INTERNATIONAL STANDARD

ISO/IEC 18012-1

First edition
2004-02

Information technology – Home electronic system – Guidelines for product interoperability –

Part 1: Introduction

Reference number
ISO/IEC 18012-1:2004(E)

INTERNATIONAL STANDARD

ISO/IEC 18012-1

First edition
2004-02

Information technology – Home electronic system – Guidelines for product interoperability –

Part 1: Introduction

PRICE CODE F

For price, see current catalogue

CONTENTS

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM – GUIDELINES FOR PRODUCT INTEROPERABILITY –

Part 1: Introduction

FOREWORD

1) ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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

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

4) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

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

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

International Standard ISO/IEC 18012-1 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

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

ISO/IEC 18012 consists of the following parts, under the general title *Information technology – Home electronic system – Guidelines for product interoperability*:

- *Part 1: Introduction*
- *Part 2: Taxonomy and lexicon*
- *Part 3: Application models*

INTRODUCTION

The widespread development of many national standard and proprietary networks within and to the home has necessitated a standard for interoperability among home system applications. This standard will ensure that applications on the same or dissimilar networks co-exist within premises and are required to interoperate, they will do so in a safe, reliable, predictable and consistent manner. This part defines the components of interoperability for the purpose of providing a framework within which subsequent parts of the standard will be drafted. This part applies to components within networks, between networks and located within dissimilar networks. It also applies to devices located at the junction of dissimilar networks.

In the field of home and building automation, products from multiple manufacturers may need to interoperate. Where widely varying devices need to interoperate, it is desirable that they do so seamlessly to present a single, uniform network and hence to deliver a variety of applications. Examples of such applications are lighting control, environmental control, audio/video equipment control and home security.

With reference to Figure 1, where there are two (or more) dissimilar networks within the same premises, they must conform to this standard if, when linked by some physical means, they are expected to behave as if both networks were logically the same network.

