PD CLC/TS 50560:2014

BSI Standards Publication

Interoperability framework requirement specification

bsi.

...making excellence a habit.™

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.

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

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. ;
- I**nteroperability** - 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.

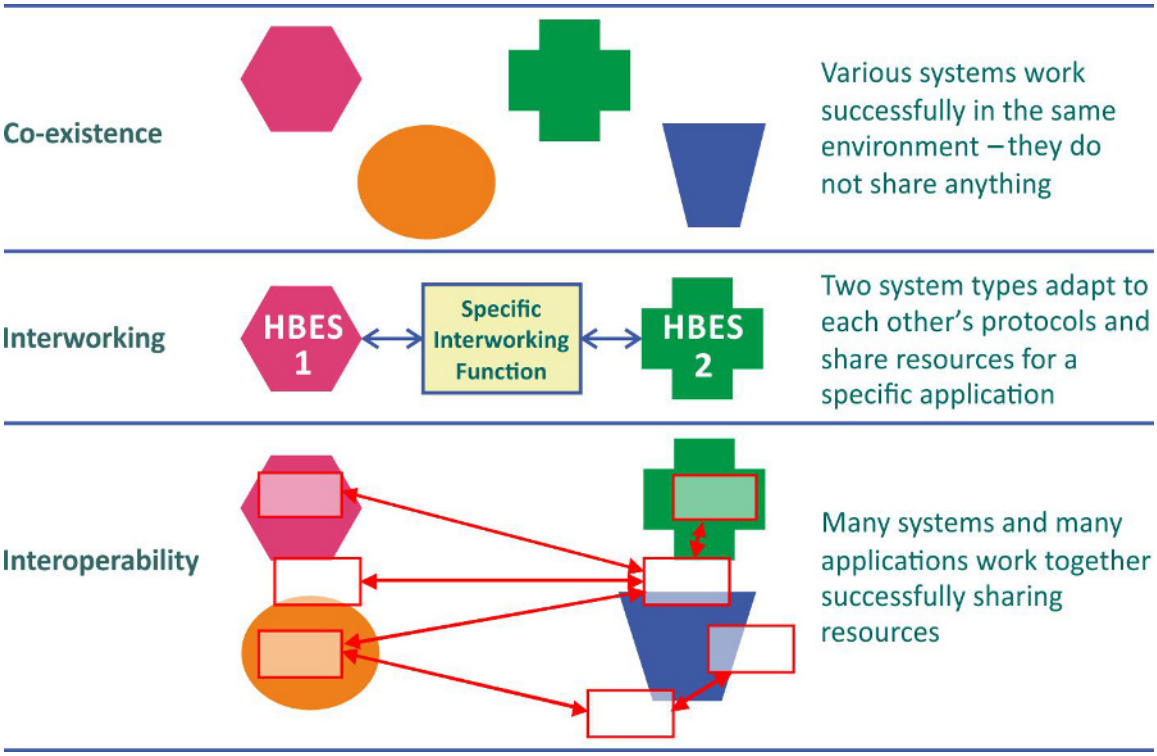

Figure 1

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 ISs.

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.

A.2 Approach

The method used to develop the IFRS is based on three main areas of potential interoperability failure, reflecting areas where designers and implementers can make choices:

- Technical – where systems are incompatible at one or more layers of the communications system, using the OSI Reference Model (OSI-RM) as a framework. These incompatibilities would be identified in a test laboratory; they are mainly the responsibility of engineers and implementers to fix, using interworking functions such as gateways or middleware. However, there are a few choices that remain and that cause interoperability problems. These might be as simple as round plugs in square sockets. ETSI has categorised the general area, using terms such as physical and syntactic interoperability;

- Semantic – where device, or other end-point, functions outside the communications system are incompatible even though they can be installed and can be shown to transmit and receive end-to-end. Semantic failures also exist within the communications system, e.g. where different options are chosen in mapping SDU fields into PDUs, layer by layer. These should be considered to be technical failures: identifiable in a test laboratory and fixed by engineers. When they have been fixed, the functions are both interworking and interoperable, layer by layer. Once outside the communications system, we are concerned with the objects in devices, the operations requested between them, and the relationship between measurements they make and communicate and the real effects that that might be caused;

- Process – where constraints imposed by policy, installer or user choice, or algorithmic behaviours prevent functions from being executed even though semantic interoperability has been proved. Some failures can be fixed by engineers but others may only be rectified by non-technical means, e.g. an instruction manual or guidelines on best practice, or a formal systematic specification of application purpose and operation. Compliance with a range of other standards, e.g. for functional safety, or with a data model appropriate to the application, may be required. This area is the most problematic because it concerns a much broader category of choices, many discretionary or not anticipated by a system's designers.

The annexes to this Technical Specification contain a informative layer-by-layer breakdown of communications layers according to the OSI Reference Model of the interworking and interoperability issues to motivate the means by which vendors and implementers declare their compliance with the IFRS.

While there are requirements on technical and process interoperability that are appropriate to include in this Technical Specification, (and these are stated in the proformas), our focus is on semantic interoperability. Failure to interoperate is observable by the inability of devices to perform functions even though they can communicate. These failures can be expressed as a sequence of steps as described in the next section.

A.3 The Function Steps

A.3.1 General

This section describes the sequence of discovery, configuration, operation and management in detail with reference to the layers of the OSI Reference Model, OSI-RM.

A.3.2 Discovery

The process and mechanisms used by a device or object to search, locate or publish, to acquire system and application object handles and to realise its designed functionality to the end-user (being the human or some other part of the system) are referred to as discovery. Any capability of the system may require some element of discovery. It is a trend that specifications offer a level of self-organisation in this process.

Discovery consists of the set of mechanisms and protocols that allow an object to discover services and functions, to announce its presence, or to respond to queries related to its service by providing information on its location (logical address or handle), what service it provides (what does it do?), and how well does this service fit the query (how well does it do it – its Quality of Service (QoS)).

Support for discovery is a fundamental requirement to ensure interoperability in loosely coupled systems 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.

Device (or object) discovery is driven by two scenarios: (i) new device/object installed in a system and wanting to offer its services (registration/announcement); (ii) new device/object installed in a system and wanting to use services from some other device(s)/object(s) (discovery query). The process is thus bilateral in interaction.

A new device that is installed into a HBES system shall become connected to it at several levels before it can do this. We assume that the device is able to make a physical link to the wired or wireless media that are present: for a cabled system, it shall have compatible connectors; for a wireless system it shall have antennas that are able to receive and transmit energy.

The table below shows the sub-steps of the discovery step that shall be followed to get the device into the system.

Table A.1

OSI Layer	**Discovery**	**Interoperability/Interworking/ Coexistence Issues**	**Options**
Medium, PHY	Identify the correct channel: (frequency and timeslot) that is being used by other devices implementing the same specification.	Multiple PHYs may exist on the same medium. They may be transparent to mutual interference or they may require scheduling.	Not needed; pre-configured, or dynamic: scan a known set of channels, or search for signatures.
	Synchronise with other devices sharing the channel.	Unknown signatures and synchronisation bit patterns.	Packet-by-packet for an asynchronous system, by negotiation with a controller to be allocated a timeslot and frequency. May change dynamically.
	Register to use the selected or assigned channel and service on the channel.	Several PHYs may appear eligible. The desired one(s) shall be selected.	Mandatory in some systems, implicit in others.
Data Link, (and medium access control (MAC) functions)	Acquire a local unique address, negotiate use of multicast addresses.	Multiple MAC and data link services may coexist on the same PHY. The desired one(s) shall be detected.	Pre-configured, or dynamic: by polling for free addresses for own use and detecting those shared with other multicast groups.
	Register use of the addresses and announce association.	Register with more the desired MAC/DLC services from of the services active on the PHY.	Mandatory in some systems, implicit in others.
	Negotiate security associations.	Keys not available	Pre-distributed keys, or exchange at registration. May not be implemented at all

Network	Acquire a unique network address, negotiate use of multicast addresses.	No addresses available, allocation processes do not respond in time.	Pre-configured, or dynamic: by polling for free addresses for own use and detecting those shared with other multicast groups.
	Register use of the addresses and announce association	Register with more than one network service from those that are offered on the registered MAC/DLC services.	Mandatory in some systems, implicit in others.
	Detect other devices present in the system, on local network and system wide through gateway functions.	Gateways shall ensure that devices on one subnetwork can communicate via a routing and forwarding database with devices on another subnetwork.	Pre-configured well-known values assigned by common convention; or dynamically assigned, requiring a additional identifier of device type.
	Negotiate security associations.	Keys not available, exchange processes do not respond in specified time.	Pre-distributed keys, or exchange at registration. May not be implemented at all.
Transport	Detect active port and session identifiers for devices discovered in the system.	Ports and sessions may be shared between applications. Gateways shall ensure that ports used by devices on one subnetwork can communicate via a routing and forwarding database with ports used by devices on another subnetwork.	Pre-defined, well known values that identify application and protocol; or dynamically assigned, requiring a additional identifier of device type..
	Negotiate security associations.	Keys not available, exchange processes do not respond in specified time.	Pre-distributed keys, or exchange at registration. May not be implemented at all
Application	Detect objects and services implemented by devices discovered in the system.	Objects and services they offer may be shared between applications. Gateways shall ensure that objects offered by devices on one subnetwork can interact via a routing and forwarding database with objects used by devices on another subnetwork.	Pre-defined, well known values that identify application and protocol; or dynamically assigned, requiring a additional identifier of device type..
	Negotiate security associations.	Keys not available, exchange processes do not respond in specified time. Information supplied by a user or other service element is inaccurate.	Pre-distributed keys, or exchange at registration. May not be implemented at all

Some, all, or none of these steps may be done. The steps that are required are related to the HBES architecture. Some systems may not require a distinct MAC/DLC and network layer; some may use only multicast or broadcast network layer (NWK) distribution and use only object identifiers. The complexity of the discovery process increases according to extent to which the system is dynamic: where identifiers are assigned statically and managed by a global naming scheme, there may be no need to discover them; however it is often the case that they are assigned on demand.

Devices and objects complying with this Technical Specification may operate in a decentralised (non-directory based) discovery infrastructure. This means that devices and objects should not depend, nor

rely, on a repository of registered active/available services to be registered with or, to acquire handles from, in order to complete their discovery and configuration process.

The scope of the discovery activity may be related to the topological (logical or network) extent of the service search. Devices and objects adhering to this standard should be able to configure and control the discovery scope. The main reasons for this requirement are potential privacy and security considerations and discovery interval duration.

If the interworking and coexistence issues are not correctly addressed then it is unlikely that mappings in gateways will contain the information needed to route messages correctly between distinct namespaces: MAC addresses, network addresses, transport/session ports, and object/service identifiers. Devices may not be aware that each other exist, or that they contain the desired objects and services, or the mappings may be incorrect.

The option for establishing secure associations is given at each layer above the PHY. Because of a general trend to interconnect more and more devices to open communications networks, the potential has increased for unwanted discovery leading to intrusion, interception (eavesdropping), and direct attack. A security mechanism that protects devices and their interactions, implemented at one or more points in a system, is essential.

A.3.3 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.

Configuration is the process by which relationships between objects are established for the purposes of the application that uses them.

NOTE Many parameter setting interactions will be part of the operation of the applications, e.g. setting a temperature threshold in a thermostat.

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 need to make such a binding depends on the HBES system: it may be implicit, e.g. when the object naming scheme is assigned statically and an active object thus always “knows” the others that it communicates with. 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 obviously makes many assumptions about the architecture, functions and protocols of a lighting system, which may not apply in a different context.

The ability of devices to interoperate to configure correctly their relationships presumes that the discovery step has completed correctly too. Potential problems include the time taken to respond during an interaction.

A.3.4 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. The stability of such processes is an interoperability issue but it is not within the scope of this Technical Specification.

The configuration step can result in bindings between objects that are more than 1 to 1: many to 1, e.g. when a light is controlled from several switches, or 1 to many, e.g. when one switch turns off all the lights, or many to many, e.g. when several switches can operate various collections of lights. In the particular case of many to 1, it may arise that the “many” concurrently invoke interactions that change the state of the “1” object’s data. There shall be provision in the interaction protocol to ensure that the “1” object’s state remains consistent.

Distributed algorithms and protocols for maintaining consistency, sometimes referred to as transactional transparency, are well known in the enterprise sector and are implemented using distributed commitment protocols supporting transaction processing. Their properties, often referred to by the acronym ACID, apply equally to appliances in HBES applications that are shared between more than one object, even though the actual protocol will vary in detail.

A.3.5 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.

A.4 The Levels

A.4.1 Level 0

Any HBES system at this level is entirely self-contained. It may operate in one or more application domains. It has no capability to interwork with other HBES technologies and has no interoperability with other HBES systems. It has a structure that is defined by its supplier and that cannot be changed without re-design and a new installation.

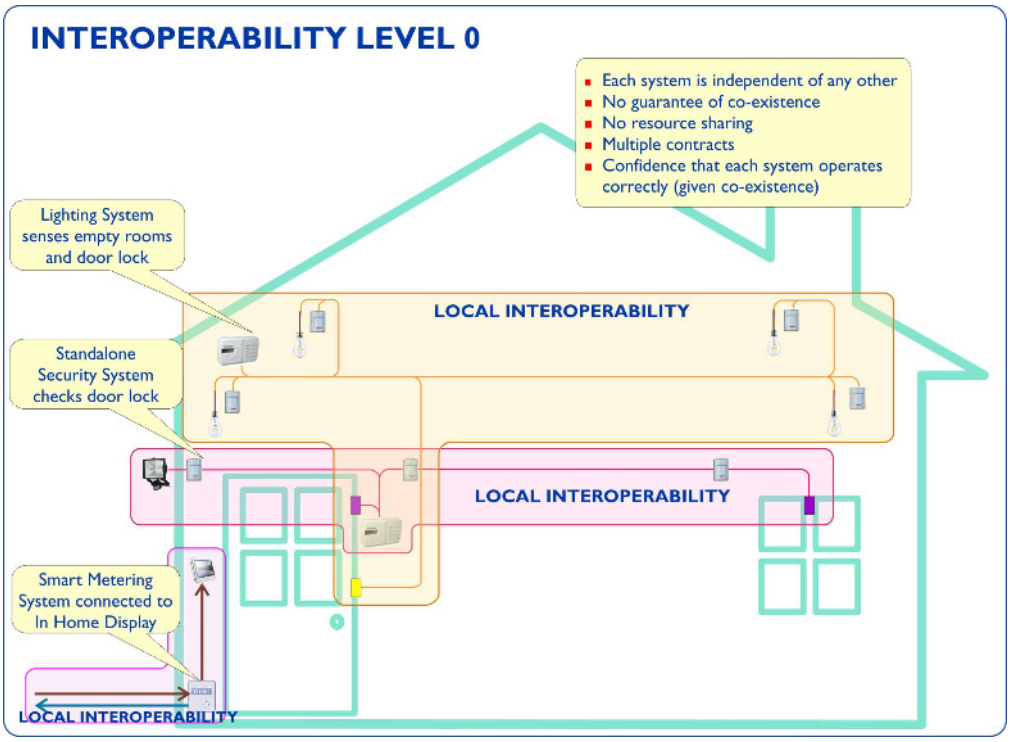

Figure A.1 - Collection of Level 0 Systems

It is not claimed that it will coexist with other HBES systems in the same premises. Figure A.1 shows a collection of Level 0 systems, using a mixture of communications specifications that cannot be guaranteed not to interfere with each other.

Any interoperability present in a Level 0 system is only that supported by its HBES specification, and the testing done by its implementers for the applications that are specified and used within the system.

Examples:

- Comfort control;
- A window, blind and curtain open/close system;
- Home entertainment and AV distribution.

Within the constraints noted above, there is no inherent limit on the structure of a Level 0 system. It may consist of multiple interconnected media, wired or wireless, and therefore have gateway/router components, but all these elements use the same HBES specification.

Devices and systems at Level 0 make no claims about being interoperable with any other devices, even those from the same vendor or a different vendor implementing the same HBES system. It is assumed that their interoperability is tested through a trade association, or by the system designers. There are no conformance requirements for Level 0 systems stated in this Technical Specification.

