SLOVENSKI STANDARD
SIST EN 16836-1:2017

01-januar-2017

Komunikacijski sistemi za merilnike - Brezžična zankasta omrežja za izmenjavo podatkov merilnikov - 1. del: Uvod in standardizacijski okvir

Communication systems for meters - Wireless mesh networking for meter data exchange - Part 1: Introduction and standardization framework

Kommunikationssysteme für Zähler - Drahtloses Mesh-Netzwerk für den Zählerdatenaustausch - Teil 1: Einführung und Standardisierungs-Rahmen

Systèmes de communication des compteurs - Réseau maillé sans fil pour l’échange de données de compteurs - Partie 1 : Introduction et cadre normatif

Ta slovenski standard je istoveten z: EN 16836-1:2016

ICS:

33.200	Daljinsko krmiljenje, daljinske meritve (telemetrija)	Telecontrol. Telemetering
35.100.01	Medsebojno povezovanje odprtih sistemov na splošno	Open systems interconnection in general

SIST EN 16836-1:2017 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16836-1

November 2016

ICS 33.200; 35.100.10

English Version

Communication systems for meters - Wireless mesh networking for meter data exchange - Part 1: Introduction and standardization framework

Systèmes de communication des compteurs - Réseau maillé sans fil pour l'échange de données de compteurs - Partie 1 : Introduction et cadre normatif

Kommunikationssysteme für Zähler - Drahtloses Mesh-Netzwerk für den Zählerdatenaustausch - Teil 1: Einführung und Standardisierungs-Rahmen

This European Standard was approved by CEN on 3 September 2016.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

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

Ref. No. EN 16836-1:2016 E

Contents

Page

European foreword

This document (EN 16836-1:2016) has been prepared by Technical Committee CEN/TC 294 "Communication systems for meters and remote reading of meters", the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2017, and conflicting national standards shall be withdrawn at the latest by May 2017.

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

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

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

The EN 16836 series of standards details requirements for gas meters, water meters and heat meters that can interoperate with products in a mesh network that conform to this standard through a smart energy profile application layer. This standard refers to documents made freely available by the ZigBee Alliance, an organization that manages a mesh network specification (see www.zigbee.org/about/centc294).

This series of standards specifies how a mesh networking radio specification applies within the scope of European standards at the application layer, networking layer and also medium access control/physical layer (MAC/PHY). All parts are intended to be used in conjunction.

The scope of this series is in line with the scope of CEN/TC 294, "Communication systems for meters and remote reading of meters", and allows data produced by utility meters to be read by a WAN communications hub, another meter, a separate meter display unit or any other device implementing this smart energy profile standard. Within the wider smart energy profile and referenced documents, there are also clusters and data objects that relate to other devices, such as programmable thermostats, but these clusters are outside the scope of CEN/TC 294 and as such are omitted from this standard. However, details of these data items can be found in the same documents that are referenced in this standard.

EN 16836 consists of the following parts:

— EN 16836-1, *Communication systems for meters — Wireless mesh networking for meter data exchange — Part 1: Introduction and standardization framework*

— EN 16836-2, *Communication systems for meters — Wireless mesh networking for meter data exchange — Part 2: Networking layer and stack specification*

— EN 16836-3, *Communication systems for meters — Wireless mesh networking for meter data exchange — Part 3: Energy profile specification dedicated application layer*

This standard series is created in compliance with the terms of a memorandum of understanding (MOU) between CEN/CELELEC and the ZigBee Alliance. The principles underpinning the relationship between CEN/CENELEC and the ZigBee Alliance are described in the Consortium Bridge procedure. A copy of the MOU and the Consortium Bridge can be obtained from CEN/CENELEC.

In a similar way to the FLAG Association providing registration services for manufacturer codes used in DLMS/COSEM and MBus for meter reading, the ZigBee Alliance acts as a Registration Authority for manufacturer identifiers so that there is a guarantee of no clash between manufacturers.

NOTE The term 'ZigBee' and the ZigBee Logo are registered trademarks of the ZigBee Alliance and their use is subject to the conditions of membership.

