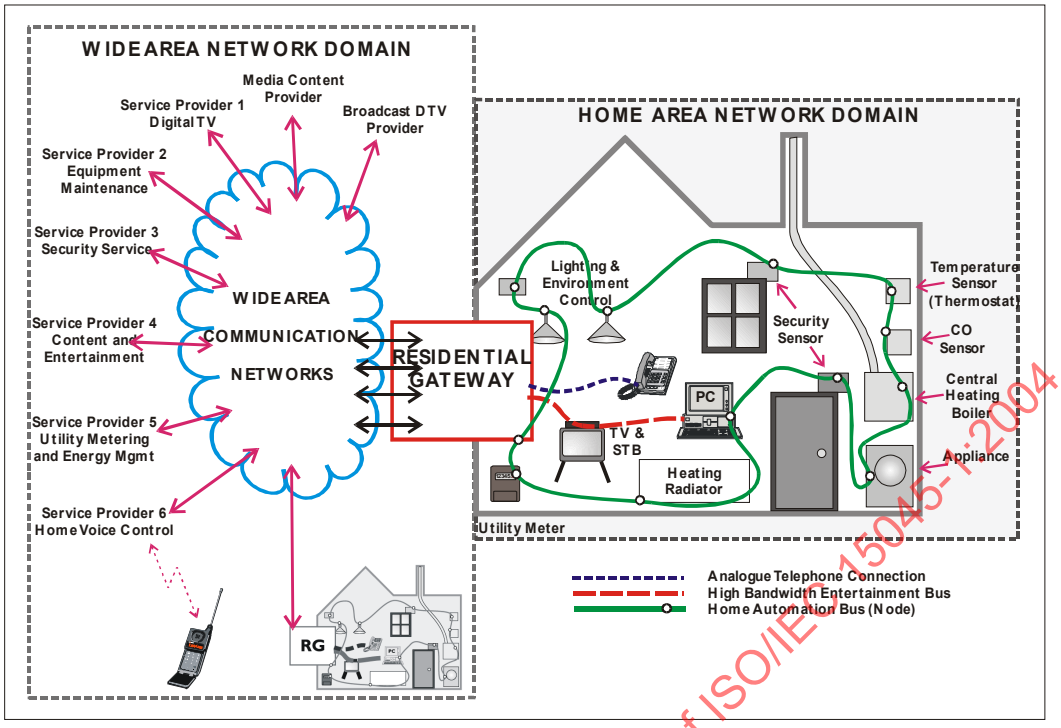


Figure 1 – Typical service provision for home network

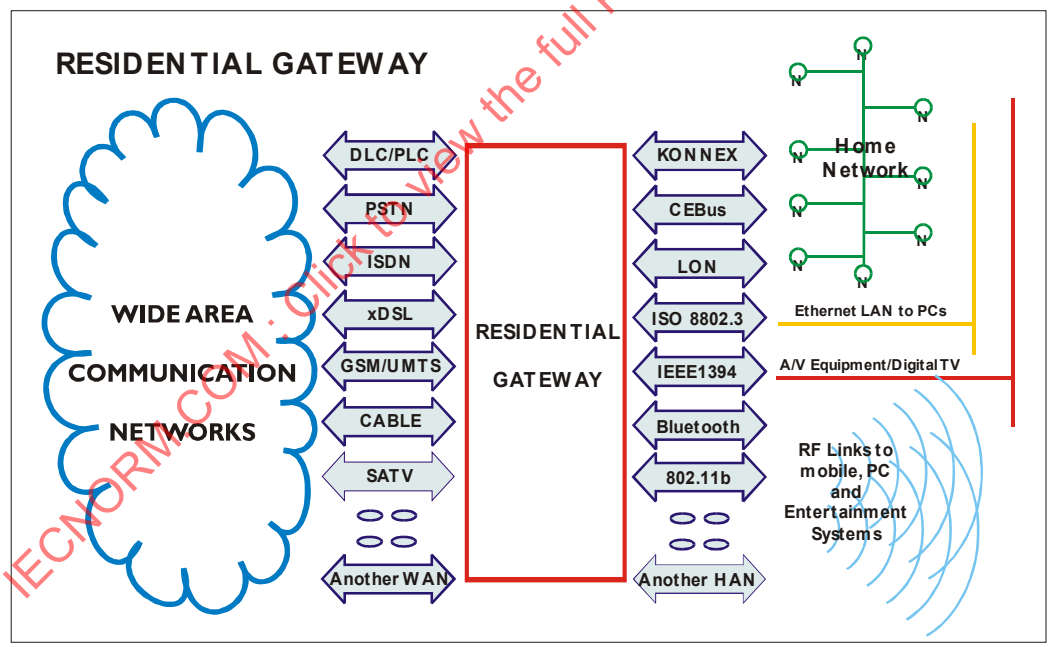


Figure 2 – Diagram of possible RG connections and interfaces

Figure 2 illustrates that multiple WANs and HANs may be supported by the RG. This figure is not intended to imply that all or any of the interfaces or connections shown need to be connected to a residential gateway (or for instance that terrestrial DTV is excluded in favour of SATV).

The physical manifestation of a residential gateway is outside the scope of this standard. This standard accommodates a range of potential configurations. These configurations may range from an approach where a single box acts as interface between two or more WANs and HANs, to a modular dedicated residential gateway, to multiple residential gateways distributed among physically separate locations within the premises.

This standard is based on a black box approach, since it specifies the interfaces of the RG and the function provided but leaves considerable freedom on how these functions are implemented within the black box[1].

This standard is applicable to all communications and other technologies that may be incorporated in the residential gateway and includes both analogue and digital systems.

This document comprises the following:

- requirements of a residential gateway;
- functional safety requirements of a residential gateway, where these are not covered by existing functional safety standards;
- security requirements of a residential gateway;
- options for the Architecture of the residential gateway and the elements of a conforming residential gateway (see Annex A);
- safety requirements of home systems connected to Wide Area Networks and the role of the residential gateway (see Annex B);
- security requirements of home systems connected to Wide Area Networks and the role of the residential gateway (see Annex C).

This document offers a future-proof[2], forwards and backwards compatible standard for residential gateways and for networks and devices to which they are interfaced.

1 In systems terminology a ‘black box’ refers to an object that has inputs, outputs and carries out functions but for which the means and methodology that convert the inputs into outputs are not specified. Only inputs, outputs and functions are specified.

2 A system that is called ‘future proof’ is expected to be adapted to technologies and meet requirements that were not specified when it was designed but may be needed in future.

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) GATEWAY –

Part 1: Residential gateway model for HES

1 Scope

1.1 Overview

This part of ISO/IEC 15045 specifies the minimum functional requirements of a residential gateway (RG) and the documentation to be provided. The standard specifies what a gateway should do in order to deliver services in a suitably safe, secure and future-proof way without being prescriptive. It also gives functional requirements.

1.2 Functional safety

This standard specifies certain safety features where commands sent from remote places to devices on the premises could cause danger to persons or property.

While this standard only specifies minimum requirements for the gateway architecture, gateway operation, and associated home systems in terms of safety, it provides an extensive checklist of functional situations that should be treated with the utmost caution and recommends appropriate measures.

1.3 Privacy and security

This standard specifies security measures to ensure the integrity of information that may pass through the residential gateway.

A residential gateway operating between the internet and the home creates significant concerns for security to the user.

Particular attention is drawn to safety, security and privacy. The attention of the user (consumer, maintainer or application service provider (ASP)) of the gateway is drawn to dangers resulting from unexpected system interoperation, from unauthorised access and from compromise of private user information. RGs that are stated to conform to this standard will be evaluated by the RG manufacturers for potential functional safety and/or security hazards arising from systems integration.

2 Normative references

The following referenced documents are indispensable for the application 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 7498, *Information technology – Open Systems Interconnection – Basic Reference Model*

ISO/IEC 14762, *Information technology – Home Control Systems – Guidelines for functional safety*

ISO/IEC 18012-1, *Information technology – Home electronic system – Guidelines for product interoperability – Part 1: Introduction*[3]

3 Terms, definitions and abbreviations

3.1 Definitions

For the purposes of this part of ISO/IEC 15045, the following definitions apply.

