8

Fundamentals of IEC 60870-5

8.1 The IEC 60870-5 standard

8.1.1 Overall structure of standard

The standard IEC 60870-5 was produced by the International Electrotechnical Commission Technical Committee 57, Working Group 03, and published progressively from 1988.

The structure of IEC 60870-5 was introduced in the Preview Section 7.1. This showed how the standard is structured in a hierarchical manner, and illustrated how the companion standards relate to the other sections making up Part 5. Table 8.1 extends the preview information by showing the full structure of IEC 60870, together with the years of publication of the component parts and sections.

The sections IEC 60870-5-1 to IEC 60870-5-5 are the core specification documents for Part 5, the Transmission Protocols part of the standard. The companion standard sections, or simply companion standards, IEC 60870-5-101 to IEC 60870-5-104, are each separate application protocols intended for specific purposes. They provide the definitions of application level data objects and functions to completely define a working protocol. They are also referred to as profiles, and may sometimes be given the shorthand references T101, T102, T103, and T104, the T standing for telecontrol.

As shown in the preview, IEC 60870-5-101 provided the first complete working SCADA protocol under IEC 60870-5. This defines all the necessary application level functions and data objects to provide for telecontrol applications operating over geographically wide areas, using low bandwidth bit-serial communications. It covers general communications with RTUs, including data types and services that are suitable for electrical and substation systems. The data types are generic and suitable for wider SCADA applications.

The IEC 60870-5-102 and IEC 60870-5-103 companion standards provide data types and functions to support electrical protection systems. These include distance protection, line differential protection, and transformer differential protection.

As explained in the preview, the IEC 60870-5-104 companion standard has special significance. This defines operation of the transmission protocol over networks using standard transport profiles specifying the TCP and IP protocols. This companion standard

is not really independent of IEC 60870-5-101, but replaces the message transport sections with a network version, leaving the application level functions largely unaltered.

Main Parts

Reference	Description	Year
IEC 60870-1	General Considerations	1988
IEC 60870-2	Operating Conditions	1995
IEC 60870-3	Interfaces (electrical characteristics)	1989
IEC 60870-4	Performance Requirements	1990
IEC 60870-5	Transmission Protocols	1990
IEC 60870-6	Telecontrol Protocols Compatible with ISO and ITU-T Recommendations	1995

Sections of IEC 60870-5

Reference	Description	Year
IEC 60870-5-1	Transmission Frame Formats	1990
IEC 60870-5-2	Link Transmission Procedures	1992
IEC 60870-5-3	General Structure of Application Data	1992
IEC 60870-5-4	Definition and Coding of Application Information Elements	1993
IEC 60870-5-5	Basic Application Functions	1995

Companion Standards of IEC 60870-5

Reference	Description	Year
IEC 60870-5-101	Companion Standard for Basic Telecontrol Tasks	1995
IEC 60870-5-102	Companion Standard for Transmission of Integrated Totals	1996
IEC 60870-5-103	Companion Standard for Protection Communication	1997
IEC 60870-5-104	Network Access using Standard Transport Profiles	2000

Table 8.1
Full structure of IEC 60870 standard

8.1.2 Development of standards

IEC standards are subject to review and the issue of amendments from time to time, and since the publication of IEC 60870-5-101, this profile has had two amendments issued. The first amendment added a small number of information object definitions. The second amendment added a significant amount of clarifying detail, the purpose of which was to remove ambiguities and so better provide for interoperability. It is anticipated that during 2002 the standard will be reissued as one document including the two amendments.

With amendments the complete version of this profile is as shown in Table 8.2.

Reference	Description	Year-Month
IEC 60870-5-101	Companion Standard for Basic Telecontrol Tasks	1995-11
IEC 60870-5-101-am1	Companion Standard for Basic Telecontrol Tasks Amendment 1	2000-04
IEC 60870-5-101-am2	Companion Standard for Basic Telecontrol Tasks Amendment 2	2001-10

Table 8.2
IEC 60870-5-101 including amendments

8.1.3 Obtaining standards

Should access to the standards be required, they may be purchased online from the IEC (at www.iec.ch). As an alternative that may be less expensive, it is worth checking if they have been published as a national standard, as is often the case. In Australia, IEC 60870-5 sections 1 to 5 are available as AS 60870.5.1 to AS 60870.5.5 and are available online (at www.standards.com.au). However, the companion standards are not presently available and must be obtained from the IEC.

