

PD CLC/TS 50560:2014



BSI Standards Publication

Interoperability framework requirement specification

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This Published Document is the UK implementation of CLC/TS 50560:2014.

The UK participation in its preparation was entrusted by Technical Committee IST/6, Data communications, to Panel IST/6/-/12, Home Electronic Systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 85910 6
ICS 35.240.99; 97.120

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2015.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CLC/TS 50560

October 2014

ICS 35.240.99; 97.120

Supersedes CWA 50560:2010

English Version

Interoperability framework requirement specification

Spécification d'exigences cadre d'interopérabilité

Rahmenspezifikation für Interoperabilitätsanforderungen
(IFRS)

This Technical Specification was approved by CENELEC on 2014-08-11.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Contents	1
Foreword	6
Introduction	7
1 Scope	9
2 Normative References	9
3 Terms, definitions and Abbreviations	10
3.1 Security Definitions	10
3.2 Process Definitions	12
3.3 Interoperability	14
3.4 Abbreviations	14
4 The Interoperability Framework	17
4.1 The Function Steps	17
4.1.1 General	17
4.1.2 Discovery	17
4.1.3 Configuration	17
4.1.4 Operation	17
4.1.5 Management	18
4.2 The Levels	18
5 Conformance clauses	19
5.1 Interoperability Conformance Requirements	19
5.1.1 General	19
5.1.2 Identifier	19
5.1.3 Object Description	19
5.1.4 Object Discovery	20
5.1.5 Object Configuration	20
5.1.6 Object Operation	20
5.1.7 Object Management	20
5.1.8 Object Access and Safety Requirements	20
5.2 Conformance sub-clauses	20
5.2.1 Object Identifier Description Requirements	20
5.2.2 Object Functional Description Requirements	21
5.2.3 Discovery Process Requirements	22
5.2.4 Configuration Process Requirements	23
5.2.5 Operation Requirements	23
5.2.6 Management Requirements	23
5.2.7 Object Security, Safety and Priority and Access Requirements	24
Annex A (informative) Steps of discovery, configuration, operation and management	25
A.1 Methodology	25
A.1.1 Objectives	25
A.1.2 Assumptions	25
A.2 Approach	26
A.3 The Function Steps	26
A.3.1 General	26
A.3.2 Discovery	26
A.3.3 Configuration	29



A.3.4	Operation	30
A.3.5	Management	30
A.4	The Levels	30
A.4.1	Level 0	30
A.4.2	Level 1	31
A.4.3	Level 2	32
A.4.4	Level 3	33
A.4.5	Level 4	34
A.4.6	Level 5	37
A.4.7	Level 6	38
A.4.8	Combinations of Different Levels in the Same Installation	40
A.5	Use Cases.....	41
A.5.1	Methodology.....	41
A.5.1.1	General.....	41
A.5.1.2	Describe use-case.....	41
A.5.2	Scenarios to Illustrate Interoperability Levels	42
A.5.2.1	General.....	42
A.5.2.2	Level 0	43
A.5.2.3	Level 1	43
A.5.2.4	Level 2	43
A.5.2.5	Level 3	44
A.5.2.6	Level 4	44
A.5.2.7	Level 5	44
A.5.2.8	Level 6	45
A.6	IFRS Methodology.....	45
A.6.1	General.....	45
A.6.2	Physical Layer, Pathways and Media (PHY)	45
A.6.3	Data Link Control (DLC)	46
A.6.4	Network Layer and Routing (NWK).....	47
A.6.5	Transport and Session (TRS)	48
A.6.6	Presentation and Application (APP).....	49
A.6.7	IFRS Issues – A Summary.....	49
A.6.8	Working Assumptions	50
A.6.9	Rationale for the Function Steps and Associated Processes.....	51
A.6.9.1	General.....	51
A.6.9.2	Architectural Issues.....	52
A.7	Security, Safety, Access and Priority Considerations	52
A.7.1	Introduction to Security Considerations	52
A.7.2	References and Standards	55
Annex B (normative)	Interoperability Implementation Conformance Statement	56
B.1	Scope.....	56
B.2	References.....	56
B.3	Definitions and abbreviations.....	56

B.3.1	Definitions	56
B.3.1.1	General Definitions	56
B.3.1.2	Security Definitions	60
B.3.1.3	Interaction Model Definitions	62
B.3.1.4	Process Definition	66
B.3.1.5	Interoperability	67
B.3.1.6	Other Definitions	68
B.4	Requirements for Conformance to this IICS	69
B.4.1	General	69
B.4.2	Object Identifier Description Requirements	69
B.4.3	Object Functional Description Requirements	69
B.4.3.1	General	69
B.4.3.2	Object Classification	69
B.4.3.3	Object Discovery Interface	70
B.4.3.4	Object Configuration Interface	70
B.4.3.5	Object Management Interface	70
B.4.3.6	Object Functional Interface	70
B.4.4	Discovery Requirements	70
B.4.4.1	General	70
B.4.4.2	Object Descriptions: Self and Objects to be Discovered	70
B.4.4.3	Communication Mode	71
B.4.4.4	Discovery Process	71
B.4.4.5	Discovery Scope	71
B.4.4.6	Security and Privacy	71
B.4.5	Configuration Requirements	71
B.4.5.1	Bindings	71
B.4.5.2	Communication Mode	71
B.4.5.3	Configuration Process	71
B.4.5.4	Security and Privacy	72
B.4.6	Operation Requirements	72
B.4.6.1	Application Operation	72
B.4.6.2	Security and Privacy	72
B.4.7	Management Requirements	72
B.4.7.1	Communication Mode	72
B.4.7.2	Management Process	72
B.4.7.3	Security and Privacy	73
B.5	Instructions for Completion of the IICS	73
B.5.1	General	73
B.5.2	Key to the Table Entries	73
B.6	Global Statement of IICS Conformance	74
B.7	Specific Statements of IICS Conformance	74
B.7.1	General	74
B.7.2	Object Catalogue	74