3.1.1
co-existence
no interference between different pieces of equipment on the premises

Specifically, the operation of one RG does not interfere with the operation of another RG.

3.1.2
documentation
all instances of product literature, brochures, data sheets, manuals and catalogues in which the product is described, defined, detailed or pictured that may be produced in paper or any electronic format

NOTE In this definition, "product" refers to a product, a system, a network or a residential gateway.

3.1.3
file transfer protocol, FTP
IP based protocol (see IETF – Internet Engineering Task Force)

3.1.4
home area network, HAN
any electronic network situated within the general environment of a residential dwelling and that connects enabled nodes within that dwelling

3.1.5
HAN to gateway interface, HGI
translates the communications protocol of HAN nodes to that of the internal processor within the RG

NOTE The specification of the RG internal processor is outside the scope of this standard. The HGI may be implemented in software, firmware or hardware and may be modular or integrated in the RG.

3.1.6
IPSec
provides security services at the IP layer that allow the user to apply combinations of integrity, replay detection and encryption to IP packets

It also provides a mechanism for users to authenticate each other and generate and exchange session keys, secret keys that are used for a limited time (a session), and then discarded.

NOTE For further explanation, see IETF.

3.1.7
local area network, LAN
any electronic network that connects computing devices together to form a group of intercommunicating devices

[3] To be published.

3.1.8
management information base
Simple Network Management Protocol (SNMP)

NOTE See also IETF.

3.1.9
network address translation, NAT
feature defined for the internet whereby one IP address is assigned to an RG

Messages intended for specific nodes on a home network are sent to that address and mapped by the NAT to specific node addresses and vice versa.

NOTE See also IETF.

3.1.10
personal area network
any electronic network that connects to enabled devices within the immediate vicinity of a person, generally within a 10 m radius including devices carried by that person

3.1.11
processing and protocol conversion
for any WGI or HGI, processing and protocol conversion may take place to present data in the format and protocol of the RG

3.1.12
residential gateway
electronic device that is situated between WANs and HANs (or LANs) in the premises

3.1.13
residential gateway internal processes
any RG will have internal processes (which are not defined in terms of software requirements) to carry out the requirements of an RG

3.1.14
route
to route information is to direct the information, command or data stream to a particular address or node in the WAN, LAN or HAN

3.1.15
spyware
trojan horse software that may report to an external entity information about a computer, device or network and its parameters

3.1.16
secure/multi purpose internet mail extensions
secure encoding for e-mail attachments

NOTE See also IETF.

3.1.17
secure sockets layer/transport layer security (SSL)
the *Secure Sockets Layer* protocol implements security on HTTP-based communications[4]

4 The IETF formed the TLS Working Group to develop a common standard. Version 1 of TLS, the Transport Layer Security protocol [N10], was issued in January 1999. See IETF.

3.1.18
specific WAN interface
specific interface for a WAN termination

3.1.19
telnet
terminal emulation program for TCP for remote access to computers

3.1.20
trojan horse virus
type of computer virus where the virus embeds itself in software delivered to the computer and carries a payload which then causes other types of events to occur and which may be of malicious intent

3.1.21
user datagram protocol
connectionless protocol

NOTE See also IETF.

3.1.22
virtual private network
a computing device is linked at a remote location from a network of computers by a secure means of communication in such a way that the remote device appears to have the same characteristics as if it were within the network of computers

3.1.23
wide area network, WAN
any electronic network which connects computing devices in the environment external to the premises

3.1.25
WAN to gateway interface, WGI
component which translates the communications protocol of WAN nodes to that of the internal processor within the RG

NOTE The specification of the RG internal processor is outside the scope of this standard. The WGI may be implemented in software, firmware or hardware and may be modular or integrated in the RG.

3.1.26
"x" digital subscriber line, xDSL
technique for superimposing digital signals on a standard analogue local telephone line at a frequency above that of audible speech; "x" may be "A" for asymmetric or "V" for very high rate

3.2 Abbreviations

ASP	Application Service Provider
FTP	File Transfer Protocol
HAN	Home Area Network
HES	Home Electronic Systems
HGI	HAN to Gateway Interface
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol See IETF
LAN	Local Area Network
MAC	Message Authentication Code
NAT	Network Address Translation
PAN	Personal Area Network
PPC	Processing and Protocol conversion
RG	Residential Gateway
RGIP	Residential Gateway Internal Process
S/MIME	Secure/Multi Purpose Internet Mail Extensions
SSL/TLS	Secure Sockets Layer/Transport Layer Security
MIB	Management Information Base
SWI	Specific WAN Interface
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WGI	WAN to Gateway Interface
xDSL	"x" Digital Subscriber Line
OSGi	Open Systems Gateway Interface
SATV	Satellite Television
UMTS	Universal Mobile Telephone System (also known as 3G)
DLC	Distribution Line Communication
PLC	Power Line Communication
KONNEX	The name of the Converged European Standards EIB, EHS and Batibus

4 Conformance clauses

4.1 Basic functions and requirements

In order to conform to this standard a residential gateway shall provide the following basic functions:

- Interface to one or more WANs;[5]
- Interface to one or more HANs:[5]
- Transfer information between WAN(s) and HAN(s);[5]
- Specify WAN and HAN interfaces that are supported using the terms specified in 5.1.2;
- Describe the support provided by the RG for transferring information from a WAN to a HAN in terms specified in 5.3.2, 5.4 and 5.5.

---

5 These items can include simple wiring terminations where no protocol conversion takes place.

4.2 Optional functions and requirements

In order to conform to this standard, a residential gateway shall specify optional functions as follows.

- Where appropriate with respect to the complexity of the RG and especially in the case of IP traffic, prevent unauthorised information from passing into and out of the premises and allow information to flow only to or from suitably authorised persons or devices as specified in clause 6 and clause 7.
- Where appropriate with respect to the complexity of the RG and especially in the case of IP traffic, protect entities within the home with respect to safety, security and privacy as specified in clause 6 and clause 7.
- If an RG meeting this standard is upgraded to support an additional WAN or HAN, then the conformance criteria specified above shall also apply to the upgraded configuration.

  NOTE A gateway may have a simple termination or pass through. In this case it will simply transmit traffic (IP or otherwise) to devices in the home domain and it will not require preventative strategies for IP, since these will be dealt with at the end device.
- The transfer of information between HANs shall be documented in terms specified in 5.3.3, 5.4 and 5.5.
- The routing of information from one device to other devices on a HAN shall be documented in terms specified in 5.3.3, 5.4 and 5.5.
- Expansion of the basic RG (a basic RG conforms to 4.1) to accommodate additional WANs or HANs in support of third party devices shall be documented as specified in 5.1.3.
- Accommodation of application-specific controllers shall be documented as specified in 5.6.1.
- Features to support WAN service delivery shall be documented as specified in 5.6.1.
- Features to support HAN applications shall be documented as specified in 5.1.
- Conversion between internal and external addresses shall be documented as specified in 5.1.2.
- Conversion between multiple internal addresses shall be documented as specified in 5.3.3.
- Conversion of protocols and data formats shall be documented as specified in 5.4.

5 Functional requirements of residential gateways

5.1 Interfacing requirements

5.1.1 General

Residential gateway shall interface to one or more Wide Area Networks and one or more Home Area Networks.

5.1.2 WAN and HAN interfaces

Interfaces to WANs or HANs supported shall be fully documented as stated in ISO 7498.

5.1.3 Additional physical modular interfaces

If the RG has internal interfaces that allow modular and interchangeable use of the RG by third party devices, these interfaces shall be fully defined and documented. The documentation shall be fully defined in terms of ISO 7498 either by reference to the relevant specifications for the various layers or by providing the detailed specification for each layer required by the designer and manufacturer of equipment to be connected to such interfaces.

5.1.4 Application-specific modularity

If modules are provided to carry out application-specific tasks related to service provision, safety and security then these shall be fully defined and documented.

