SLOVENSKI STANDARD
SIST-TS CLC/TS 50586:2019

01-december-2019

Odprti protokol pametnega omrežja (OSGP)

Open Smart Grid Protocol (OSGP)

Protocole ouvert pour Réseau Intelligent

Ta slovenski standard je istoveten z: **CLC/TS 50586:2019**

ICS:

33.200	Daljinsko krmiljenje, daljinske meritve (telemetrija)	Telecontrol. Telemetering
35.240.99	Uporabniške rešitve IT na drugih področjih	IT applications in other fields

SIST-TS CLC/TS 50586:2019 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50586

November 2019

ICS

English Version

Open Smart Grid Protocol (OSGP)

Protocole ouvert pour Réseau Intelligent

Open Smart Grid Protocol (OSGP)

This Technical Specification was approved by CENELEC on 2019-09-02.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Ref. No. CLC/TS 50586:2019 E

Contents

Page

European foreword

This document (CLC/TS 50586:2019) has been prepared by CLC/TC 13 “Electrical energy measurement and control”.

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

This Document does not have the status of a harmonized Standard and cannot therefore be listed in the Official Journal of the EU and therefore provides no presumption of conformity. However, this Document may be used for the risk evaluation in the framework of the EU conformity declaration. If this document provides requirements below the level of a harmonized standard, the harmonized standard takes precedence.

Introduction

One of the outcomes of the mandate M/441 is the indentification of OSGP as one of the protocols which can be used for Smart Metering deployment in Europe.

1 Scope

This document describes the data interface model, application-level communication, management functionalities, and security mechanism for the exchange of data with smart-grid devices. The following five areas are referred to as the Open Smart Grid Protocol (OSGP).

- Data exchange with smart-grid devices allows Utility Suppliers to collect customer usage information such as billing data and load profiles, monitor and control grid utilization, provision scheduling of tariffs, detect theft and tampers, and to issue disconnects, to name a few. Meter features are described in Clauses 7 and 8.
- The OSGP data interface uses a representation-oriented model (tables and procedures) which require low overhead. The model is described in Clause 5, with specific tables specified in Annex A, Annex B, and procedures in Annex C and Annex D.
- The OSGP application protocol is designed to use the EN 14908-1:2014 communication stack over narrow-band power line channels. Clause 9 describes the messages that are used to access OSGP data. An essential feature of the protocol over power line channels is a repeating mechanism which gives the application layer the control and responsibility for forwarding packets among devices, independent of the routing protocol or limitations of underlying layers. Therefore OSGP can be adapted to other communication stacks and medium, although such adaptation is outside of the scope of this specification. The repeating mechanism is described in Annex G.
- OSGP management features include the discovery of devices and the routing topology in a protocol called Automated Topology Management (described in Clause 4) commissioning of devices for secured communication (Annex F), monitoring of device connectivity, and updating of device firmware.
- OSGP security covers authentication, encryption, and key management. This is detailed in Annex F.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

EN 14908-1:2014, *Information technology - Control network protocol - Part 1: Protocol stack*

ISO 8859-1 (or ECMA-94), *Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1*

ISO/IEC 646:1991, *Information technology - ISO 7-bit coded character set for information interchange*

IEEE Std 802.11ac-2013, *IEEE Standard for Information technology- Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11 Wireless LAN Medium Access Control*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply. ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1.1
active energy/power
measure of active power expended over time (resistive load)

3.1.2
apparent energy/power
multiplication of the rms voltage with the rms current

3.1.3
Byte Encryption Key
BEK
128-bit key derived from the OMAK for the purpose of OSGP encryption

3.1.4
Billing Interface Definition Number
BIDN
identifier used to identify billing-related data in OSGP device logs, see table EP 32 in annex D

3.1.5
bootrom
part of the OSGP device firmware which is fixed and cannot be changed over the network

3.1.6
broadcast
message directed at all of the network population. In OSGP systems, only the data concentrator initiates broadcast messages

Note 1 to entry: OSGP devices may repeat a broadcast message.

3.1.7
clone domain
special logical network address format that signals a node to receive rather than reject messages from a sender having the same source address as itself

Note 1 to entry: This facilitates the discovery process by allowing discovery messages to be propagated throughout nodes all having the same pre-assigned address, without requirement them to be commissioned. The clone domain address is distinguished from a normal address by having the node number byte’s most significant bit set to zero instead of one.

Note 2 to entry: In addressing there can be up to 255 subnets and 127 nodes/subnet, so the high order bit of the node number byte is free for this special use.

3.1.8
Packet Cycle Count
maximum number of packet cycles over which to randomize access to the link

3.1.9
Data Concentrator
DC
gateway which supervises electrical utility OSGP devices and other devices, performing data collection and network management functions and allows access to the data and device by the HES

3.1.10
device (or OSGP device)
device which implements the OSGP protocol

3.1.11
dip
measured quantity detected at a level below a defined threshold

3.1.12
energy
summation of power over time

3.1.13
Fast Commission Message
FCM
specific OSGP message type used for PLC traffic optimization during initial commissioning of an OSGP device

3.1.4
group ID
mechanism for selecting a subset of devices to process a broadcast message

Note 1 to entry: the group ID used in OSGP is an application-layer entity, and is unrelated to the 14908-1 Group ID which is used in the network layer.

3.1.15
in-phase
condition when the phase angle between two sine waves is 0 degrees

3.1.16
Interface Change Alarm
ICA
alarm bit in BT03 to indicate the possible change of the device's interface definition or dimensions of some OSGP device tables, due to modification of device tables or invocation of device procedures

Note 1 to entry: Attempts to read or write some device tables will not succeed until the alarm has been cleared by the HES to acknowledge the interface change. Tables affected by the Interface Change Alarm in this manner are marked with the ICA NACK attribute throughout the present document. Tables and procedures that may cause the Interface Change Alarm to be triggered are marked with the ICA SRC attribute throughout the present document.

3.1.17
load profile
recording of one or more pieces of electrical load data at specified intervals

3.1.18
M-Bus
protocol developed for netwoking and remote reading of utility meters that are attached (wired or wirelessly) to the smart grid device

Note 1 to entry: the M-Bus capabilities in the OSGP device according to the present document can discover and query up to four M-Bus devices, such as gas, water, or heat meters. The OSGP device stores the consumption data collected from the M-Bus devices along with any alarm or status messages.

3.1.19
M-Bus Auto-discovery
process by which the device which play the role of the M-Bus master polls the M-Bus network for new and previously commissioned devices

Note 1 to entry: newly discovered devices are added to the commissioned device list for regular polling, up to a maximum of four devices.

3.1.20
M-Bus Data Type
MDT
mapping of a M-bus Data Record Header (DRH) definition to a 5-bit ordinal