B.7.3	Operation Catalogue	75
B.7.4	Object and Operation Interoperability Catalogue	76
B.7.5	Upper Layer PICS (APP)	77
B.7.5.1	General	77
B.7.5.2	Additional Requirements for Gateways at APP Layer.....	77
B.7.6	Network Layer and Routing PICS (NWK)	78
B.7.6.1	General	78
B.7.6.2	Additional Requirements for Gateways at NWK Layer.....	79
B.7.7	Data Link Control and MAC PICS (DLC/MAC)	80
B.7.7.1	General	80
B.7.7.2	Additional Requirements for Gateways at DLC/MAC Layer	81
B.7.8	Media and PHY PICS (PHY).....	82
	Bibliography.....	83

Foreword

This document (CLC/TS 50560:2014) has been prepared by CLC/TC 205, "Home and Building Electronic Systems (HBES)".

This document supersedes CWA 50560:2010.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Introduction

The objective of this Technical Specification, the Interoperability Framework Requirements Specification (IFRS), is to specify a methodology that will give consumers the confidence to buy products from different companies both now and in the future, knowing that they will operate together.

Achieving this requires several phases of standardisation to ensure integration from the physical connectors to the way systems function. There are three phases of integration:

- **Co-existence** - where different systems can operate in the same environment without hindering each other's' operation;
- **Interworking** - where different technologies are connected together to transfer data end-to-end. It is primarily a technical solution encompassing connectors, protocols, bridges, etc. ;
- **Interoperability** - where different application functions are able use the shared information in a consistent way. This requires interworking as a building block as well as coexistence, and adds business rules, processes, and security provisions that enable applications to be joined together.

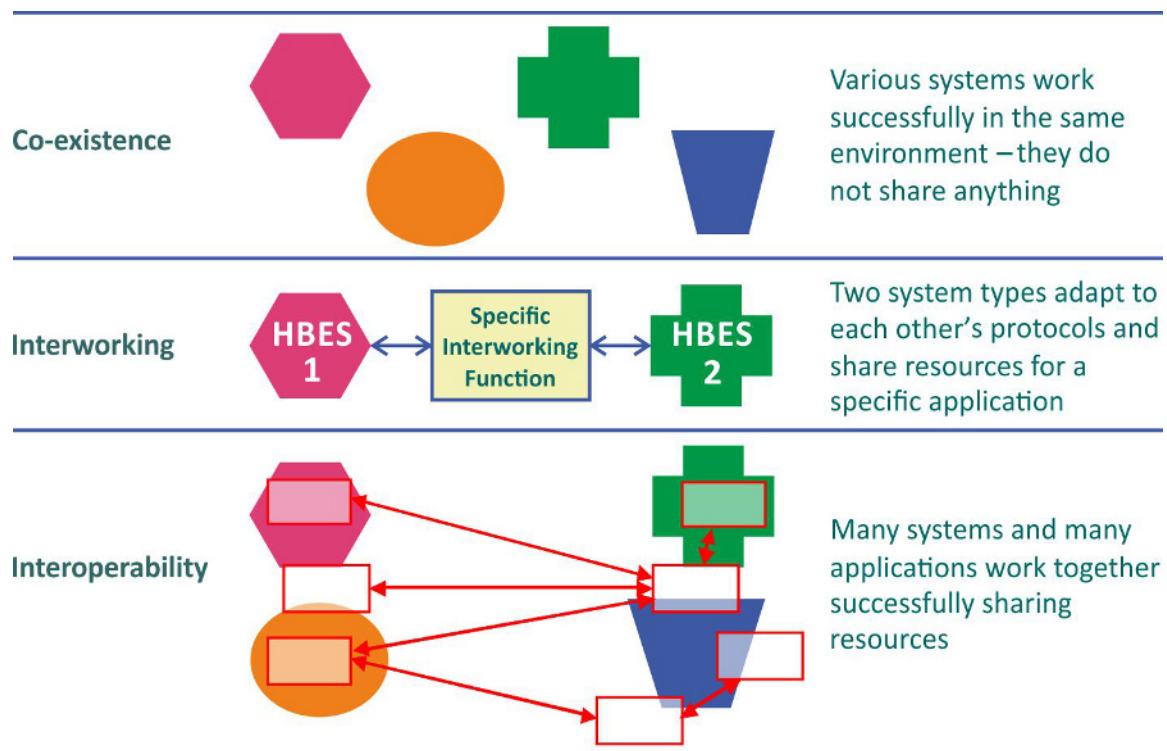


Figure 1

The Interoperability Framework Requirements Specification, IFRS, addresses the third of these terms. It provides a common set of rules to enable products that use different standards to interoperate when they are present in an installation.