5.2 Co-existence

If RGs are installed in premises where the configuration consists of multiple distributed RGs, then the activity of one Standard RG shall not in any way interfere with the proper operation of another Standard residential gateway. Multiple RGs shall interoperate according to the compliance requirement of ISO/IEC 18012-1.

5.3 Address translation requirements

5.3.1 General

If an RG translates addresses, then the following requirements shall be observed (as defined in ISO/IEC 18012-1).

5.3.2 External to internal (WAN to HAN)

5.3.2.1 HAN supporting IP addressing

If the HAN to which the RG is interfaced supports IP, then the RG shall provide basic IP services such as address assignment, IP-to-physical layer address translation, router function (gateway) (and optionally host name resolution (DNS)). The RG may not be the only device on the HAN capable of delivering these services. If so the RG shall ensure interoperability with other resources.

5.3.2.2 HAN not supporting IP addressing

If the HAN to which the RG is interfaced does not support IP addressing, the RG shall maintain knowledge of the local address of the devices in the HAN and provide address translation as required. The RG shall have the capability of routing information reliably between an entity in the WAN and a device on the HAN. It may also need security access parameters for such devices.

NOTE 1 It is most likely that the RG will be provided with an IP address if it contains an interface to a WAN that uses the internet. Additionally, there may be devices within premises that also have IP addresses. For these devices, the RG will know about and recognise the IP addresses of devices on networks within premises and route messages to these devices.

NOTE 2 Attention is drawn to the potential migration of IP addresses from IPv4 to IPv6.

5.3.3 Internal to internal (HAN to HAN)

If the RG is interfaced to more than one HAN (type or specific system) and devices on one HAN may be required to communicate (or provide information for) devices on another HAN, then the RG should, where appropriate, maintain knowledge of those devices including local HAN addresses and provide address translation.

NOTE The purpose is to facilitate communications among devices even on different HANs. The RG will assume the burden of address and message translation across incompatible HANs. This may be a bilateral or multilateral requirement since this requirement may not be limited to two HANs on an RG. In the case where two HANs have the same addressing format, the RG may only be required to provide a routing function (between different communication media for instance).

5.4 Protocol conversion

If the RG provides protocol conversion, then the features shall be fully documented in the specification, for example by specifying them according to the Interoperability Standard for Home Electronic System (see ISO/IEC 18012-1). In addition, any WAN-to-HAN and HAN-to-HAN communications shall ensure that (within the confines of the set of commonality between the two networks) there is conversion from the terminology and protocols of one WAN or HAN to those of the other HAN. Furthermore, information and commands shall be delivered in the terms of the receiving HAN or WAN.

5.5 Information transfer

An RG shall transfer the information between WAN and HAN and between HAN and HAN as required by the application and interfaces supported. Examples of this type of information include voice, data, text, control and video. The types of information transfers supported shall be documented in the specification of an RG for all interfaces supported by the RG. The function provided by the gateway shall be given by performance data for parameters such as bandwidth, bit rate, format, coding, addressing, latency time and bit error rate.

5.6 Auxiliary RG services

5.6.1 Application-specific services

If the RG provides application-specific services, for example for safety or security, then these services shall, wherever possible, meet the requirements of existing relevant standards and standardized methods (software/hardware). If the application specific functions do not conform to any particular standard, then all operations and features shall be fully documented.

NOTE These requirements apply to application-specific services provided either within the operating parameters of the basic gateway or implemented by the use of plug-in modules for a modular RG.

6 Functional safety with residential gateways[6]

6.1 Introduction

Functional safety is a shared responsibility of objects in the HAN and the gateway. Devices controlled via a network shall be inherently safe as described in ISO/IEC TR 14762. The control of objects from remote systems via the RG may compromise safety more seriously than remote control via a local network. Although the primary responsibility for safe operation of objects lies with the devices containing these objects, the RG is able to assist in reducing the increased risks created by enabling control from a distant location. Annex B discusses some of the particular safety concerns of the residential gateway.

6.2 Requirements for safety

6.2.1 General

If the RG has the capability of processing commands or information directed through it (such as a firewall capability) then it shall also grant it.

6.2.2 Blocking capability

The RG shall be able to block commands to objects specified during installation or configuration. This capability shall be documented.

---

6 A standard is under development to address security requirements for HES; when it is published, the current clause will be updated or replaced as relevant.

6.2.3 Discriminative blocking capability

If an RG is able to discriminate particular commands, then it shall be able to block specific commands which could lead to hazardous states. This capability and its use shall be documented.

6.2.4 Feedback on blocking

Where commands may be blocked, the RG shall be able to give feedback to the originating system or device as to the fact of blocking.

NOTE For discussion of these requirements, please see Annex B.

7 Specific privacy and security requirements concerning residential gateways

7.1 Introduction

There are many potential security threats to a home network (especially if the RG supports IP), that may originate from the WAN or from within the HAN. These threats may compromise the integrity of the home network or expose private messages between HAN devices or between the WAN and HAN. The residential gateway through which messages and information pass shall provide both defensive and proactive services to ensure the privacy and security of messages, information and media content directed to and from trustworthy entities outside the premises and devices on the home network. Information from other non-trustworthy entities outside the premises shall be screened before being forwarded into the premises.

7.2 Security requirements of a residential gateway

7.2.1 General

Annex C provides an overview of the security issues facing the Home Electronic System. Most of the issues involve the information and traffic that pass through the residential gateway. In many cases (especially if the RG supports IP) the gateway is responsible for ensuring that the security, privacy, and integrity of the network are not compromised and that transactions, such as financial transactions, take place securely between trusted entities. There are two main cases:

7.2.2 Devices with direct or secure connections to associated hosts

Devices in the home may be categorised as secure entities in their own right, in which case they will provide means for ensuring the security of information that passes between them and secure hosts in the external environment. For the devices and applications that require security (which is highly recommended), it is likely to be end-to-end security provided by SSL/TLS or IPSec (or a similar encryption methodology of appropriate strength according to the information security required for the device). This should apply also to their software upgrading. See C.2.5.

7.2.3 Devices on HANs, without inherent security

This class of device is characterised by the networked appliance. The HAN is likely to have a different address structure than the (general) IP addressing of the external environment. In this case the RG shall carry out Network Address Translation (of necessity, to the address structure of the HAN or for IP), which to a large extent protects that device from direct attack from the external environment. If these devices need to access their trusted server on the WAN, then the RG shall prevent access to any other address on the WAN.

7.3 Information security

The information to and from devices is likely to be sensitive and needs protection against interception and modification. Typical applications of this type are meter reading and energy control.

Selected sensitive traffic between the RG and the trusted server associated with devices on the HAN shall be capable of being secured using an encryption methodology of appropriate strength according to the information security required for the device.

NOTE Where the delivery HAN in the home uses a technology that can be monitored surreptitiously, it is highly recommended that traffic between devices in the house and the RG should be encrypted.

7.4 External attack on the RG

The RG is also a target for attack and it too shall accept IP packets only from a source that is trusted.

7.5 Security requirements for a residential gateway

The following functions are defined for use by an RG and shall be completely documented where implemented:

- firewall capability;
- encryption for information passing between the RG and service providers in the WAN;
- prevention of unauthorised access to devices in the HAN;
- support for the security measures associated with financial transactions;
- support for the security measures associated with content provision and IPR.

7.6 Security requirements for IP connected residential gateways

Additionally, an RG with IP (except for IP6 and higher) connections that provides an open port to the internet shall meet the following requirements.

- It shall maintain a “firewall capability” that controls access between the WAN and the HAN and vice versa.
- It shall provide adequate security services between itself and trusted servers in the WAN.
- It shall be possible to control access into the HAN from unknown addresses external to the RG and it shall be possible to prevent devices of any sort on the HAN accessing unknown addresses on the WAN.
- If financial transactions may be carried out between automatic devices on the HAN and ASPs in the WAN, appropriate security features shall be provided to prevent surveillance of information exchanged between the device on the HAN and the ASP.
- Optionally, the end user may be supplied with secure remote access service into the HAN.

NOTE For discussion of these requirements, see Annex C.

