IEC 61158-6-15

Edition 2.0 2010-08

INTERNATIONAL STANDARD

Industrial communication networks – Fieldbus specifications – Part 6-15: Application layer protocol specification – Type 15 elements

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XD

ICS 25.04.40; 35.100.70; 35.110

ISBN 978-2-88912-131-1

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 9
1.1 General 9
1.2 Specifications 9
1.3 Conformance 10
2 Normative references 10
3 Terms and definitions, abbreviations, symbols and conventions 10
3.1 Terms and definitions 10
3.2 Abbreviations and symbols 17
3.3 Conventions 19
3.4 Conventions used in state machines 21
4 Abstract syntax for client/server 22
5 Transfer syntax for client/server 22
5.1 General 22
5.2 Common APDU structure 22
5.3 Service-specific APDU structures 26
5.4 Data representation ‘on the wire’ 51
6 Abstract syntax for publish/subscribe 51
7 Transfer syntax for publish/subscribe 52
7.1 General 52
7.2 APDU structure 52
7.3 Sub-message structure 53
7.4 APDU interpretation 55
7.5 Service specific APDU structures 57
7.6 Common data representation for publish/subscribe 79
8 Structure of FAL protocol state machines 83
9 AP-context state machines for client/server 85
10 FAL service protocol machine (FSPM) for client/server 85
10.1 General 85
10.2 FSPM state tables 85
10.3 Functions used by FSPM 92
10.4 Parameters of FSPM/ARPM primitives 92
10.5 Client/server server transactions 92
11 Application relationship protocol machines (ARPMs) for client/server 94
11.1 Application relationship protocol machines (ARPMs) 94
11.2 AREP state machine primitive definitions 95
11.3 AREP state machine functions 96
12 DLL mapping protocol machine (DMPM) for client/server 96
12.1 AREP mapping to data link layer 96
12.2 DMPM states 97
12.3 DMPM state machine 97
12.4 Primitives exchanged between data link layer and DMPM 98
12.5 Client/server on TCP/IP 98
13 AP-Context state machines for publish/subscribe 102

14 Protocol machines for publish/subscribe 102
14.1 General 102
14.2 Publish/subscribe on UDP 104
Bibliography 105

Figure 1 – APDU Format 22
Figure 2 – Client to server confirmed service request 24
Figure 3 – Normal response from server to client 24
Figure 4 – Exception response from server to client 24
Figure 5 – Client to server unconfirmed service request 25
Figure 6 – Publish/subscribe APDU 52
Figure 7 – Flags of issue request 58
Figure 8 – Flags of heartbeat request 60
Figure 9 – Flags of VAR request 64
Figure 10 – Flags of GAP request 66
Figure 11 – Flags of ACK request 68
Figure 12 – Flags of INFO_DST request 72
Figure 13 – Flags of INFO_REPLY request 73
Figure 14 – Flags of INFO_SRC request 75
Figure 15 – Flags of INFO_TS request 77
Figure 16 – Flags of PAD request 78
Figure 17 – Encoding of octet 80
Figure 18 – Encoding of boolean 80
Figure 19 – Encoding of unsigned short 80
Figure 20 – Encoding of unsigned long 80
Figure 21 – Encoding of unsigned long long 81
Figure 22 – Encoding of float 81
Figure 23 – Encoding of double 81
Figure 24 – Relationships among protocol machines and adjacent layers 84
Figure 25 – State transition diagram of FSPM 85
Figure 26 – Transaction state machine, per connection 86
Figure 27 – Client/server server transactions 93
Figure 28 – State transition diagram of the Client ARPM 94
Figure 29 – State transition diagram of the server ARPM 95
Figure 30 – State transition diagram of DMPM 97
Figure 31 – APDU Format 98
Figure 32 – TCP/IP PDU Format 99
Figure 33 – Publish/subscribe receiver 103

Table 1 – Conventions used for state machines 21
Table 2 – Exception code 25
Table 3 – Read discretes request 26
Table 4 – Read discretes response 26