This TS covers four high level functional activities: discovery, configuration, operations and system management. It puts forward a common set of requirements that if complied with, and if coexistence and interworking are assured, will enable interoperability. It does not address co-existence or interworking on the basis that this is achieved by technology standards.

Interoperability is provided by alliances of commercial businesses (and there are several such alliances), but to ensure interoperability customers are limited to purchasing products from members of the alliance. This TS acknowledges the work and the value of such alliances but specifically addresses the ability for customers to purchase products and services from competing alliances and still achieve interoperability. In doing so it expects to increase the market for those alliances that conform to the IFRS as customers will purchase their products with greater freedom of choice and confidence that they will work.

1 Scope

This Technical Specification contains a specification of an Interoperability Requirements Framework, specifying seven levels of interoperability, based on four groups of interoperability steps specified by five types of interaction, plus a methodology based on conformance clauses for satisfying requirements related to the claimed level of interoperability of devices installed in a Home and Building Electronic System (HBES, HES).

It is applicable to installations of a single type of HBES, or that interconnect two or more dissimilar HBESs. Within a HBES of a single type any of its capabilities for service, applications and connectivity topology can be used. Interconnection technologies used to interconnect dissimilar HBES are similarly unconstrained.

For applicable installations, the scope of its provisions applies to: the connection of devices to the various communications services to enable them to communicate end-to-end across internetworked media; the processes of discovery by which devices find out about each other and configuration to associate them with each other; and the generic aspects of application operation; and management.

This Technical Specification is not applicable to the interoperability required between devices to implement specific applications, such as heating or lighting control, energy management, or entertainment. The interoperability requirements defined in this Technical Specification are necessary for such application interoperability but not sufficient. This Technical Specification does not define how measurements are made; nor the algorithms that receive, process and respond to them; nor the interaction between users, service providers, and the HBES application(s). This is the responsibility of experts and organisations that specialise in particular application domains.

2 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ETSI/TS 101 761-2, *Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) Layer; Part 2: Radio Link Control (RLC) sublayer*

ETSI/TS 300 406:1995, *Methods for testing and Specification (MTS); Protocol and profile, conformance testing specifications; Standardization methodology*.

ISO/IEC 9646-1, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 1: General concepts*.

ISO/IEC 9646-7, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements*

ITU X.800, *Data communication networks: Open systems interconnection (OSI); Security structure and applications - Security architecture for open systems interconnection for CITT applications*

3 Terms, definitions and Abbreviations

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

3.1 Security Definitions

3.1.1

access control

the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

[SOURCE: ITU X.800]

Note 1 to entry : Access Control becomes important when more than one entity or system is required to access a resource. In such cases and especially where safety is an issue, there may need to be levels of Access Rights depending on the priority of the accessing application and the nature of the resource. Permission and ability to use an object for a specified purpose – requesting information from it, changing values of variables in it or modifying its state.

Note 2 to entry: Where more than one service or Application requires access to an Object for one or more specific purposes, then levels of access shall be defined, including the definition of the primary owner of the Access Rights (possibly the owner of the Object)

EXAMPLE: Read access to a shared variable; permission to turn on, or off, i.e. execute certain operations.

3.1.2

access rights

permission and ability to use an Object for a specified purpose – requesting information from it, changing values of variables in it or modifying its state

Note 1 to entry: Where more than one service or application requires access to an Object for one or more specific purposes, then levels of access shall be defined, including the definition of the primary owner of the access rights (possibly the owner of the Object)

EXAMPLE: read access to a shared variable; permission to turn on, or off, i.e. execute certain operations.

3.1.3

authentication

the validation of a claimed identity

Note 1 to entry: The validation of a claimed identity of a user can be made by verifying some secret knowledge, key, or property associated with that user, e.g. a password, a SSL key, a PGP private key, or a hand-written signature.

3.1.4

authorisation

the decision to permit a user to make none (deny access), one or more types (permit access) of operations on an object

Note 1 to entry: The permission is made by comparing the validated user's Access Rights with the user's requested action(s) on an Object, for example to read and to modify some content of an Object.

3.1.5

confidentiality

the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ITU X.800]

3.1.6**denial of service**

the prevention of authorized access to resources or the delaying of time-critical operations (by unwanted or malicious messages that render network resources non-functional)

[SOURCE: ITU X.800]

3.1.7**eavesdropping**

attack where an unauthorised user is listening in on transmissions to which they should not have access. Information remains intact, but its privacy is compromised

EXAMPLE: intercepting credit card numbers or classified information – the interception of any communications information may render the eavesdropper useful information. See Privacy

3.1.8**encryption**

the process of disguising data to hide its content. As used in a network security context, Encryption is usually accomplished by putting the data through any of several established mathematical algorithms developed specifically for this purpose

3.1.9**information security**

provides confidentiality, integrity, availability and accountability of data

EXAMPLE: key for Encryption or detection of tampering, access permissions for reading and writing objects, audit trails for modifications to data.

3.1.10**integrity**

the property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ITU X.800]

3.1.11**non-repudiation**

proves communications took place so that the sender (or receiver) cannot refute sending (or receiving) information

EXAMPLE: a digital signature may provide proof of non-repudiation as it links the sender with the message.

