IEC TS 60839-7-8

Edition 1.0 2019-05

TECHNICAL SPECIFICATION

Alarm systems – Part 7-8: Message formats and protocols for serial data interfaces in alarm transmission systems – Requirements for common protocol for alarm transmission using the Internet protocol

IEC TS 60839-7-8:2019-05(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC TS 60839-7-8

Edition 1.0 2019-05

TECHNICAL SPECIFICATION

Alarm systems – Part 7-8: Message formats and protocols for serial data interfaces in alarm transmission systems – Requirements for common protocol for alarm transmission using the Internet protocol

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.320 ISBN 978-2-8322-6813-1

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM SYSTEMS –

Part 7-8: Message formats and protocols for serial data interfaces in alarm transmission systems – Requirements for common protocol for alarm transmission using the Internet protocol

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

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

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees 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, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) 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.

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

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 60839-7-8, which is a technical specification, has been prepared by IEC technical committee 79: Alarm and electronic security systems.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
79/419/DTS	79/453A/RVDTS

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

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

A list of all parts in the IEC 60839 series, published under the general title *Alarm systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International Standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

ALARM SYSTEMS –

Part 7-8: Message formats and protocols for serial data interfaces in alarm transmission systems – Requirements for common protocol for alarm transmission using the Internet protocol

1 Scope

This Part of IEC 60839 specifies a protocol for point-to-point transmission of alarms and faults, as well as communications monitoring, between a supervised premises transceiver and a receiving centre transceiver using the Internet protocol (IP).

The protocol is intended for use over any network that supports the transmission of IP data. These include Ethernet, xDSL, GPRS, WiFi, UMTS and WIMAX.

The system performance characteristics for alarm transmission are specified in IEC 60839-5-1.

The performance characteristics of the supervised premises equipment comply with the requirements of its associated alarm system standard and apply for transmission of all types of alarms including, but not limited to, fire, intrusion, access control and social alarms.

Compliance with this document is voluntary.

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.

IEC 60839-5-1:2014, *Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements*

RFC 793:1981, *Internet standard – Transmission control protocol, DARPA Internet program, protocol specification*

NIST 800-38A:2001, *Recommendation for block cipher modes of operation: methods and techniques*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60839-5-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

AES	Advanced Encryption Standard
ARC	Alarm Receiving Centre
ATS	Alarm Transmission System
CA	X.509 Certificate Authority
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
HL	Header Length
IP	Internet Protocol
IV	Initialization Vector
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVM	Non-Volatile Memory
P-MTU	Path Maximum Transmission Unit
RCT	Receiver Centre Transceiver
RX	Receive
SCTP	Stream Control Transmission Protocol
SNTP	Simple Network Time Protocol
SPT	Supervised Premises Transceiver
TFTP	Trivial File Transfer Protocol
TX	Transmit
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
WS	Window Size

4 Objective

The object of this document is to specify the protocol details (transport and application layers) for alarm transmission systems using Internet Protocol (IP), to ensure interoperability between SPTs and RCTs supplied by different manufacturers. Mechanisms to commission SPT and RCT and build mutual trust between the communicating parties are also described.

As compliance with this document is voluntary, any other alarm transmission protocol or equipment not covered by this document may be used, provided that the requirements of IEC 62642-1 are met.

This protocol is designed to run on top of UDP and is designed to support both IPv4 and IPv6.

NOTE For further discussion of IP and UDP in alarm transmission, please see F.3.

5 Messaging

5.1 General

This clause defines the messaging layer, on top of which the alarm event data is transmitted using the existing reporting formats like for example Sia and Contact ID. Clause 7 defines the initial commissioning of an SPT, as well as how SPTs connect to the RCT.

The functionality of the alarm messaging and polling protocol includes:

- exchanging master and session parameters;
- (alarm) event reporting (including linking to out-of-band additional data related to events, like audio/video);
- line monitoring;
- transparent message transmission, e.g. vendor specific messages that, for example, can be used for remote commands from RCT to SPT.