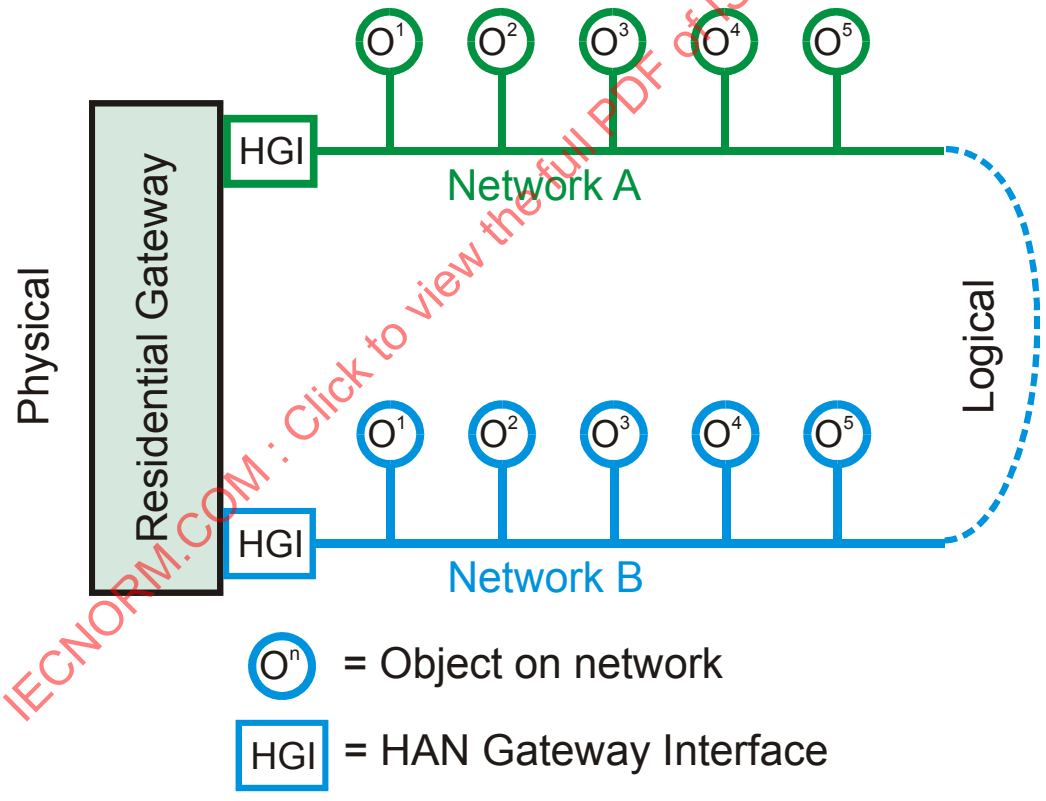

Figure 1 – Two interoperating networks

This document comprises the following sections.

- A conformance section (clause 4) with which all interoperating networks and intermediary equipment on the home electronic system comply.
- A requirements section (clause 5) that defines the normative functional safety requirements of product interoperability of HES products and networks, where these are not covered by existing functional safety standards.
- A requirements section (clause 6) that defines the management of product interoperability among HES products and networks.
- A requirements section (clause 7) that defines the normative operational requirements of product interoperability among HES products and networks.

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM – GUIDELINES FOR PRODUCT INTEROPERABILITY –

Part 1: Introduction

1 Scope

This part of ISO/IEC 18012 specifies requirements for product interoperability in the area of home and building automation systems. It specifies layers six and seven of the OSI reference model (see ISO/IEC 7498-1) with sufficient detail needed to design interoperable home electronic system products, while layers one to five are only specified to the point needed to check whether devices will be able to interoperate with one another.

ISO/IEC 18012-1 is applicable to

- stand-alone local/home networks, connected devices and applications,
- mixed local/home networks, connected devices and applications,
- automatically configured devices,
- installer configured devices,
- installer configured groups/clusters of devices.

ISO/IEC 18012-1 specifies interoperability for system set-up, operation and management applied to devices connected to a single home control system or to different home control systems. Although a single uniform home control system would simplify operations, this standard recognises that multiple different networks may co-exist in the same house. This standard specifies requirements to assure that devices from multiple manufacturers work together to provide a specific application. Also, a specific device could be used for multiple applications.

ISO/IEC 18012-1 specifies interoperability requirements with respect to

- safety,
- addressing,
- applications,
- transport of information,
- set-up of devices/elements within home networks – static and/or dynamic binding between objects,
- management.

This document does not specify how two home control systems share a common resource or how to ensure that two home control systems used within the same premises do not interfere with each other. However, this document requires that two home control systems may share a common resource, and that they do not interfere with one another.

2 Normative references

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

ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC TR3 14762, *Information technology – Home Control Systems – Guidelines for Functional Safety*

3 Terms, definitions and abbreviations

3.1 Definitions

For the purposes of this International Standard, the following definitions apply.

3.1.1
API
application programming interface
collection of invocation methods and associated parameters used by one piece of software to request actions from another piece of software

3.1.2
co-existence
two or more networks within premises that do not interfere with one another

3.1.3
component
logical subunit of a larger, encompassing concept

NOTE The concept of interoperability is broken down into constituent components such as safety, management and operation. These constituent components are further broken down within their respective sections. The term component is also used to refer to logical subunits of system architecture concepts, such as the components of a networking implementation (for example, addressing).

3.1.4
device
distinct physical unit on a network

NOTE It can either be an end node on the network, or an intermediate node (as in the case of a network gateway device connecting two distinct physical networks).

3.1.5
interoperability
logical entities functioning together for applications on a network

3.1.6
network
distinct interconnection of devices that share a single physical layer implementation in terms of the OSI layered network model

NOTE See ISO/IEC 7498-1:1994.

3.1.7
object
unit of software functionality

NOTE This definition is similar to that traditionally used in object-oriented programming.

3.1.8
product
device or network that may be purchased to constitute a Home Electronic System

3.1.9
single implementation
single, homogeneous network implementation, where interoperability is only of concern within the single network

3.1.10
multiple implementation
mixed collection of two or more network implementations

NOTE To establish interoperability, each network has a routing path to every other network in the system. This path may involve one or more hops through multiple intermediate networks.