3.1.12**physical security**

rules and systems put in place to safeguard the physical access to a premise or devices from physical interference

EXAMPLE: a self-opening and closing door for wheelchair access, compliant with standards for such devices.

3.1.13**priority**

relative ordering given to a process or action with respect to other processes

EXAMPLE: Life critical processes may have a higher priority than other user processes.

3.1.14**privacy**

the protection of information that might be derived from the observation of network activities (see Eavesdropping)

[SOURCE: ITU X.805]

3.1.15**replay attack**

the interception and recording of messages for sending out at a later time so that the receiver unknowingly thinks the bogus traffic is legitimate

3.1.16**repudiation**

denial by one of the entities involved in a communication of having participated in all or part of the communication

[SOURCE: ITU X.800]

3.1.17**safety**

the state of being certain that adverse effects will not be caused by some agent under defined conditions

Note 1 to entry: As an actuator becomes progressively more remote from a device or action, the scope for actions that may result in unsafe conditions increases. This problem is accentuated when there are two or more actuators acting on that device or action.

3.1.18**security**

rules and policies stated by owners that control the use of their property by other owners

EXAMPLE: people allocated car-parking spaces are allowed to open the garage doors. People with no allocation may not open the doors.

3.1.19**security requirements****the purpose, objectives and success criteria applied to an Application or service**

Note 1 to entry: This Technical Specification specifies requirements for Security in relation to Levels of Interoperability that cover both Physical Security and Information Security and these shall be combined with Safety and other considerations such as the permission and Priority of access, Discovery, Configuration and Management.

3.1.20**validation**

the act of examining information provided by a person (or a system) to ascertain what rights, privileges, or permissions they may (or may not) have to perform some action

3.1.21**verification**

in cryptography, the act of testing the authenticity of a digital signature by performing special mathematical operations on data provided by a sender, to see if it matches an expected result. If the information provided by the sender yields the expected result, the signature is valid, because calculating the proper answer requires secret data known only by the sender. Verification proves that the information was actually sent by the signer and that the message has not been subsequently altered by anyone else

3.2 Process Definitions**3.2.1****object**

an embodiment of information as data structures and operations upon them realised in electronic hardware, software, or embedded in a stream of data, that can be referenced and with which interaction can be achieved by processes, other Objects and users

3.2.2

application

a collection of functions that have measurable effects on the physical world and are used by people to achieve objectives consistent with the specified capabilities of the Application

Note 1 to entry: Also used to refer to use of a technology, system, or product. An Application may consist of a number of elements or entities working together to provide a service or product. It may utilise specific elements in a system or technology in delivering the application. Alternatively, an application may be a program that carries out a particular service within a computer, processor or (home) system.

EXAMPLE: Devices in the Smart House collaborate to execute an energy management Application that the owner uses to reduce electricity consumption. No additional service is required.

3.2.3

configuration

the set of status parameters for an Object or device

EXAMPLE: a device is connected to the application using a certain network address, its Objects are registered with Objects in other devices.

3.2.4

configuration process

configuration of parameters of an object or objects or applications. This may be carried out by means of a Configuration tool and other actions that may be automatic and driven by other services and/or applications

EXAMPLE: the association of objects in a device with those in other devices.

3.2.5

discovery

enabling users, Applications, Objects, and devices participating in systems to discover new units and to recognise what they are

Note 1 entry: Objects may present or publish their parameters or respond to a broadcast for information about specific object types).

EXAMPLE: UPnP.

3.2.6

discovery process

the process of execution of discovery activities

3.2.7

middleware

middleware is a generic term for functions that make a communications infrastructure that is part of a distributed system usable by applications

Note 1 to entry: Middleware may be used for the purposes of Interoperability to translate the data presented by an Object under one specific home system specification to the requirements of another.

EXAMPLE 1: the IP routing functionality in a home gateway to ISP services provides middleware to connect with the ISP, register local devices for access to Internet services and route IP packets between local processes and external ones.

EXAMPLE 2: a smart meter provides middleware that authenticates application objects downloaded into it before allowing them to use its communications services to implement specific application functions.

3.2.8

operations

application services requested between Objects in the system that collectively implement its function

3.2.9**system management**

application services requested between objects in the system that are not related to the Applications that it executes

Note 1 to entry: Examples: collection of statistics, diagnostic troubleshooting, firmware and software upgrade installation.

3.3 Interoperability**3.3.1****coexistence**

objects and Applications exist in the same environment and they do not conflict with one another

Note 1 to entry: their functions may, or may not, be related to, or dependent on, one another.

EXAMPLE: a security service monitors events in a home via the smart electricity meter communicating via a Zigbee link to the home security gateway. Due to excessive traffic between other Zigbee connected devices, such as the Consumer Display Unit, the meter is temporarily too busy to relay security events and there is a delay in reporting a break-in. The systems do not coexist.

3.3.2**interoperability**

interoperability is the ability of two or more networks, systems, devices, Applications or components to exchange information between them and use the information so exchanged

Note 1 to entry: this definition is due to IEEE/CENELEC.

EXAMPLE: see elsewhere in this Technical Specification.