It fulfils the following requirements:

- encryption, fulfilling requirements for most demanding category of EN 50136-1;
- authentication, fulfilling requirements for most demanding category of EN 50136-1;
- SPT: allows a broad range of hardware (limited demands on memory footprint as well as CPU power);
- RCT: allows support for at least 10 000 SPTs in compliance with any category in EN 50136-1, using modern general purpose server hardware;
- allow Dynamic IP addresses of the SPTs;
- allow one or more SPTs to be placed behind a NAT firewall.

5.2 Message format overview

5.2.1 General

This subclause describes the basic outline of all messages.

Each message shall be explicitly acknowledged, including line supervision messages.

Backwards compatibility is achieved by the implementation of the RESP_CMD_NOT_SUPPORTED result value, which the receiving party can send as answer to unsupported messages.

Multi-byte values will be transmitted using network byte order (big-endian).

5.2.2 Identifiers

The identifiers given in Table 1 below exist.

Table 1 – Identifiers

Description	Purpose	Present in	Encrypted	See
Connection handle	Look up the current symmetric encryption key	All messages	No	5.2.4
Device ID	Uniquely identify the hardware	Contributing to hashes in all messages	N / A	5.2.5

The connection handle is unencrypted. It is a unique number, initialized during the setup of the connection. Its sole purpose is to be able to look up the encryption key. It is valid for the communication session only.

The Device ID uniquely identifies the hardware once the connection has been established. The Device ID is used when computing the hash value for each message. In combination with the encryption of the hash this is used for substitution detection.

NOTE Device ID is not equivalent to any account code or similar ID specified by application protocol.

The Device ID shall be stored in non-volatile memory within the SPT.

The IP address is not used for identification purposes, in order to allow for the use of dynamic or translated IP addresses.

5.2.3 Message format

The basic unencrypted format of all messages is as follows. Message in this format is never transmitted. It is described in Table 2 below only to clarify the hash value calculation.

Table 2 – Basic unencrypted format of messages

Byte index	Bytes	Description	See	Group
0	4	Connection handle	5.2.4	Header
4	16	Device ID	5.2.5	
20	2	Tx Sequence number	5.2.8	
22	2	Rx Sequence number	5.2.8	
24	2	Flags	5.2.9	
26	1	Protocol version number	5.7	Message
27	1	Message ID	5.2.6	
28	2	Message length	5.2.7	
30	*n*	Message data	Clause 6	

The basic encrypted, transmitted format of all messages is as shown in Table 3. Note that the Device ID field is not included in the encrypted message, but its value is used to compute the message hash value i.e. the hash is calculated from the unencrypted version of the message described above.

Table 3 – Basic encrypted format of messages

Byte index	Bytes	Description	See	Encrypted	Group
0	4	Connection handle	5.2.4	No	Header
4	2	Tx Sequence number	5.2.8	Yes	
6	2	Rx Sequence number	5.2.8	Yes	
8	2	Flags	5.2.9	Yes	
10	1	Protocol version number	5.7	Yes	Message
11	1	Message ID	5.2.6	Yes	
12	2	Message length	5.2.7	Yes	
14	*n*	Message data	Clause 6	Yes	
14 + *n*		Padding	5.3.1	Yes	Tail
	32 32	Hash – SHA-256, or Hash – RIPEMD-256	5.4	Yes	

The connection handle is unencrypted; the remainder of the message is encrypted using the encryption method as negotiated during the commissioning stage.

Message ID's are defined in pairs: each message has its matching response. For responses the first byte of the Message Data always holds a 'Result code' as defined in Annex A.

All fields are described in detail in the following subclauses.

5.2.4 Connection handle

The connection handle is assigned (uniquely for the RCT to which a SPT reports) using the commissioning protocol. The RCT creates a unique connection handle and links this to the Device ID of the SPT in its internal database. This translation results in a compact, fixed length connection handle.

The purpose of the connection handle is to be able to determine the encryption key to be used to decrypt the received message, independent of the IP address of the message.