An alternative to purchase of the standards is to view them at a public or university library.

8.1.4 Description of contents

In this section the contents of each section of IEC 60870-5 are briefly described. This is intended to provide a guide to assist the reader should it be necessary to refer to them.

IEC 60870-5-1 1990

Transmission frame formats

This describes the operation of the physical and data link layers in terms of the services provided to higher layers. It provides a choice of four data link frame types identified as FT1.1, FT1.2, FT2 and FT3, each with a different level of security against data errors. Fixed and variable length versions of the frames are described, and a set of transmission rules is provided for each. Two single control character transmissions are provided as an efficient means of transmitting control information such as acknowledgments.

8.1.5 IEC 60870-5-1 1990

Link transmission procedures

This section represents the four frame formats from IEC 60870-5-1 and then describes the internal processes in terms of the service primitives and transmission procedures. The service primitives are the control indications passed between the link layer and its higher level user, and the transmission procedures describe the sequence of events occurring over the physical communications link. A control field is described that is transmitted over the link and is used by the link layer procedures of each side of the link in controlling the transmission process. The terms unbalanced and balanced transmission are presented and used to describe whether transmission can be initiated only by a master station, or by any station. Services and transmission procedures are presented in detail for both unbalanced and balanced transmissions.

8.1.6 IEC 60870-5-3 1992

General structure of application data

This section presents two models of the structure of data at the application level. The reference model 2 version shows how application user data, for example point information to be transmitted, is encapsulated within an application protocol data unit, with or without application protocol control information added, and then passed to the underlying link layer for transmission. It also describes a general structure for application data, and rules for forming application data units in general.

8.1.7 IEC 60870-5-4 1993

Definition and coding of application information elements

This section provides rules for the definition of information elements, and defines a common set of information elements that may be used for transmission of information in telecontrol applications. These include generic elements such as signed and unsigned integers, fixed and floating point numbers, bit-strings, and time elements. The intention of this section is to provide a set of information building blocks from which a companion standard, or profile can utilize selectively to build a complete set of application level information objects. No such set of information objects is selected by this section, however.

8.1.8 IEC 60870-5-5 1995

Basic application functions

This section describes the highest level functions of the transmission protocol, which are those application functions above layer 7 of the OSI model. Application service primitives are the request and response indications passed between the application layer and the application user. Application functions are described.

A set of basic application functions and associated service primitives, or requests and indications, are presented. These cover the highest level functions that would be required to carry out telecontrol operations. They include station initialization, methods of acquiring data, clock synchronization, transmission of commands, totalizer counts, and file transfer. Again, it is stated in this section that it would be the role of a specific companion standard to select from these functions and possibly add to them in defining a complete working protocol.

8.1.9 IEC 60870-5-101 1995

Companion standard for basic telecontrol tasks (including amendments 1 and 2).

The companion standard defines a complete telecontrol protocol by detailing selections from options described in sections 1 to 5 of IEC 60870 Part 5, and by defining a complete set of application service data units (ASDUs).

Its main sub-sections are listed below, and a short description of the contents of these follows this list:

- General rules
- Physical layer
- Link layer
- Application layer and user process
- Interoperability

General rules

This is really an introduction that states the main selections made for the physical layer, link layer, application layer, and user process. They in effect provide a brief overview of each of the following sections.

Physical layer

This describes the requirements for the interface with external data communication equipment using standard ITU-T V.24/V.28 (RS-232) or balanced X.24/X.27 (RS-485) signals. The types of fixed network configurations such as point-to-point, and multi-point, are described.

Link layer

Selections of the frame format F1.2, and the fixed and variable frame lengths are made. The detailed operation of the link layer is specified, making selections from IEC 60870-5-2. Operation of the link is described for both unbalanced and balanced operation, which corresponds to whether only the master station, or any station, may initiate message transmissions. Amendment 2 contains significant additional information clarifying the procedures with the use of state transition diagrams.