A.4.2 Level 1

Interoperability at level is identical to Level 0 except that coexistence of Level 1 systems is ensured – It is a system that comprises a single HBES specification and is implemented entirely according to that specification. (e.g. the case of a system entirely composed of the EN 50090-x-x standards series).

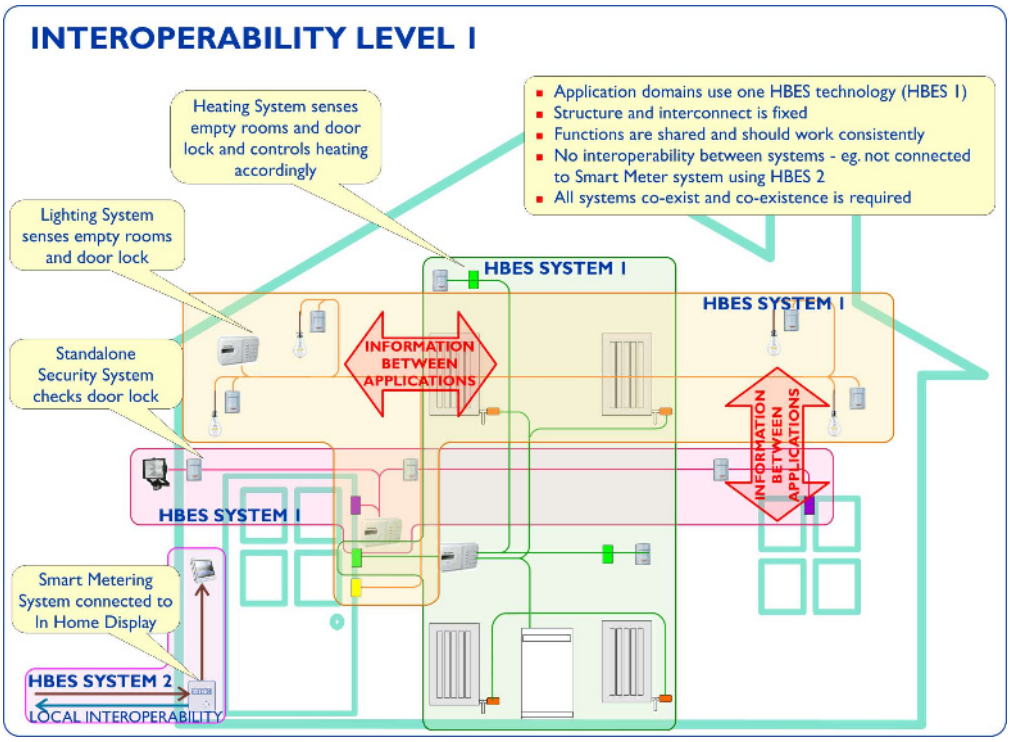

Figure A.2 - HBES System at Level 1

Figure A.2 shows a dwelling where there is HBES system predominately employed (HBES 1). Because the same HBES system operates in all the application domain areas, there is no barrier to information passing between them. There are a number of such HBES solutions and they have set requirements to enable this level of interoperability.

However, where another system (HBES2) is employed by the Smart Metering application, there is no linkage between that and the other application domains.

Examples:

- Comfort control that integrates heating, lighting and ventilation;
- Electricity consumption management for appliances (fridges, washing machines) cooperating with comfort control.

Within the constraints noted above, there is no inherent limit on the structure of a Level 1 system. It may consist of multiple interconnected media, wired or wireless, and therefore have gateway/router components, but all these elements use the same HBES specification.

Devices that claim compliance at Level 1 make no claims about being interoperable with any other devices, even those from the same vendor or a different vendor implementing the same HBES system. It is assumed that their interoperability, in particular the integrity of operations executed on devices shared between two or more applications, is tested through a trade association, or by the system designers. No claim is made of compliance with this Technical Specification.

A.4.3 Level 2

A Level 2 system implements two or more HBES, specifications. There will be at least one gateway, or bridge, capability that links media from two or more systems and provides for interworking between them. This interworking enables interoperability between devices implementing any of the HBES specifications involved. It will also allow different application domains to interoperate and share devices and resources as in Level 1.

It is assumed that such interoperability is tested and certified through a trade association, or by the system designers. The certification refers to industry, not standards-based compliance and conformance tests.

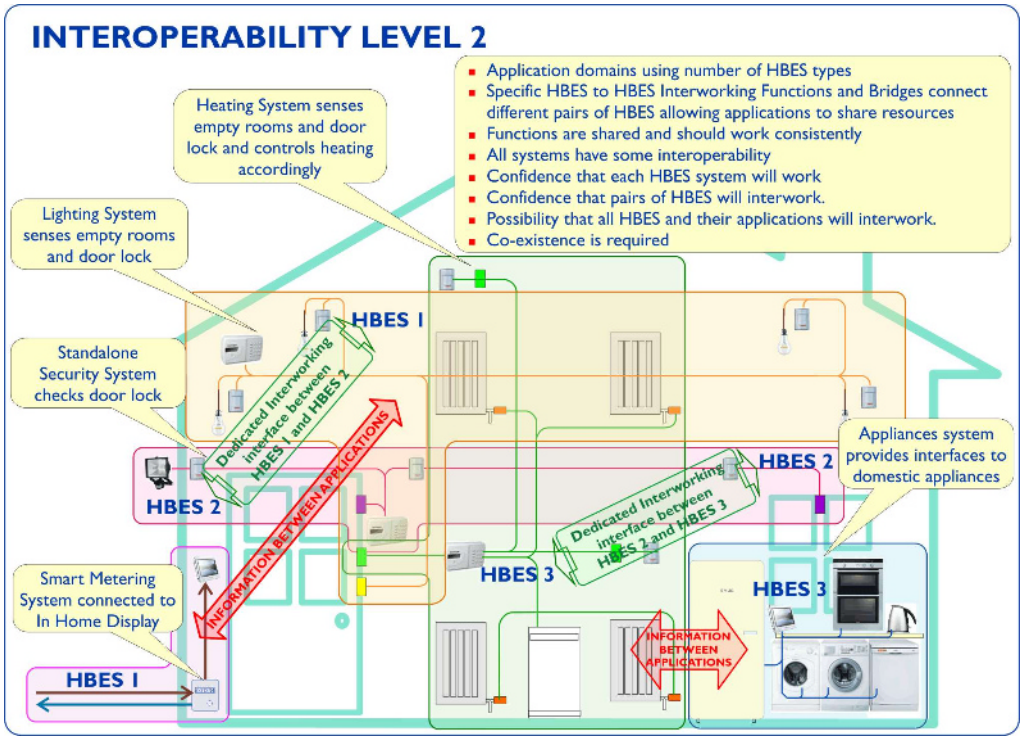

Figure A.3 - Multiple interworking systems at Level 2

Figure A.3 shows the interconnection between the security system and the smart meter by a dedicated interface that provides interworking of their communications protocols, thus enabling interoperation between the applications. Such an interface may be a gateway or a bridge between the two HBES systems which has been agreed by the associations of each system (or it may be an ad hoc solution provided by an installer). At some date after the initial installation the energy supplier may provide the consumer with a PC application, possibly linked to a Web service, that interworks with both applications.

Examples:

- A security system that communicates with its owner using GSM SMS messages for alerts and control;

- An electricity consumption management system that interacts with the electricity retailer using embedded Web services executing in a residential gateway or computer system;

- A smart meter that communicates with the energy supplier on a private network using proprietary protocols, with the appliances in the home using powerline and local short-range wireless media to implement energy consumption management, and with a local display unit using a Zigbee profile and 802.15.4 media.

A.4.4 Level 3

The difference from a Level 2 system is that the interoperability has been verified with reference to International Standards. This interoperability allows resource sharing and will usually be carried out by a dedicated installer under a single installation and maintenance contract.

However, interoperability at Level 3 requires installers with highly qualified engineers to create an interoperable system across a number of HBES types. Each installation will require engineering to ensure it works and any changes will require the attentions of highly qualified engineers.

NOTE The applications are the same as for Level 2 but at Level 3 significant engineering effort has been expended to ensure that there is reliable interoperability between all the functions and applications of this installation. Other installations may require similar effort and any changes require equivalent effort. (Many installations will be similar and this will save repetitive effort, but any differences such as adding a new application such as Assisted Living will require major effort to an installation).

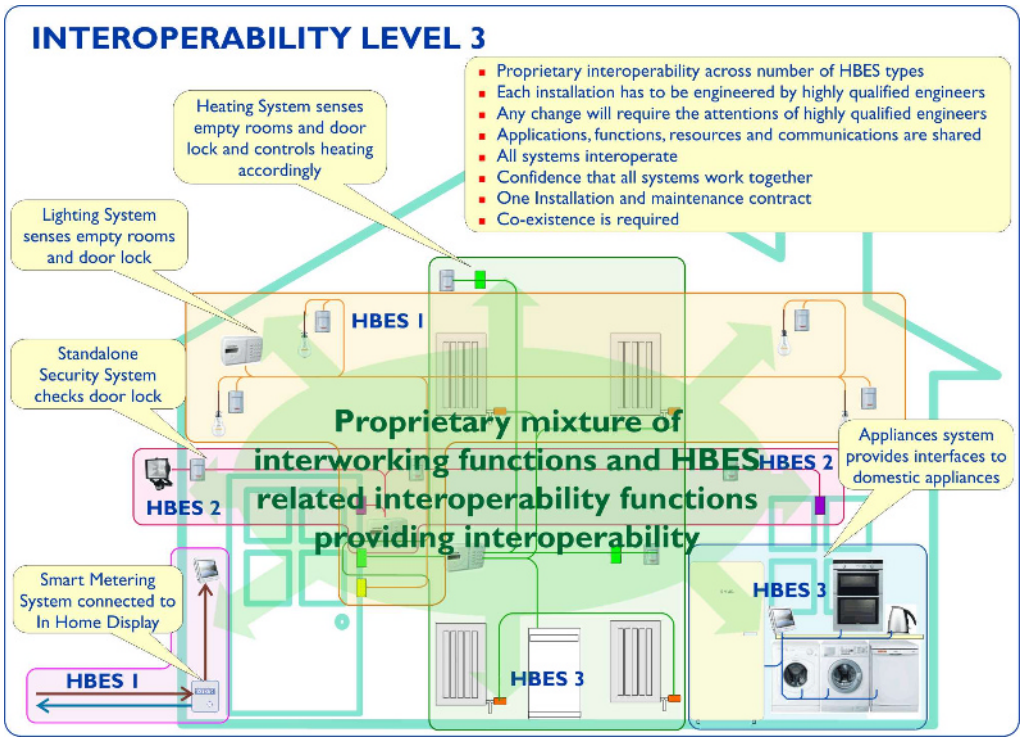

Figure A.4 - Interoperability at Level 3

A Level 3 system has the features of Level 1 (multiple applications coexisting) and Level 2 (multiple communications systems interworking).

Examples:

- A home security system that communicates with its owner using GSM SMS messages for alerts and control;. The owner can interact with the home comfort management system using SMS;

- A smart meter that communicates with the energy supplier on a private network using proprietary protocols, with the appliances in the home using powerline and local short-range wireless media to implement energy consumption management, and with a local display unit using a Zigbee profile and 802.15.4 media. The smart meter also executes a telecare application to monitor occupants' activities and shares the electricity supplier's private network with the healthcare provider to deliver alerts concerning occupants' potential health conditions.

A.4.5 Level 4

Level 4 differs from Levels 0 – 3 because under IFRS conformance there is a standard set of tools that permits the devices and applications that are present and the interconnect between them to be installed, managed and changed during the operation of the system. In other respects, it includes Level 3 capabilities.

Devices offering a certain functionality that claim compliance at Level 4 will be interoperable with other devices of the same functionality or complementary functionality at that level. They can be substituted for one another if their specific purpose is the same.

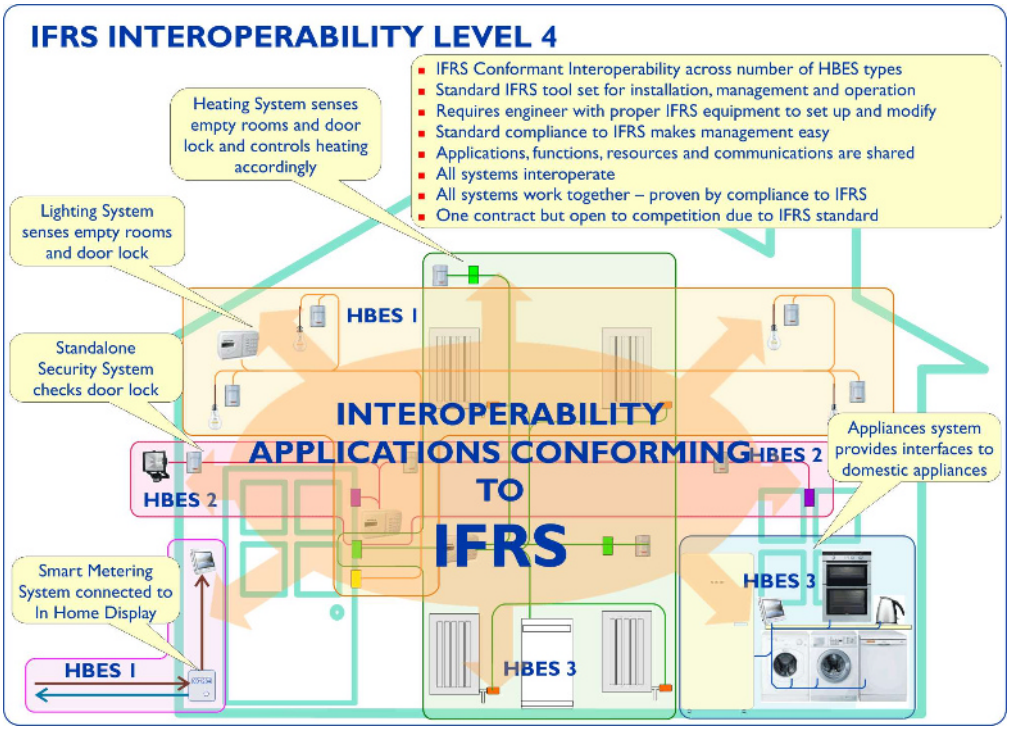

Figure A.5 - IFRS Interoperability at Level 4

The mechanism by which Level 4 is verified is likely to vary from that used for Levels 0 – 3. Devices claiming Level 4 interoperability will satisfy the conformance requirements of this Technical Specification with respect to their communications capabilities in respect of discovery and configuration together with appropriate security measures. An application provider wishing to use them shall seek further verification that they are fit for their intended purpose, using a test organization specialized in that application.

Table A.2

Step/Function	Discovery	Configuration	Operations	System Management
Processes	Should support these steps internally during initial set-up, reset, and system modification. The user may intervene during these steps to selectively admit and enable device capabilities.		Appropriate to the function of the system. Devices shared between applications should be used in a consistent and secure way.	Not accessible to the user.
Security	Because the installation may be accessible from outside the premises, sufficient protection against intrusion, eavesdropping and denial of service should be provided. Access control should be provided to allow an installer to request de-installation (reset) of devices that have been removed and installation of new ones,		User interface may implement access control, e.g. PIN code. Conflicts shall be resolved in ensuring that priority events and actions take place in preference to low priority ones.	Because the installation may be accessible from outside the premises, sufficient protection against intrusion and denial of service should be provided.
Enablers	Not accessible by the user.			Accessible to the installer.
Interaction Model	Accessible and invokeable by the installer but not by the user.			
	Operations can be invoked via gateways between different technologies. Interworking and interoperability measures are agreed for the purpose of the integrated system.			
Cross Standard Support	Contains one or more gateways that are aware of devices and their capabilities on the connected media.			

Examples:

- A telecare application that receives alerts from devices carried by a patient receiving care at home. The device communicate using Bluetooth via a secure embedded eHealth manager executing in a custom residential gateway supplied by the healthcare and communications service providers. The eHealth manager cooperates with the patient's energy manager and comfort control applications to ensure that power, heating and lighting levels are maintained.