The connection handle is not a (by the installer/operator) configurable parameter, nor made visible on user interfaces. It is generated and used internally by the SPT/RCT equipment only.

5.2.5 Device ID

5.2.5.1 General

The Device ID uniquely identifies the SPT and RCT. It is used (in combination with the encryption) for substitution detection. Both SPT and RCT can verify the identity of the connected party using this field, and create a substitution alarm in case it has changed.

Within the message header, the Device ID itself is never transmitted. However Device ID is used to contribute to the message hash calculation.

Device ID is 16 bytes long.

5.2.5.2 SPT device ID

The device ID of the SPT is an ID that is random to the SPT, but fixed and read-only over the lifetime of the SPT, i.e. a hardware serial number. It is unique within the SPT database in the RCT.

The device ID is created during manufacturing time of the device; in messaging, it is never transmitted itself in clear text, but is needed to be known in clear text for the ARC to configure the RCT accordingly.

Thus, it is only transmitted during initial commissioning phase to the RCT.

Uniqueness is assured by the following principles:

- each SPT manufacturer shall use his 24 bits "organizationally unique identifier" as assigned to him by the IEEE for MAC-address generation;
- each SPT manufacturer not having such a code shall attend for such a code from IEEE;
- if an interface in the SPT makes use of a MAC address, the next 24 bits in the device ID shall be the same as the rest of MAC address specified by the manufacturer. If such an interface does not exist, the manufacturer shall use another numbering scheme documented by the manufacturer;
- the manufacturer shall use non-consecutive, randomly distributed numbers for the rest of the device ID field and guarantee uniqueness for all his delivered SPT devices.

5.2.5.3 RCT device ID

The device ID of the RCT is an ID that is unique within the receiver and never changes within the lifetime of a receiver. It represents the unique identity of the RCT.

The RCT device ID is made available to the SPT during the commissioning phase.

5.2.6 Message ID

The message IDs as used are listed in the following Table 4.

Table 4 – Message ID overview

Message name	Description	Direction SPT ←·→ RCT	Version	Message ID
POLL_MSG	Poll message	→	1	0x11
EVENT_MSG	Event message	→	1	0x30
CONN_HANDLE_REQ	Connection handle request	→	1	0x40
DEVICE_ID_REQ	Device ID request	→	1	0x41
ENCRYPT_SELECT_REQ	Encryption selection request	→	1	0x42
ENCRYPT_KEY_REQ	Encryption key exchange	← →	1	0x43
HASH_SELECT_REQ	Hash selection request	→	1	0x44
PATH_SUPERVISION_REQ	Path supervision request	← →	1	0x45
SET_TIME_CMD	Set time command	←	1	0x47
VERSION_REQ	Protocol version request	→	1	0x48
PMTU_REQ	P-MTU	→	1	0x60
PMTU_PROBE	P-MTU probe	→	1	0x61
DTLS_COMPLETE_REQ	DTLS completed request	→	1	0x62
TRANSPARENT_MSG	Transparent message	← →	1	0x70
POLL_RESP	Poll response	←	1	0x91
EVENT_RESP	Event response	←	1	0xB0
CONN_HANDLE_RESP	Connection handle response	←	1	0xC0
DEVICE_ID_RESP	Device ID response	←	1	0xC1
ENCRYPT_SELECT_RESP	Encryption selection response	←	1	0xC2
ENCRYPT_KEY_RESP	Encryption key exchange response	← →	1	0xC3
HASH_SELECT_RESP	Hash selection response	←	1	0xC4
PATH_SUPERVISION_RESP	Path supervision response	← →	1	0xC5
SET_TIME_RESP	Set time response	→	1	0xC7
VERSION_RESP	Protocol version response	←	1	0xC8
PMTU_RESP	P-MTU response	←	1	0xE0
PMTU_PROBE_RESP	P-MTU probe response	←	1	0xE1
DTLS_COMPLETE_RESP	DTLS completed response	←	1	0xE2
TRANSPARENT_RESP	Transparent response	← →	1	0xF0

The message ID of any response is the same as the message ID of the corresponding command, but with bit 7 set.