3.3.3**interworking**

the capability to exchange information between services and devices of dissimilar capability and/or provenance such that Interoperability is achieved

EXAMPLE: a home gateway to ISP services provides interworking between Ethernet and Wifi media in the home and the ADSL media outside the home to support routing of IP packets so that the applications objects in the home are interoperable via IP protocol with application objects elsewhere.

3.3.4**open standard**

in the context of this Technical Specification, a document available to all, approved by the processes of designated international standards bodies defining architecture, function, protocols and conformance criteria of aspects of communications systems

3.4 Abbreviations

Acronym	Explanation
AC	Alternating Current
ACID	Atomic, consistent, isolated, durable – properties of interactions involving multiple distributed objects sharing resources concurrently.
ADSL	Asymmetric DSL
API	Application Programming Interface
APP	Application, Presentation, Transport and Session layers, specific to this Technical Specification.
AS	Autonomous system

ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
CDU	Consumer Display Unit
CENELEC	Comité Européen de Normalisation Electrotechnique
CWA	CENELEC Workshop Agreement
DLC	Data Link Control
DLNA	Digital Living Network Alliance
DOS	Denial of Service
DSL	Digital Subscriber Link
DVB	Digital Video Broadcast
ETSI	European Telecommunications Standards Institute
FCD	Final Committee Draft
FDL	Formal Description Language
GPRS	General Packet Radio Service
GSM	Groupe Special Mobile, Global System for Mobiles
HAN	Home Area Network
HBES	Home and Building Electronic System
HDMI	High-Definition Multimedia Interface
HES	Home Electronic Systems
HSPA	High Speed Packet Access
HTTPS	HyperText Transfer Protocol - Secure
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFRS	Interoperability Framework Requirements Specification
IICS	Interoperability Implementation Conformance Statement
IP	Internet Protocol
IR	Infra-Red
IS	International Standard
ISO	International Standards Organisation
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunications
LAN	Local Area Network
MAC	Medium Access Control
MAC	Message Authentication Code
Mbps	Megabit per second
NWK	Network (Layer of the OSI-RM)
OMG	Object management Group
OSI	Open System Interconnection

OSI-RM	Reference Model (for OSI)
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PHY	Physical (Layer of the OSI-RM)
PICS	Protocol Implementation Conformance Statement
PIN	Personal Identification Number
PIXIT	Protocol Implementation Extra Information for Testers
PLC	Powerline Communications
PPPoATM	Point-to-Point Protocol over ATM
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RJ45	Registered Jack No. 45 – standardised as TIA/EIA-568-B, used for telephony and communications applications
RPC	Remote Procedure Call
RPC IDL	RPC Interface Definition Language
RS232	Recommended Standard 232, a standard for serial connection between a Data Terminal Equipment and a Data Circuit-terminating Equipment. The ITU-T standard is V.24.
SDU	Service Data Unit
SLA	Service Level Agreement
SLR	Service Level Requirement
SMS	Short Message Service
SSL	Secure Socket Layer
STB	Set Top Box
TCP	Transmission Control Protocol
TRS	Transport (Layer of the OSI-RM)
TS	Technical Specification
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VC	Virtual Circuit
VP	Virtual Path
WAN	Wide Area Network
WiFi	Wireless Fidelity, IEEE 802.11
WiMAX	Worldwide Interoperability for Microwave Access
XML	Extensible Markup Language

4 The Interoperability Framework

4.1 The Function Steps

4.1.1 General

This section outlines the steps of discovery, configuration, operation and management. They are described in detail in A.3

4.1.2 Discovery

Support for discovery is a fundamental requirement to ensure interoperability in systems of dynamic composition such as envisioned by this Technical Specification, where devices and services will be installable professionally or by end users directly, and where these devices and services will evolve in time.

4.1.3 Configuration

When the discovery process has completed, objects in the system will have a map of the objects elsewhere that they will need to interact with to implement the application. This Technical Specification does not constrain the form, content or location of such a map, nor the means by which it is created.

The main step in configuration is to make an association (or binding) between objects that are required to interact. In some systems this binding may be implemented as part of the last sub-step in discovery. The binding may be permanent for the lifetime of the system, or it may be repeatedly renewed and torn down. One object may have multiple bindings with others when its capabilities are reused by multiple applications.

Binding may be permitted, or forbidden, depending on policy or access control. The object may require a password supplied by another object that wishes to interact with it before it will perform an action or return information. It may initiate a sequence of interactions with its owners and users to enable a binding to be made. Key exchange may be done during binding as part of the system security provisions.

The configuration step may also involve one object supplying information to others that enables them to interact with yet other objects. For example, in a lighting application using a powerline medium, switches and lights have no natural binding: it is quite likely that any switch can discover all the lights in an installation, and vice versa. The manager object may interact with the occupants to map the relationship between switches and lights. Once this map has been built, the switch/light pairs can be told of each other's existence and set up bindings accordingly. This example makes many assumptions about the architecture, functions and protocols of a lighting system, which may not apply in a different context

4.1.4 Operation

After configuration, the system and its applications enter the operational phase. Interactions between objects will implement functions of an application and achieve its overall purpose.

The overall sequences of interactions will arise from execution of those functions and the algorithms that they implement. Real changes will be effected on the environment in which the applications are running, and the changes will be initiated by sensor readings that may themselves be changed by actions that the application initiates.

