SLOVENSKI STANDARD
SIST-TS CLC/TS 50560:2014

01-december-2014

Okvirne specifikacije zahtev za interoperabilnost

Interoperability framework requirement specification

Rahmenspezifikation für Interoperabilitätsanforderungen (IFRS)

Spécification d'exigences cadre d'interopérabilité

Ta slovenski standard je istoveten z: **CLC/TS 50560:2014**

ICS:

35.240.01	Uporabniške rešitve informacijske tehnike in tehnologije na splošno	Application of information technology in general
97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

SIST-TS CLC/TS 50560:2014 **en**

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

Ref. No. CLC/TS 50560:2014 E

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.

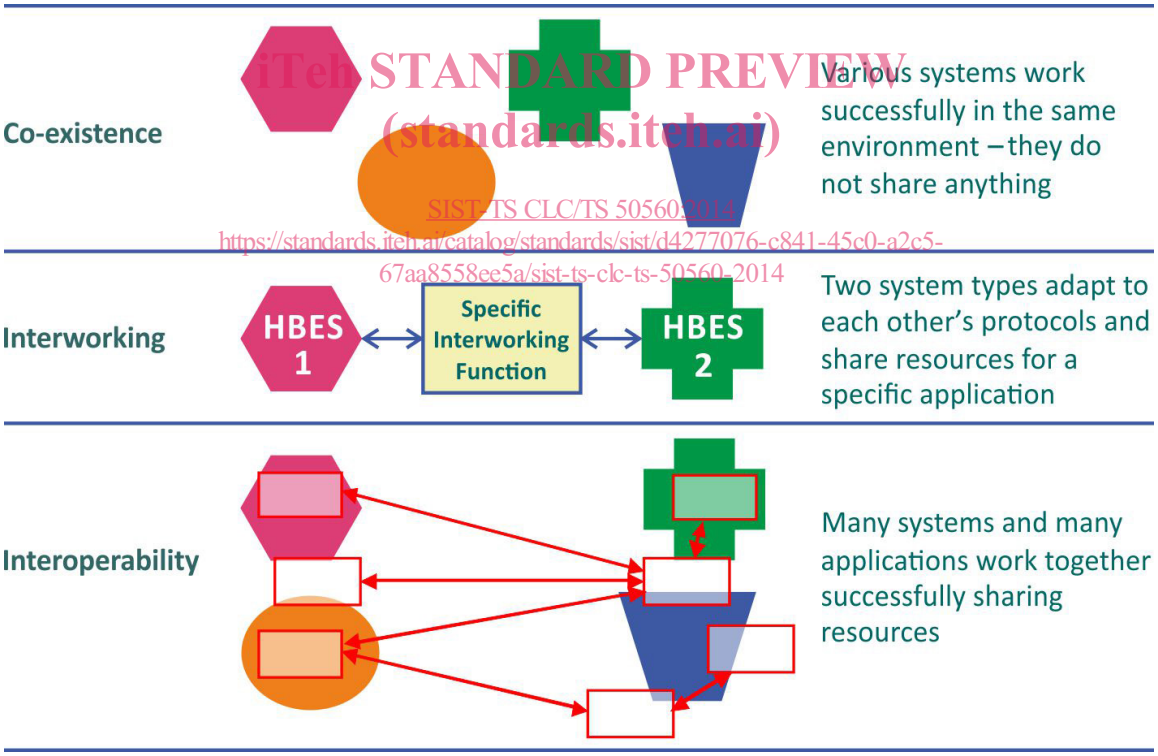

Figure 1

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