

# 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

|  |    |
|--|----|
| FOREWORD .....                               | 6  |
| 1 Scope .....                                | 8  |
| 2 Normative references .....                 | 8  |
| 3 Terms, definitions and abbreviations ..... | 8  |
| 3.1 Terms and definitions .....              | 8  |
| 3.2 Abbreviations .....                      | 9  |
| 4 Objective .....                            | 9  |
| 5 Messaging .....                            | 10 |
| 5.1 General .....                            | 10 |
| 5.2 Message format overview .....            | 10 |
| 5.2.1 General .....                          | 10 |
| 5.2.2 Identifiers .....                      | 10 |
| 5.2.3 Message format .....                   | 11 |
| 5.2.4 Connection handle .....                | 12 |
| 5.2.5 Device ID .....                        | 12 |
| 5.2.6 Message ID .....                       | 13 |
| 5.2.7 Message length .....                   | 14 |
| 5.2.8 Sequence numbers .....                 | 14 |
| 5.2.9 Flags .....                            | 14 |
| 5.3 Padding and message length .....         | 14 |
| 5.3.1 Padding .....                          | 14 |
| 5.3.2 Message length .....                   | 15 |
| 5.4 Hashing .....                            | 15 |
| 5.5 Encryption .....                         | 15 |
| 5.5.1 General .....                          | 15 |
| 5.5.2 Key exchange .....                     | 16 |
| 5.6 Timeouts and retries .....               | 16 |
| 5.7 Version number .....                     | 17 |
| 5.8 Reverse commands .....                   | 17 |
| 5.9 Initial values .....                     | 18 |
| 6 Message types .....                        | 18 |
| 6.1 General .....                            | 18 |
| 6.2 Path supervision .....                   | 18 |
| 6.2.1 General .....                          | 18 |
| 6.2.2 Poll message .....                     | 18 |
| 6.2.3 Poll response .....                    | 19 |
| 6.3 Event reporting .....                    | 19 |
| 6.3.1 Event message format .....             | 19 |
| 6.3.2 Event response format .....            | 22 |
| 6.4 Configuration messages .....             | 23 |
| 6.4.1 General .....                          | 23 |
| 6.4.2 Connection handle request .....        | 23 |
| 6.4.3 Connection handle response .....       | 24 |
| 6.4.4 Device ID request .....                | 24 |
| 6.4.5 Device ID response .....               | 25 |
| 6.4.6 Encryption selection request .....     | 25 |

|  |  |    |
|--|--|----|
| 6.4.7  | Encryption selection response.....                   | 26 |
| 6.4.8  | Encryption key exchange request.....                 | 26 |
| 6.4.9  | Encryption key exchange response.....                | 27 |
| 6.4.10   | Hash selection request.....                          | 27 |
| 6.4.11   | Hash selection response.....                         | 28 |
| 6.4.12   | Path supervision request.....                        | 28 |
| 6.4.13   | Path supervision response.....                       | 29 |
| 6.4.14   | Set time command.....                                | 29 |
| 6.4.15   | Set time response.....                               | 29 |
| 6.4.16   | Protocol version request.....                        | 30 |
| 6.4.17   | Protocol version response.....                       | 30 |
| 6.4.18   | Transparent message.....                             | 30 |
| 6.4.19   | Transparent response.....                            | 30 |
| 6.4.20   | DTLS completed request.....                          | 31 |
| 6.4.21   | DTLS completed response.....                         | 31 |
| 6.4.22   | RCT IP parameter request.....                        | 31 |
| 6.4.23   | RCT IP parameter response.....                       | 32 |
| 7  | Commissioning and connection setup.....              | 32 |
| 7.1  | Commissioning.....                                   | 32 |
| 7.1.1  | General.....   | 32 |
| 7.1.2  | Procedures.....                                      | 33 |
| 7.1.3  | Commissioning message sequence.....                  | 33 |
| 7.1.4  | Commissioning using shared secret.....               | 34 |
| 7.1.5  | Commissioning using X.509 certificates and DTLS..... | 35 |
| 7.2  | Connection setup.....                                | 36 |
| Annex A (normative)                            | Result codes.....                                    | 38 |
| Annex B (normative)                            | Protocol identifiers.....                            | 39 |
| Annex C (normative)                            | Shared secret.....                                   | 40 |
| C.1  | Formatting of the shared secret.....                 | 40 |
| C.2  | Checksum for shared secret formatting.....           | 40 |
| C.3  | Example of secret encoding and formatting.....       | 40 |
| Annex D (informative)                          | Examples of messaging sequences.....                 | 42 |
| D.1  | Commissioning.....                                   | 42 |
| D.2  | Connection setup.....                                | 45 |
| Annex E (informative)                          | Examples of application protocols.....               | 48 |
| E.1  | SIA.....   | 48 |
| E.2  | Ademco contact ID.....                               | 48 |
| E.3  | Scancom fast format.....                             | 49 |
| E.4  | VdS 2465.....  | 49 |
| Annex F (informative)                          | Design principles.....                               | 51 |
| F.1  | General.....   | 51 |
| F.2  | Information security.....                            | 51 |
| F.3  | Use of UDP signalling.....                           | 51 |
| Bibliography                                   | .....  | 52 |
| Table 1 – Identifiers                          | .....  | 10 |
| Table 2 – Basic unencrypted format of messages | .....  | 11 |