Application layer and user process

This defines the overall structure of the application level data, the application service data unit or ASDU, defines the set of ASDUs available, and makes selections of application functions from IEC 60870-5-5. The definition of ASDUs is carried out in two sub-sections. The first sub-section defines the available information elements. These are used in the second sub-section as building blocks in constructing the full set of ASDUs. The user process sub-section makes selections from IEC 60870-5-5 and includes additional detail for some of the functions.

Interoperability

This provides a check-box method for specifying the particular features supported by a specific product, under the following type headers:

- System or device
- Network configuration
- Physical layer
- Link layer
- Application layer

8.2 Protocol architecture

8.2.1 EPA and OSI reference models

As for DNP3, IEC 60870-5 is based on the three-layer enhanced performance architecture or EPA model for data communications. These models are described in detail later in this text, which shows how the EPA model is a simplified form of the OSI seven layer reference model to provide optimum performance for telecontrol applications.

In the Figure 8.1, the relationship between the OSI model and the EPA model is represented. This shows that the EPA model basically omits the presentation, session and transport layers of the OSI model.

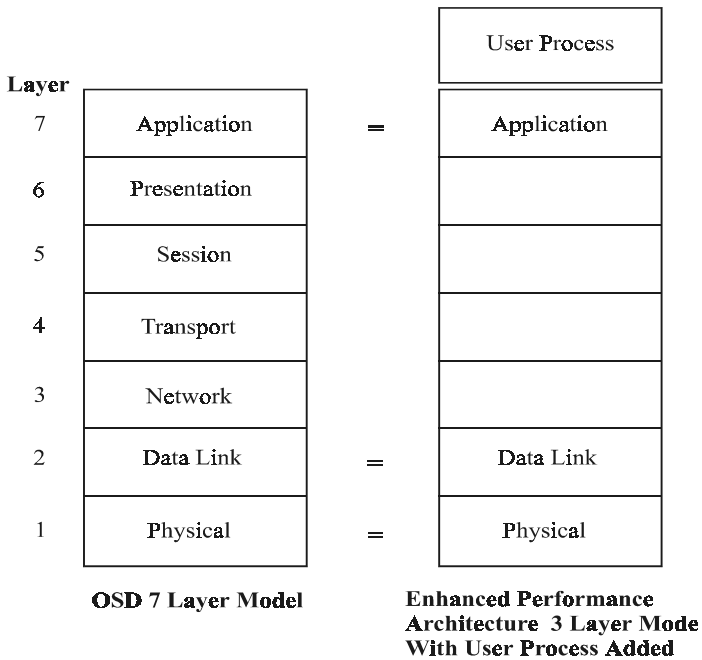


Figure 8.1
Relationship of EPA model to OSI 7 layer model

The structure of the EPA model is appropriate for a continuously operating system that operates over a single network. One layer is normally added to the top of the basic EPA model representation is identified as the user layer. This is included to represent the various functions or processes that must be defined to provide telecontrol system operations. These are required to be defined to provide for the interoperability between equipment that will result in a fully operable telecontrol system, rather than merely a data communication system.

For the first defined companion standard IEC 60870-5-101 or T101 profile, a four layer model as illustrated at the right-hand side of Figure 8.1 provides an accurate representation of the architecture of the protocol. In the case of the networked version IEC 60870-5-104, or the T104 profile, additional layers of the OSI model must be included to

provide for transport of messages over networks using standard network protocols. These are the transport and network layers corresponding to the use of the TCP and IP protocols.

The two architectures are shown in Figure 8.2 below.