Within the constraints noted above there is no inherent limit on the structure of a Level 4 system or its connectivity inside and outside the premises.

Devices offering a certain functionality that claim compliance at Level 4 will be interoperable with other devices of the same functionality or complementary functionality at that level. They can be substituted for one another if their specific purpose is the same. This capability applies to the respective devices independent of the media that they use to communicate. For example:

- A Level 4 fall detector embedded in a mobile cellular telephone using its built-in accelerometers communicates using IEEE 11073 application object protocol transported in SOAP over GPRS. It is interchangeable with a legacy fall detector using Bluetooth. The elderly person may use either, or both, at once. The carer will install the detectors. The certification of the detectors for actual falls is the responsibility of the healthcare actors who have confidence that the devices will interoperate in the installation and coexist with other applications;

- A thermostat using Zigbee and 802.15.4 is installed in the living room of a house. The occupants complain that the rest of the house is too cold and decide to install a second thermostat to be used to manage the temperature upstairs. They go to their preferred online supplier and,

mistakenly, buy a Level 2 thermostat. When it is delivered, they install it in the desired location upstairs and power it up: as we would expect, nothing happens because it has no mechanisms for being discoverable by a Level 4 system. Having returned it and selected a Level 4 thermostat, they try again. Nothing happens until they press the big red reset button that they just noticed on the thermostat. The comfort control system detects the thermostat and, because the TV is on, it is able to display a message asking for confirmation that the device is to be admitted.

Level 4 interoperability may also be claimed by software components, such as Java applications that are downloaded into a softphone or a gateway or activated for execution in a cloud outside the premises.

A.4.6 Level 5

Devices claiming Level 5 interoperability will adapt automatically to changes, which may be initiated by the consumer owning the system. This does not mean that there is no interaction with the owner, user or occupants of the premises because it is highly probable that either the device requires this interaction or that the application itself does to complete the configuration step.

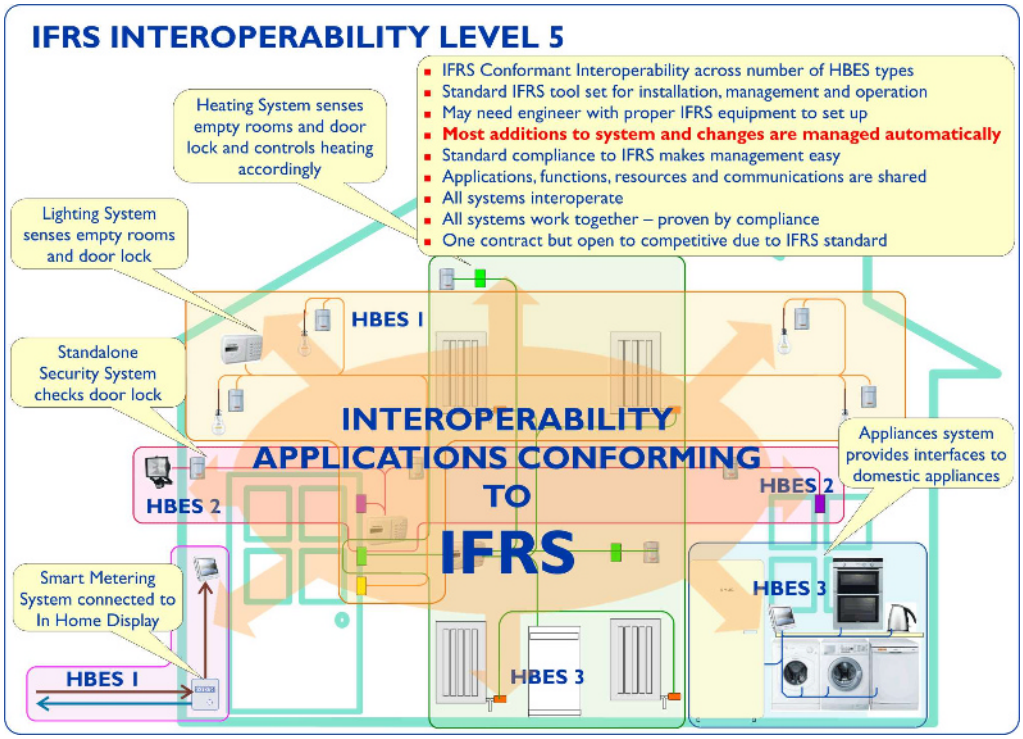

Figure A.6 - IFRS Interoperability at Level 5

For example, a Level 5 motion detector does not require interaction with its local communications infrastructure to discover a gateway, acquire a network address, and publish its object identifier and function handles to partially complete the configuration process. To be admitted to the application, the installer or owner will probably have to tell the application where the detector has been located and this requires interaction with the control function.

Table A.3

Step/Function	Discovery	Configuration	Operations	System Management
Processes	Should support these steps internally during initial set-up, reset, and system modification. The user may intervene during these steps to selectively admit and enable device capabilities.		Appropriate to the function of the system. Devices shared between applications should be used in a consistent and secure way.	Not accessible to the user.
Security	Because the installation may be accessible from outside the premises, sufficient protection against intrusion, eavesdropping, and denial of service should be provided. Access control should be provided to allow an installer to request de-installation (reset) of devices that have been removed and installation of new ones,		User interface may implement access control, e.g. PIN code. Conflicts shall be resolved in ensuring that priority events and actions take place in preference to low priority ones.	Because the installation may be accessible from outside the premises, sufficient protection against intrusion and denial of service should be provided.
Enablers	Accessible to the user, including external programmatic interfaces and protocols.			Accessible to the installer only.
Interaction Model	Accessible and invokeable by the installer and by the user.			
	Operations can be invoked via gateways between different technologies.			
Cross Standard Support	Contains one or more gateways that are aware of devices and their capabilities on the connected media.			

A.4.7 Level 6

Level 6 extends Level 5 and opens up additional access to devices to enable management functions to be executed. These may be needed for diagnostic purposes, for firmware upgrades, or for collection of statistics.

By contrast with Levels 1 – 5, Level 6 requires stricter security and control of access to protect against intrusion. Because management operations may require consent of the owner, provision shall be made for verification of operations and their non-repudiation by any participants.

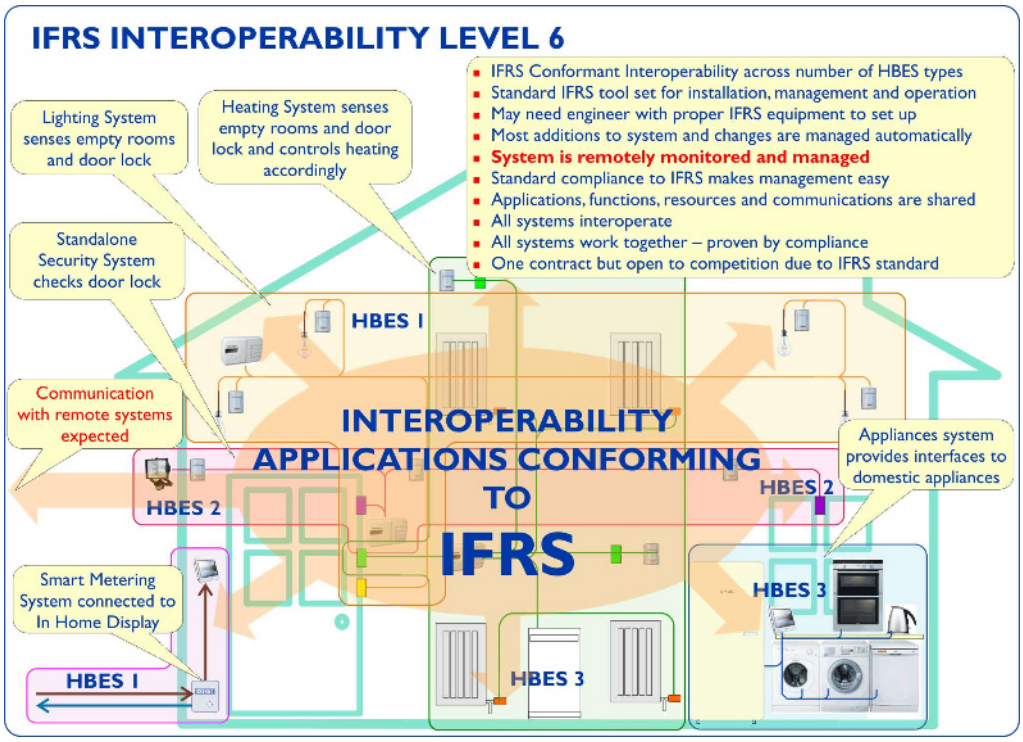

Figure A.7: IFRS Interoperability at Level 6

By contrast with Levels 1 – 5, Level 6 requires stricter security and control of access to protect against intrusion. Because management operations may require consent of the owner, provision shall be made for verification of operations and their non-repudiation by any participants.

In other respects Level 5 and Level 6 are the same.

Table A.4

Step/Function	Discovery	Configuration	Operations	System Management
Processes	Should support these steps internally during initial set-up, reset, and system modification. The user may intervene during these steps to selectively admit and enable device capabilities.		Appropriate to the function of the system. Devices shared between applications should be used in a consistent and secure way.	Accessible to the user.
Security	Because the installation may be accessible from outside the premises, sufficient protection against intrusion, eavesdropping, and denial of service should be provided. Access control should be provided to allow an installer to request de-installation (reset) of devices that have been removed and installation of new ones,		User interface may implement access control, e.g. PIN code. Conflicts shall be resolved in ensuring that priority events and actions take place in preference to low priority ones.	Because the installation may be accessible from outside the premises, sufficient protection against intrusion and denial of service should be provided.
Enablers	Not accessible by the user. Accessible to the user, including external programmatic interfaces and protocols.			

Interaction Model	Accessible and invokeable by the installer and by the user.
	Operations can be invoked via gateways between different technologies. Interworking and interoperability measures are agreed for the purpose of the integrated system.
Cross Standard Support	Contains one or more gateways that are aware of devices and their capabilities on the connected media.

A.4.8 Combinations of Different Levels in the Same Installation

As the interconnect and diversity of HBES technologies and applications evolves, and as individual installations themselves change, it is likely that devices and applications compliant with different IFRS Levels will be installed in the same premises.

The following expectations of interoperability between different Levels are laid out in the table below. The table should be read as: expectation of interoperability of products at Level [*row*] when installing them with products in a system at Level [*column*].

Levels 2 and 3 are included for completeness because they have the capability to interwork and are interoperable within themselves. This may give them access to higher Level products.

Table A.5

Level	2,3	4	5	6
2,3		Level 2-3 products should be able to interoperate with any products at Levels 4, 5 and 6 within the scope of the capabilities of the Level 2 -3 system. However integration of Level 4, 5 and 6 devices requires expert installation and configuration.		
4	With expert installation products at Level 4, 5 and 6 and may be able to participate in Level 2 and 3 systems and be interoperable with Level 2 and 3 products but only with manual configuration.		Level 4 products should be interoperable with Level 5 products with manual intervention. They will not adapt to changes in Level 5 product configuration without manual intervention.	Level 4 products may be interoperable with Level 6 products with manual intervention. They will not adapt to changes in Level 6 products without manual intervention. *They will not support Level 6 management functions, either locally or remotely invoked*
5		Level 5 products should be interoperable with Level 4 products and should be able to discover and configure them automatically.		Level 5 products should be interoperable with Level 6 products and should be able to discover and configure them automatically.

6		Level 6 products should be interoperable with Level 4 and Level 5 products and should be able to discover and configure them automatically, locally and remotely. *They will not be able to perform Level 6 management functions upon Level 4 or 5 products.*	

A.5 Use Cases

A.5.1 Methodology

A.5.1.1 General

The use cases listed at this section are used as the base to develop this standard. They also serve as test cases to validate the design. These cases try to illustrate the generic problems rather than exhaust all possibilities.

Describe Scenario – assumptions about the overall nature of the environment in which the system operates;

- eg someone/something

  (*is doing* …..)

  (*needs to know* ….) and

  needs (*to have the following information* …..)

  (*control the following …….)*

  and will need to use the following resources

  (*Object 1, Object 2, .. Object n – 1, Object n*)

  in the following manner (*set of methods* . .. .)

A.5.1.2 Describe use-case

The use case is a way of capturing the required system behaviours and requirements requested by the stakeholders. It is applied in the same way to all behaviours and requirements. The use case is a focus to support various aspects of system requirements. The interoperability requirements should be highlighted and the major parts of normal use case detail only provide the context and background to comprehend the them. To achieve this, the five “W”s (who, what, where, when and why) and one “H” (how) approach has been adopted to extract the interoperability concerns and avoid unnecessary details.

When the use cases record interoperability requirements for a part of a system, the cases under consideration should focus on the interactions between the IFRS and other system components. The approach is tabular. Five Ws should be provided by the installer or user, who is stating the requirements, and the one H defines the elements of the IFRS that apply.

Table A.6

Who	It states the primary stakeholder, who initiates the interactions with system, especially with IFI framework. The primary stakeholder can be system components (e.g. sensor, actuator) and system users (e.g. end user, installers, and maintenance engineer). The statement of primary stakeholder implies the intention and its perspective.
What	Similar to the normal use case description, it provides the step-by-step interaction details to extract what the requirements are. Rather than recording the operation process detail, it provides the context of interoperable action and identifies the involvement of interoperation.
Why	It underpins and justifies the interoperable challenges described by the case. It is also desirable to state its necessary and importance.
Where	It outlines the place where the interoperations occur.
When	It states the phase during the system lifecycle: installation, commission, operation, maintenance and upgrade.
How	It provides conceptual solutions requesting the IFI framework to achieve.
Priority	It relates the case to the interoperability level and will be given priority in term of IFI framework design and development.

The following table is an example to illustrate how to document a use case. The use case is for a movement detection sensor to turn a light on/off. When the sensor detects occupancy, the light is on; otherwise, the light is off.

Table A.7

Who	Movement detection sensor (system integration)
What	1. Movement detection sensor detects movement. 2. The sensor informs a light switch. 3. The light switch switches the light.
Why	1. Movement detection sensor and light switch use different home network technology. 2. Movement detection sensor exists at high security network and light switch exists at low security network.
Where	The movement information transfers from sensor to light switch
When	Operation phase
How	1. Transform the sensor network format to the light switch network format. 2. Align the security level between sensor and light switch.
Priority	Interoperability level 2-3 and priority high

A.5.2 Scenarios to Illustrate Interoperability Levels

A.5.2.1 General

The scenarios are the 7 Interoperability Levels. We assume that any of the security levels could be applied to any of these interoperability levels. The safety levels are properties of any use-case that shall be proved to apply.

A.5.2.2 Level 0

A consumer, Mr. X, a first time buyer, buys a flat in a new-build block of apartments. Each flat is equipped with the following systems: security (from company A); smart metering with consumer display for gas and electricity (from company B), that has the optional capability (also from company B) to manage appliances in the flat; and comfort control for heating, (from company C). Company A offers the security product as a service that Mr X can subscribe to through the building management company. The smart metering system is an early product available from company B that is certified to comply with the CEN/CENELEC requirements for interoperability of smart meters and consumer displays. The appliances were supplied by company D and implement the International Standard (IS) P. The comfort control system, also from company D, implements IS Q.

All the above products are standalone and use system specific communications media: hardwired detectors and a second telephone line for the security system; the PLC for the smart meter, with short-range wireless to the consumer display and a mixture of PLC and wireless to appliances; and proprietary wired media for the comfort control system.

Mr X is happy to accept these systems due to a discount from the developer of the apartment block.

Lesson: there is no problem until Mr. X creates one, and he is about to do just that.

A.5.2.3 Level 1

Mr. X likes his individual systems but is mystified that comfort control is separate from appliance management. He would like his comfort control system to work with the smart meter system and save him more energy. The salesman from company D explains that his engineers plan to develop products that provide adaptation between P and Q, but that company B does not supply any comfort control application. However, company D can supply a separate management system that does manage all devices, P or Q, but it does not communicate with the meter or the CDU, requiring a separate console or a PC, USB interface to P or Q, and special application.

Lesson: Mr. X has entered into more of a commitment than he imagined by accepting the vendor’s packaged up systems. The gateways and adaptors add complexity.

