IEC 61158-6-28

Edition 1.0 2023-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Industrial communication networks – Fieldbus specifications – Part 6-28: Application layer protocol specification – Type 28 elements

Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-28: Spécification du protocole de la couche application – Éléments de type 28

IEC 61158-6-28:2023-03(en-fr)

IEC Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 61158-6-28

Edition 1.0 2023-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Industrial communication networks – Fieldbus specifications – Part 6-28: Application layer protocol specification – Type 28 elements

Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-28: Spécification du protocole de la couche application – Éléments de type 28

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040

ISBN 978-2-8322-6621-2

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS –

Part 6-28: Application layer protocol specification – Type 28 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.

Attention is drawn to the fact that the use of the associated protocol type is restricted by its 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 layer protocol type to be used with other layer protocols of the same type, or in other type combinations explicitly authorized by its intellectual-property-right holders.

NOTE Combinations of protocol types are specified in the IEC 61784-1 series and the IEC 61784-2 series.

IEC 61158-6-28 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65C/1206/FDIS	65C/1235/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

INTRODUCTION

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

INDUSTRIAL COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS –

Part 6-28: Application layer protocol specification – Type 28 elements

1 Scope

1.1 Overview

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

This part of IEC 61158 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 28 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 can cause failure of the applications requesting the actions, with attendant risk to equipment, plant and possibly human life.

This document defines in an abstract way the externally visible behavior provided by the Type 28 of the fieldbus Application Layer in terms of:

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

The purpose of this document is to define the protocol provided to:

- the wire-representation of the service primitives defined in IEC 61158-5-28, and
- the externally visible behavior associated with their transfer.

This document specifies the protocol of the Type 28 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 document is to specify the syntax and behavior of the application layer protocol that conveys the application layer services defined in IEC 61158-5-28.

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 series.

1.3 Conformance

This document 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 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.

NOTE All parts of the IEC 61158 series, as well as the IEC 61784-1 series and the IEC 61784-2 series are maintained simultaneously. Cross-references to these documents within the text therefore refer to the editions as dated in this list of normative references.

IEC 61158-1:2023, *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series*

IEC 61158-5-28:2023, *Industrial communication networks – Fieldbus specifications – Part 5-28: Application layer service definition – Type 28 elements*

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

ISO/IEC 7498-3, *Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing*

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

ISO/IEC 8825-7:2021, *Information technology - ASN.1 encoding rules − Part 7: Specification of Octet Encoding Rules (OER)*

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

ISO/IEC/IEEE 8802-3:2021, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet*

IETF RFC 791, J. Postel, *“Internet Protocol”, September 1981, available at https://www.rfc-editor.org/info/rfc791* [viewed 2022-09-14]

IETF RFC 2460, S. Deering and R. Hinden, *“Internet Protocol, Version 6 (IPv6) Specification”, December 1998, available at https://www.rfc-editor.org/info/rfc2460* [viewed 2022-09-14]

3 Terms, definitions, symbols, abbreviated terms and conventions

For the purposes of this document, the following terms, definitions, symbols, abbreviated terms and conventions apply.

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

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

3.1 Terms and definitions from other ISO/IEC standards

3.1.1 Terms and definitions from ISO/IEC 7498-1

a) abstract syntax
b) application entity
c) application process
d) application protocol data unit
e) application service element
f) application transaction
g) presentation context
h) transfer syntax

3.1.2 Terms and definitions from ISO/IEC 9545

a) application-association
b) application-process-type
c) application-service-element
d) application control service element

3.1.3 Terms and definitions from ISO/IEC 8824-1

a) object identifier
b) type
c) value
d) simple type
e) structured type
f) integer type
g) octet string type
h) null type
i) tagged type
j) any type
k) module
l) production

3.1.4 Terms and definitions from ISO/IEC 8825-7

a) encoding (of a data value)
b) data value
c) identifier octets (the singular form is used in this document)
d) length octet(s) (both singular and plural forms are used in this document)
e) contents octets

3.1.5 Terms and definitions from IEC 61158-5

a) cyclic

b) field device

c) clock synchronization

3.2 Type 28 fieldbus application-layer specific definitions

3.2.1
control device
device that controls all field devices for logical operations, timing, calculations, etc.

3.2.2
management node
device for allocating and managing Type 28 network physical communication resources

3.2.3
terminal node
device in Type 28 network that communicates based on allocated physical communication resources

3.2.4
RT Data
data sensitive to time deterministic requirements

3.2.5
non-RT Data
data insensitive to time deterministic requirements

3.3 Abbreviations and symbols

AL	Application layer
ALCE	Application layer clock entity
ALDE	Application layer data entity
ALME	Application layer management entity
ALS	Application layer service
AE	Application entity
AP	Application process
APDU	Application protocol data unit
APO	AP object
AR	Application relationship
ASE	Application service elements
C/S	Client/Server
DTU	Data transmission unit
DLSDU	Data-link service data unit
DLPDU	Data-link protocol data unit
MN	Management node
PUD	Protocol unit data
RT	Real-Time
RTA	Real-Time acyclic
RTC	Real-Time cyclic
TCD	Time command code

TCV Time Consumption value

TID Time ID

TIV Time information value

nRT non-Real-Time

TN Terminal node

3.4 Conventions

3.4.1 General concept

The FAL is defined as a set of object-oriented ASEs. Each ASE is specified in a separate subclause. Each ASE specification is composed of three parts: its class definitions, its services, and its protocol specification. The first two are contained in IEC 61158-5-28. The protocol specification for each of the ASEs is defined in this document.