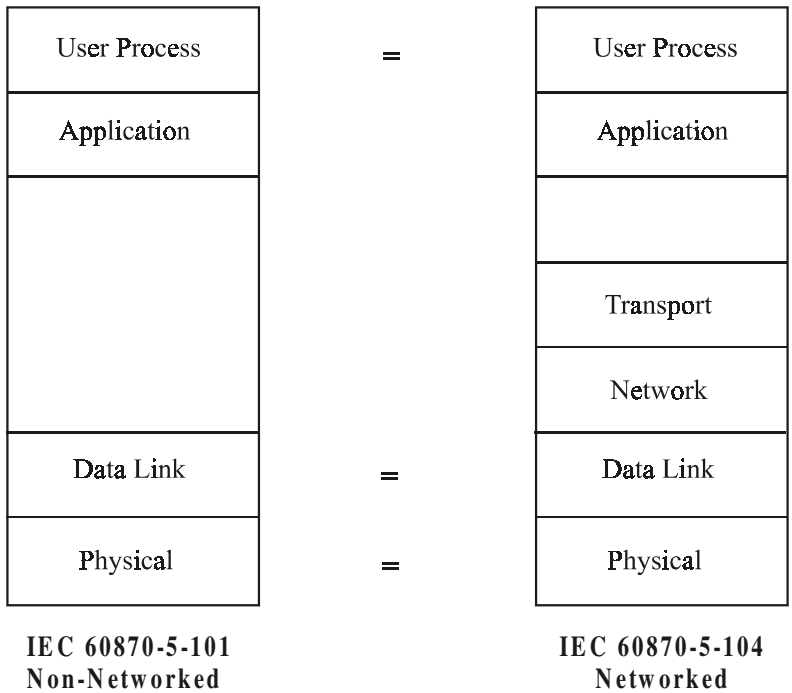


Figure 8.2
Architectures for T101 and T104

As is clear from Figure 8.2, the operation of the lower layers of the networked version, IEC 60870-5-104 is completely different from that of the non-networked version, IEC 60870-5-101. These layers correspond to all the layers below the application layer, which for these architectures are the layers concerned with message transport.

The remainder of this chapter will focus on the non-networked version only. The networked version will be returned to in Chapter 9.

8.2.2 Selections from standards

The benefit of the OSI reference model, and the EPA models derived from it and shown in Figure 8.2, is that they provide a framework for description of protocol operation. Describing the operation of the protocol is a matter of specifying the functions of each layer, and specifying the structure of information passing between the layers.

Under the IEC standard, it is the companion standard IEC 60870-5-101 that completely specifies the protocol. It does this by referring to the main sections of the IEC 60870-5 standard, and by making particular selections from options that may be available within those sections.

Table 8.3 shows how the different sections of the IEC 60870-5 set of standards correspond with the layers of the model.

Layer	Source	Selections
User Process	IEC 60870-5-5	Application functions
Application	IEC 60870-5-4	Application information elements
	IEC 60870-5-3	ASDUs
Link	IEC 60870-5-2	Transmission procedures
	IEC 60870-5-1	Frame formats
Physical	ITU-T	Interface specification

Table 8.3
Standards selections for IEC 60870-5-101

For comparison the corresponding information for the networked version IEC 60870-5-104 is shown in Table 8.4. This illustrates how the lower layers of the IEC 60870-5-101 companion standard have been completely replaced by the standard TCP/IP transport profiles.

Layer	Source	Selections
User Process	IEC 60870-5-101	Application functions
Application	IEC 60870-5-101	ASDUs and Application Information Elements.
Transport	TCP / IP Transport and network protocol suite	
Network		
Link		
Physical		

Table 8.4
Standards selections for IEC 60870-5-104

8.3 Physical layer

The physical layer is concerned with the transmission and reception of data over the physical medium. This level is concerned with the transmission of bits and bytes, but not with the meaning of those bytes. The physical interface is defined in terms of the electrical characteristics, and individual signals passing over the interface.

The definition of the physical layer includes specification of the signal interface between the IEC 60870-5 and the communications devices to external world, and the network configurations that are attached to these. These are illustrated in Figure 8.3. This shows a SCADA master station server connected to a radio modem via a serial port operating at 9.6 kB/s. The radio modems form a multi-point-star configuration in which the master communicates with both outstations simultaneously, and either outstation can communicate back to the master.