A.5.2.4 Level 2

Mr. X decides to change his energy supplier to company E, that offers the option to communicate with appliances using IS Q. The consumer display has to be exchanged because the wireless technology is different, although there are numerous products from companies F, G and H that offer protocol translation and adaptation, Neither company B nor company E guarantee that these gateway products will work. Company E warrants that devices implement Q (the comfort control system) can be managed using its approved consumer displays and recommends a gateway product from company I that can adapt P and Q to allow communication with the appliances. However company B does not make any claim that the appliances will work with company E’s products and cancels the optional agreement with Mr. X to manage the appliances.

Through a change in supplier, Mr. X has gained integrated energy and comfort control management but has lost the capability to manage other appliances unless he buys the gateway, even though this will not help him unless he can replace company D’s management product. He has a redundant consumer display unit. Also, he bought a new thermostat, made by company L, that claims compliance to the same specifications as some of his other devices. Unfortunately, it cannot be used by the energy management system because company L uses a correct but incompatible variation of the security protocol, even though this is an IS.

Lesson: more gateways and loss of functionality. More options appear as devices get more diverse.

A.5.2.5 Level 3

Mr. X falls in love and gets married. Mrs. X moves into the flat and brings with her an entertainment system that uses IS R. The manufacturer, J, of R compatible products supplies a product (a set-top box plugin with wireless, PLC and Ethernet capability) that can communicate with products implementing P and Q, and the X's can now detect that they have access to all their consumer appliances and systems via their TV set. They cannot use the management applications that they used previously (which came from other vendors) but they can adjust parameters manually.

Stop press: Mrs. X's aged parents have recently become unable to continue to live independently and want to move in with the X's. They need to move to a larger premises. With the P-Q-R gateway from company J, they can now take all their appliances from the flat and continue to use them in the new home. The senior residents often use the TV to communicate with their GP, which required a change of broadband supplier, and it is promising that there are products implementing P that also provide health care sensing. However, the security requirements arising from the external connection are far in excess of the features implemented by other P products, which cease to function when the parents system is running.

Lesson: better gateways and restoration of some functions. Incompatibility at higher layers of more complex function combinations.

A.5.2.6 Level 4

Company J enhances its gateway product to accommodate the lower security capabilities of some products. A side-effect is that the TV can now be the smart metering CDU, although the energy supplier, while welcoming increased connectivity, is less confident about the possible security issues. Unfortunately the set-top box power-supply is now overloaded and the device fails frequently, losing all functionality. However, mass replacement of set top boxes is already underway for the latest upgrade to digital TV, so this is smoothed over. Too late – consumers lose confidence in that product and an opportunity opens for equivalent adaptation functions that could live in the meter, or the broadband gateway, or an entirely separate but equivalently connected device.

Company J sells its gateway capability to meter and home gateway vendors and the market expands rapidly. However, many operations are manual, especially configuration for different applications, even though discovery is automated, but just within the single home. J corrects this rapidly and offers the X's the facility, via its web pages to download applications compatible with its gateways and with devices and services from A, B, C, D, etc.

Meanwhile, consumers have forgotten that P, Q and R exist. In fact, they have converged, and the role of J's gateway is to manage applications and devices – discover what is in the vicinity, configure it to execute the applications to which the consumer has subscribed.

Lesson: the gateway element is critical, even if there are fewer instances. The evolution of protocols means that its role has changed.

A.5.2.7 Level 5

Exploiting external connectivity, third party service providers compete and collaborate with the X's energy, communications and healthcare companies to offer outsourcing of application functions.

Compatibility of in-home protocols with external communications services in compliance with International Standards allows a decentrallisation of functions. Company J goes entirely virtual with a massive solar-powered datacenter in the Sahara offering customized services and applications, downloaded and managed via key interconnection functions, usually in a consumer's main gateway into his preferred supplier of Internet services (DSL, WiMAX, HSPA, PLC, etc.).

In spite of this capability, installers and service engineers from a range of providers continually visit the X's to investigate unexpected behaviours, especially after Mr. X has downloaded a new module and installed it himself. Because the devices and external services in his installation are Level 5 interoperable, these modules are able to install themselves automatically and function to a certain extent.

Lesson: unless an installation has the capability to link with external management for diagnostic purposes and to control installation expansions and consumer-installed upgrades, the necessary control over a system cannot be maintained.

A.5.2.8 Level 6

Company J implements additional functionality in its discovery and configuration processes so that only known compatible revisions of Level 5 compliant products can seek out and associate their functions with devices in the X's system and services offered by J. It does this partly by implementing stricter policies for these processes that match product codes, serial numbers and revisions of hardware or software to a database of matching configurations, and partly through better communication with Mr. X through Web services so that he is aware of potential problems and issues.

A.6 IFRS Methodology

A.6.1 General

The concepts of interoperability and interworking seem widely accepted but definitions of the terms vary in detail. The definitions given earlier in this Technical Specification are:

Interoperability	Interoperability is the ability of two or more networks, systems, devices, applications or components to exchange information between them and use (intelligently) the information so exchanged.

Interworking	The capability to exchange information between services and devices of dissimilar capability and/or provenance such that interoperability is achieved.

The interpretation of the definitions given above in 3.3 in this document can be built up layer by layer to illustrate why they are different and how they differ.

For the purposes of this Technical Specification, the information is provided to motivate the content of the IICS proformas, (Annex B).

A.6.2 Physical Layer, Pathways and Media (PHY)

The elements that shall be interoperable are wired and wireless media, plugs and sockets. Incompatible plugs and sockets are commonplace: mains power and telephone points being common examples. In these cases, devices using the service, e.g. 220V 50Hz AC, are basically interoperable but cannot interwork due to regional choices: a gateway in the form of an adapter, or maybe a change of cable, restores interworking on the medium. When mains power is 110V 60Hz AC, a device that accepts only 220V cannot interoperate. However, because power supplies have an internal gateway that senses the type of power being supplied, this interoperability failure has virtually disappeared.

It is often the case that a single communications medium is used by more than one service. This may give rise to coexistence problems, and there are two causes:

- They use different protocols (signalling, time parameters, and message formats including spectrum band, coding and modulation, termed collectively the PHY layer) that interfere with each other: this is more of a coexistence issue; they may be able to operate in parallel, e.g. if they use

different parts of the spectrum, but frequently they do not. For example, devices that implement ITU-T G.9960 (IEEE 1990) on powerline are provided with a protocol, G.cx, that allows them to support multiple services. First, they shall periodically announce their presence and type by transmitting a signature that unambiguously identifies them to each other and to different devices; second they shall obey a multiplexing protocol that ensures that they are separated in time of access to the medium. It is not clear in this case how legacy devices are supported: they were installed and working prior to deployment of G.9960 devices but cannot coexist because they do not implement G.cx. The 2.4 GHz ISM band, as another example, is very cluttered with devices implementing different protocols that potentially conflict through mutual co-channel interference, or register with each other in unexpected and unwanted ways. Achieving satisfactory segregation in time and space is necessary for interoperability;

- They use the same access protocol but still prevent each other from working properly because the device implementation is faulty or has interpreted ambiguities in a standard in a different way from other active devices. This is partly an issue for type approval and testing at the PHY level but is more likely to be resolved at higher layer.

A.6.3 Data Link Control (DLC)

The DLC layer often provides for medium access control (MAC), although the MAC will generally have aspects that depend on the PHY specification too, such as synchronisation or channel selection: the boundary is not always clear. The OSI Reference Model (OSI-RM) identifies the DLC responsibilities in a specific device-to-device context but many contemporary specifications provide at DLC level for local/remote bridging, relaying and routing, and virtual subnetworks, (e.g. IEEE 802.1q VLANs, or ITU-T G.9960). In some systems, routing may be done only at DLC level. The OSI-RM envisaged that these would be done at the Network Layer, for which a more detailed explanation is given below.

Providing PHY layer coexistence is ensured, see above, different DLCs will be mutually transparent and can coexist. Therefore the interoperability issues are related to specific choices about DLC implementation and operation within the scope of individual specifications, and communication (interworking) between different DLCs, or different instances of the same DLC, at gateways that perform bridging, relaying and routing functions.

DLC implementation and operational choices are generally described in guidelines published for the respective specifications. They aim to ensure that compliant devices can connect to media and exchange packets with other compliant devices, requiring that devices use MAC protocols, addresses and addressing modes (unicast, broadcast, multicast – dealt with in more detail below), and control information consistently.

DLC gateway functions are found wherever different media/PHYs are interconnected. The dial-up analogue ITU-T V-series modem is an example. This type of DLC gateway is a transparent bridge, or relay: its functions are similar to that implemented in domestic broadband DSL gateways at the DLC layer: a call is made to the ISP on a designated VP/VC pair using a control protocol such as Q.931 or X.21; user data is encoded using PPPoATM or some similar framing protocol. Interoperability problems associated with Q.931 are often related to incompatible choices of circuit numbering: conventions exist for using VP and VC numbers but these are chosen by implementers and may conflict.

Example: an analogue dial-up modem implements RS232, (an EIA specification) on one link facing a computer serial port, and one or more ITU-T V series protocols on a second link facing into the PSTN towards another modem attached to the device that provides the dial-up service: it interworks between the two, translating user character bit-streams into V-series signalling. There is also a control requirement imposed by the PSTN: the modem has to be told the number to dial, and this is presented to it using a separate protocol – Hayes AT is widely used. If the number is presented in standard ITU-T X.121 format then the call should be established anywhere, and the modem should also understand dial-tones, busy-tones and unobtainable tones, which are still different across the world. Historically there were frequent interoperability failures between modems that did not implement these features correctly or because PSTNs did not comply, or interworking failures, when the features were

implemented correctly but excessive delay, echo and noise on the line exceeded normal grade-of-service levels.

Example: a DLC gateway may interconnect media within the premises. For example a set-top-box (STB) with a HDMI port for a local TV plus a relay to other TVs using G.9960 on powerline. The STB shall use the correct time(s) and space(s) on the powerline multiplex for the protocols it supports. It may provide a port compliant with an IEEE 802 protocol (.3 – Ethernet; .11 – WiFi) through which it acquires programme content, (in addition to content received via an antenna); and possibly a Zigbee or IR port for local programming or communication with telecare devices. This type of DLC gateway is, again, at DLC level, a relay: although it has obvious higher layer functions, such as transcoding content in 802.2 format into an HDMI or G.9960 stream, information is not interpreted for routing purposes.

Example: Future smart meters may also have a comparable role: they connect to an external service, possibly a DSL broadband service, GPRS, or PLC. They may connect one or more media internal to the premises, including powerline, or a short-range wireless link that connects to unpowered meters (e.g. gas).

DLC gateways that implement routing to support virtualised networks are commonplace in ICT applications but, so far, less widely used in home and building systems, with the exception of larger premises. This may become commonplace in future but the technology is already well established, interoperable and interworking. The routing processes are outlined below in A.6.4.

A.6.4 Network Layer and Routing (NWK)

The OSI-RM assigns the internetwork routing capability to the Network Layer.

A network is a collection of identifiers, a namespace under a single administration, with address semantics, i.e. they denote a location in a network. The purpose of identifiers is to determine the forwarding of information, (routing), based on criteria that they are told about, or learn, using user intervention or a management protocol.

A device that supports two or more network layer instances is a router between namespaces. It will have connections to multiple media. Therefore it has gateway functions at DLC layer as noted above, and optionally some or all of the DLC capabilities. However, their operation may be modified by requirements of this layer.

By our definition of interoperability, devices shall be able to exchange information (they are not required to use it at this level). Any device shall be able to identify any other device in the installation so that they can do this exchange from source, via one or more routers, to destination. It is therefore necessary for routing purposes that devices are able to share identifiers with a common understanding of what they mean. They shall be assigned in such a way that a message can be delivered end-to-end by routers on the path between sources and destinations. The Internet has a single naming and addressing scheme to enable this delivery that is used by all IP-capable devices and there are authorities that assign identifiers in a systematic way. HBES systems use different schemes with different semantics. There are industry bodies that manage assignments, or give guidelines, for individual systems but no overall authority .

It is the router interworking functions' task to make sure that information is routed appropriately and manage the discontinuities of HBES namespaces. This may be network-centric and operated by the routers hop-by-hop; or it may be device-centric, e.g. when source routing is used. In either case the necessary information for mapping between identifiers and selecting the correct onward links will consume memory to store the routing rules and next-hop forwarding information databases.

The information exchange is not necessarily 1-to-1. Most contemporary systems have multiple addressing modes, including unicast (1 to 1), multicast (1 to designated n), anycast (1 to designated n, a variant of multicast), and broadcast (1 to all). Routers have specific obligations for forwarding multicast and broadcast data:

- Multicast addresses are drawn from a designated subset of the namespace. They may be pre-assigned with a defined meaning, i.e. anycast, with one value meaning “lighting devices” and another meaning “heating devices”. They may be taken from a pool on demand and this requires additional protocol support to share the choice amongst devices that wish to use them and to establish routing paths. In either case, a message sent to the multicast address will be received by all devices willing to receive on that address. Multicast may be implemented by onward broadcast, but this creates redundant traffic and may lead to duplicates if there are loops in the media interconnect;

- A broadcast message is identified by a designated destination address. Every device shall be prepared to accept it. Routers should limit the propagation of broadcast messages to a certain number of hops to avoid overload and circulating duplicates. In IP networks this limit is normally 0, i.e. broadcasts stop at any router and a separate decision is taken on whether to forward them or not;

- Applications may be implemented in diverse ways, using unicast, multicast and broadcast according to implementation options, and they may use them in different ways in different systems. Thus, what is multicast in one subnetwork may be unicast in another, and vice-versa.

Finally, because the communication is now end-to-end, there are protocol interoperability issues to address. We did not need to consider this at DLC and below because the interactions are not visible outside the DLC layer even when multiple DLC instances of the same technology are interconnected. At the network layer however we may have to deal with the following:

- Incompatible message lengths – a message from a device on one network may be too long to send as a single message on the next hop. If it cannot be fragmented then the two networks cannot interwork and the devices cannot interoperate;

- Windowing, acknowledgements and flow control – the protocols may be fundamentally incompatible, e.g. the source system requires an acknowledgement that the receiver will never generate; or the receiver may generate an acknowledgement at a lower layer, e.g. the DLC, or a higher layer, e.g. Transport, (see below) that the gateway shall then translate into a Network layer acknowledgement;

- Other control information, e.g. sequence numbers, which may be directly exchangeable;

- Source routing vs. hop-by-hop routing;

- Timing: indicate time to respond, or timeouts on response or acknowledgement.

A.6.5 Transport and Session (TRS)

These layers shall establish the bindings between objects resident in the devices. They use the end-to-end connectivity established by lower layers to deliver messages from source to destination. They may also establish ownership of devices and their functions so that they can be shared consistently between different applications.

For most HBES systems the entities that are visible at these layers are handles that identify application layer objects. Many of the detailed issues of interoperability and interworking between different object naming and referencing schemes are similar to those for the addresses used by the network layers. The mechanisms for matching between different systems are comparable: a database is required that translates between the namespaces.

The protocol interoperability issues are also similar to those described for the Network layer.

A.6.6 Presentation and Application (APP)

To a certain extent, the interoperability and interworking issues discussed above for the Network, Transport and Session layers apply here: there are naming and protocol discontinuities to be overcome so that communication can be achieved end-to-end. As before, the gateway functions shall be capable of matching incompatible protocols, e.g. an acknowledgement that is generated as a specific Application Layer message by a receiver back to the sender that is expecting a Transport layer acknowledgement.

More specific to these two layers, the format of messages will vary between systems; so will the interaction model. Some use a read/write, or get/set, model in which the handle of the object receiving the message and the contents of other message fields determine the actions that the receiver will perform. A standard response to a read or a write will be returned. Others may use a richer model, e.g. based on ASN.1 or IDL, where the operations, their encodings and information fields vary according to application. Information fields may be encoded in several ways: e.g. fixed format, or variable format such as Type-Length-Value (TLV), (TLV is also used in OSI Presentation layer Basic Encoding Rules). The position of fields may be significant.