1 Scope

This European Standard gives provisions on the standardization framework of communication systems applicable to the exchange of data from metering devices to other devices within a mesh network. It includes information on the application process functions, layered protocols and metering architecture.

This European Standard also specifies how to interpret Parts 2 and 3 of EN 16836 which give a list of references to the ZigBee documents. This standard is applicable to communications systems that involve messages and networking between a meter or multiple meters and other devices in a mesh network, such as in home displays (IHDs) and communications hubs. This standard allows routing between devices and also allows channel agility to avoid contention with other networks of the same type, or networks of other types operating in the same frequency bands.

This standard is designed to support low power communications for devices such as gas and water meters which can make data from such devices available on the mesh network at any time through a proxy capability within a permanently powered device

NOTE 1 This standard specifies a communication protocol that can embrace a multitude of smart metering architectures from a variety of countries. This standard is not designed to limit, or indeed imply a choice or preference to any one of the many possible architectures, but more over provide information on how devices can use this communications standard to publish and receive information from meters over a network.

NOTE 2 This standard defines a protocol that can be used for either a type M interface, or a type H1 interface, however H1 interfaces are not within the scope of CEN/TC 294.

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.

CEN/CLC/ETSI/TR 50572:2011, *Functional Reference Architecture for Communications in Smart Metering Systems*

IEEE 802.15.4, *IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)*

ZigBee Specification – 05-3474 Rev 20, September 7, 2012

ZigBee Pro Stack Profile – 07-4855 Rev 05, January 2008

ZigBee Cluster Library – 07-5123 Rev 04, April 26, 2010

ZigBee Smart Energy Standard 07-5356 Rev 19, December 3, 2014

OTA Cluster Specification 09-5264 Rev 23, March 12, 2014

NOTE The above ZigBee documents and OTA Cluster Specification can be obtained from www.zigbee.org/about/centc294.

3 Terms, definitions, acronyms and abbreviations

For the purposes of this document, the terms, definitions, acronyms and abbreviations given in the following apply.

- ZigBee Specification – 05-3474 Rev 20,
- ZigBee Pro Stack Profile – 07-4855 Rev 05,
- ZigBee Cluster Library – 07-5123 Rev 04,
- ZigBee Smart Energy Profile Specification 07-5356 Rev 19, and
- OTA Cluster Specification 09-5264 Rev 19

4 Application process functions

4.1 Architecture

The ZigBee Protocol operates using a concept of a client server relationship between logical devices in a network and uses a concept of clusters to exchange information. A cluster is a related collection of commands and attributes, which together define an interface to specific functionality. Typically, the entity that stores the attributes of a cluster is referred to as the server of that cluster, and an entity that affects or manipulates those attributes is referred to as the client of that cluster.

In general terms all clusters have a server and a client side, meaning that all information either published or requested on the network is owned by the device attached to the server side of a cluster and received or requested by the device attached to the client side of that particular cluster.

4.2 Basic principles

4.2.1 Mirroring

Mirroring is described in detail in Annex D of the ZigBee Smart Energy Profile Specification 07-5356 Rev 19. The concept of this functionality is to allow data from a battery operated, sleepy device to be available all of the time to other devices on the network by allowing another 'always on' device to hold a copy of the device's data in a proxy or mirror. This proxy or mirror can also be used to allow commands or instructions from an AMI Head End System to be issued to a sleepy device without necessitating the sleepy device to be awake at the time of transmitting the command.

This functionality is commonly used in the case of a gas meter that wakes up every so often to check for commands awaiting it, and to publish its own meter readings, status, alarms etc. The principle is that the gas meter will awaken and query the mirror that is supported in the 'always on' device to determine what commands are awaiting it. The 'always on' device will inform the sleepy device that there are instructions or commands awaiting it and tell the gas meter to stay awake to receive them. The gas meter will then have the chance to write its own cluster data to the mirror ready for other devices on the network to read this data or be sent it (depending on the device and data item).