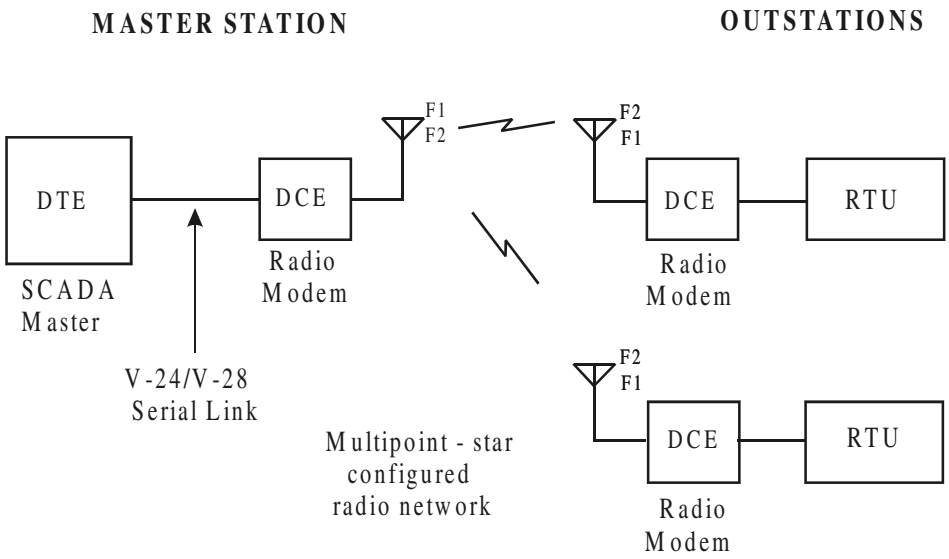


Figure 8.3
Interfacing to communications network

8.3.1 Communications interface

To allow the use of standard data communications equipment, the standard utilizes existing widely used standards covering the exchange between data terminal equipment (DTE) and data communication equipment (DCE). These communication interface standards are the ITU-T equivalents to the well known Electrical Industries Association RS-232 and RS-485 standards. These provide for unbalanced and balanced full-duplex serial data transmission between the data device and communications equipment such as a modem.

The use of this interface is illustrated in Figure 8.3, at the connection between the server of a SCADA master station, and a radio modem. The DTE-DCE interface is simply an RS-232 cable between a serial port of the computer, and a similar port on the radio modem. It is also used between the RTUs and their radio modems.

The data transmission speeds are defined as follows:

Interface Type	Transmission Speed (bits/sec)
V.24/V.28 FSK Interface	100, 200, 300, 600, 1200
V.24 / V.28 Modem Interface	300, 600, 1200, 2400, 4800, 9600
X.24 / X.27 Synchronous	2400, 4800, 9600, 19200, 38400, 56000, 64000

Table 8.5
DTE-DCE interface transmission speeds

In addition to interfaces using the specified standards, it should be noted that the T101 profile does allow the use of other physical interfaces by agreement between vendor and user.

8.3.2 Network configurations

The T101 profile specifies support for the following network configurations or topology:

- Point-to-point
- Multiple point-to-point
- Multi-point-star
- Multi-point-party line
- Multi-point-ring

These are defined by IEC 60870-1-1, and are depicted in Figure 8.4. In the drawing the square symbols represent controlling or master stations, and the triangles represent controlled, or outstations. The small circles at the points of connection are the ports.