A.6.7 IFRS Issues – A Summary

The preceding sections have built up a picture of typical problems of coexistence, interoperability and interworking.

It is not the role of this Technical Specification to propose how the problems should be solved, or to specify gateway functionality. Its role is to give vendors the opportunity to provide necessary and sufficient information to enable interoperability between devices end-to-end. Clearly, middleware and gateways have essential roles to play. Again it is not the purpose of this Technical Specification to say how such entities operate: there are already several architecture, functional and protocol specifications from various working groups, some of which have become standards already.

From our discussion so far, we can summarise the information that an edge device claiming interoperability at levels 4 and above should supply at the key layers of the communications system:

- PHY: state base PHY standard complied with and optional features used. According to interoperability level state capability for discovery, configuration and management and security if implemented;

- DLC: state base DLC standard complied with and optional features used. According to interoperability level state capability for discovery, configuration and management and, if used, indicate PHY layer functions that are used to support these capabilities. Identify address ranges and mappings;

- NWK: state base NWK standard complied with and optional features used. State range of addresses used and algorithm for acquisition. State range of values of data and control information fields used and algorithm for usage. State timing parameters: min/typ/max delays to respond, min/typ/max time to wait for response. According to interoperability level state capability for discovery, configuration and management and security and, if used, indicate DLC and/or PHY layer functions that are used to support these capabilities;

- TRS: state base TRS standard complied with and optional features used. State range of object references used and algorithm for acquisition. State range of values of message data and control fields used and algorithm for generating them. State timing parameters: min/typ/max delays to respond, min/typ/max time to wait for response. According to interoperability level state capability for discovery, configuration and management and, if used, indicate NWK, DLC and/or PHY layer functions that are used to support these capabilities;

- APP: state base APP standard complied with and optional features used. State range of object references used and algorithm for acquisition. State ranges and values of other identifiers used

and algorithms for acquisition. State range of values of message data and control fields used and algorithm for generating them. State timing parameters: min/typ/max delays to respond, min/typ/max time to wait for response. According to interoperability level state capability for discovery, configuration and management and, if used, indicate TRS, NWK, DLC and/or PHY layer functions that are used to support these capabilities.

These are the basis of technical and semantic interoperability between devices attached to the same subnetwork and between devices and gateways attached to that subnetwork. It is anticipated that most information required can be supplied by reference to existing standards.

Functions embedded in a device that implement gateway capabilities have additional obligations to achieve interoperability. First, the information above shall be supplied for each subnetwork medium/technology that is supported. Then, for each of the subnetwork media to which a gateway is connected, the following additional information should be supplied with reference to pairs of In and Out pathways:

- PHY: according to interoperability level state mapping between In PHY and Out (any level) discovery, configuration and management and security if implemented;

- DLC: according to interoperability level state mapping between In DLC and Out (any level) discovery, configuration and management capabilities. If any are used, state address/identifier ranges and mappings between In and Out. State mappings of control information;

- NWK: according to interoperability level state mapping between In NWK and Out (any level) discovery, configuration and management capabilities. If any are used, state address ranges and mappings. State mappings of control information;

- TRS: according to interoperability level state mapping between In TRS and Out (any level) discovery, configuration and management capabilities. If any are used, state address ranges and mappings. State mappings of control information;

- APP: according to interoperability level state mapping between In APP and Out (any level) discovery, configuration and management capabilities. If any are used, state address ranges and mappings. State mappings of control information.

These are the basis of technical and semantic interoperability between devices attached to subnetworks and communicating across gateways that interconnect those subnetworks. It is anticipated that most information required can be supplied by reference to existing standards.

A.6.8 Working Assumptions

The collection and categorisation of information that supports a conformance claim and allows it to be tested in an appropriate setting is provided for within the standardisation process, for example via the PICS and PIXIT proforma model. This model should be used;

- A data model that captures object specifications and relationships is not a priority for the IFRS Technical Specification stage of the standardisation process. Ultimately one may be required, and a language will be selected for expressing it. It is desirable that this is compatible with the language and methodology in which scenarios and use-cases will be captured;

- PICS and PIXIT proformas may be needed wherever issues of interoperability arise. Following further study, some issues may be deemed to be interworking requirements as distinguished above.

- Topics to be covered by the PICS and PIXIT include: PHY (pathway, plug/socket, media); Link (MAC, DLC, including layer 2 forwarding); Network (sub-network and device addressing, distribution mode); Transport (end-to-end delivery and end-point addressing); Session (discovery, configuration and platform-specific protocols); Presentation (abstract and concrete syntax of

message structure); Application (object specification and interaction protocols). It is recognised that these terms may not be compatible with terms used in other specification approaches;

- Specific HBES technology platforms may already have equivalent conformance proformas for all, some or none of these layers (e.g. where reference is made to existing standardised conformance specifications);

- Furthermore, there are several platforms with interoperability guidelines that are well-established, and standardised by CENELEC, CEN and ETSI. These provide a basis on which to build the proformas to be included in the IFRS Agreement;

- Security in such cross-platform, mixed location systems is a key issue and the source of many interoperability failures and vulnerabilities. Some terminology may need further examination. The focus will be on requirements and conformance, not solutions.

A.6.9 Rationale for the Function Steps and Associated Processes

A.6.9.1 General

Table A.8

Step/Function	Discovery	Configuration	Operations	System Management
Processes	Outlines the methods associated with the discovery of an object in the specific system.	Outlines the methods used to configuring an object or application object in the specific system.	Outlines the action of how applications are instantiated and operate in the specific system.	Outlines how an object or set of objects may be managed within the specific system.
	Discovery			
Security	The level of security provided solely by the specific system in the action of discovery.	The level of security provided solely by the specific system in the action of configuration.	The level of security provided by any application provided under the specific system.	The level of security provided solely by the specific system in the action of management.
		Object access and safety requirements		
Enablers	The methods used by the specific system to execute discovery.	The methods used by the specific system to execute configuration.	The methods used by the specific system to define and create applications and application models.	The methods used by the specific system to execute management.
	Identifier Object description	Object configuration		Object Management
Interaction Model	The methods used by the specific system to provide interaction between objects and other objects in the process of discovery.	The methods used by the specific system to provide interaction between objects and other objects in the process of configuration.		The methods used by the specific system to provide interaction between objects and other objects in the process of management.
			Object Interaction	

			Model	
Cross Standard Support	Records ny standard, system, sub-system or protocol that has been identified as having a specific interface between it and another protocol, such translations or APIs are often created by a specific protocol and flow from it or to it,			

For each column, a product may comply with IFRS at any level between 0 and 6.

A.6.9.2 Architectural Issues

It is implicit that there will be a function that is able to match between systems, media and protocols for products offering interoperability at Level 3 and above. Such functions already exist in a variety of forms from Level 0 upwards:

- A device supporting 2 interfaces to separate media implementing a single HBES specification. The device implements interworking at link level, receiving a message on one link and retransmitting it on the other without change to the contents. Interoperability issues remain between the functions implemented in interacting devices attached to the media;

- A device supporting 3 or more interfaces to separate media implementing a single HBES specification. The device is a router and shall observe the routing protocol of the specification. Other interoperability considerations are as noted above;

- A device implementing one media interface to a single HBES specification and a second interface to another system. This is commonplace with devices that connect to the Internet through a home gateway, using IP as a bridging protocol;

A.7 Security, Safety, Access and Priority Considerations

A.7.1 Introduction to Security Considerations

Interoperability implies the interworking and co-operation of multiple devices, systems and networks and as the level of interoperability reaches above Level 3 and certainly by Level 6 there are new requirements on what an object can or cannot do, who or which system may have permission to control it and consideration shall be given to the aspects of safety for specific objects systems and applications. It is evident that what may be both safe and secure within a closed system may become unsafe or insecure if that same system is opened up to multiple other systems by interoperability.

With respect to security, any system using RF is susceptible to eavesdropping and even with messages being encrypted an eavesdropper can learn valuable information about a premise. At any level of Interoperability where messages flow between and / or different but interoperating systems there needs to be protection against an intruder modifying the message or other exploits or attacks being caused by denial of service. At levels where the operation of the systems is largely remote messages shall be authenticated and validated and verified.

With respect to safety, any application or connected device will be liable to safety risks if control is made remote from the basic device (unless the remote control is directly paired with the device). The further from the application or device that control is and the more remote actors there are that wish to control the application or device the greater the risk becomes. For applications which are fully remote and automatically initiated, the application and process design shall ensure (a). that it can inform any device of its presence and the safety concerns associated with third party control and (b). it can evaluate such information from third party applications or devices in order that its own actions do not compromise the third party application or device (for instance an energy control application shall be aware of a life support device (“Do not turn off the power supply”) and know not turn off the electricity supply at source (The Smart Meter).

With respect to Priority wherever a safety critical application or device is involved, it is likely that some applications will have priority over others and the use of a device or application by other devices or applications may be subject to lower priorities and access right to certain functions.

In general, as the level of interoperability increases the responsibility on the application designer and the installer (and ultimately only the application designer) and becomes more and more onerous. There will need to be strategies for identifying risk and ensuring it is avoided where automatic and remote operation is employed. Furthermore, the greater the remoteness of control and the number of messages transmitted to enable that control the greater is the risk to security.

The passage of traffic from originator to recipient(s) shall pass certain tests before being forwarded or executed. Within a certain scope no checks may be needed, e.g. when the system is entirely self-contained and cannot communicate externally.

This may be seen according to the following table:

Table A.9 - Security, Safety and Access Rights and their priority by Interoperability Level

Interoperability Level	Security	Safety	Priority	Access Rights
0	May require communication security to defeat an eavesdropper	Components should always function in a safe manner if they are controlled remotely. See footnote a	N/A	N/A
1	May require communication security to defeat an eavesdropper	Components should always function in a safe manner if they are controlled remotely. See footnote a	In any safety or life critical device, component or application, one application should have priority for control	Except for the application with the highest priority, lesser applications may have limited functionality.
2	Protection against intrusion, denial of service and eavesdropping should be provided	Where components are controlled by two or more applications possibly from different systems, there should be assurance that any resulting operation is safe. See footnote a	In any safety or life critical device, component or application, one application should have priority for control	Except for the application with the highest priority, lesser applications may have limited functionality for a specific device or object.
3	Protection against intrusion, denial of service and eavesdropping should be provided	Where components are controlled by two or more applications possibly from different systems, there should be assurance that any resulting operation is safe. See footnote a	In any safety or life critical device, component or application, one application should have priority for control	Except for the application with the highest priority, lesser applications may have limited functionality for a specific device or object.
4	Protection against intrusion, denial of service and eavesdropping should be provided See footnote b	Where components are controlled by two or more applications possibly from different systems, there should be assurance that any resulting operation is safe. See footnotes a & c	In any safety or life critical device, component or application, one application should have priority for control It is the Installer's responsibility to	Except for the application with the highest priority, lesser applications may have limited functionality for a specific device or object. It is the Installer's

			ensure safety is not compromised. See footnote c	responsibility to set access rights and levels
5	Protection against intrusion, denial of service, and eavesdropping should be provided See footnotes b & d The authenticity of applications automatically managed and controlled is essential	Where components are controlled by two or more applications possibly from different systems, there should be assurance that any resulting operation is safe. See footnotes a, c & e	In any safety or life critical device, component or application, one application should have priority for control It is for the designer of the application to ensure safety is not compromised. See footnotes c & e	Except for the application with the highest priority, lesser applications may have limited functionality for a specific device or object. It is for the designer of the application to set access rights and levels. See footnote e
6	Protection against intrusion, denial of service, and eavesdropping should be provided. See footnotes b & d The authenticity of applications remotely and automatically installed and managed is essential. See footnote f	Where components are controlled by two or more applications possibly from different systems and remotely, there should be assurance that any resulting operation is safe and remote instructions are validated. See footnotes a, c, e & g	In any safety or life critical device, component or application, one application should have priority for control It is for the designer of the application to ensure safety is not compromised. See footnotes c, e & g	Except for the application with the highest priority, lesser applications may have limited functionality for a specific device or object. It is for the designer of the application to set access rights and levels. See footnotes e & g

a) It is important to recognise that there are many instances where automatic operation can result on unsafe conditions. Where these are similar to (say) the setting of controls on a (cooker) oven or washing machine or central heating boiler, then provided the automatic remote control does not set conditions that a person manually would not set up, the conditions are no more or less safe than a non-automatic set up. However, when the setting up is physically remote, it is important to ensure that the conditions of the operation are safe when the operation takes place and have not changed since the conditions were inspected manually and set for automatic operation. Thus an oven may be set for remote operation with specific cooking cycle requested but if between the set up and the operation, the door is opened, the oven shall be reset for automatic operation before the operation can take place.

If the operation of a remotely controlled device is life critical (for instance with a telehealth device) it is necessary to ensure that activities by applications other than those directly associated with that device may not carry out actions (even in other application areas) that may compromise the life criticality. For instance: an energy management system shall have knowledge of the life critical system and ensure that essential electrical power to it is not removed.

At levels 0 – 3 it is the responsibility of the developer of applications and the designer of the device or appliance to ensure safety and that this may be backed up by access rights. Beyond level 3, the requirements set out under footnote c also apply.

b) Under this Framework, it is the Installer's responsibility to ensure that the configuration of the operation and the local management of applications is appropriate and protected by secure means. This may mean that the use of local password protection is necessary or that information flows are encrypted.

c) At Interoperability Level 3 and above, multiple applications may control any one device or object. It is the installer's responsibility to ensure that a device may be given specific access rights that relate to specific applications. For instance an object or device may carry out a life critical operation and also be part of an application that is important to another service. It is essential that there shall be a hierarchy of access, priority and control that prioritises life critical actions over mission critical actions over other important applications. It is also important to recognise that circumstances may change and therefore priorities of access will also change and that the installer shall recognise this and be able to change these when new equipment, devices or objects are installed or new uses are made of them.

d) When systems are automatically configured, when new devices, equipment or objects are installed or when new applications are implemented with new equipment or systems, the burden of configuration shall be suitably protected by secure means as appropriate.

e) As with footnote c. there is a responsibility for ensuring the safety through access control and understanding the priority of specific equipment and devices. Whereas under footnote c this is the responsibility of the installer, when applications are set up automatically, the application itself shall determine its priority to have access and control specific equipment, objects or devices. For instance an energy management application may control the temperature in a room to ensure the most efficient use of energy but it would be overridden by a life support system whose task was to ensure a patient was kept at a particular level of comfort. This implies that all applications used at Interoperability Level 5 shall be authenticated, they shall be designed to evaluate the actions of other applications and devices active in the shared space and where it is discovered that some actions that might be undertaken by an application was able to cause safety or operational issues in other devices or applications, then such actions shall be suppressed or negotiated with that other application.

f) As with footnote e. there is a need to secure specific operations as appropriate. However, with control and operation remote from the house the whole communication chain shall have a level of security that is appropriate to the application being controlled. Since any application could be subverted by an insecure communication link, this may mean at Interoperability level 6 all communication shall be both reliable and secure for home control, security and life critical applications.

g) As with footnote e., priority, safety and access control are highly important but in addition to the application having control, this control may be proxied to remote systems that may use intelligent means to set priorities. They may also set up new applications and it will be necessary for the remote system to be able to interrogate applications and devices to determine their settings, attributes and parameters and be able to reset safely the hierarchy of access rights, priorities in order to maintain the maximum level of safety. It is appreciated that this is difficult to achieve, but it is however, very important to ensure any modification of an existing system is fully considered and thought through especially when designing autonomous systems.

A.7.2 References and Standards

There are many standards and specification that relate to securirty, encryption of messages under many standards organisations. It is not the role of this Technical Specification to provide a listing of relevant documents (although a few are cited). The main objective of this specification with regard to security, safety, access rights and priority of control of objects, systems and devices is to ensure that the developer of applications takes account of the risks and potential for breaches in security, the potential safety issues and how these may be addressed by setting correct access provisions and priorities of control where two or more entities have access or control of an object.

Annex B
(normative)

Interoperability Implementation Conformance Statement

B.1 Scope

This document provides the Interoperability Implementation Conformance Statement (IICS) proforma for the Conformance Clauses in the IFRS specification.