4.1.5 Management

Management is a special step that operates in parallel with, but is quantitatively different from, normal system operation. When present, it allows special designated management objects, or processes, to take a privileged view of a system, its components and their state. Management objects may have the capability to simulate object behaviour, to perform remote diagnostics, and to collect data from registers that are not normally accessible to non-privileged users. They may be able to do local or global system resets, restarting the discovery and configuration processes and forcing the system into certain states.

The level of security required to admit these objects to a system and allow them to interact with it is much higher than that needed for other steps

4.2 The Levels

The purpose of the classification by level of interoperability reflects the choice available to installers, service providers and users and the dynamic nature of the systems at the respective levels. Level 0 offers no choice: a standalone system from one supplier with a fixed set of functions that cannot be guaranteed to run alongside other systems. As we move up the levels, the degree of choice expands: systems can coexist; they can be interconnected; their applications can be joined together; and eventually they can be operated and managed by their users, locally and remotely using products from a wide range of suppliers and interconnect technologies.

Levels 0 – 3 are representative of the state of the HBES domain for systems that are designed and engineered for a specific purpose. Implementers of these systems are able to rely on a well-defined hierarchy of system, user and business requirements in conjunction with known technical requirements when deriving their solutions. This Technical Specification states no conformance requirements for such systems – it relies on interoperability agreements made by the suppliers and installers and these may be ISs. The classification by levels is used as an informal reference to understand their capabilities.

For applications that are now being proposed and for open systems of the future, the situation is entirely open: there is no set of overarching, general, open user requirements from which system and technical solutions and interoperability requirements are derived. Interoperability shall exist throughout the lifetime of the system, surviving changes, additions and upgrades, while offering backwards compatibility. Levels 4 – 6 represent systems that have this interoperability requirement. This Technical Specification defines the conformance requirements for systems that claim compliance with Levels 4 – 6.

Table 1 - Interoperability Levels

Level 0		A single system of supplier-defined structure built from devices using a single HBES specification and locally defined interoperability verified by the supplier for one or more application domains. No assurance of coexistence is provided.
Level 1		A Level 0 system operating across one or more application domains. Verified coexistence is required.
Level 2		Multiple Level 1 systems that interwork to exchange information and interoperate across specification and application domains verified by the suppliers using conformance specifications agreed by each HBES specification used.
Level 3		As Level 2, and the interoperability is verified with respect to international standards applicable to the HBES specifications used in the system.
CONFORMS TO IFRS	Level 4	As Level 3, but conforming to IFRS so that the applications and devices can be installed, managed and changed during the operation of the system by a qualified installer.
	Level 5	As Level 4, and changes of application and devices will be done automatically.
	Level 6	As level 5, and with remote management, diagnostics and maintenance. (automatic installation, operation and support).

Table 1 gives an overview of the interoperability levels. These are described in detail, identifying motivating scenarios or use-cases and describing their differences in A.4 and beyond

5 Conformance clauses

5.1 Interoperability Conformance Requirements

5.1.1 General

This Interoperability Framework Specification Technical Specification is applicable to systems and devices claiming interoperability at Levels 4, 5 and 6. There are no conformance requirements for systems and devices at Levels 0 to 3.

It has the following general requirements for conformance at Levels 4, 5 and 6

5.1.2 Identifier

Any object should have an identifier within the scope of the system in which it is installed that permits it to be uniquely distinguished from other objects in the system in terms of its functionality and location, to be addressed individually, as a member of a group, and in broadcast mode by the communications system.

Identifiers can be chosen by the designer and implementer of a system and different HBES specifications have different formats and semantics. Freedom of choice means that there is a risk of incompatibility, and this is a key source of interoperability failure: objects cannot be accessed by the communications system and their functions are not available to its applications.

Compliance with this Technical Specification requires the details of identifier choices and the mappings between different HBES identifier schemes to be stated.

See 5.2.1 for detailed identifier requirements.

5.1.3 Object Description

Any object that can be identified should (provided access rights allow) supply its specification, status and other requested information to services or applications including those external to the system.

Having established interoperability at identifier level, the next step is to be specific about the functionality that has been made available. HBES specifications include definitions of the functions associated with objects in terms of basic datatypes and structured datatypes. In addition, implementers are free to define their own objects and extend the capabilities of objects that are already in the catalogue. Interoperability failures arise when implementations of the objects do not comply with these definitions or the extensions are inadequately documented. Different HBES specifications define basic and structured datatypes in different ways.

Compliance with this Technical Specification requires the composition and functionality of objects, including access control and other security provisions, to be described and the mappings between objects defined in different HBES specification to be stated where such objects interact with one another.

See 5.2.2 and below for detailed object status requirements.

5.1.4 Object Discovery

Any system, specification or protocol should have a means for enabling the discovery (of location, identity and description) of objects within the system by services or applications including those external to the system.

See 5.2.3 for detailed discovery requirements. At Level 4, the discovery process is initiated by a means that is not integrated with the system, such as a management application run by a professional installer. At Level 5 the discovery process is initiated by the system automatically. At Level 6, the discovery process may be initiated by an entity that is installed remotely from the system.

5.1.5 Object Configuration

Any object that can be discovered (provided access rights allow) may be configured by services or applications including those external to the system or protocol within which they exist.