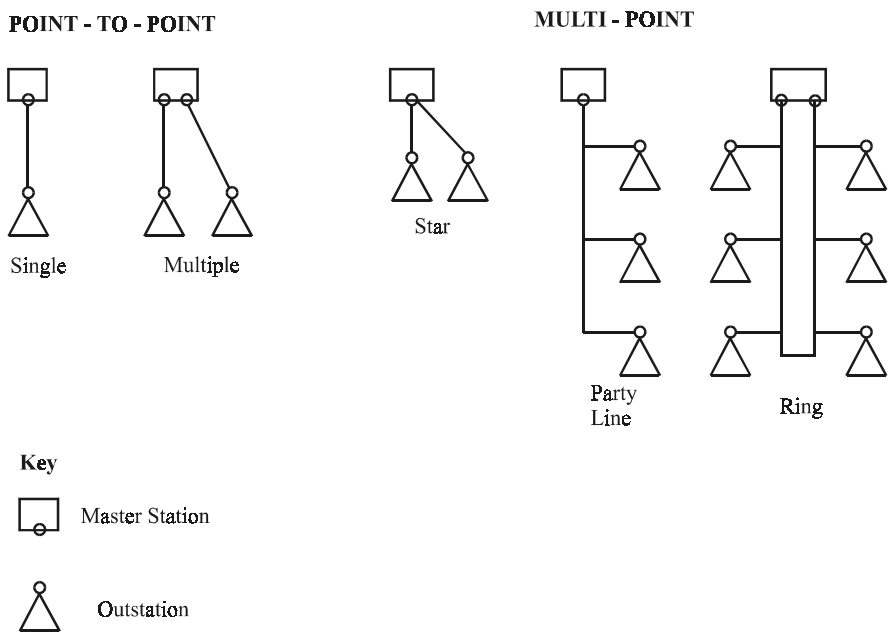


Figure 8.4
Network configurations

From the diagram it may be seen that these fall into two basic types; point-to-point and multi-point. A point-to-point link has one master station and one outstation. A multi-point network has a master station connected to a number of outstations. The ring configuration is only different in that it incorporates redundancy by providing a second port on the master station that can be used for communications should the ring be broken.

In the point-to-point configurations either the master or the outstation(s) can transmit messages, provided that a full-duplex channel is used. In the multi-point configurations the master communicates in parallel to all connected outstations. The outstations share a return communications channel, and therefore only one may transmit at a time.

Note that combinations of links may form a hierarchical network where intermediate RTUs may act as local master stations to RTUs connected to them. These are sometimes referred to as sub-master stations.

8.4 Data link layer

The data link layer is responsible for the passing of data across the communications channel, and ensuring that the data is received in full and uncorrupted by errors. It does this using a unit of data known as a frame, combined with procedures to govern its transmission and reception. The frame is made up of an amount of data that is large enough to carry control information such as a destination address, checking information used to detect errors, and a payload of data, if required. It is also an amount of data that is not too large, so that a transmission error will not cause the loss of too much data, or so that timing discrepancies between transmitter and receiver can lead to loss of synchronism.

IEC 60870-5-101, or T101, specifies the operation of the data link layer by referring to and making selections from the standards identified in Table 8.1, repeated in the following extract:

Link Layer	IEC 60870-5-2	Transmission procedures
	IEC 60870-5-1	Frame formats

In this section the operation of the data link layer is explained in detail, commencing with the data frame structure and then looking at the transmission procedures.

8.4.1 Frame format

The frame format used by T101 is referred to as the FT1.2 format. There are two forms of this, one of fixed length and the other of variable length. The fixed length frame is restricted to use for frames carrying no user data, and therefore is used only for data link control command and acknowledgment frames. In addition to the fixed and variable length frames, there is a 'single control character' frame which consists of a single byte. This may be used for acknowledgment only.

These frames are shown in Figures 8.5 and 8.6. Figure 8.5 shows the actual bit pattern that would be seen on the physical channel, interpreted from left to right. This representation includes the start and stop bits that are transmitted with every byte or octet of the frame. The overall frame construction is shown in Figure 8.6. This does not represent the bit pattern, but shows only the information content down to the octet level. For consistency with the applicable standards, these are presented vertically in octet order. Thus, the first octet is shown at the top, and following octets are shown below. Clarification of the order of bits and octets is included in the following section.

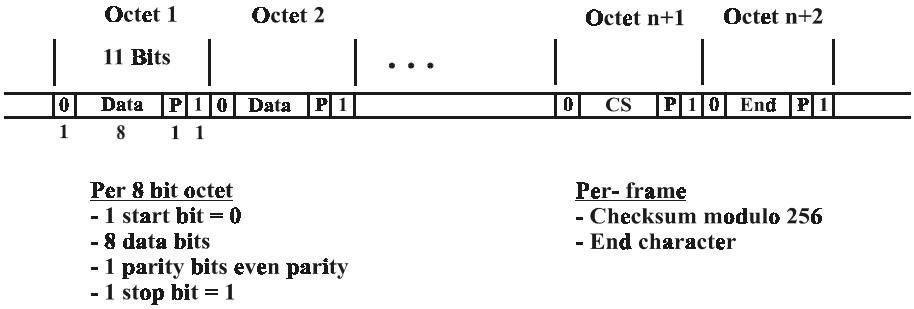


Figure 8.5
Bit-sequence representation of FT1.2 Frame

From the bit-sequence representation above, it is possible to see that the maximum data rate of the frame is approximately eight-elevenths of the bit transmission rate. This is reduced further when the frame overheads such as addressing, start and stop characters, checksum, and control information are accounted for. These overheads can be seen in Figure 8.6 which shows the overall frame structure.