Table 5 – Read coils request 27
Table 6 – Read coils response 27
Table 7 – Write single coil request 28
Table 8 – Write single coil response 28
Table 9 – Write multiple coils request 29
Table 10 – Write multiple coils response 29
Table 11 – Broadcast write single coil request 30
Table 12 – Broadcast write multiple coils request 31
Table 13 – Read input registers request 31
Table 14 – Read input registers response 32
Table 15 – Read holding registers request 32
Table 16 – Read holding registers response 33
Table 17 – Write single holding register request 33
Table 18 – Write single holding register response 34
Table 19 – Write multiple holding registers request 34
Table 20 – Write multiple holding registers response 35
Table 21 – Mask write holding register request 36
Table 22 – Mask write holding register request 36
Table 23 – Read/Write multiple holding registers request 37
Table 24 – Read/Write multiple holding registers response 38
Table 25 – Read FIFO request 38
Table 26 – Read FIFO response 39
Table 27 – Broadcast write single holding register request 40
Table 28 – Broadcast write multiple holding registers request 41
Table 29 – Read file record request 42
Table 30 – Read file record response 43
Table 31 – Write file record request 44
Table 32 – Write file record response 46
Table 33 – Read device identification request 47
Table 34 – Device identification categories 48
Table 35 – Read device ID code 48
Table 36 – Read device identification response 49
Table 37 – Conformity level 50
Table 38 – Requested vs. returned known objects 51
Table 39 – APDU structure 53
Table 40 – Sub-message structure 54
Table 41 – Publish/subscribe service identifier encoding 54
Table 42 – Attributes changed modally and affecting APDUs interpretations 56
Table 43 – Issue request 57
Table 44 – Meaning of issue request flags 58
Table 45 – Interpretation of issue 59
Table 46 – Heartbeat request 60
Table 47 – Meaning of heartbeat request flags 61

Table 48 – Interpretation of heartbeat 62
Table 49 – VAR request 63
Table 50 – Meaning of VAR request flags 64
Table 51 – Interpretation of VAR 65
Table 52 – GAP request 66
Table 53 – Meaning of GAP request flags 67
Table 54 – Interpretation of GAP 67
Table 55 – ACK request 68
Table 56 – Meaning of ACK request flags 69
Table 57 – Interpretation of ACK 69
Table 58 – Header request 70
Table 59 – Change in state of the receiver 71
Table 60 – INFO_DST request 71
Table 61 – Meaning of INFO_DST request flags 72
Table 62 – INFO_REPLY request 73
Table 63 – Meaning of INFO_REPLY request flags 74
Table 64 – INFO_SRC request 75
Table 65 – Meaning of INFO_SRC request flags 75
Table 66 – INFO_TS request 76
Table 67 – Meaning of INFO_TS request flags 77
Table 68 – PAD request 78
Table 69 – Meaning of PAD request flags 78
Table 70 – Semantics 79
Table 71 – FSPM state table – client transactions 87
Table 72 – FSPM state table – server transactions 92
Table 73 – Function MatchInvokeID() 92
Table 74 – Function HighBit() 92
Table 75 – Parameters used with primitives exchanged between FSPM and ARPM 92
Table 76 – Client ARPM states 94
Table 77 – Client ARPM state table 94
Table 78 – Server ARPM states 94
Table 79 – Server ARPM state table 95
Table 80 – Primitives issued from ARPM to DMPM 95
Table 81 – Primitives issued by DMPM to ARPM 95
Table 82 – Parameters used with primitives exchanged between ARPM and DMPM 96
Table 83 – DMPM state descriptions 97
Table 84 – DMPM state table – client transactions 97
Table 85 – DMPM state table – server transactions 98
Table 86 – Primitives exchanged between data-link layer and DMPM 98
Table 87 – Encapsulation parameters for client/server on TCP/IP 99

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS –

Part 6-15: Application layer protocol specification – Type 15 elements

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.