4.2.2 Tunnelling

This functionality is discussed in detail in ZigBee Smart Energy Profile Specification, D.6, and allows the transport of another protocol over a ZigBee smart energy network without the need for any other device on the network having to understand or interpret the payload of the other protocols packets. Fragmentation functionality within the ZigBee Protocol allows the packets of the tunnelled protocol to be broken down and transported across the smart energy (SE) network in packets that are of appropriate size to be managed by the SE Network. Once packets have been transported from one device to the other over the tunnel, these native format packets are reassembled and presented to the application that understands them.

EXAMPLE A ZigBee smart energy network containing a communications hub, an electricity meter and an IHD, in which the IHD and communications hub only understand ZigBee Smart Energy Profile whereas the electricity meter understands ZigBee Smart Energy Profile and DLMS/COSEM.

Use of this tunnelling function within a ZigBee smart energy network enables the user to route a DLMS/COSEM message to the electricity meter from the head end system through the hub, without the hub having to understand the COSEM message. This equally applies to any other protocol that has the possibility to be transported over a wireless connection, and can be used in many applications including for the transport of manufacturers' own proprietary protocols.

4.2.3 Commissioning

This functionality within the ZigBee Smart Energy Profile is discussed in detail within ZigBee Smart Energy Profile Specification 07-5356 Rev 19, 5.5. However, first every device on the ZigBee smart energy network shall be authorized to join that network and as such has to undergo some form of commissioning process. Within the specification this has been left deliberately flexible in terms of approach to ensure that innovation is not stifled within different implementations. For security purposes it is necessary for certain information relevant to a prospective joining device to be passed to the device on the network containing the trust centre and coordinator. This passing of information happens in an out of band communication which is not in the scope of this European Standard. Normally this passing of information happens through a message from an upstream system connected via the back haul network. Once this joining information is within the coordinator of the network it is possible for joining to be turned on and allow the joining of devices to the network.

4.2.4 Joining and binding

Joining and binding is described in detail in ZigBee Smart Energy Profile Specification 07-5356 Rev 19, 5.5.5. In simple terms it can be described as the process that a device goes through in order to join the network and access services at the application layer of the network. There are a number of security procedures that a device shall complete to establish a secure authenticated connection to the network, as described within ZigBee Smart Energy Profile Specification 07-5356 Rev 19, Annex C and also within ZigBee Specification – 05-3474 Rev 20, Section 4. After a device has joined the network it reviews the services or clusters of other devices on that network and matches with services and clusters that it supports so that it can obtain data concerning those services.

EXAMPLE Binding to price cluster server

If a device connects to a ZigBee smart energy network supporting the price cluster client, it needs to find another device on the network that supports the price cluster server in order to receive pricing messages. The process of joining the network and service discovery allows the IHD to identify all clusters that are of interest to it and 'bind' to those clusters so that it can receive updates as and when the information on the server of that particular cluster is updated. Devices can bind to as many clusters as they like depending on the features that they support. It is also possible for information to be obtained from a device on the network without binding to a cluster by asking for that information after service discovery and also after joining at the application layer.

4.2.5 Discovery

Discovery is described in detail within ZigBee Smart Energy Profile Specification 07-5356 Rev 19, 5.5.5. As discussed in 4.2.4, it relates to the process that a joining device undergoes when binding to clusters on a ZigBee smart energy network. When joining any cluster it is also necessary to see which attributes that cluster supports to be sure to not try and bind to elements that are not present at either the client or server end of the binding relationship.

For every cluster there are required attributes and optional attributes, and it is entirely at the will of the implementer which if any of the optional attributes are supported. During the discovery process when binding it is possible for both client and server devices of a given cluster to find out which common attributes are supported by both parties. Once this has been established both devices will know what can be published by the server and requested by the client.

4.2.6 Security

Zigbee smart energy utilizes a high level of security designed to protect utility network data and maintain the privacy of the users interacting with devices on the network. There are two security levels within ZigBee: network security and application security. Application security uses a hybrid system of symmetric and asymmetric keys, whereby a certificate based key establishment mechanism is utilized in order to establish a symmetric key for communications between two devices on the network. There is a trust centre function within the network that is responsible for managing keys and network access.