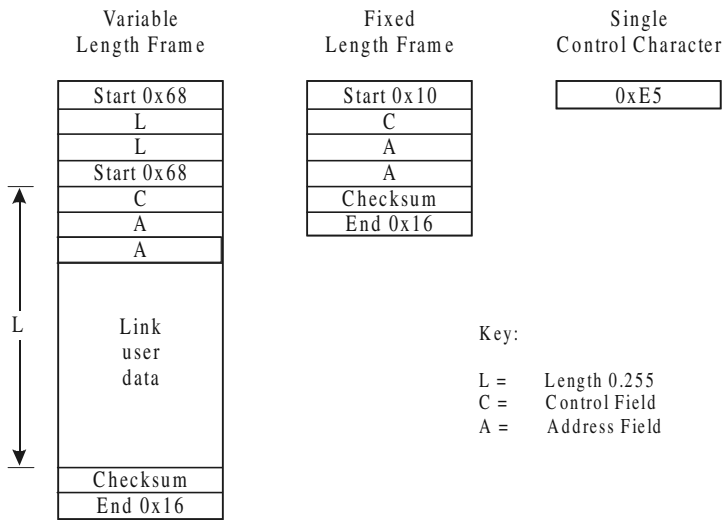


Figure 8.6
FT1.2 frame options under IEC 60870-5-101

The following points are noted about the data link frames:

- Only the variable length frame can carry user data
- The variable length frame can carry up to 253 octets of link user data
- The length L is repeated twice, and the two values of L must be equal for the frame to be accepted as valid
- The maximum frame length is 261 octets. However, a lower maximum frame length may be specified by a manufacturer or by the system user as a system parameter

- The fixed length frame is 5 or 6 octets long
- Address field A may be 1 or 2 octets, determined by a fixed system parameter
- A broadcast address is defined as 0xFF or 0xFFFF for 1 and 2 octet addresses respectively
- The checksum is the modulo 256 sum of the frame user data (not the link user data). This is the data between the last start character and the checksum, L octets for the variable frame
- Rules state that no more than one bit-time idle interval is allowed between characters within the frame, and that an idle interval of 33 bit-times must be allowed after detection of a frame error by the receiver

8.4.2 Order of information

One technical detail that can be difficult to find in the standards is the ordering of bits and bytes. Under IEC 60870-5, as for DNP3, the following ordering is standard.

Bits are transmitted starting with the least significant byte (LSB) and ending with the most significant byte (MSB). When a bit-sequence representation is given, the bits are shown in this order. However, when the structure of a message in terms of bytes or octets is depicted, the msb is at the left, and the lsb is at the right, which is consistent with the numerical weighting of the bits. A good way to mentally resolve this is to envisage the octet being right-shifted out of a UART register onto the communication channel.

Similarly for bytes, the least significant byte (LSB) is transmitted first, and the most significant byte (MSB) is transmitted last.

The ordering of bits and bytes is illustrated in Figure 8.7.