Annex A
(informative)

Architecture of residential gateways

A.1 Overview of architecture

The residential gateway (RG) is a physical or logical device that provides a common, secure, safe and intelligent interface between Wide Area Networks (WAN) in the external environment (to the premises) and internal (to the premises) Home Area Networks (HAN) and devices on HANs. The interface and translation capabilities of the RG enable independent evolution of the technologies and physical media used in the WAN and HAN. This attribute of the RG makes evolution and innovation in both service delivery and consumer electronics feasible. It enables service providers and application vendors to offer a variety of multimedia services while masking the complexity of the service access from the consumer.

The physical architecture of a residential gateway is outside the scope of this standard. However, this standard accommodates a range of potential configurations. They may range from a "black box" approach, where the function of interfacing between two or more WANs and HANs is provided within the single box, to a modular, dedicated residential gateway, to situations where multiple residential gateways are distributed to physically separate locations within premises.

A.2 Architectural domains

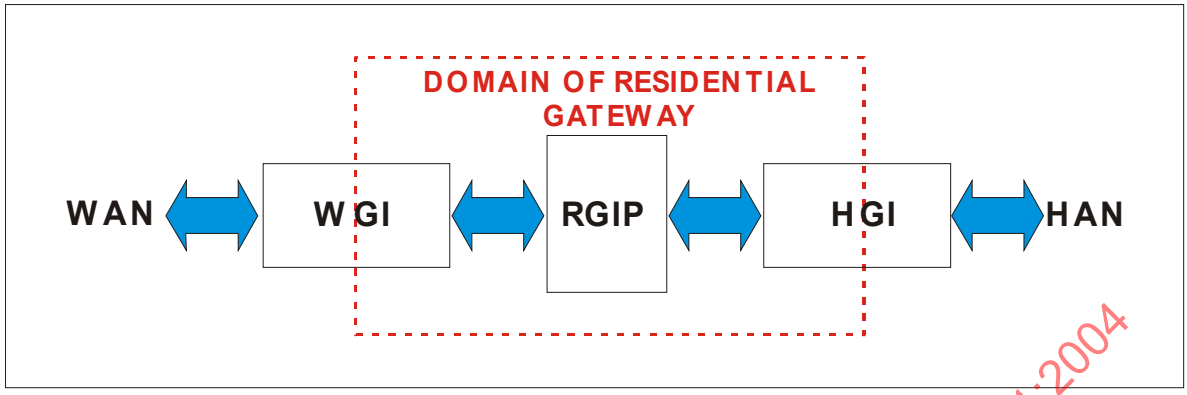
A.2.1 General

This standard applies to systems within the domain of the residential gateway and to the components of a Home Electronic System which are directly responsible for the functions and operation of the gateway. These components are:

- internal gateway architecture;
- network interfaces;
- requirements of distributed gateways.

These components are shown in the following subclauses.

A.2.2 Domain of the RG



Legend

WAN Wide Area Network

WGI WAN to Gateway Interface

RGIP Residential Gateway Internal Processes

HGI HAN to Gateway Interface

HAN Home Area Network

Figure A.1 – Domain of the residential gateway

This standard applies to the transmission of information between the external environment of the premises (the wide area) and the internal environment of the premises (the Home Area). In the external environment, information is delivered using wide area networks (WANs) such as telephone or TV networks. In the internal environment information is transmitted across home area networks (HANs) such as internal telephone connections or the home electronic system. The residential gateway is concerned with ensuring that information can be transmitted between networks in a secure, safe and transparent manner.

A conforming residential gateway may, if necessary, convert information into data, entertainment services or voice transmissions between the protocols, addresses and data structures of a WAN to those of a HAN and vice versa. Where there is more than one possible WAN or HAN to be considered, the data traffic passing through the gateway may be normalised. This applies equally to an RG where a number of Networks are interfaced within a single (integral) device or where flexibility in the form of a modular architecture is to be offered.

A.2.3 Basic residential gateway architecture

A.2.3.1 General

There are two basic categories of residential gateway architectures: the unit and the modular architecture.

Both architectures comprise the same basic three component parts, i.e. WGI, RGIP, and HGI, as shown as in Figure A.1.

A.2.3.2 Unit architecture

The unit architecture is based upon fixed interfaces between WAN and HAN, as shown in Figure A.2.

This architecture has no internal RGIP interfaces and has direct protocol conversion features.

Unit architecture is therefore more cost efficient than modular architecture. A unit architecture design specification results from selecting WAN and HAN, and usually has one WAN interface and one HAN interface.

The unit architecture is called a black box approach.

Unit architecture is found in a satellite antenna booster, DSU for ISDN, ADSL splitter, etc.

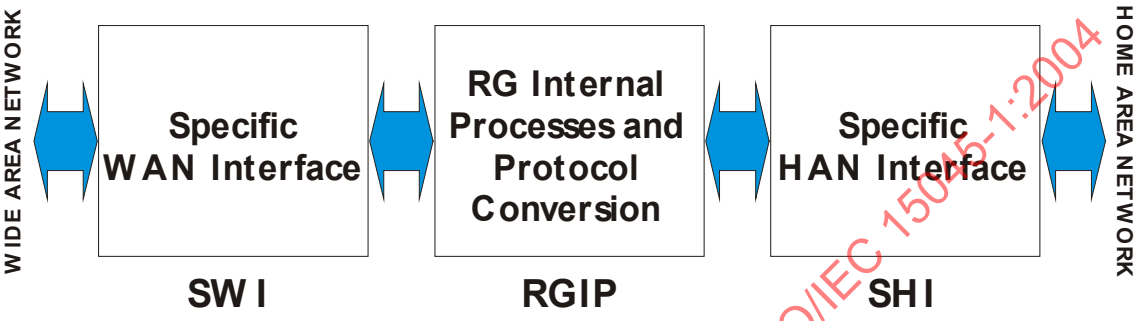


Figure A.2 – Unit architecture

A.2.3.3 Modular architecture

Modular architectures have high flexibility to adapt to user requirements by combination of one WAN interface and one HAN interface. They are also highly flexible when new WAN or HAN interfaces have to be added, as shown in Figure A.3.

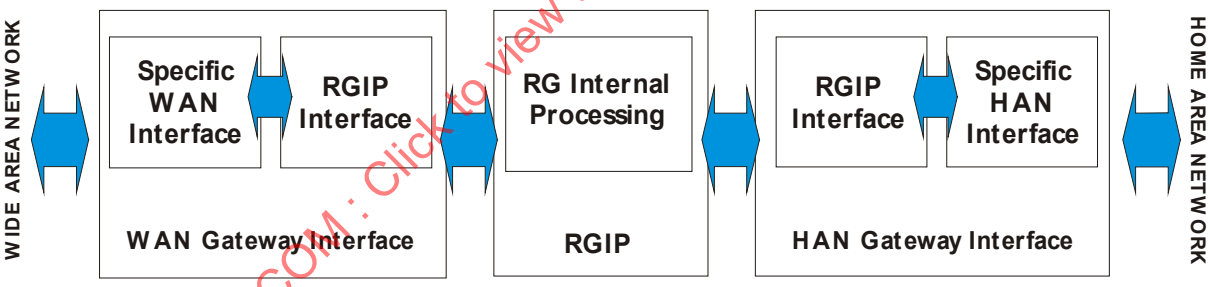


Figure A.3 – Modular architecture

NOTE RG internal processing requires high performance for multiple information processing.

A.2.4 Interfaces and processes

Conceptually an RG consists of three parts.

- A part which interfaces to a WAN communication system (shown as WGI in Figure A.1).
- A part which interfaces to a HAN communication network (shown as HGI in Figure A.1).
- An internal process (shown as RGIP in Figure A.1).