The present document details in tabular form the implementation options, i.e. the optional functions additional to those which are mandatory to implement.

B.2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific;

- For a specific reference, subsequent revisions do not apply;
- For a non-specific reference, the latest version applies.

1. ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile, conformance testing specifications; Standardization methodology".
2. ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts".
3. ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

B.3 Definitions and abbreviations

B.3.1 Definitions

B.3.1.1 General Definitions

Building	A man-made structure with an interior, an exterior boundary, and an owner. NOTE By this definition a building may be composed of a collection of buildings. Example: a house (owner-occupied or rented), a block of flats, a hotel (containing rooms or suites whose occupants have temporary ownership), a station, airport or hospital. Example: a business located at several sites; multiple buildings with a single owner, with interconnection providing for communication between management systems.

Consumer	A Natural Person who uses, requests or purchases products and services. NOTE For the purposes of this document the “consumer” is considered to be the end user of smart house technology. Consumers differ in their abilities and the different requirements are an aspect of interoperability, e.g. when a motor-impaired consumer interacts with an installed system. Example: the occupant of a smart house and any visitors. In fact any people at home.
Customer	A person or organisation who contracts with any entity in order to design, install or maintain a smart house system or to use any service or application provided by a service provider to the end-user or consumer in the smart house. Example: a *Consumer* as defined above may be a customer. A company that sub-contracts the management of its *Building* is a customer of the service provider (defined below).
Device	An electronic object comprising instances of sensing and/or actuation and/or communications functions implementing them on behalf of one or more owners. NOTE 1 It may be a *Product* in its own right or part of a Product together with other Devices. See also Device Object. NOTE 2 For the purposes of this Technical Specification, a device may be a physical sensor or actuator and also a software objects such as a Java application. Example: a proximity detector that activates a light by direct power switching and also sends a message to a security system to alert it that a person (or an animal) is nearby.
End User	Any natural person who is the user of equipment or recipient of services in the home environment NOTE May be used interchangeably with User, defined below. Example: the children in a household. They are *Consumers* but not *Customers* according to the definitions above.
Function	The collection of instructions that process information and communicate it to other functions with measurable effects. NOTE A function may be a collection of one or more functions. Example: a thermostat, whose function is a capability to monitor ambient temperature against thresholds set by End Users. Such a function may reside in a variety of locations depending on system, application or service architecture and actual installation. For example, it might be implemented in an energy manager in an End User’s personal communicator or computer, or a smart meter, that polls, or receives, values from temperature sensors; or in a multi-function thermostat that receives thresholds from a controller, monitors them locally and notifies other functions when they are exceeded. The distribution of functionality, the information flows and locus of control will vary accordingly.
Home	Premises in which a person lives, or people live. Example: a house, an apartment in a block of flats, farm or estate comprising a house and outbuildings.
Instance	An object or service embodied in a product that possesses an identity and one or more owners and that may originate and or respond to events external to it. Example: the thermostat described above following its integration into a working installation, which implies acquisition of an identifier such as a network address and references to its internal objects.
Identity	A means of distinguishing objects of any kind from one another.

	NOTE The specific means will vary according to the type of object. An identifier will be drawn from a Namespace. Examples: a serial number, product code; a barcode, the MAC address of a network interface, the IP address of a network interface comprised of a host number, a network number and prefix mask that distinguishes them.
Namespace	A collection of Identifiers constructed from a collection of symbols according to conventions agreed between users of that Namespace. Example: the 48 bit IEEE 802.2 medium access controller address. The specification states that the top address bit if set defines the address as a group, or multicast, address. If all bits are set then the address is defined to be a broadcast address.
Network	A collection of devices that are connected together for the exchange of data and sharing of resources. It is characterised by a collection of identifiers with one or more owners. The term “Address” is usually used to refer to such identifiers. Example 1: the Internet sub-network numbers and sub-network masks (or prefixes) constituting the Autonomous System (AS) assigned to an ISP or other operator of Internet services. Example 2: a collection of telecare devices installed in a Consumer’s Premises that have discovered each other, configured automatically as a network, acquiring network addresses, and have registered through a gateway with a Service Provider.
Legal Entity	An individual or organization which is legally permitted to enter into a contract, and be sued if it fails to meet its contractual obligations. NOTE It is used as a general term to describe all entities recognized by the law, including both juristic and natural persons.
Natural Person	A human being in the eyes of the law. NOTE This is different from an artificial, legal or juristic person, i.e., an organization that the law treats for some purposes as if it were a person distinct from its members or owner.
Owner	A Legal Entity in possession of rights over objects, applications and services in the smart house that may define access rights, authorisation, authentication, service level agreements, and policies and may delegate those from time to time. NOTE A Consumer will often be an Owner. An End User may not be an Owner, i.e. it has no authority to define, or delegate the elements listed above. Issues of information, privacy and who owns which element. Example: an individual who installs and manages a collection of objects that implement applications ; a service provider that offers a service under a service level agreement to manage a collection of objects on behalf of other owners.
Occupant	A Natural Person resident in Premises.
Occupier	The Owner of Premises.
Policy	A collection of conditional instructions that allow, or deny, the execution of operations on objects. Example: if time of day before 0830 UTC then heating on; if the cat at the cat-flap is ours then let it in. The combinations of such policies form an interoperability issue.
Premises	One or more buildings with one or more owners, Example: for multiple building premises would be a business located at several sites, or multiple buildings with a single owner. The interconnection provides for

	communication between management systems, hence a potential interoperability issue.
QoS	The requesting and delivery of specific, quantifiable performance levels on a shared network or on services delivered. NOTE Typical QoS parameters include: throughput, loss, latency (or delay), response time, and jitter to describe a network's performance in the treatment of specific classes of data. Example: a security system shall have a throughput of 300 bps, 0% loss, 200 ms response time.
Schema	The structure and contents of any information resource. Example: As a data catalogue for a database, a schema identifies the entities and the types of attributes for those entities. A schema for an enterprise may also define rules of use and validated values. Example: an XML schema defines the structure of an XML document. An XML schema defines things such as which data elements and attributes can appear in an object (such as a document or application) and how the data elements relate to one another.
Service	A product or good provided by a Service Provider to a consumer. NOTE In the smart house many of these will be provided through electronic systems that regulate the home or provide entertainment, healthcare, security or safety in the home. In this context a service is delivered by a service application. Example: a mobile telecommunications operator provides a Services for voice and SMS. Voice telephony and SMS are Applications implemented by the mobile communications Network. SMS requires Services that are often provided by third parties for message storage. Example: the Owner of a Home who is running an Application locally to reduce electricity consumption enters into an agreement with the electricity supplier to use the supplier’s energy management service to optimise use of electricity in combination with pricing offered by the supplier.
Service Agreement	Contract(s) between a Service Provider and the customer (end user, subscriber, consumer). NOTE The service agreement may be backed up by subordinate service agreements for the whole Service Supply Chain. Example: a contract to supply electricity, gas, water and sewerage services to a home.
Service Bundle	A set of services delivered through a common means therefore attracting synergistic benefits. Example: a collection of TV services delivered using a DVB application. It may be a combination of freeview and paid-for channels, sometime called a “bouquet”.
Service Level Agreement	A formal agreement between a Service Provider and Customers to provide a certain level of service relating to Service Level Specifications. Example: a broadband service is offered with a SLA that guarantees 8 Mbps downlink and 2 Mbps uplink with 99.999% availability.
Service Level	Parameter of a service as delivered to an end user by a service provider. Example: data-rates, availability.
Service Level	A collection of Service Levels that describe a service.

Specification	
Service Provider	Any organisation or entity that provides any good or service to a consumer. Example: a telecommunications operator; a supplier of gas.
Service Supply Chain	The services, products and other elements that are necessary to deliver a service. Example: The Application Home Initiative has identified 11 such entities that span the creator of the service, the service aggregator, service provider, service operator, network operator, service distributor, subscriber and the end user. The European Application Home Alliance has further subdivided the end user entity into customer and consumer. Each Entity shall have an overall contractual relationship with the service provider and will have back to back contracts with the adjacent entity in the service supply chain. These contracts will each ensure that the Service level requirements of the service are fulfilled and that each entity obtains a benefit from the service supply.
Subscriber	A person or organisation who contracts with a provider to use a service on a subscription (regular and renewed payment) basis. NOTE A subscriber may be the consumer or the subscription may be provided by organisations such as social service or healthcare provider. Example: a Consumer who has a Service Agreement with a provider of TV services.
System	A collection of components organized to accomplish a specific function or set of functions. [IEEE STD 610.12] NOTE 1 There are several alternative definitions. For example: a system (process operation, function or activity) is an arrangement, a set, or a collection of concepts, parts, activities and/or people that are connected or interrelated to achieve objectives and goals. This definition applies to both manual and automated systems. NOTE 2 A system may also be a collection of subsystems operating together for a common objective or goal. Example: a security system providing control of access to premises based on smart ID cards.
User	An entity that has the capability to originate, or respond to, events. Example: a human being, an application .

B.3.1.2 Security Definitions

Access Control	[ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. NOTE 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. Example: read access to a shared variable; permission to turn on, or off, i.e. execute certain operations. 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)

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. Example: read access to a shared variable; permission to turn on, or off, i.e. execute certain operations. 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)
Authentication	The validation of a claimed identity. Example: 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.
Authorisation	The decision to permit a user to make none (deny access), one or more types (permit access) of operations on an object. Example: 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.
Confidentiality	[ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Denial of Service	[ITU-T X.800]: 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)
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. [various sources] For example, intercepting credit card numbers or classified information – the interception of any communications information may render the eavesdropper useful information. See Privacy
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.
Information Security	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.
Integrity	[ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.
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.
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.
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

Privacy	[Draft ITU-T Recommendation X.805] The protection of information that might be derived from the observation of network activities. (see Eavesdropping)
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.
Repudiation	[ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.
Safety	The state of being certain that adverse effects will not be caused by some agent under defined conditions. NOTE 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.
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.
Security Requirements	The purpose, objectives and success criteria applied to an Application or Service. This Technical Specification specifies Requirements for Security in relation to Levels of Interoperability that cover both Physical 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.
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.
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.

B.3.1.3 Interaction Model Definitions

All methods or protocols that operate under particular specifications use models for the transmission of information and the configuration and managements of objects. The commonly used methods are listed below:

An interaction between two interacting application entities (device or object) consists of the complete set of messages accepted by the device or object and the synchronisation of the outcome for each interaction between the two communicating entities using these messages. The messages define the application-layer protocol by which devices and/or objects communicate over a binding. The method of synchronisation defines the interaction model.

Acknowledgement	A message generated in response to receipt of a message, indicating a confirmation of acceptance or rejection of the message. NOTE 1 A confirmation of acceptance, or positive acknowledgement, may confirm receipt. It may additionally confirm that an action was taken and was successful. NOTE 2 A rejection, or negative acknowledgement confirms that the receiver was unable to accept the message, or could not complete the action requested by the message. It may supply a reason and may return

	parameters of its changed configuration following the completion of the command. Example: a door-opener device acknowledges that it received an instruction to open the door. It does not confirm that it acted upon the instruction.
Anycast	The mode of communication in which a message is transmitted in Multicast mode and expects a response from objects that receive the message. NOTE This mode is often used to discover capabilities in devices, or objects, present in a system.
Broadcast	The mode of communication in which a message is addressed to all objects. NOTE Characterised by a single transmit operation that is used to distribute information to all receiving entities in a system. Example: there is a fire, open all the doors!
At Least Once	Execution semantics in which an operation requested by, or upon, an object may, when completed, have been performed one or more times. NOTE Also termed Idem potency Repeated instances of the operation do not make the state inconsistent. The requestor is always informed that the outcome was successful. Example: turn the light on, which may be requested by multiple users or applications.
At Most Once	Execution semantics in which an operation requested by, or upon, an object may, when completed, have been performed zero or once. NOTE The operation may not be executed more than once without the state becoming inconsistent and the requesting operation is informed that it was successful. Example: adding a time period to the schedule of a heating controller. If the time period is within an existing time period of the same type (e.g. the heating is on or off), then the operation is not executed.
Atomicity	The divisibility of the steps executed in performing an operation or sequence of operations. NOTE A sequence of operations is said to be atomic if it can not be interrupted or divided into smaller sequences of steps.
Command/ Response	An object initiates an interaction by transmitting a message (the Command) to another object; that object executes it and notifies the initiating object by transmitting a message optionally containing information about the outcome (the Response). NOTE 1 There are several terms in common use that distinguish the participating objects: e.g. Initiator, Responder; Requester, Server. NOTE 2 The response typically contains information of new state or failure reports if not able to carry out the command contained in the originating message. NOTE 3 There is an implication that the operation requested in the Command has actually been executed, by contrast with the Acknowledgement model above. In some protocols, both the Command and Response are acknowledged. Example: the door is now open; the door was locked and could not be opened.

Consistency	The state of variables changed by an operation or sequence of operations shall be with the range of variation specified by the application. NOTE This is most critical in systems in which multiple applications share the capabilities of objects and their services. No element of the application may set the state of the object to a value that is invalid for another element. Example: the energy manager turns an appliance off, but the occupant, who had previously turned it on, thinks it is still on. A notification shall be sent to the occupant, or to the device that manages state on the occupant's behalf.
Data Driven	Activity in objects present in the system is invoked by the information contained in messages and specifically not by Command/Response interactions between objects. NOTE Data-driven interactions often use Multicast or Broadcast distribution of messages to objects in the system. On receipt of a message addressed to a Multicast group of which they are a member, objects may execute actions in response to the information in that message and then may respond with another message addressed to the same Multicast group. Example: an electric kettle generates a message to inform other devices that it has boiled the water.
Distributed Shared memory	The mechanism by which objects share a common Namespace representing a range of addresses in memory that are used to exchange information. NOTE 1 Local changes of content of memory locations are propagated between objects by a suitable communication protocol. NOTE 2 Naïve implementations are vulnerable to attack and inadvertent or deliberate misuse. Example: read the data at this location, write this data to that address. There is an expectation that something will happen, e.g. the location written to may be the actuator that opens the door; the location read from may contain the bits that say that the door is opening, i.e distributed shared memory is a data-driven system.
Durability	The outcome of an operation persists and survives failures of the system and its elements. Example: a tariff loaded into a smart meter remains in that meter during a supply interruption.
Event Driven	Certain types of information sent by objects are related to specific changes of state or events detected by objects in the system. NOTE 1 This interaction model is implicitly data-driven. Messages containing events are transmitted using Multicast or Broadcast modes. NOTE 2 A message designated as an event may receive preferential treatment, and the system may be able to respond better to real-time changes and stimuli than conventional request/reply mechanisms. The system may be designed and implemented with a pre-defined schedule of events – also termed time-triggered. Example: Everyone! Somebody opened the door!
Exactly Once	Execution semantics in which an operation requested by, or upon, an object shall, when completed, have been performed only once. NOTE The semantics is exceptionally strict and many systems implement a two-phase approach in which the operation can be cancelled by either party (rollback) until the requester indicates that the responder shall commit the execution of the operation. Even after this, elements of the system may fail and a recovery phase will be invoked when service is restored.