See 5.2.4 for detailed object configuration requirements. At Level 4, the configuration process is optional and is initiated by a means that is not integrated with the system, such as a management application run by a professional installer. At Level 5 the configuration process is initiated by the system automatically and will in general require the user to assent to commitment to configuration changes. At Level 6, the configuration process may be initiated by an entity that is installed remotely from the system and will in general require the user to assent to commitment to configuration changes.

5.1.6 Object Operation

Any object that can be configured may be used by services or applications including those external to the system or protocol within which they exist.

See 5.2.5 for detailed object operation requirements.

5.1.7 Object Management

Any object that can be discovered (provided access rights allow) may be managed by services or applications including those external to the system within which they exist.

See 5.2.6 for detailed object management requirements. The management capability applies only to Level 6.

5.1.8 Object Access and Safety Requirements

Before any action is made by a service or application, it should establish that it has permission to undertake the action.

The security, safety and priority rules should be enforced at both object level and application model level, demonstrated by certification of compliances with relevant ISs. However, operations and interactions within underlying standards are out of scope of compliance with this Technical Specification.

See 5.2.7 for Object Security, Access and Safety Requirements.

5.2 Conformance sub-clauses

5.2.1 Object Identifier Description Requirements

It is a requirement of this Technical Specification at Levels 4, 5, and 6 that any object (device, equipment, system, application or service) shall be identifiable within the namespace(s) of the overall system and its sub-systems. The requirement for uniqueness of the identifier depends on the mode of

access, e.g. by unicast (1-1, in which case the identifier should be unique within the namespace from which it is drawn), by multicast (1-m, when an identifier is used to identify one or more objects), or by broadcast (1-all, using an identifier designated to be used for addressing all objects). In some circumstances, the identifiers may be used interchangeably as names or addresses as required below.

Objects compliant with this sub-clause should make available their:

- Name(s) for use by external objects that may use the interfaces offered by this object. The means by which this name is derived is not prescribed by this Technical Specification;
- Data type by stating an identifier, the means by which it is derived, and its semantics, e.g. a product code or the name of an abstract datatype specification;
- Location in the system, by stating one or more network addresses, the number of such address that can be supported, their modes (unicast, anycast or multicast), the means by which they are derived and the underlying HBES specifications to from which they are derived;
- Handle, or other means of referring to it during its lifetime in the operational system, if used;
- Other permanent identifiers, such as a serial number;

5.2.2 Object Functional Description Requirements

5.2.2.1 General

It is a requirement for compliance with this Technical Specification that sufficient information about objects should be made available. Except where explicitly stated otherwise, the following sub-requirements apply to Levels 4, 5 and 6.

5.2.2.2 Object Classification

An object should provide sufficient information to allow it to be used by other objects, including aspects of security, safety and accessibility. The minimum information should include: intended purpose, targeted application domain, and text description. It may include communication means, quality rating and quality guarantee and other optional information at the manufacturer's discretion. The description shall be in human readable text.

For the following sub-clauses, one of the International Standard Formal Description Languages (FDL) of its data type, operations, and attributes shall be used to describe the supported interfaces. Operations shall be defined by their function signature, including input, output and input/output parameters and returned result and should state input values accepted and outputs generated. Attributes may include time to accept and respond to requested operations, the rate at which operations can be requested, read/write permission restrictions, identifiers used in PDUs to distinguish fields from which they are composed and other information considered sufficient to ensure interoperability. Permissible FDLs include ASN.1, XML (OMG standard schemas shall be stated), Corba IDL, ISO RPC IDL, JSON, SENML. Where a language does not permit inclusion of mandatory information, the description shall state the syntax used to described such information and shall supply the necessary details in the form of comments embedded in the text.

5.2.2.3 Object Functional Interface

An object should provide a description using one of the International Standard Formal Description Languages (FDL) of its data type, operations, and attributes.

5.2.2.4 Object Discovery Interface

An object should provide a description of its data types, operations and attributes that support discovery. Specific aspects of the discovery process are given in 5.2.3.

5.2.2.5 Object Configuration Interface

An object should provide a description of its data types, operations and attributes that support configuration.

Compliance with this requirement is optional at Level 4 and mandatory for Levels 5 and 6.

5.2.2.6 Object Management Interface

An object should provide a description of its data types, operations and attributes that support management.

Compliance with this requirement is optional at Level 4 and mandatory for Levels 5 and 6.

5.2.3 Discovery Process Requirements

5.2.3.1 General

The means by which information describing an object is derived from its Object Functional Interface, and supplied as input and output parameters to discovery interface functions, should be stated, including the syntax and semantics of information encoded in discovery operations. The syntax and semantics should be drawn from one of the FDLs listed above.

5.2.3.2 Object Descriptions: Self and Objects to be Discovered

An object participating in the discovery process should state the information describing itself that it supplies to objects wishing to discover it. It should state the number of associations with requesting objects that it will support.

An object participating in a discovery process should state by reference to their self-descriptions (as defined in 5.2.2) the objects that it wishes to discover and constraints upon that discovery. It should state the number of associations with discovered objects that it will support.

5.2.3.3 Communication Mode

An object should state the communications mode used to communicate messages related to discovery, including multicast, anycast or unicast.