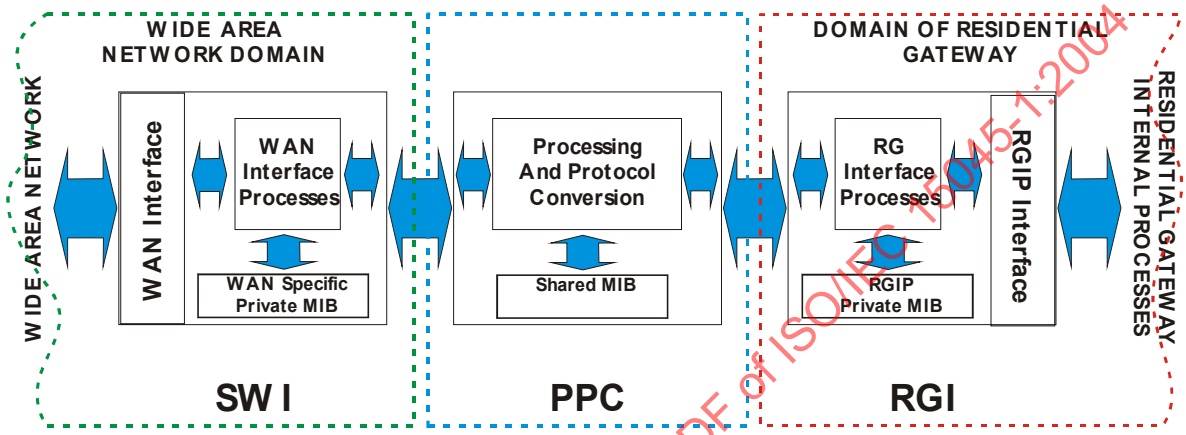
Each of these parts may be considered in modular terms as being realised in either hardware, firmware or software and as being constructed in an integrated or modular form. This document makes no distinction between these forms in compliance. However, where particular internal software or physical interfaces exist, they should be defined.

Both the WGI and the HGI lie partly within the domain of the RG. This is because the part that interfaces to a WAN or a HAN is defined in terms of that WAN or HAN and should conform to the standards and specifications of that WAN or HAN. The following subclauses referring to the constituents of an RG are presented to clarify typical functions of these modules and do not imply a design requirement.

A.2.5 Details of component parts

A.2.5.1 WGI

A.2.5.1.1 General



Legend

SWI Specific WAN Interface

RGI Residential Gateway Interface

PPC Processing and Protocol Conversion

RGIP Residential Gateway Internal Processes.

Figure A.4 – WAN Gateway gateway interface

The WAN gateway interface (WGI) may consist of the following parts:

A.2.5.1.2 SWI

A specific WAN interface (SWI) that conforms to the standards and requirements for connection to that wide area network. This part of the WGI presents the network with a WAN interface (WI) or network termination that conforms to the standards of that Network. The information that is WAN specific may be stored in a WAN specific private management information base (MIB).

A.2.5.1.3 PPC

A processing and protocol conversion (PPC) element of the WGI ensures that signals and data from the RG are converted to the correct format for transmission to systems in the wide area over the communication channel that the SWI has opened and vice versa. The PPC requires information about the address(es) of the data it is handling, the addresses and associated characteristics in the wide area and how these relate to objects in the HAN and associated addresses. This information may be stored in a shared MIB.

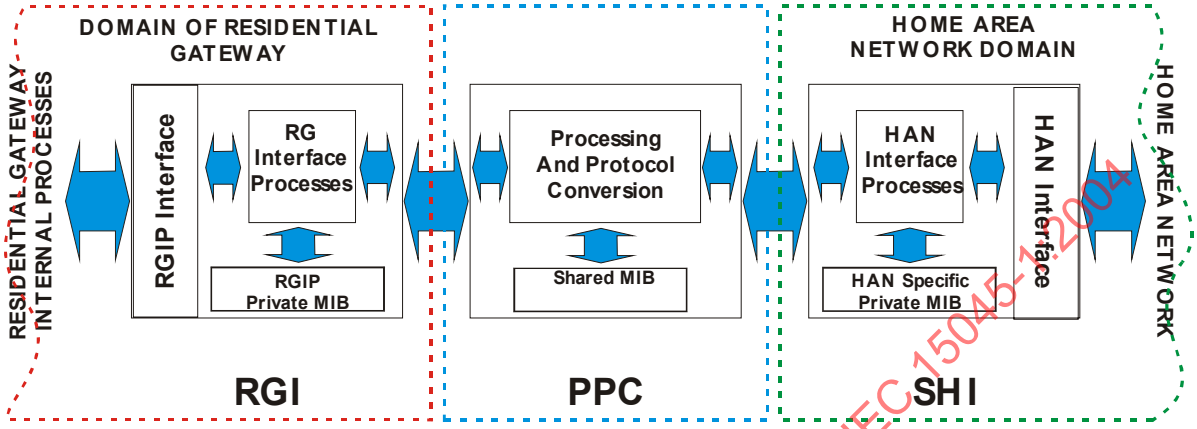
A.2.5.1.4 RGI

An RG interface (RGI) is the common interface to all modules of the RG. It ensures that all signals between the WGI and the RG are presented to the RGIP interface (RI) in the correct manner. It also needs to know which other modules are attached to the RG and which signals

should be routed to and from these other modules via the RG. This information may be stored in a private RG specific MIB.

A.2.5.2 HGI

A.2.5.2.1 General



Legend

SWI Specific WAN Interface

RGI Residential Gateway Interface

PPC Processing and Protocol Conversion

RGIP Residential Gateway Internal Processes

Figure A.5 – HAN Gateway gateway interface

The HAN gateway interface (HGI) may consist of the following parts:

A.2.5.2.2 SHI

A specific HAN interface (SHI) that conforms to the standards and requirements for connection to the home area network. This part of the HGI presents the network with a HAN interface (HI) or network termination that conforms to the standards of the network. The HAN-specific information may be stored in a HAN-specific private MIB.

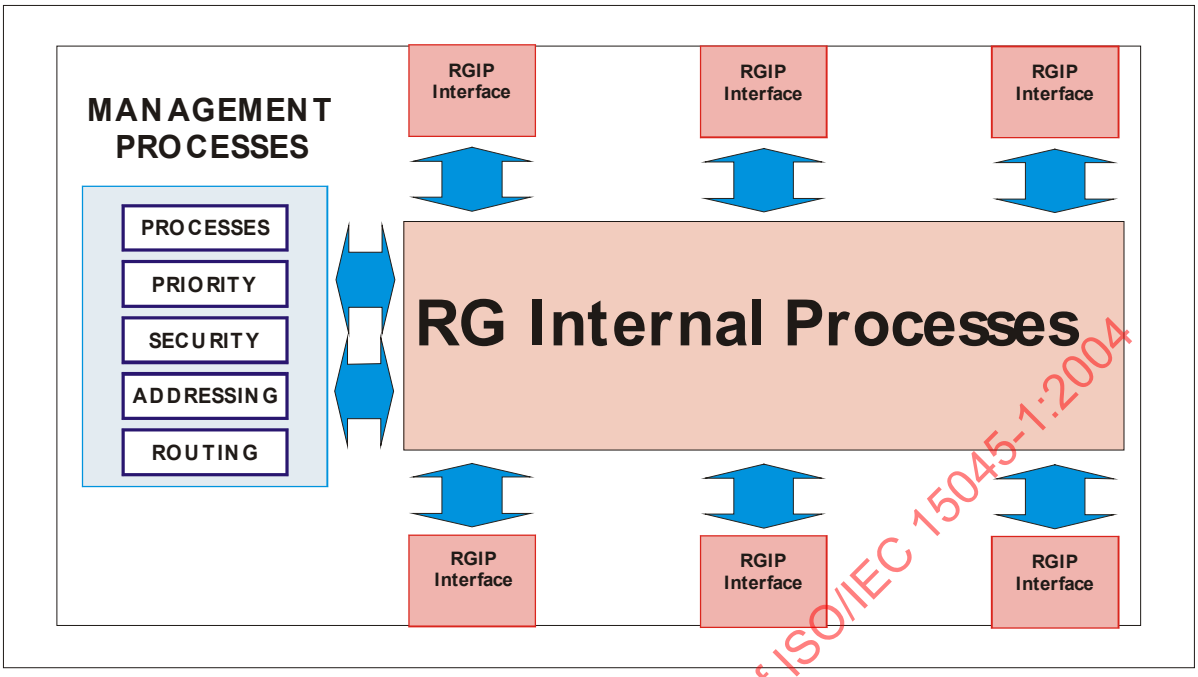
A.2.5.2.3 PPC

A processing and protocol conversion (PPC) element of the HGI ensures that signals and data from the RG are converted to the correct format for transmission to systems in the wide area over the communication channel that the SHI has opened and vice versa. The PPC will require information about the address(es) of the data it is handling, the addresses and associated characteristics in the home area and how these relate to objects in the WAN and associated addresses. This information may be stored in a shared MIB

A.2.5.2.4 RGI

AN RG interface (RGI) is common to all modules that interface to an RG. It ensures that all signals between the HGI and the RG are presented to the RGIP interface (RI) in the correct manner. It also needs to know which other modules are attached to the RG and which signals should be routed to and from these other modules via the RG. This information may be stored in a private RG specific MIB.