	Example: make a reservation, take $10 from my bank account – at the heart of commercial enterprises.
Execution semantics	Defines the outcome of operations requested by, or upon, an object. NOTE 1 It is the outcome that is important, not the process that arrives at the outcome. There may be repeated disruptions to the progress of the operation due to failure of any of the elements in the chain between requester and responder. These may be reported to both parties during execution. NOTE 2 See definitions of Exactly Once, At Most Once, At Least Once.
Isolation	The outcome of operations, or sequences of operations, performed by or upon an object within an atomic action is independent of concurrent operations affecting that object.
Message	Information transmitted between objects in a system. NOTE In the OSI Reference Model, the terms Service Data Unit (SDU) and Protocol Data Unit (PDU) are used to refer to information passed between layers in the communications stack and between objects connected to communications media respectively. A message represents a collection of SDU fields and is encoded for transmission as a PDU.
Multicast	The mode of communication in which a message is addressed to a group of objects that have subscribed to use a designated address. Example: Security devices! Somebody opened a door!
Remote Operation	A mode of interaction using the Command/Response model. NOTE The Remote Operation model was standardised in ISO/IEC xxxxxx. It comprises four variants: unacknowledged (no response) and acknowledged (with response); synchronous (the requestor blocks until a response is received) and asynchronous (the response will be delivered at some later time).
Remote Procedure Call	A mode of interaction similar to synchronous Remote Operation where the locus of control is passed from the requestor to the server, and the requester blocks until control is returned. NOTE This mode is logically equivalent to a procedure or function call executed locally by a program.
Shared Variable	Designated addresses in a system using the Distributed Shared Memory interaction model. Example: a interaction model used in ISO/IEC 14908.
Unacknowledged	No response or acknowledgement is generated in response to a received message. Example: open the door! I expect it to be open when I get to it.
Unicast	The mode of communication in which a message is addressed to a single object that has a designated address. NOTE Command/response interactions are often implemented using unicast communications. Example: a comfort controller asks the kitchen sensor how for the temperature.

B.3.1.4 Process Definition

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 An Application is composed from many of the items defined below. In particular it may include Services, made available under Service Level Agreements by Service Providers, that themselves are composed of Applications. NOTE 2 The distinction between Application and Service is made for the purposes of this Technical Specification. NOTE 3 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 Service is required.
Application Service	A function provided through a well-defined API by a device or object to another device or object. Example: getting a temperature value, arming the alarm system, etc.
Application Programming Interface	A defined set of calling conventions allowing a software application to access a particular set of services. An API consists of the routines, protocols and tools that programmers shall use to ensure that their programs are compatible with the software that the API is defined for. A well defined API helps applications work together by providing the same basic tools for all programmers to use. Example: the TCP socket programming interface: open(), close (), listen(), accept(), select(), read(), write().
Binding	The mechanism by which objects request the capability to interact with each other.
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.
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.
Discovery	Enabling users, applications, objects, and devices participating in systems to discover new units and to recognise what they are. NOTE Objects may present or publish their parameters or respond to a broadcast for information about specific object types). Example: UPnP.
Discovery Process	The process of execution of discovery activities.

Middleware	Middleware is a generic term for functions that make a communications infrastructure that is part of a distributed system usable by applications. 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.
Operations	Application Services requested between objects in the system that collectively implement its function.
System Management	Application Services requested between objects in the system that are not related to the Applications that it executes. Examples: collection of statistics, diagnostic troubleshooting, firmware and software upgrade installation.

B.3.1.5 Interoperability

Address	An Identifier that is used to locate an object for the purposes of communicating information. Example: a telephone number locates a specific phone line in the PSTN.
Application Object	A description of an application in terms of describing the action an application carries out. The “Application Object” carries a description of the action and of how it is identified, configured, managed and what its parameters are. Example: a shared variable that represents the temperature at a location defined by the name of the variable.
Device Object	A physical object or instance of a physical object. Example: a temperature sensor.
Functional Object	An object that carries out a particular identifiable application task. A collection of objects and actions on objects that models a particular identifiable application function within an application domain. Example: none.
Handle	An Identifier with an assigned meaning in a specific context. NOTE A handle is often used with only temporary local meaning. It is often said to be “opaque”, meaning it cannot be used except by the functions that understand how it was created, or “transparent”, meaning that there is an agreed semantics that all can use. Example: when a shared object is opened, a handle is created by the local middleware that is communicated to remote objects that wish to use the shared object. All requests they make are with reference to the handle and they can never know where the object actually is. Example: the address in memory of a shared object is returned by the local middleware that is communicated to remote objects that wish to use the shared object. All requests they make are with reference to the memory location and they can overwrite its contents as they wish.
Name	An Identifier that is used to identify an object to an application, possibly

	uniquely, possibly within a defined context or scope. NOTE The name may be a Handle as defined above: it may be opaque or transparent according to application requirements.
Object	A formally defined unit of software functionality, NOTE Generally an "Object" has an identity and parameters and may be configured or managed and these properties may be discovered. This definition of an object may therefore apply to any element of a system, it may be a wholly discrete entity or it may be a more complex object made up of a number of elements which act as one object and this may apply to applications and services as well as physical entities. Example: in programming languages such as C++ or Java, an object is specified as a constructed datatype including private and public information and offering a collection of services to applications that use it. Example: in a HBES system an object is a function that possesses a handle that other objects use to access it, which may be its address in the network supporting the system, one or more identifiers that may define its Type, serial number, or product code, and that offers a collection of Application Services, also with distinguishing identifiers.
Type	A name that is used to identify the capabilities of an object for the purposes of an application. Example: in C:*typedef temperature double*;i.e. a double-precision real number that represents a quantity denoted by temperature as understood by an application.

B.3.1.6 Other Definitions

For the purposes of the present document, the terms and definitions given in ETSI/TS 101 761-2, ISO/IEC 9646-1, ISO/IEC 9646-7 and the following apply:

Abstract Syntax Notation One (ASN.1): a FDL used to specify data types for communications protocol applications.

Common Object Request Broker Architecture (CORBA): a system for distributed processing defined by OMG.

Formal Description Language (FDL): a machine processable formally defined syntax and semantics for expressing abstract properties of a system.

Implementation Conformance Statement (ICS): statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented.

NOTE The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS, etc.

ICS proforma: document, in the form of a questionnaire, which when completed for an implementation or system becomes an ICS.

Protocol ICS (PICS): ICS for an implementation or system claimed to conform to a given protocol specification.

Interoperability ICS (IICS): ICS for an implementation or system claimed to conform to the IFRS requirements.

Object Management Group (OMG): an industry consortium that has set standards for distributed object-oriented systems, modeling (programs, systems and business processes) and model-based standards.

Remote Procedure Call (RPC): as defined in ETSI/TS 101 761-2.

B.4 Requirements for Conformance to this IICS

B.4.1 General

This Interoperability Framework Requirements Specification is applicable to systems and devices claiming interoperability at Levels 4, 5 and 6. It has the following general requirements for conformance at these levels except where qualified below:

B.4.2 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 uniquely identifiable within the namespace(s) of the overall system and its sub-systems.

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

- Unique name 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 or required to be stated 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 from which they are derived;

- Handle, or other means of referring to it during its lifetime in the operational system, and the means by which it is created;

- Other permanent identifiers, such as a serial number.

B.4.3 Object Functional Description Requirements

B.4.3.1 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.

B.4.3.2 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 or Other defined by de-facto standard or practice. 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.

B.4.3.3 Object Discovery Interface

An object should provide a description using one of the International Standard Formal Description Languages (FDL)of its data types, operations and attributes that support discovery. Specific aspects of the discovery process are given in B.4.4.

B.4.3.4 Object Configuration Interface

An object should provide a description using one of the International Standard Formal Description Languages (FDL) of its data types, operations and attributes that support configuration. Specific aspects of the configuration process are given in B.4.5.

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

B.4.3.5 Object Management Interface

An object should provide a description using one of the International Standard Formal Description Languages (FDL) of its data types, operations and attributes that support management. Specific aspects of the discovery process are given in B.4.4.

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

B.4.3.6 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. Specific aspects of these operations are given in B.4.6.

B.4.4 Discovery Requirements

B.4.4.1 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.

B.4.4.2 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.

B.4.4.3 Communication Mode

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

B.4.4.4 Discovery Process

An object should state the interaction model and message exchanges that it uses to initiate and/or respond to interactions for the discovery operations it implements. It should additionally state for each such operation where applicable: the execution semantics, the response(s) and error(s) that it will accept and action taken, the time it will wait for responses, the time taken to respond, the rate at which it generate interactions; the errors that it will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

An object may supply a catalogue of products (end devices, gateways, software, Web services) and their objects with which it has tested interoperability for discovery operations.

B.4.4.5 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.

B.4.4.6 Security and Privacy

An object participating in the discovery process should state the provisions made for achieving authorisation and authentication of requests made upon it.

An object participating in the discovery process should state the circumstances under which it will accept and reject requests made upon it and the response(s) that it will give.

B.4.5 Configuration Requirements

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

B.4.5.1 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.

B.4.5.2 Communication Mode

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

B.4.5.3 Configuration Process

An object should state the interaction model and message exchanges that it uses to initiate and/or respond to interactions for the configuration operations it implements. It should additionally state for each such operation where applicable: the execution semantics, the response(s) and error(s) that it will accept and action taken, the time it will wait for responses, the time taken to respond, the rate at which it generate interactions; the errors that it will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

An object may supply a catalogue of products (end devices, gateways, software, Web services) and their objects with which it has tested interoperability for configuration operations.

B.4.5.4 Security and Privacy

An object participating in the configuration process should state the provisions made for achieving authorisation and authentication of requests made upon it.

An object participating in the configuration process should state the circumstances under which it will accept and reject requests made upon it and the response(s) that it will give.

B.4.6 Operation Requirements

B.4.6.1 Application Operation

Objects should state by reference in human readable text to relevant specifications the algorithms and performance capabilities that they implement.

An object should state the interaction model and message exchanges that it uses to initiate and/or respond to interactions for the application operations it implements. It should additionally state for each such operation where applicable: the execution semantics, the response(s) and error(s) that it will accept and action taken, the time it will wait for responses, the time taken to respond, the rate at which it generate interactions; the errors that it will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

An object may supply a catalogue of products (end devices, gateways, software, Web services) and their objects with which it has tested interoperability for application operations.

B.4.6.2 Security and Privacy

An object participating in operations to provide application services should state the provisions made for achieving authorisation and authentication of requests made upon it.

An object participating in operations to provide application services should state the circumstances under which it will accept and reject requests made upon it and the response(s) that it will give.

An object participating in operations to provide application services to more than one application concurrently should state the provisions made for achieving atomicity, consistency, isolation and durability of the operations requested by those applications.

B.4.7 Management Requirements

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

B.4.7.1 Communication Mode

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

B.4.7.2 Management Process

An object should state the interaction model and message exchanges that it uses to initiate and/or respond to interactions for the management operations it implements. It should additionally state for each such operation where applicable: the execution semantics, the response(s) and error(s) that it will accept and action taken, the time it will wait for responses, the time taken to respond, the rate at which it generate interactions; the errors that it will generate; the action taken upon receipt of error messages or rejections; and any other constraints implemented at the discretion of the supplier.

B.4.7.3 Security and Privacy

An object participating in management operations should state the provisions made for achieving authorisation and authentication of requests made upon it.

An object participating in management operations should state the circumstances under which it will accept and reject requests made upon it and the response(s) that it will give.

An object participating in management operations requested by more than one management application concurrently should state the provisions made for achieving atomicity, consistency, isolation and durability (ACID) of the operations requested by those applications.

B.5 Instructions for Completion of the IICS

B.5.1 General

The IICS uses a tabular approach with supplementary text. Detailed instructions and guidelines are given in the respective sections.

Where possible, claims of compliance should be made by reference to the underlying base standards.

Supplementary information may be supplied in the fields provided. Sometimes this is required; but it may also be supplied at the discretion of the supplier.

B.5.2 Key to the Table Entries

-	No information required or supplied.
M	Required information
O	Information may be supplied according to implementer wishes. If not supplied then no claim is made about interoperability and no judgement can be made.
C	If supported, then this is required information (M); otherwise “-“.

The information supplied may have the following forms:

1. A specific reference to a standard that applies to the particular entry, with indication of the applicable clauses. This is the preferred affirmative response;

2. **“Yes”**, meaning that the capability has been verified;

3. **“No”**, which means that the capability is not present or has been tested and found to be faulty. In this case, it is possible that the product does not completely satisfy the IFRS conformance requirements. However, where the capability is supported by other means then this should be stated separately.

4. **“-“**, meaning that no information is given.

Fields marked as “<string>” are supplied by the organization completing the tables in this IICS. The “string” may indicate the type of information required, e.g. “<Identifier>” requests an “Identifier” meaningful in the context in which “Identifier” is used.

B.6 Global Statement of IICS Conformance

Complete the table below:

Conformance Clause		Level 4	Level 5	Level 6
Discovery	Process	M	M	M
	Security	M	M	M
	Enablers	M	M	M
	Interaction Model	M	M	M
Configuration	Process	M	M	M
	Security	M	M	M
	Enablers	M	M	M
	Interaction Model	M	M	M
Operation	Process	M	M	M
	Security	M	M	M
	Enablers	M	M	M
	Interaction Model	M	M	M
Management	Process	-	-	M
	Security	-	-	M
	Enablers	-	-	M
	Interaction Model	-	-	M

B.7 Specific Statements of IICS Conformance

B.7.1 General

The following information should be supplied in partial fulfilment of the requirements of B.4.2 and B.4.3 of this Technical Specification IICS.

Device Identifier	<Identifier used by the organisation to denote this device>							
Standard(s) implemented	<List of standards implemented>							
Interoperability compliance	<List compliance with standard interoperability specifications>							
FDL used in catalogues	ASN.1	C	XML	C	IDL	C	Other	C
Device description	<Descriptive information about the device>							
Interoperable Devices[a]	<List of products that have been tested for interoperability compliant with the provisions of the IICS>							
[a] The relationship between this device and the interoperable devices is presumed to be end-to-end independent of topology of intervening gateways.								

B.7.2 Object Catalogue

The information given in the object catalogue supports partial compliance with provisions given in B.4.2 and B.4.3 of this Technical Specification IICS.

For each object supported by a device the following information should be supplied.

Object Identifier	Purpose	Can Request	Will Accept
<Object identifier>[a]	<What the object does>	<Operation identifier>[b]	<Operation identifier>[b]
		… as needed	… as needed
		<Operation identifier>[b]	<Operation identifier>[b]
Object classification	<Descriptive information about the object as outlined in Object Classification, B.4.3>		
Access control	<Overview of constraints upon requesting and accepting operations>		
Security provisions	<Overview of mechanisms to ensure security>		
[a] The <Object identifier> should be easily traceable in the underlying base standard or device product description; [b] The <Operation identifier> should be traceable in the underlying base standard, and be the same as the <Operation identifier> used in B.7.3 below.			

B.7.3 Operation Catalogue

The information given in the object catalogue supports partial compliance with provisions given in B.4.2 and B.4.3 of this Technical Specification IICS.

For each operation supported by the objects in a device the following information should be supplied.

Operation Identifier	Purpose	Description	Message Encoding
<Operation Identifier>[a]	<What the operation does>	<FDL clauses>[b]	<Encoding>[b]
		… as needed	… as needed
		<FDL clauses>[b]	<Encoding>[b]
Functional Interface Description[c]	<Descriptive information about the operation as outlined in Object Functional Interface sub-clause of B.4.3, including access control and security provisions>		
Discovery Interface Description[c]	<Descriptive information about the operation as outlined in Object Discovery Interface sub-clause of B.4.3, including access control and security provisions>		
Configuration Interface Description[c]	<Descriptive information about the operation as outlined in Object Configuration Interface sub-clause of B.4.3, including access control and security provisions>		
Management Interface Description[c]	<Descriptive information about the operation as outlined in Object Management Interface sub-clause of B.4.3, including access control and security provisions>		

Execution semantics	At most once	Exactly once	At least once	Concurrency	<Number of concurrent instances>

Timing	Wait	<Maximum time will wait>	Respond	<Maximum time to respond>
Rate	Generate	<Minimum rate>	Accept	<Minimum rate>
		<Average rate>		<Average rate>
		<Peak rate>		<Peak rate>

Responses	<Accepted>[d]	<Rejected>[d]
Errors	<Accepted>[d]	<Rejected>[d]
Notes	<Additional information>	

[a] The <Operation Identifier> should be easily traceable in the base standard;

[b] Where possible this description should be given using the FDL stated in B.7.1 for as many rows as required to reflect the communications steps needed to achieve the operation. It should specify the name of the operation, its input parameters, output . It should specify the name of the operation, its input parameters, output parameters, and in/out parameters and result(s) or error(s) returned. If considered more appropriate and clear, the information can be supplied in the Notes field;

[C] Information about the operation should be supplied in the applicable row. In general it is anticipated that one row will be selected from the four, but more than one may be completed;

[d] Information should include a description of the respective outcomes, or codes, and action taken. As many entries as required may be added.