3.1.11
intermediate implementation
mixed collection of two or more network implementations

NOTE To establish connectivity, an intermediate implementation provides for a common intermediate translation between any two networks, assuring a worst-case translation path of two hops (from any network to the common translation, and then from the common translation to the destination network).

3.2 Abbreviations

API	Application Programming Interface
HAN	Home Area Network
HES	Home Electronic System
OSI	Open Systems Interconnect (ISO/IEC 7498-1)

4 Conformance clauses

4.1 Basic functions and requirements

HES products and networks shall implement the requirements of this standard when at least one of the following conditions is met:

- two or more dissimilar HANs are installed or implemented in premises;
- two or more dissimilar HANs are required to interoperate or interwork in premises;
- a product acts as a bridge, router, gateway or residential gateway between two or more dissimilar HANs in premises.

4.2 Compliance of qualifying products and networks

In order to conform to this standard, products and networks in the cases described in 4.1 shall:

- implement functional safety as specified in ISO/IEC TR 14762 ;
- implement measures to avoid or minimise potential hazards as specified in Clause 5:

  - prevent the unattended initiation/operation of potentially hazardous devices as specified in 5.2;
  - allow initiation commands to be sent to automatic or relocatable programmable devices only if the device can return reliably explicit information as to the state of the load on the device as specified in 5.3 and 5.4;
  - implement specific rules for instances where commands from one HAN actuate devices on another dissimilar HAN, as specified in 5.5, or if there is a situation of linked state changes between them, as specified in 5.6;
  - ensure that security measures are implemented if commands derive from a WAN source as specified in 5.7;
  - ensure that address translation between dissimilar HANs is clearly defined and disallow commands and broadcast messages if not, as specified in 5.8 and 5.9;
- manage the installation of HES products and configuration interworking as specified in Clause 6:
  - installation, configuration and management shall be carried out by personnel and systems appropriate to the procedures provided by the HAN as specified in 6.2 and 6.3;
  - if two dissimilar HANs are configured in premises, the installation and configuration shall be carried out by personnel and systems conforming to the procedures provided by the more complex HAN as specified in 6.2 and 6.3;
  - to provide configuration interoperability, devices are required to support the components of configuration levels 1 to 4 as specified in 6.2 and Table 1;
  - to provide configuration interoperability for devices on multiple and dissimilar networks, the components of configuration levels 1 to 4 shall be supported by the end-point devices as well as the device between the networks as specified in 6.2 and Table 1;
- require that, in a network or networks operating within premises, addressing, transport, data and applications interoperate as specified in Clause 7:
  - the logical addressing scheme used shall be independent of the underlying transport mechanism as specified in 7.2;
  - translation between the logical addressing scheme and the transport addressing scheme shall be handled as a mapping function of the layer that binds the logical network to a particular transport as specified in 7.2;
  - for a networked system to be interoperable, it shall support one of the three network configurations as specified in 7.3;
  - to provide information exchange interoperability, there shall be a common, defined set of value type primitives in a common lexicon as described in 7.4 and 7.5;
  - a lexicon of common actions shall be defined as specified in 7.5 such that actions of an application on one network shall be translated correctly to the actions of the same application on another network in the premises.

5 Functional safety

5.1 Introduction

ISO/IEC TR 14762 is referred to for the general safety requirements of home control systems. It concentrates on the requirements for safety in home control systems. These requirements shall be followed by applications, systems, networks and equipment that interoperate in home electronic systems which conform to this standard. However, where interoperability between networks and systems occurs, there are situations that shall be addressed in terms of functional and consequential safety in interoperating home electronic systems. The following paragraphs highlight some of the particular considerations of home equipment and network design when two or more networks are called upon to interoperate.

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

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

The implementation of product interoperability of HES products and interworking networks shall consider and implement measures to avoid or minimise the following potential hazards:

5.2 Commands to potentially hazardous devices

When configuring home networks, there shall be systems to prevent the unattended initiation/operation of potentially hazardous devices. An example is the remote or automatic switching on of radiant heat sources (open fires or hot cooker burners), i.e. a system cannot automatically control the potentially hazardous device, except by a switch or manual controller operated by a human operator and placed within reach or sight of the device.