A.2.5.3 RG internal processes



NOTE This figure is entirely functional and does not imply an RG with plug-in modules, but simply that an RG may interface to more than one WAN or HAN.

Figure A.6 – RG internal processes and interfaces

RG internal processes may conform to any standard or open (published but still proprietary) specification. The RG internal processes may be realised in software, firmware or in a plug-in modular configuration. The interfaces to the PGIP may be realised in software or firmware and may or may not be a physical plug/socket arrangement.

For any RG internal interface where plug-in modules interface to it, they should conform to the standard or open specification used. An RG that does not fully reveal the specification for plug-in modules (where these are used) does not fully conform to this standard and becomes the equivalent of an integrally realised RG.

The internal architecture of the RG consists of the following:

- common interfaces to the RG internal process;
- a standard set of functions for the operation of the RG;
- a standard set of calls (commands, addressing, etc,) for invoking the functions;
- a mechanism for routing data between WGI and HGI modules (and optionally between HGI modules);
- management processes to control the activity of the RG and of modules attached to it;
- security mechanisms to prevent unauthorised access or egress of data to or from the premises and to implement other security functions;
- application-specific processes for services such as
  - energy control,
  - AMR,
  - time and date services,
  - remote management of RG (and HAN).

A.2.6 Structural implementations of the RG

A.2.6.1 General

The RG may be realised in a variety of implementations, ranging from a 1:1 integral box implementation to a many WAN-to-many HAN modular realisation and may be realised in a distributed configuration. It may interface to any local area network such as Ethernet, IEEE 1394 or any of several standard or proprietary home electronic systems (buses).

It is intended that the RG standard be modular and that elements such as the WGI and HGI can be merged (as in the case of a simple WAN-to-HAN gateway) and that elements can be selected as the complexity of the gateway increases.

Wherever elements are explicitly interfaced, they and associated interfaces should conform to the protocols, addressing and data formats specified by their relevant standards or be fully documented as stated in 5.1. Some examples of gateway implementations are given in Figure A.7.

A.2.6.2 Simple gateway

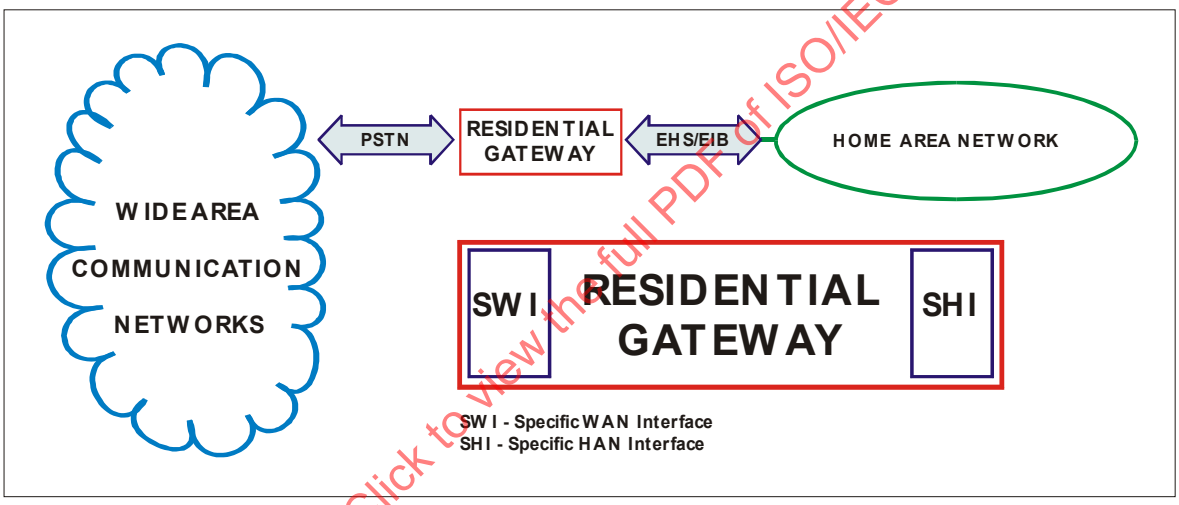


Figure A.7 – Simple 1:1 implementation of RG

In the example where the gateway is a 1:1, WAN:HAN configuration residential gateway, only the elements for security and interoperability (for which future standards are planned) need to be compliant. This configuration may include additional connection and interfacing specifications that are outside the domain of this residential gateway standard. This type of gateway may use the paradigm of the RG and have internal interfaces to the RG that conform to the requirements of this standard. The 1:1 configuration is shown in Figure A.7.

A.2.6.3 Complex integral gateway

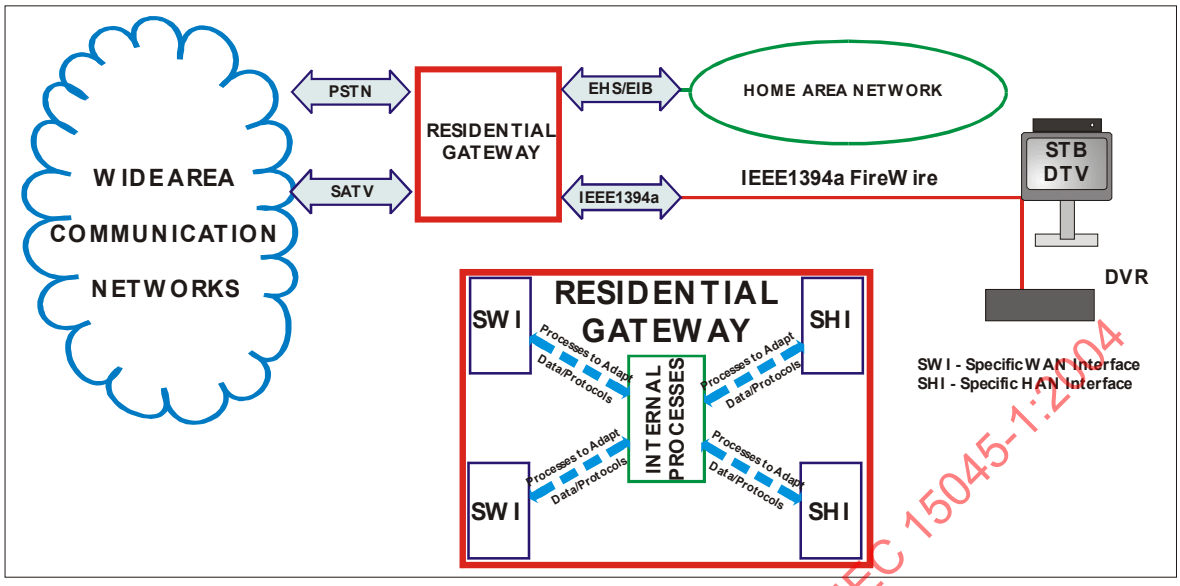


Figure A.8 – Complex integral RG implementation

In the complex integral implementation of the gateway one or more WANs or one or more HANs interface to the residential gateway. The Gateway is a one box device but it may have three or more interfaces. To conform to this standard residential gateway, this configuration should comply with the requirements for interoperability and security and should utilise some form of RGIP. Also, this configuration should implement processes to adapt the data and addresses of the WANs to which it interfaces for presentation to the RG and similarly for the HANs to which it interfaces. Instances of this residential gateway configuration may be set top boxes delivering satellite DTV or cable TV with interactive applications such as video on demand, DSL adapters and cable modems and certain proprietary gateways. This configuration is shown in Figure A.8.