B.7.4 Object and Operation Interoperability Catalogue

If end-to-end interoperable products have been listed in the table of B.7.1, then the following information may be supplied for each peer product, identifying the interoperable object identifiers and operation/service identifiers.

Peer Product	<Product Identifier>		Product Code	<Code>	Revision	<Version>
Description	<Descriptive text>					
Gateways[a]						
<Gateway Identifier$_1$>	<Product Identifier>	Product Code		<Code>	Revision	<Version>
	Input	<Standard complied with>		Output	<Standard complied with>	
	Notes	<Descriptive text>				
<Gateway Identifier$_2$>	<Product Identifier>	Product Code		<Code>	Revision	<Version>
	Input	<Standard complied with>		Output	<Standard complied with>	
	Notes	<Descriptive text>				
…						
<Gateway Identifier$_1$>	<Product Identifier>	Product Code		<Code>	Revision	<Version>
	Input	<Standard complied with>		Output	<Standard complied with>	
	Notes	<Descriptive text>				

Objects		Operations		Additional Information, Warnings
<My Object Identifier$_1$>	<Peer Object Identifier$_1$>	<My Operation$_{11}$>	<Peer Operation$_{11}$>	<Should state Interoperability Level claimed for this combination>
		<My Operation$_{12}$>	<Peer Operation$_{12}$>	

		…	…	
		<My Operation$_{1n}$>	<Peer Operation$_{1n}$>	
<My Object Identifier$_2$>	<Peer Object Identifier$_2$>	<My Operation$_{21}$>	<Peer Operation$_{21}$>	
		<My Operation$_{22}$>	<Peer Operation$_{22}$>	
		…	…	
		<My Operation$_{2n}$>	<Peer Operation$_{2n}$>	
[a] Descriptions of the gateway products may be supplied.				

B.7.5 Upper Layer PICS (APP)

B.7.5.1 General

Devices that claim interoperability at a certain level for end-to-end interactions, i.e. application, presentation, session and transport layer functionality (denoted here by APP) should provide the information indicated in the table below for each attachment to supported media (one for an end device, more than one for a device with gateway capability) that operates an application layer protocol.

Level	Discovery	Configuration	Management	Security
4	O	O	O	C[b]
5	M[a]	M[a]	M[a]	C[b]
6	M[a]	M[a]	M[a]	C[b]
[a] If these functions are supported at APP level then the respective standard and part if applicable should be stated by reference to the standards listed in B.7.1; [b] If security mechanisms are either provided in the APP, or by a separate capability, then the respective standard should be stated. If no security mechanisms are used then the field should be set to "-".				

B.7.5.2 Additional Requirements for Gateways at APP Layer

For devices that implement gateway capabilities, supply as many instances as needed of the following table for each pair of interfaces and each direction. The presumed flow of information is from APP In (received into the gateway) to APP Out (transmitted by the gateway), and multiple entries in each row may be filled. Any entry may be "-" if a flow or mapping is not supported.

APP Identifier	APP Out						
APP In	NWK/DLC Distribution Mode (M[a])			Discovery	Configuration	Management	Security
	Unicast	Multicast	Broadcast				
Discovery	M[b]	M[b]	M[b]	*M*[c]	*M*[c]	*M*[c]	*M*[c]
Configuration	M[b]	M[b]	M[b]	*M*[c]	*M*[c]	*M*[c]	*M*[c]
Management	M[b]	M[b]	M[b]	*M*[c]	*M*[c]	*M*[c]	*M*[c]
Security	M[b]	M[b]	M[b]	*M*[c]	*M*[c]	*M*[c]	*M*[c]
Notes							

[a] Indicate which lower level service is used. If more than one service is used, supply details in a separate note;

[b] Indicate how the protocols are mapped to the respective distribution modes;

[c] The protocol that is used on the In path should be stated, qualified by the communications layer at which it applies; if the function is not implemented by a capability then it should be entered as "-". This information could be supplied as a separate note.

	APP Out		
APP In	Acknowledge	Flow-control	Timing
Acknowledge	-	M[a]	M[b]
Flow-control	M[a]	M[a]	M[b]
Data	M[a]	M[a]	M[b]
Control[c]	M[a]	M[a]	M[b]

[a] State combinations that apply, with specific protocols. It is assumed that acknowledgements will not themselves be acknowledged;

[b] The response time by Out to the respective messages from In should be stated (min/typ/max);

[c] Control functions may include establishing sessions for individual applications at APP layer.

	TRS Out		
TRS In	Acknowledge	Flow-control	Timing
Acknowledge	-	M[a]	M[b]
Flow-control	M[a]	M[a]	M[b]
Data	M[a]	M[a]	M[b]
Control[c]	M[a]	M[a]	M[b]

[a] State combinations that apply, with specific protocols. It is assumed that acknowledgements will not themselves be acknowledged;

[b] The response time by Out to the respective messages from In should be stated (min/typ/max);

[c] Control functions may include establishing sessions for individual applications

B.7.6 Network Layer and Routing PICS (NWK)

B.7.6.1 General

Devices that claim interoperability at a certain level should provide the information indicated in the table below for each attachment to supported media that operates a network layer protocol.

Level	Routing	Discovery	Configuration	Management	Security
4	C[a]	O	O	O	C[c]

5	C[a]	M[b]	M[b]	M[b]	C[c]
6	C[a]	M[b]	M[b]	M[b]	C[c]

[a] If the device has no routing capability then this entry should be "-". If the device is a router then the entry should be "Yes", and the routing protocol should be stated;

[b] If these functions are supported at NWK level then the respective standard should be stated;

[c] If security mechanisms are either provided in the NWK, or by a separate capability, then the respective standard should be stated.

B.7.6.2 Additional Requirements for Gateways at NWK Layer

Additionally, where the entry under Routing is not "-",the following information is required according to the table below for each function. The presumed flow of information is from Network In to Network Out, and multiple entries in each row may be filled. Any entry may be "-" if a flow or mapping is not supported.

	Network Out						
Network In	Unicast	Multicast	Broadcast	Discovery	Configuration	Management	Security
Unicast	M[a]	M[a]	M[a]	-	-	-	-
Multicast	M[a]	M[a]	M[a]	-	-	-	-
Broadcast	M[a]	M[a]	M[a]	-	-	-	-
Discovery	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Configuration	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Management	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Security	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Address range	M[d]	M[d]	M[d]	M[d]	M[d]	M[d]	M[d]

[a] These entries indicate the mapping of the respective distribution modes from In to Out, e.g. if a unicast message received from In is converted into a message that is multicast on Out;

[b] Indicate how the protocols are mapped to the respective distribution modes, e.g. Discovery may be achieved through broadcast;

[c] The protocol that is used on the In path should be stated, qualified by the communications layer at which it applies; if the function is not implemented by a NWK capability then it should be entered as "-". For example: a discovery request on In from an external DSL connected Internet-capable device encoded in HTTPS is converted into a DLC layer discovery request on the Out path, which is a specific HBES technology. The entry might read: "Y, In: HTTPS (APP) -> <NWK function>". This information could be supplied as a separate note;

[d] The mapping between address ranges from In to Out for the respective functions should be stated. If no mapping is done then the entry will be "-".

	Network Out				
Network In	Fragmentation	Acknowledge	Flow-control	Source/hop-by-hop	Timing
Fragmentation	M[a]	M[a, b]	M[a]	-	C[b]
Acknowledge	-	-	M[a]	-	M[d]
Flow-control	-	M[a]	M[a]	-	M[d]
Source/hop-by-hop	-	-	-	M[c]	M[d]
Data	M[a]	M[a]	M[a]	-	M[d]
Control	M[a]	M[a]	M[a]	-	M[d]

[a] State combinations that apply, with specific protocols. It is assumed that acknowledgements and flow-control on In will not be fragmented; and that acknowledgements will not themselves be acknowledged;

[b] If fragments from In are individually acknowledged then the response time (min/typ/max) by Out should be given;

[c] Indicates the combination of source and hop-by-hop routing on In and Out;

[d] The response time by Out to the respective messages from In should be stated (min/typ/max).

B.7.7 Data Link Control and MAC PICS (DLC/MAC)

B.7.7.1 General

Devices that claim interoperability at a certain level should provide the information indicated in the table below for each attachment to supported media that operate a DLC protocol.

Level	DLC			Discovery	Configuration	Management	Security
	Control	Data	Gateway				
4	M[a]	M[a]	C[b]	O	O	O	C[d]
5	M[a]	M[a]	C[b]	C[c]	C[c]	C[c]	C[d]
6	M[a]	M[a]	C[b]	C[c]	C[c]	C[c]	C[d]

[a] The supported standards or specifications should be stated;

[b] If the device has no gateway capability then this entry should be "-". If the device is a gateway then the entry should be "Yes", with further details given to clarify the type of function: bridge, relay or router (in which case the routing protocol should be stated, e.g. IEEE 802.1q);

[c] If these functions are supported at DLC level then the respective standard should be stated. If they are not supported then the entry should be "-" and further details given in the Gateway table below;

[d] If security mechanisms are either provided in the DLC, or by a separate capability, then the respective standard should be stated.

B.7.7.2 Additional Requirements for Gateways at DLC/MAC Layer

Additionally, where the entry under DLC Gateway is a "Y", the following information should be provided according to the table below for each DLC gateway function. The presumed flow of information is from DLC In to DLC Out, and multiple entries in each row may be filled. Any entry may be "-" if a flow or mapping is not supported, e.g. if a particular function on DLC In is implemented in a different way on DLC Out.

	DLC Out							
DLC In	Unicast	Multicast	Broadcast	Gateway	Discovery	Configuration	Management	Security
Unicast	M[a]	M[a]	M[a]	-	-	-	-	-
Multicast	M[a]	M[a]	M[a]	-	-	-	-	-
Broadcast				-				
Gateway	-	-	-	M[b, d]	M[d]	M[d]	M[d]	M[d]
Discovery	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Configuration	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Management	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Security	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Address ranges	-	-	-	M[e]	M[e]	M[e]	M[e]	M[e]

[a] These entries indicate the mapping of the respective message types from In to Out according to distribution mode, e.g. if a unicast message received from In is converted into a message that is multicast on Out. The entry should also indicate if there is any differentiation of message types;

[b] The type of gateway function: bridge, relay, or router, with standards if applicable, should be stated;

[c] Indicate how the protocols are mapped to the control or data messages, e.g. Discovery may be achieved through a message that is designated as control;

[d] The protocol that is used on the In path should be stated, qualified by the communications layer at which it applies. If the function is not implemented by a DLC capability then "-" should be entered. For example: a discovery request on In from an external DSL connected Internet-capable device encoded in HTTPS is converted into a DLC layer discovery request on the Out path, which is a specific HBES technology. The entry might read: "Y, In: HTTPS (APP) -> <DLC function>". This information could be supplied as a separate note;

[e] The mapping between address ranges from In to Out for the respective functions should be stated. If no mapping is done then the entry can be "-".

B.7.8 Media and PHY PICS (PHY)

Devices that claim interoperability at a certain level should provide the information indicated in the table below for each attachment to supported media.

Level	Connector	Media	PHY	Discovery	Configuration	Management	Security
4	M[a]	M[a]	M[a]	O	O	O	C[c]
5	M[a]	M[a]	M[a]	C[b]	C[b]	O	C[c]
6	M[a]	M[a]	M[a]	C[b]	C[b]	C[b]	C[c]

[a] The supported standards should be listed, e.g. RJ45 (connector), Cat 5 UTP (media), IEEE 802.3 (PHY);

[b] If the PHY supports these functions, e.g. IEEE 802.11 AP/STA scanning, then the respective standard should be stated. If not then "-";

[c] If security mechanisms are either provided via connector, media or PHY functions, or by a separate capability, then the respective standard should be stated.

Bibliography

Standard	Responsible body (input from)	Status
ISO/IEC 18012-1:2004 Information technology -- Home Electronic System -- Guidelines for product interoperability -- Part 1: Introduction	ISO/IEC JTC 1/SC 25	IS
ISO/IEC 18012-2:2012 Information technology – Home Electronic System – Guidelines for product interoperability – Part 2: Taxonomy and Lexicon	ISO/IEC JTC 1/SC 25 WG1	Work in progress (FCD)
ISO/IEC 14543-2-1 Part 2-1: Introduction and device modularity	ISO/IEC JTC 1 SC25	IS
ISO/IEC 14543-3-x (7 parts) Home Electronic Systems (HES) Architecture	ISO/IEC JTC 1 SC25	IS
EN 50090 Series	CENELEC TC205	IS, equivalent to ISO/IEC 14543
ISO/IEC 14908-x (6 parts) Open data Communication in Building Automation	ISO/IEC JTC 1 SC25 CEN TC247	EN, publication by ISO under discussion.
ISO/IEC 29341-2:2008 Information technology -- UPnP Device Architecture -- Part 2: Basic Device Control Protocol - Basic Device	ISO/IEC JTC 1/SC 25	IS
ISO/IEC 29341-1:2008 Information technology -- UPnP Device Architecture -- Part 1: UPnP Device Architecture Version 1.0	ISO/IEC JTC 1/SC 25	IS
ISO/IEC 29341-x-y Information technology -- UPnP Device Architecture -- Part 1: UPnP Device Architecture Version 1.0 (remaining 70 parts)	ISO/IEC JTC1 SC25	IS
ISO/IEC 14543-4-1 & -2 Home Electronic System (HES) Architecture	ISO/IEC JTC1 SC25 (ECHONET Association http://www.echonet.gr.jp)	IS Industry Association
ISO/IEC 14543-5-x (7 drafts) Intelligent Grouping and Resource Sharing	ISO/IEC JTC1 SC25 (IGRS Alliance)	Work in progress, some parts IS
CENELEC Smart House CoP	CEN/CENELEC CWA 50487	WA
EN 62481-1 & -2 Digital Living Network Alliance (DLNA) Home Networked Device Interoperability Guidelines - Part 1: Architecture and Protocols & Part 2: DLNA media formats	CLC/TC100	IS
CENELEC EN 50523-1	Household appliances interworking -	IS

	Part 1: Functional specification and EN 50523-2: Household appliances interworking - Part 2: Data structures	
EN ISO 16484-x (5 parts) Building automation and control systems	ISO TC 205, ASHRAE BACNET organisation	IS
ISO/IEC 14908-1 (Lonworks)	Communication protocol	IS
ISO/IEC 14908-2 (Lonworks)	Twisted-pair wire signaling technology	IS
ISO/IEC 14908-3 (Lonworks)	Power line signaling technology	S
ISO/IEC 14908-4 (Lonworks)	IP compatibility (tunneling) technology	IS
X.509, Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks	ITU-T	IS, ISO equivalent is ISO/IEC 9594-8
ISO 7498-x (4 parts) Information technology - Open Systems Interconnection - Basic Reference Model: Part 1: The basic model	ISO	IS, ITU-T equivalent is X.200
ISO 8824-x (4 parts) Information technology -- Abstract Syntax Notation One (ASN.1)	ISO	IS, ITU-T equivalent is X.208, obsoleted by X.680
ISO 10746-x (4 parts) **Information technology -- Open Distributed Processing -- Reference Model**	ISO	IS
ISO 14750 Information technology -- Open Distributed Processing -- Interface Definition Language	ISO, OMG	IS, see also OMG CORBA IDL specification
Simple Object Access Protocol (SOAP), V1.2	OMG, also standardised by the IETF	IETF RFC
ISO 11578 Information technology -- Open Systems Interconnection -- Remote Procedure Call (RPC)	ISO	IS

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information:

[1] ISO/IEC 11578:1996, *Information technology — Open Systems Interconnection — Remote Procedure Call (RPC)*

[2] ISO/IEC 29180:2012, *Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor networks*

[3] ITU-T Recommendation X.805:2003 (Formerly X.css), *Security architecture for systems providing end-to-end communications*

[4] Sensor Network Security: More Interesting Than You Think - Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives, and Insup Lee - Department of Computer and Information Science - University of Pennsylvania - 2006

[5] SPINS: Security Protocols for Sensor Networks - Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar - Department of Electrical Engineering and Computer Sciences - University of California, Berkeley – 2001

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™