5.2.3.4 Discovery Process

An object should state the interaction model and protocol that it uses to achieve discovery and/or respond to discovery interactions. It should additionally state: the time it will wait for responses, the time taken to respond, the rate at which it generates interactions; the errors that will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

5.2.3.5 Discovery Scope

An object that limits the scope of its discovery activity should state the extent of such limit in time, space and logical aspects. An object resident in a gateway participating in discovery processes should state limits applicable to scope and any optional constraints.

5.2.3.6 Security and Privacy

Refer to 5.2.7.

5.2.4 Configuration Process Requirements

5.2.4.1 General

Except where explicitly stated otherwise, the following sub-requirements apply to Levels 4, 5 and 6.

5.2.4.2 Bindings

An object participating in the configuration process should state the number of bindings with requesting objects that it will support.

An object participating in the configuration process should state the number of bindings with discovered objects that it will support.

5.2.4.3 Communication Mode

An object should state the communications mode used to communicate messages related to configuration, including multicast, anycast or unicast.

5.2.4.4 Configuration Process

An object should state the interaction model and protocol that it uses to initiate and/or respond to configuration interactions. It should additionally state: the time it will wait for responses, the time taken to respond, the rate at which it generate interactions; the errors that will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

5.2.4.5 Security and Privacy

Refer to 5.2.7.

5.2.5 Operation Requirements

5.2.5.1 Application Operation

Compliance with application operation or functionality is outside the scope of this Technical Specification. However, objects should state by reference to relevant specifications, such as interoperability guidelines published as International Standards or profiles supported by industry alliances, the algorithms and performance capabilities that they implement.

5.2.5.2 Security and Privacy

Refer to 5.2.7.

5.2.6 Management Requirements

5.2.6.1 Communication Mode

An object should state the mode used to communicate messages related to management, including multicast, anycast or unicast.

5.2.6.2 Management Process

An object should state the interaction model and protocol that it uses to initiate and/or respond to management interactions. It should additionally state: the time it will wait for responses, the time taken to respond, the rate at which it generate interactions; the errors that will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

5.2.6.3 Security and Privacy

Refer to 5.2.7.

5.2.7 Object Security, Safety and Priority and Access Requirements

5.2.7.1 Object Security

An object (or group of collaborating objects or application(s)) should state any security requirements it may apply concerning access to, or communication of data between it and other objects, including policies and processes.

5.2.7.2 Object Safety

An object should state by reference to International Standards applicable to the application domains in which it participates, the provisions made, and certifications obtained, that verify its compliance with those ISSs.

5.2.7.3 Object Access Rights

The access rights to any object (group of collaborating objects or application(s)) should be set by the entity or application to which it belongs or the owner of the object with respect to secondary and third party entities which may require certain control or receive information from it. Where access offered by an object to one party is used implicitly to provide access to other parties, the priority and hierarchy of such relationships and any additional policies that apply should be stated.

5.2.7.4 Object Priority of Control

Where two or more applications have a requirement to utilise or receive information from an object (or group of collaborating objects or application(s)) the mechanism by which priority of access is decided should be stated.

For more information refer to A.7

Annex A

(informative)

Steps of discovery, configuration, operation and management

A.1 Methodology

A.1.1 Objectives

The objective of the IFRS is to enable service procurers, installers, system integrators and service providers to identify equipment and devices that may be deployed in customer premises and utilise them in new applications and services regardless of the underlying communication protocol, external communications technology, or internal in-home HBES the devices use. In order to do this, these requirements imply a set of conditions that services and applications utilising this specification shall observe in order to obtain interoperability.

A.1.2 Assumptions

The assumptions concerning current capabilities and practice are:

- There are already many existing systems and protocols supported by major organisations. These have been developed over many years and have led to stable products. Some are already International Standards (IS) and there is a great deal of work in progress to develop new ones that will encourage convergence in the long-term. Others are not IS but have received consistent support from industry and users. Some are already widely deployed. The organisations that support and promote these systems have defined rules, guidelines and practices that ensure that products are interoperable within the respective systems;
- The expectation is that new protocols for interacting between devices using one or more of these systems and protocols will be developed, especially those that link external providers through one or more gateways to the in-home network or Home Area Network (HAN). An interoperability specification should ensure that the requirements it proposes are compatible with those used by such systems;
- Interoperability failures are possible wherever a specification offers a choice or ambiguity. The scope for choice is reduced by adoption of a common transport and internetworking architecture, functions and protocols, and operational practices, i.e. by a process of convergence. However, even if this is done, choice remains in several key areas: the abstract data types that are implemented in devices at the end points of the system tend to evolve; the interaction with the user at installation and during operation, e.g. for entering a password, will vary; security policies may be inconsistent; and the physical quantities that are measured, and the real effects of changes made by actuators, may use different systems and algorithms;
- Interworking between dissimilar technologies is achieved through gateway functions. Because the heterogeneity of technologies is increasing, there will always be gateways that allow them to interwork. The level at which the gateway implements interworking will vary according to the extent to which different communications functions converge;
- Interoperability requirements apply to any object, including: device, equipment, sensor, actuator, network, protocol, application, and business service; that may be utilised in buildings, premises and particularly in the domestic environment. The implementation of the Interoperability Framework should be the remit of the many developers and organisations active in the field.