SLOVENSKI STANDARD
oSIST prEN ISO 22510:2018

01-junij-2018

Odprta izmenjava podatkov pri avtomatizaciji stavb, regulaciji in upravljanju stavb - Elektronski sistemi za stanovanja in stavbe - Komunikacija KNTnet/IP (ISO/DIS 22510:2018)

Open data communication in building automation, controls and building management - Home and building electronic systems - KNXnet/IP communication (ISO/DIS 22510:2018)

Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Elektrische Systemtechnik für Heim und Gebäude - Teil 2: KNXnet/IP-Kommunikation (ISO/DIS 22510:2018)

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment - Systèmes électroniques pour les foyers domestiques et les bâtiments - Communication KNX/IP (ISO/DIS 22510:2018)

Ta slovenski standard je istoveten z: **prEN ISO 22510**

ICS:

35.240.67	Uporabniške rešitve IT v gradbeništvu	IT applications in building and construction industry
97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

oSIST prEN ISO 22510:2018 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 22510

ISO/TC **205**

Secretariat: **ANSI**

Voting begins on:
2018-04-05

Voting terminates on:
2018-06-28

Open data communication in building automation, controls and building management — Home and building electronic systems — KNXnet/IP communication

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment — Systèmes électroniques pour les foyers domestiques et les bâtiments — Communication KNX/IP

ICS: 91.040.01; 35.240.67

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 22510:2018(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

Page

European Foreword

This document (EN ISO 22510:2018) has been prepared by Technical Committee ISO/TC 205 “Building environment design” in collaboration with Technical Committee CEN/TC 247 „Building Automation, Controls and Building Management” the secretariat of which is held by SNV.

This document is currently submitted to the CEN Enquiry

Endorsement notice

The text of ISO 22510:2018 has been approved by CEN as EN ISO 22510:2018 without any modification.

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 205, *Building environment design*.

Introduction

This International Standard is intended for the design of new buildings and the retrofit of existing buildings in terms of acceptable indoor environment, practical energy conservation and efficiency.

KNXnet/IP is a protocol designed to transport KNX home and building electronic system (HBES) control frames over an IP network. It is used as an infrastructure backbone for connecting KNX sub-networks, as a communication medium for KNX-IP devices and to provide IP based services for clients (e.g. connecting a tool software to a KNX installation). The main advantages of using IP for these purposes are that IP network infrastructure is inexpensive, available almost everywhere and that the distance of two communication parties on an IP network is virtually unlimited.

KNXnet/IP differentiates between unicast and multicast services. KNXnet/IP unicast services are used to connect a single client to a single KNXnet/IP server (e.g. KNXnet/IP Tunnelling). KNXnet/IP multicast services are mainly used to connect different KNX sub-networks using IP communication on the KNX backbone. The KNXnet/IP Routing services are defined for this purpose. KNXnet/IP multicast services build on top of IP multicast.

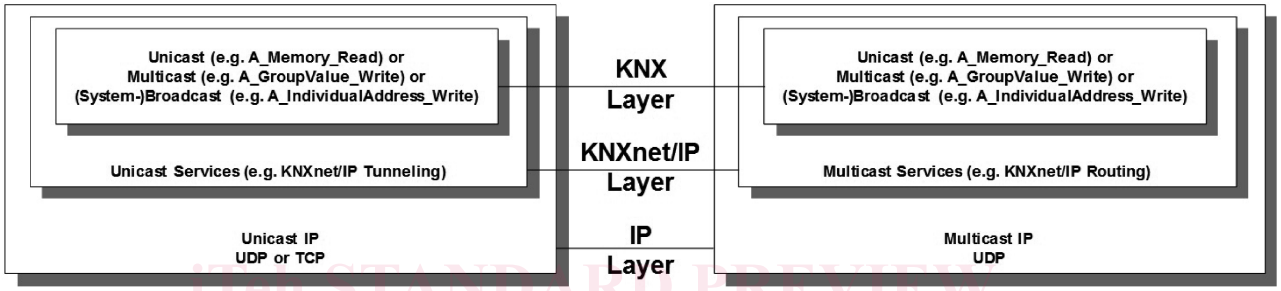

Figure 1 — Unicast and Multicast in the sense of KNX, KNXnet/IP and IP

This standard defines the integration of KNX protocol implementations within the Internet Protocol (IP) named KNXnet/IP.It defines a standard protocol, which is implemented within KNX devices, Engineering Tool Software (ETS) and other implementations to support KNX data exchange over IP networks. In fact, KNXnet/IP provides a general framework, which accommodates several specialised "Service Protocols" in a modular and extendible fashion.