|   |    |
|---|----|
| Table 3 – Basic encrypted format of messages .....              | 11 |
| Table 4 – Message ID overview .....                             | 13 |
| Table 5 – Flags.....  | 14 |
| Table 6 – Hashing IDs .....                                     | 15 |
| Table 7 – Encryption IDs.....                                   | 16 |
| Table 8 – Reverse commands .....                                | 17 |
| Table 9 – Initial values.....                                   | 18 |
| Table 10 – Poll message SPT ← → RCT.....                        | 18 |
| Table 11 – Poll response RCT ← → SPT.....                       | 19 |
| Table 12 – Event message format – SPT → RCT .....               | 20 |
| Table 13 – Event message format – Fields .....                  | 20 |
| Table 14 – Event field.....                                     | 21 |
| Table 15 – Time event field.....                                | 21 |
| Table 16 – Time message field.....                              | 21 |
| Table 17 – Link field – IP address.....                         | 22 |
| Table 18 – Link field – IP port number .....                    | 22 |
| Table 19 – Link field – URL.....                                | 22 |
| Table 20 – Link field – Filename.....                           | 22 |
| Table 21 – Event response message format.....                   | 23 |
| Table 22 – Connection handle request message format .....       | 24 |
| Table 23 – Connection handle response message format.....       | 24 |
| Table 24 – Device ID request message format.....                | 24 |
| Table 25 – Device ID request flags .....                        | 25 |
| Table 26 – Device ID response message format.....               | 25 |
| Table 27 – Encryption selection request message format .....    | 25 |
| Table 28 – ‘Master encryption selection request’ flag .....     | 26 |
| Table 29 – Encryption selection response message format .....   | 26 |
| Table 30 – Encryption key exchange request message format.....  | 26 |
| Table 31 – ‘Master key request’ flag.....                       | 27 |
| Table 32 – Encryption key exchange response message format..... | 27 |
| Table 33 – Hash selection request message format .....          | 28 |
| Table 34 – Hash selection response message format .....         | 28 |
| Table 35 – Path supervision request message format.....         | 28 |
| Table 36 – Path supervision response message format.....        | 29 |
| Table 37 – Set time command message format.....                 | 29 |
| Table 38 – Set time response message format .....               | 29 |
| Table 39 – Protocol version request message format .....        | 30 |
| Table 40 – Protocol version response message format .....       | 30 |
| Table 41 – Transparent message format .....                     | 30 |
| Table 42 – Transparent response format.....                     | 31 |
| Table 43 – DTLS completed request message format .....          | 31 |
| Table 44 – DTLS completed response message format.....          | 31 |
| Table 45 – RCT IP parameter request message format.....         | 32 |

|  |    |
|--|----|
| Table 46 – RCT IP parameter response message format.....           | 32 |
| Table 47 – Message flow during the commissioning of a new SPT..... | 33 |
| Table 48 – Message flow during connection setup.....               | 36 |
| Table A.1 – Result codes .....                                     | 38 |
| Table B.1 – Protocol identifiers.....                              | 39 |
| Table D.1 – Commissioning messaging sequence .....                 | 42 |
| Table D.2 – Messaging sequence during connection setup.....        | 45 |

## 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*