NOTE 1 Use of some of the associated protocol types is restricted by their intellectual-property-right holders. In all cases, the commitment to limited release of intellectual-property-rights made by the holders of those rights permits a particular data-link layer protocol type to be used with physical layer and application layer protocols in Type combinations as specified explicitly in the profile parts. Use of the various protocol types in other combinations may require permission from their respective intellectual-property-right holders.

International Standard IEC 61158-6-15 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision.

The main changes with respect to the previous edition are listed below:

- editorial corrections.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/607/FDIS	65C/621/RVD

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

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

A list of all parts of the IEC 61158 series, published under the general title *Industrial communication networks – Fieldbus specifications*, can be found on the IEC web site.

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:

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

NOTE 2 The revision of this standard will be synchronized with the other parts of the IEC 61158 series.

INTRODUCTION

This part of IEC 61158 is one of a series produced to facilitate the interconnection of automation system components. It is related to other standards in the set as defined by the “three-layer” fieldbus reference model described in IEC/TR 61158-1.

The application protocol provides the application service by making use of the services available from the data-link or other immediately lower layer. The primary aim of this standard is to provide a set of rules for communication expressed in terms of the procedures to be carried out by peer application entities (AEs) at the time of communication. These rules for communication are intended to provide a sound basis for development in order to serve a variety of purposes:

- as a guide for implementers and designers;
- for use in the testing and procurement of equipment;
- as part of an agreement for the admittance of systems into the open systems environment;
- as a refinement to the understanding of time-critical communications within OSI.

This standard is concerned, in particular, with the communication and interworking of sensors, effectors and other automation devices. By using this standard together with other standards positioned within the OSI or fieldbus reference models, otherwise incompatible systems may work together in any combination.

INDUSTRIAL COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS –

Part 6-15: Application layer protocol specification – Type 15 elements

1 Scope

1.1 General

The Fieldbus Application Layer (FAL) provides user programs with a means to access the fieldbus communication environment. In this respect, the FAL can be viewed as a “window between corresponding application programs.”

This standard provides common elements for basic time-critical and non-time-critical messaging communications between application programs in an automation environment and material specific to Type 15 fieldbus. The term “time-critical” is used to represent the presence of a time-window, within which one or more specified actions are required to be completed with some defined level of certainty. Failure to complete specified actions within the time window risks failure of the applications requesting the actions, with attendant risk to equipment, plant and possibly human life.

This standard defines in an abstract way the externally visible behavior provided by the Type 15 fieldbus Application Layer in terms of

a) the abstract syntax defining the application layer protocol data units conveyed between communicating application entities,
b) the transfer syntax defining the application layer protocol data units conveyed between communicating application entities,
c) the application context state machine defining the application service behavior visible between communicating application entities; and
d) the application relationship state machines defining the communication behavior visible between communicating application entities; and.

The purpose of this standard is to define the protocol provided to

a) define the wire-representation of the service primitives defined in IEC 61158-5-15, and
b) define the externally visible behavior associated with their transfer.

This standard specifies the protocol of the Type 15 IEC fieldbus Application Layer, in conformance with the OSI Basic Reference Model (ISO/IEC 7498) and the OSI Application Layer Structure (ISO/IEC 9545).

1.2 Specifications

The principal objective of this standard is to specify the syntax and behavior of the application layer protocol that conveys the application layer services defined in IEC 61158-5-15.

A secondary objective is to provide migration paths from previously-existing industrial communications protocols. It is this latter objective which gives rise to the diversity of protocols standardized in IEC 61158-6.

1.3 Conformance

This standard does not specify individual implementations or products, nor does it constrain the implementations of application layer entities within industrial automation systems. Conformance is achieved through implementation of this application layer protocol specification.

2 Normative references

The following referenced documents are indispensable for the application 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.

IEC 61158-5-15:2010[1], *Industrial communication networks – Fieldbus specifications - Part 5-15: Application layer service definition – Type 15 elements*

ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC 8822, *Information technology – Open Systems Interconnection – Presentation service definition*

ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 9545, *Information technology – Open Systems Interconnection – Application Layer structure*

---

1 To be published.