The KNXnet/IP specification consists of the following clauses as specified in further detail in section 5, Requirements:

— Clause 1, Overview

— Clause 2, Core Specification

— Clause 3, Device Management

— Clause 4, Tunnelling

— Clause 5, Routing

— Clause 6, Remote Diagnosis and Configuration

— Clause 7, Secured Communication

Additional clauses may be added to the KNXnet/IP specification in the future at which time Clause 1 "Overview" as well as Annex A will need to be updated.

KNXnet/IP supports different software implementations on top of the protocol. More specifically, these software implementations can be Building Management, Facility Management, Energy Management, or simply Data Base and SCADA (Supervision, Control and Data Acquisition) packages.

Most of these packages need to be configured for the specific user application. In order to simplify this process and cut costs for engineering, KNXnet/IP provides simple engineering interfaces, namely a description "language" for the underlying KNX system. This may be done off-line, e.g. generated as an ETS export file, or on-line by a mechanism that self-describes the underlying KNX system (reading data from the system itself).

In conjunction with the EIB/KNX-to-BACnet mapping described in EN ISO 16484-5, EIB/KNX installations can very easily be integrated into BACnet system environments.

KNXnet/IP supports:

- on-the-fly change-over between Operational modes (configuration, operation);
- event driven mechanisms;
- connections with a delay time greater than $t_{KNX\_transfer\_timeout}$ (e.g. network connection via satellite).

Clause 1, Overview

Clause 1 "Overview" provides a general overview of KNXnet/IP.

Clause 2, Core specification

Clause 2 "Core Specification" defines a standard protocol that is implemented within KNXnet/IP devices and the Engineering Tool Software to support KNX data exchange over IP networks.

This specific implementation of the protocol over the Internet Protocol (IP) is called KNXnet/IP.

This specification addresses:

- definition of data packets sent over the IP host protocol network for KNXnet/IP communication;
- discovery and self-description of KNXnet/IP servers;
- configuration and establishment of a communication channel between a KNXnet/IP client and a KNXnet/IP server.

Clause 3, Device Management

Clause 3 "Device Management" defines services for remote configuration and remote management of KNXnet/IP servers.

Clause 4, Tunnelling

Clause 4 "Tunnelling" defines services for point-to-point exchange of KNX telegrams over an IP network between a KNXnet/IP device acting as a server and a KNXnet/IP Client. This point-to-point exchange may be established by a super ordinate system for building automation or management functions or by an Engineering Tool Software. It supports all ETS functions for download, test, and analysis of KNX

devices on KNX networks connected via KNXnet/IP servers. This includes changes of single KNX device object properties.

Tunnelling assumes that a data transmission round-trip between a KNXnet/IP Tunnelling client and KNXnet/IP servers takes less than $t_{KNX\_transfer\_timeouts}$.

Clause 5, Routing

Clause 5 “Routing” defines services for a point-to-multipoint exchange of KNX telegrams over an IP network between KNXnet/IP routers and/or KNX/IP devices.

Clause 6, Remote Diagnosis and Configuration

Clause 6 “Remote Diagnosis and Configuration” defines services for a point-to-point exchange of KNX telegrams over an IP network between KNXnet/IP routers and/or KNX/IP devices. The services provide means for diagnosing communication settings and for changing these remotely.

Clause 7, Secured Communication

Clause 7 “Secured Communication” of the KNXnet/IP specification defines the security wrapper for securing KNXnet/IP unicast and multicast traffic, putting an additional layer of security – transparent to all existing KNXnet/IP services – around the complete KNXnet/IP traffic.

1 Scope

This International Standard defines the integration of KNX protocol implementations on top of Internet Protocol (IP) networks, called KNXnet/IP. It describes a standard protocol for KNX devices connected to an IP network, called KNXnet/IP devices. The IP network acts as a fast (compared to KNX Twisted Pair transmission speed) backbone in KNX installations.

Widespread deployment of data networks using the Internet Protocol (IP) presents an opportunity to expand building control communication beyond the local KNX control bus, providing:

— remote configuration;

— remote operation (including control and annunciation);

— fast interface from LAN to KNX and vice versa;

— WAN connection between KNX systems (where an installed KNX system is at least one line);

— an interface to super ordinate building management and energy management systems.

A KNXnet/IP system contains at least these elements:

— one EIB line with up to 64 (255) EIB devices;
OR
one KNX segment (KNX-TP1, KNX-RF, KNX-PL110);

— a KNX-to-IP network connection device (called KNXnet/IP server);

and typically additional

- software for remote functions residing on e.g. a workstation (may be data base application, BACnet Building Management System, browser, etc.).