The class definitions define the attributes of the classes supported by each ASE. The attributes are accessible from instances of the class using the Management ASE services specified in IEC 61158-5-28. The service specification defines the services that are provided by the ASE.

3.4.2 Conventions for class definitions

The data-link layer mapping definitions are described using templates. Each template consists of a list of attributes for the class. The general form of the template is defined in IEC 61158-1.

3.4.3 Abstract syntax conventions

When the "optional Parameters Map" parameter is used, a bit number which corresponds to each OPTIONAL or DEFAULT production is given as a comment.

3.5 Conventions used in state machines

3.5.1 State machine conventions for Type 28

The protocol sequences are described by means of state machines.

In state diagrams, states are represented as boxes, and state transitions are shown as arrows. Names of states and transitions of the state diagram correspond to the names in the textual listing of the state transitions.

The textual listing of the state transitions is structured as follows, see also Table 1.

– The first column contains the name or number of the transition.

– The second column defines the current state.

– The third column describes the condition of state transition and how it transits.

– The last column contains the next state.

Table 1 – State machine description elements

Number	Current state	Description	Next state

4 APDU structure

4.1 APDU header

When the Type 28 AL data is transmitted in the network, it has a unified APDU header structure as shown in Figure 1.

	Bit Offset								
Octet Offset	7	6	5	4	3	2	1	0	
0 to1	STF								
2 to 5	DID								
6 to 9	SID								
10	Pri								
11	OffSet								Len
12	OffSet				ULen				
13	ULen								
14	UNum								
15	Reserved								

IEC

Figure 1 – APDU header structure

– STF: Service Type Flag with 2 octets, which identifies the application service type. See Table 2 for the definition.

Table 2 – AL service type flag encoding

STF	Description
0x0100	Configuration notification service sent by the MN to the TN
0x0101	Work notification service sent by the MN to the TN
0x0102	Configuration response service provided by TN to the MN
0x0105	ID allocation service applied by TN to the MN.
0x0106	TN response confirmation service after the MN assigns an ID
0x0107	Reassign request service when dynamic ID assignment conflicts
0x0108	Request configuration service of dynamic online TN
0x0109	MN's response service after dynamic online TN fails to set up.
0x0110	Dynamic offline request service
0x1010	Periodic cycle data processing service
0x1020	RTC data writing operation service
0x1021	RTC data read operation service
0x1022	RTA data writing operation service
0x1024	RTA data reading operation service
0x1041	nRT data writing operation service
0x1042	nRT data reading operation service
0x1000	nRT MN requesting connection service
0x1001	nRT TN answering connection service
0x1002	nRT MN confirmation connection service
0x1003	nRT connection-based MN sending APDU service
0x1004	nRT connection-based MN sending configuration APDU service
0x1005	nRT connection-based TN response MN command service

STF	Description
0x1006	nRT connection-based TN response MN configuration service
0x1007	nRT non-connected mode MN command service
0x1008	nRT non-connected mode MN service
0x0200	Time service
0x0301	Resource application
0x0302	Resource release
0x0304	Resource update
0x0308	Resource confirmation
0x0310	Resource writing
0x0320	Resource reading
0x0400	Set NETWORKID (see IEC 61158-5-28, 6.6.6)
0x0401	Get NETWORKID (see IEC 61158-5-28, 6.6.6)
0x0402	Add MAC (defined in ISO/IEC/IEEE 8802-3) mapping table
0x0404	Delete MAC (defined in ISO/IEC/IEEE 8802-3) mapping table
0x0408	Modify MAC (defined in ISO/IEC/IEEE 8802-3) mapping table
0x0410	Query MAC (defined in ISO/IEC/IEEE 8802-3) mapping table
0x0411	Add IP (see IETF RFC 791) mapping table
0x0412	Delete IP (see IETF RFC 791) mapping table
0x0414	Modify IP (see IETF RFC 791) mapping table
0x0418	Query IP (see IETF RFC 791) mapping table
0x0421	Add IPv6 (see IETF RFC 2460) mapping table
0x0422	Delete IPv6 (see IETF RFC 2460) mapping table
0x0424	Modify IPv6 (see IETF RFC 2460) mapping table
0x0428	Query IPv6 (see IETF RFC 2460) mapping table
0x0500	Set network configuration parameters
0x0501	Get network configuration parameters
0x0502	Import network profile
0x0504	Export network profile
0x0508	Diagnose network operation state
0x0510	Diagnose node operation state
0x0511	Request log write
0x0512	Request to get logs
0x0514	Log file export
0x0600	Config virtual bus
0x0601	Load virtual bus
0x0602	Start virtual bus
0x0604	Suspend virtual bus
0x0608	Reset virtual bus
0x0610	Stop virtual bus
0x0611	Unload virtual bus