As well as establishing secure communications on the network there are also mechanisms within this series of standards for the prevention of replay attacks and also non-repudiation via means of digital signatures.

4.3 Robust messaging

This series describes a number of mechanisms in place for acknowledgements and retries both at the data link layer and also the application layer. There are also message integrity checks at the data link layer.

4.4 Mesh routing

This series includes support for multiple repeaters within a network to assist with message delivery and supports self-healing, scalable mesh networking.

4.5 Interoperability

The ZigBee Smart Energy Profile (as referred to in EN 16836-3:2016) accommodates the interoperable interaction of devices from multiple manufacturers attached to the same network. This goes as far as a mechanism for managing unsupported device features without causing either device or network failure.

4.6 Battery powered device management

This series allows the management of sleeping devices (devices with constrained power sources such as battery operated devices). Sleeping devices behave in a manner such that they are not always connected to the network in a send/receive capacity, and only wake up and connect periodically. This series has provision for supporting these sleeping client devices, and specifies the necessary behaviour on both the client and server side of the protocol.

One of the key functionalities provided for sleeping devices is the ability for a permanently powered device to provide a proxy service for the sleeping device; this behaviour is known as mirroring; please refer to 4.2.1

5 Layered protocols

5.1 General

To facilitate the functionality described in Part 3 of this series, it is assumed a protocol stack divided into layers is used, in order to reduce the complexity of the communicating system. Each layer provides services to the layer above on the basis of the layer below.

The layered model chosen maps to the OSI Seven layer reference model as shown in Table 1:

Table 1 — Mapping of OSI Seven layer reference model to EN 16836–2:2016 and EN 16836–3:2016

OSI Layer	ZigBee layer	Standard Reference
6 + 7	ZigBee Smart Energy Profile	EN 16836–3:2016
3 + 4 + 5	ZigBee Pro Networking	EN 16836–2:2016
1 + 2	IEEE 802.15.4	IEEE 802.15.4

NOTE The OSI 7 layer model is described in ISO/IEC 7498-1 [1].

5.2 Application layer

5.2.1 General

The application layer references of this standard are in three parts:

— ZigBee Smart Energy Profile Specification 07-5356 Rev 19, December 3, 2014

— ZigBee Cluster Library – 07-5123 Rev 04, April 26, 2010

— OTA Cluster Specification 09-5264 Rev 23, March12, 2014

NOTE 1 Tunnelling of other protocols such as EN 13757–3 [2], EN 62056–5–3 [3], EN 62056–6–1 [4] and EN 62056–6–2 [5], is also permitted within this series using the tunnelling cluster specified in EN 16836–3.

NOTE 2 Tunnelling of protocols and alternative object models is possible within other standards from CEN/TC 294.

5.2.2 Companion specification

A companion specification (CS) is a supplementary text relating to the implementation of a standard, usually drafted and published by a market authority such as a consortium, government or customer. It may contain permitted extensions to the existing standard, as well as operating rules within the scope of the existing standard. If a number of options are available within a standard then the companion specification can enumerate which options are required for a particular implementation.

ZigBee Smart Energy Profile is a very diverse and technically capable application profile that specifies a large amount of functionality, as well as the behaviour of devices and how they interface with each other within a network. Many of the clusters and commands are not required for implementation and as such companion specifications are generally used to enumerate which optional features are required for a particular project.

Each implementer shall make a choice about which optional clusters and attributes they wish to code into their particular product. CSs make clear the description of which attributes and clusters are to be implemented as well as describe what extra manufacturer specific profile (MSP) objects they may add to their given product. In a similar way to the existence of CSs within DLMS/COSEM and also Mbus, this concept exists with ZigBee Smart Energy Profile.

The protocol implementation conformance statement (PICS) forms an important part of any CS and effectively lists the clusters, attributes, and commands that the device supports.