5.3 Commands to relocatable programmable devices

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

5.4 Commands to automatic devices

Many devices and equipment in the home carry out automatic functions. A simple example is cooker ovens, which are switched on at a preset time. In many cases, external or system control of such devices can result in an unintended outcome. For instance, when the operation is carried out at some future time, either by external command or automatically, the contents of the oven may no longer be those intended. Where such automatic control is possible, it shall only be available for a preset time period from when the equipment was set up for any particular instance of automatically controlled operation, and shall operate only if the automatic control has not been changed.

5.5 Command translation

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

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

5.6 Linked state changes

Where a changed state on one network is linked to a changed state on another, safety or security rules may be breached if there is a converse assumption. For example, if unlocking the front door turns on a courtesy light, the converse must not apply: i.e. leaving the courtesy

light on must not leave the front door unlocked. Some linked change state situations may result in hazardous interactions.

Where such situations exist or potentially exist, explicit rules shall be implemented to prevent hazards and security breaches.

5.7 External control of secure devices

Where remote control of systems is set up, special precautions need to be taken to ensure that it is not possible for unauthorised persons or systems to gain control of security systems and locks. Hacking in these circumstances may result in random commands being sent to systems with uncontrolled and potentially hazardous actions or breaches of security.

If networks and gateways co-exist or contain devices such as web-based controllers that accept IP addressed instructions, security methods such as encryption shall be used.

5.8 Addressing

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

5.9 Broadcast messages, variables and commands

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

This standard defines requirements for safe configuration, operation and management to which networks and devices interfacing between them shall conform to be compliant with this standard for interoperability.

5.10 General

Safety is the overarching consideration for the Management and Operation components of interoperability.

6 Management

6.1 General

Installation, configuration and management of HANs in premises, and especially multiple dissimilar HANs, shall be carried out by personnel and systems appropriate to the complexity and degree of automatic configuration of the most complex HAN involved.

6.2 Configuration

Configuration of networks within premises may be carried out either by expert installers or end users, or the configuration may be fully automatic. Involvement of end users in device and application configuration shall be limited to applications that have been specifically

designed for this purpose. There may be overlap between methods of configuration used by dissimilar networks. This subclause defines requirements for configuration interworking.

A four-level model is useful for describing the necessary components of configuration interworking. This model classifies the requirements for configuration into the categories "Application Layer Services," "Management Procedures," "Configuration Procedures" and "Installer Procedures" (see Table 1).

In this model the lowest level is a common set of service primitives on the Application layer (OSI layer 7). Each service represents a function in the management server that is accessible by a management client, either via a home network or by local access to a device.

The second level is represented by management procedures. A management procedure is a sequence of application layer service primitives as received and sent by the management server in order to perform a specific part of the configuration process. A management procedure might contain conditional branches depending on the reaction of the management server.

The next higher level of abstraction is level 3, configuration procedures. A configuration procedure is a set of management procedures needed for the configuration of a system. A configuration procedure might contain conditional branches depending on the results of the management procedures used.

The top level, level 4, is the description of the actions an installer performs when introducing new devices into the network. Such a description is called an installer procedure and makes use of one or more underlying configuration procedures.

In order to provide configuration interoperability, devices are required to support the same components of configuration levels 1 to 4. Some parts of level 4 might be not relevant to configuration interoperability (for example the design of user interfaces) and their implementation is therefore open to the manufacturer.

Table 1 – Configuration levels

No.	Level	Description	Comment
4	Installer procedures	Description of installer's actions, implicitly using one or more configuration procedures	Normally a manual operation by either the installer or the end user
3	Configuration procedures	A sequence of management procedures that implement part of the configuration process	Normally an automated operation, initiated by an action at level 4
2	Management procedures	A sequence of application layer service primitives	Automated
1	Application layer services	Service primitives that implement the management API	Automated

6.3 Configuration process

6.3.1 General

The configuration process usually takes the following steps.