NOTE It is anticipated that there will be overlap between the complex modular configuration and the complex integral configuration where designers wish to utilise particular WANs but interface to multiple HANs.

A.2.6.4 Complex modular gateway

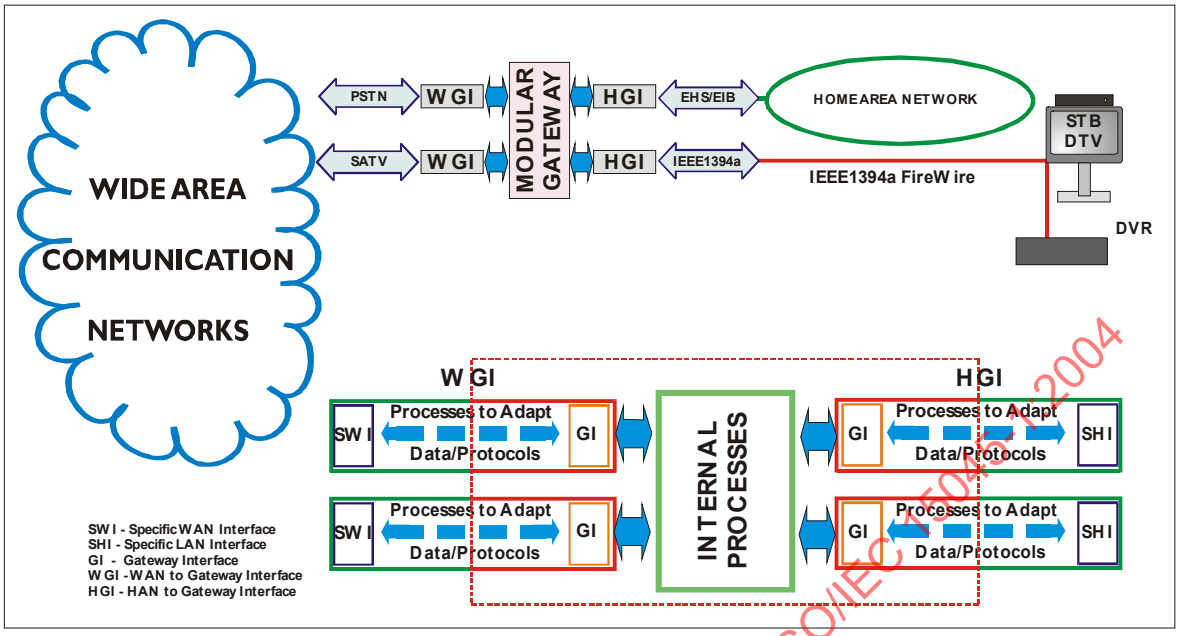


Figure A.9 – Complex modular RG implementation

The complex modular implementation of the residential gateway enables flexibility in the functions of the gateway and the services it can offer. In this configuration plug-in interface modules sit between the Network and the RG and interface to the RGIP. In this implementation, the gateway and modules should comply with the requirements for Security and Interoperability specified in clauses 5, 6 and 7. Additionally, the modules should be compliant with the physical and logical RG interface(s) referenced in this standard and present their data flows in a correct format at both the network interfaces and to the RG interface. Each Module should carry out processes to adapt Data and Protocols as described in 5.4 and interface with the RG as specified in 5.1. This configuration is shown Figure A.9.

A.2.6.5 Distributed RGs

More than one residential gateway unit may be installed in premises. This Standard requires that the behaviour of residential gateway units compliant with this standard should be the equivalent of a single complex gateway. Also, a conforming RG should be capable of complying with the requirements of Interoperability and Security as specified in clauses 5, 6 and 7. Gateways in a distributed configuration should function as if each element were contiguous with routing and addressing between HANs and WANs equivalent to a single residential gateway. Some potential configurations of distributed gateways are shown in Figure A.10, Figure A.11 and Figure A.12.

There are three generic ways in which the RGII of residential gateways may be linked to form a distributed gateway.

- The Link may be implemented on the HAN side and can use the home network or Higher Speed Networks such as ISO 8802-3 or IEEE 1394.
- The Link may be implemented directly from the RGIP of one RG to the RGIP of a second RG. In this case, the RGIP should be the same for both RGs and be an extension of the bus (or other architecture) type used.
- The Link may be implemented over the WAN and may be a high speed IP link between two "always on" devices - for instance a cable modem for one RG and a xDSL modem for the other.

NOTE There may be two or more distributed gateways in any premises.