Figure 1 shows a typical scenario where a KNXnet/IP client (e.g. running ETS) accesses multiple KNX installed systems or KNX subnetworks via an IP network. The KNXnet/IP client may access one or more KNXnet/IP servers at a time. For subnetwork, routing server-to-server communication is possible.

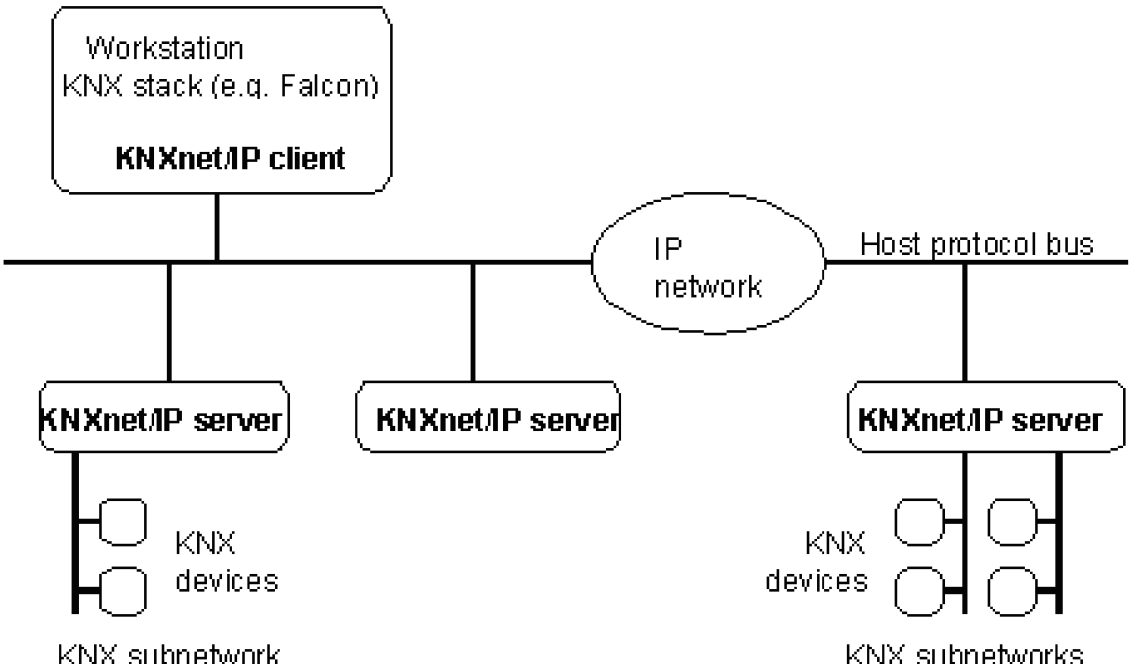

Figure 2 — Device types and configuration examples

2 Normative references

Not applicable.

3 Terms and definitions

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

3.1
Backbone Key
The key used for encryption and message authentication of secure KNXnet/IP multicast communication in a KNXnet/IP Routing multicast group. This key will be configured by ETS and is a shared secret between all members of the secure KNXnet/IP Routing multicast group.

3.2
Cipher Text
Cipher text is a generic term that denotes the encrypted data.

Note 1 to entry: Cipher text opposes to plain data.

3.3
common External Message Interface
cEMI
generic structure for medium independent KNX messages

Note 1 to entry: cEMI (common EMI) frames are used to encapsulate KNX messages within Internet Protocol (IP) packets.

3.4
communication channel
logical connection between a KNXnet/IP client and a KNXnet/IP server (or, in case of routing, between two or more KNXnet/IP servers)

Note 1 to entry: A communication channel consists of one or more connections on the definition of the host protocol used for KNXnet/IP.

3.5
communication channel
as defined by the KNXnet/IP Core specification, this is represented by one or two IP channels

3.6
Engineering Tool Software
ETS
software used to configure KNX devices

3.7
Host Protocol Address Information
HPAI
structure holding the IP host protocol address information used to address a KNXnet/IP endpoint on another KNXnet/IP device

3.8
IP channel
logical connection between two IP host/port endpoints

Note 1 to entry: IP channels are either a guaranteed, reliable TCP (transmission control protocol) or an unreliable point-to-point or multicast (in case of routing) UDP (user datagram protocol) connection.

3.9
KNX node
device implementing a KNX protocol stack and fulfilling the requirements according to the KNX standard

3.10
Internet Control Message Protocol
ICMP
extension to the Internet Protocol (IP) for error, control, and informational messages

Note 1 to entry: ICMP is defined by RFC [1)] 92 and supports packet containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

1) Request for Comment: Internet Standards defined by the Internet Engineering Task Force (IETF) are firstly published as RFCs.