- Device individualization/device identification: assign an individual address to a device. If several instances of the same device are present in the network, device individualization also means distinguishing the instances, for example by assigning a meaningful name to them.
- Set parameters/download application: configure the functionality of each device. This step is optional in the sense that some devices might contain their application and parameters

after manufacture. Some devices require the setting of parameters, others the downloading of an application program plus parameters.

- Set links: link objects contained in several devices in order to establish functionality.
- Start device: initiate the running of an application program.

There are several configuration modes that differ in the way the installer interacts during the configuration process:

6.3.2 Expert installer configuration

In the expert installer configuration mode, the installer accesses the network components either via the network or by connecting locally to a device. The installer prepares an image of the device data with a configuration tool and downloads this data into the network device.

The installer may assign addresses, links and parameters. This gives the installer a high degree of flexibility when installing a network, especially when connecting devices from several application domains or from different networks over a gateway. This installation mode is most suitable for installations in large buildings.

6.3.3 Easy configuration

The easy configuration mode hides low-level details of the installation process (such as exact addresses) from the installer. The installer is only concerned with linking devices together. Those devices will have been previously configured (either by an expert installer or directly during the manufacturing process). There are practical limits to the number of easy configuration nodes that may be configured within one system.

6.3.4 Automatic configuration

This configuration mode enables the installer or the end user to introduce a new device to the network by simply connecting it (plug and play), and devices with automatic configuration will normally be installed by the end user. Address and link assignments are done by the device communicating with peer devices.

6.3.5 Multiple network and dissimilar network configuration

In order to provide configuration interoperability for devices on multiple and dissimilar networks, the same level 1 to 4 mechanisms shall be supported by the end-point devices as well as the device between the networks (for example the gateway).

7 Operation

7.1 Introduction

Network or networks operating within premises require that addressing, transport, data and applications shall interoperate. This clause defines the operational requirements of

- addressing,
- transport connectivity,
- information encapsulation,
- application models and lexicon.

The intention in specifying these semantic requirements is to allow freedom of choice within individual network implementations, while assuring that there is a direct logical mapping of these various operational components between network implementations. This logical mapping shall be used when implementing gateways or bridges between network implementations (for example, in ISO/IEC 15045-1).

7.2 Addressing

7.2.1 Transport-independent format

The logical addressing scheme used shall be independent of the underlying transport mechanism. Translation between the logical addressing scheme and the transport addressing scheme shall be handled as a mapping function of the layer that binds the logical network to a particular transport.

Whether that binding is dynamic or static and whether it supports one or multiple transport layers is not relevant to this standard.

NOTE In the case of bilateral (single) Network to (single) Network, direct mapping may be implemented. However, such instances do not support the general interoperability requirements of this standard and the attention of manufacturers and implementers is drawn to this fact.

7.2.2 Broadcast addressing

The logical addressing scheme shall define a transport-independent broadcast mechanism.

This requires that any underlying transport layer shall either implement or be able to simulate a broadcast address.

7.2.3 Individual node addressing

The logical addressing scheme shall support unambiguous addressing of individual devices or nodes within all networks of the system.

7.2.4 Group addressing

The logical addressing scheme shall support at least a single layer of device or node group addressing. An example is addressing all lighting devices within a network, or the collection of devices that react to an occupant arriving home.

The network shall support a multi-layer hierarchical group-addressing scheme in implementations where they are required. For example, the group of lighting devices may be sub-grouped as indoor lights and outdoor lights.

7.3 Transport connectivity

7.3.1 General

For a networked system to be interoperable, it shall support one of the following three network configurations (described in terms of the OSI layered network model).

This clause applies to the OSI transport layer. The assumption is made that, because of the hierarchical nature of the OSI model, providing transport layer interoperability will assure proper operation of the lower layers (physical to network).

7.3.2 Single implementation

This is a single, homogeneous network implementation, where interoperability is only of concern within the single network (i.e. there are no other networks in the environment with which interoperability will be established). In this case, it is sufficient to assure that all devices implement the same supporting stack from the physical layer up to and including the transport layer.