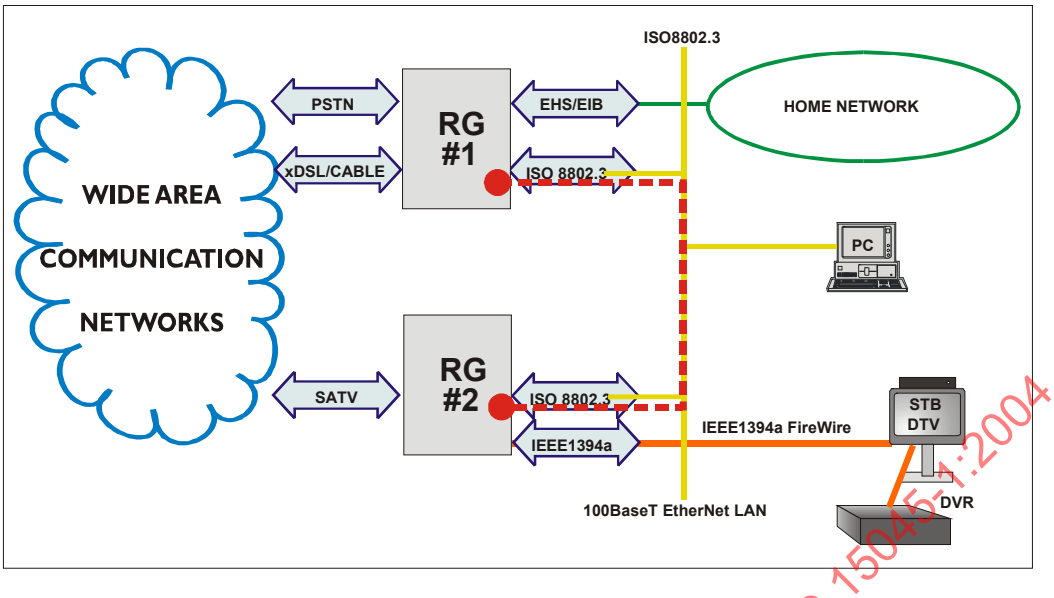


Figure A.10 – Distributed RGs linked via HAN

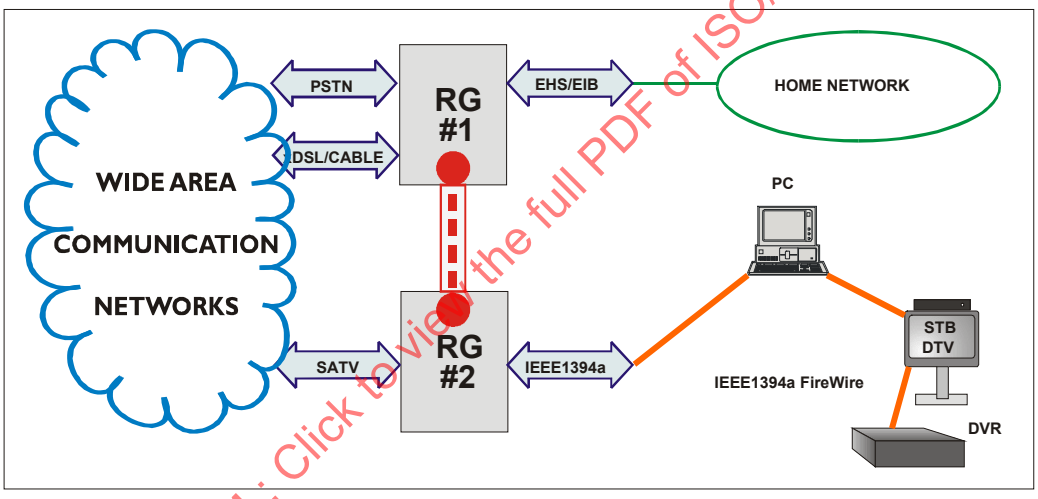


Figure A.11 – Distributed RGs directly linked

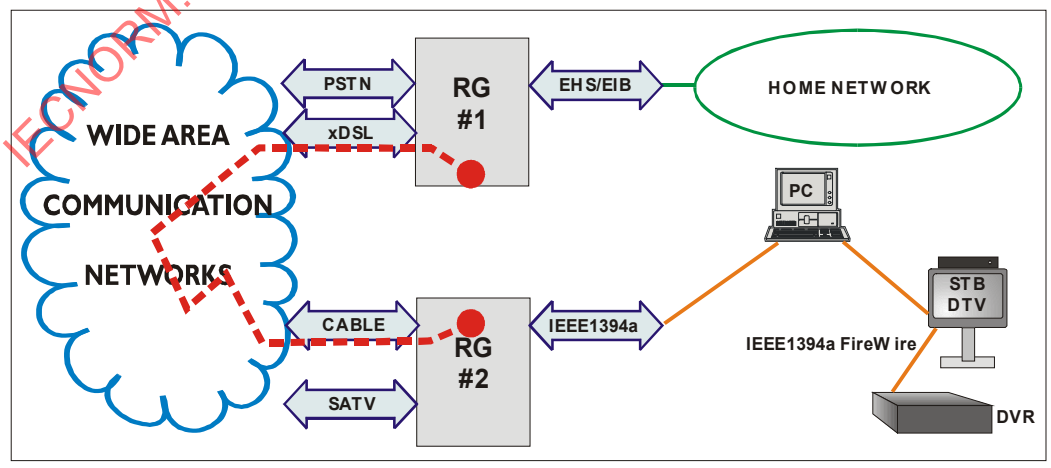


Figure A.12 – Distributed RGs linked via WAN

Annex B
(informative)

Functional safety considerations[7]

B.1 Introduction

B.1.1 General

The overriding concern of any network is the safe operation of all elements and systems within the network. Also of concern is the assurance that whatever configuration these elements may take, configurations, operations or management of the network must not result in an unsafe condition.

Where multiple or dissimilar networks are required to interoperate, the potential for unsafe operation is increased.

Some examples of potential hazards include (but are not exhaustive) the following.

B.1.2 Commands to potentially hazardous objects

When configuring home networks, there must be systems to prevent the unattended initiation/operation of potentially hazardous objects (a gateway must be able to block certain commands to objects identified by their manufacturer).

The remote or automatic switching on of radiant heat sources (open fires or cooker hob burners) is an example of such a hazardous object. A system must not automatically control the potentially hazardous object, except by a switch or manually operated controller placed within reach or sight of the object.

If the gateway has a function to block certain commands to potentially hazardous objects, then this function must be documented.

B.1.3 Commands to relocatable programmable objects

Some objects such as intelligent power plugs do not explicitly carry information about the load they switch. Such objects may not be initiated/controlled automatically by the home network or by commands from external systems unless the use of the object is explicitly programmed into it (with automatic reset to 'unknown purpose', if disconnected). This limitation is specified because such devices may be used for a range of purposes. Unless the system has reliable information about the current purpose of the device, automatic operation may have unreliable or dangerous outcomes.

The RG must have a function to block commands to objects where the device under the control of the object is not defined.

B.1.4 Commands to automatic objects

B.1.4.1 General

Many devices and equipment in the home carry out automatic functions. A simple example is an oven that is switched on at a pre-set time. In many cases, external or system control of

7 A standard is under development to address security requirements for HES; when it is published, the current annex will be updated or replaced as relevant.

these objects can result in an unintended outcome. For instance when the operation is carried out at some future time, either by external command or automatically, the contents of the oven may no longer be those intended. Where such an automatic control is possible, it must only be available for a pre-set time period from when the equipment was set up for automatic operation, and must operate only if the automatic control has not been changed.

B.1.4.2 Notification on blocking

Where commands from external devices are blocked in order to prevent potentially hazardous operation, it is necessary that information be provided to the source of the command. This is to prevent the source of the command from continuing to send this command. Such a notification will inform the source about the failure of the command, and alert it to the risk of issuing commands to other objects on the assumption that the blocked command has been successfully executed.

B.1.5 Command translation

There are many potential instances where commands (or variables) sent by one home network will have different meanings and/or parameters for a similar command in another network. This is likely to be the case for switches and dimmers where one system will use a feedback loop (less, compare, less, compare, less, compare, less, compare, less, OK) and another will set a level (set light output at 70 %). While not necessarily a safety issue for lighting, when energy management and environment control are concerned some actions could be counter intuitive and potentially hazardous.

Where such situations exist or potentially exist, explicit rules must be implemented for command translation to prevent hazard.

B.1.6 Linked changed state

If a changed state on one network is linked to a changed state on another, the converse operation may result in a breach of safety or security rules. For example, if unlocking the front door turns on a courtesy light, leaving the courtesy light on must not leave the front door unlocked. Some linked change-state situations may result in hazardous interactions.

Where these situations exist or potentially exist, explicit rules must be implemented to prevent hazard or security breaches.

B.1.7 Addressing

Few home networks share the same addressing scheme. Thus bridges and gateways that provide inter-operation must also include accurate address translation. Where the address space is different, either smaller or larger between the sending network and the target network, there is the possibility that commands intended for a particular object will be misrouted. If there is any doubt whatsoever that due to addressing mismatch data could be delivered to the wrong address and result in an insecure or hazardous operation, then the device or system must prevent the data from being transmitted.

B.1.8 Broadcast messages, variables and commands

In general, interoperating devices and systems between dissimilar networks must ensure that any message, broadcast message, command, broadcast command, variable, broadcast variable value, or object parameter passed between dissimilar networks results in safe operation in the other network(s). If there is any doubt whatsoever that passing such data could result in an insecure or hazardous operation, the device or system must prevent the data from being transmitted.

Annex C
(informative)

Specific privacy and security of residential gateways[8]

C.1 Introduction

There are many security threats to a home network that may originate from the WAN or from within the HAN. These attacks may compromise the integrity of the home network or expose private messages between HAN devices or between the WAN and HAN. The residential gateway through which messages and information pass should incorporate both defensive and proactive entities to ensure the security of the home network and that messages, information and media content directed to and from trustworthy service and application providers retains its privacy and integrity.

C.2 Threats

C.2.1 General

RGs will be designed to carry out many roles in transferring data to and from the home and the security aspects will differ with respect to the types of data transferred; however, all of these can be considered as threats to the integrity of a Home Electronic System.

C.2.2 Masquerade and replay

Perhaps the most obvious threat to the home is unauthorised access to devices or databases on the home network. A *masquerade* takes place when an impostor pretends to be a legitimate user, such as the homeowner. The impostor could also pretend to be a service provider that has contracted with the homeowner.

A masquerade may be effected by defeating the authentication mechanism, for example, guessing a password or stealing a token. Another way an impostor may trick the home network into thinking it is an authorised 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 could be *replayed* later to achieve the same result.

C.2.3 Interception: eavesdropping and modification

An *interception* occurs when an unauthorised party gains access to a message passing between the home network and an external user. The intruder may be an automated system that is programmed to search for vulnerable messages, or it may be a person who has wiretapped or otherwise violated the integrity of the communications channel.

The interception may be passive or active; a passive interception amounts to *eavesdropping* – in effect, reading someone else's traffic. An active interception may 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 may also be used to thwart modification attacks.

---

8 A standard is under development to address security requirements for HES; when it is published, the current annex will be updated or replaced as relevant.