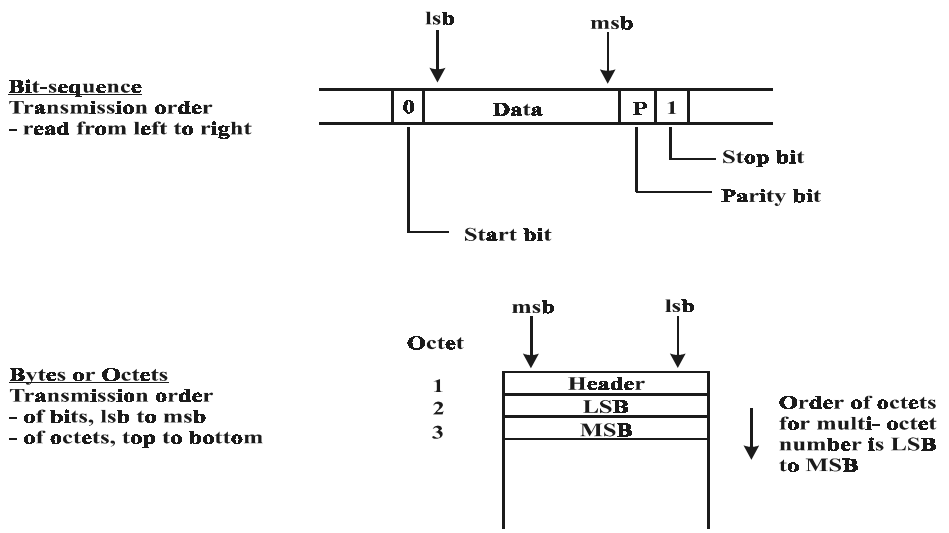


Figure 8.7
Order of information

8.4.3 Link layer concepts

This section presents some concepts that are important for understanding the operation of the link layer transmission procedures. The detailed operation of link layer is then discussed in terms of these concepts.

These are:

- Primary and secondary
- Unbalanced and balanced
- Service procedures
- Service primitives
- Transmission procedures

8.4.4 Primary and secondary

The terms primary and secondary refer to the ability of a station to initiate communications on a communication channel. Only a primary station can initiate communications. Secondary stations must wait until they are polled by the primary station before they can transmit data. More accurately these terms are applied to individual communications ports of stations, because in a hierarchical system, an intermediate station will be both a controlled and a controlling station. This is illustrated in Figure 8.8. This shows a hierarchical network configuration with primary and secondary ports marked P and S.

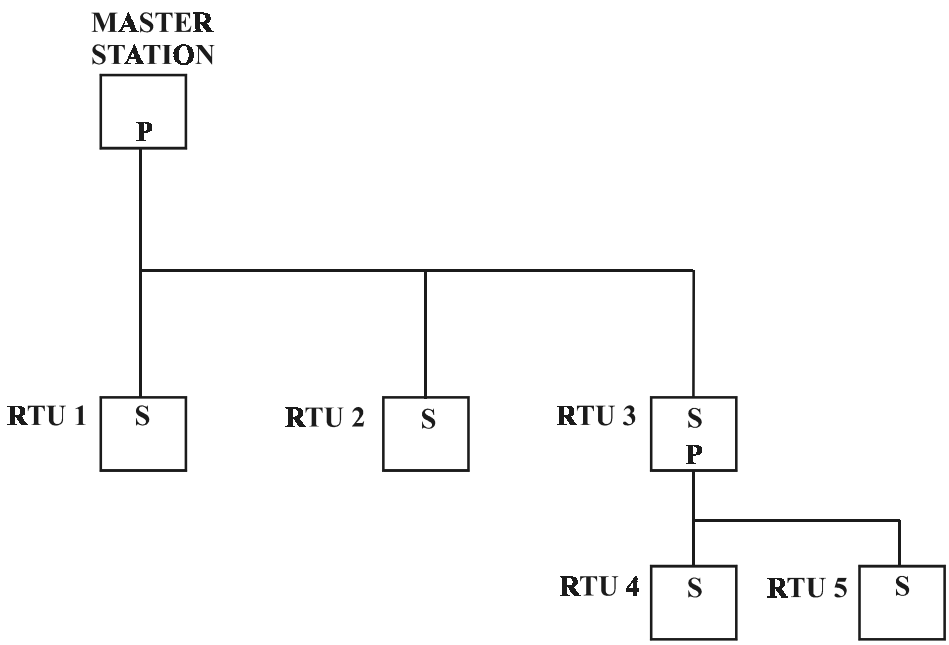


Figure 8.8
Primary and secondary stations

In Figure 8.8 RTU 3 is both a controlling and controlled station. Note that each of the two communications links has only one primary station.

8.4.5 Unbalanced and balanced transmission

The terms ‘unbalanced transmission’ and ‘balanced transmission’ are related to the terms ‘primary’ and ‘secondary’. Unbalanced transmission refers to the configuration where the controlling station acts as a primary on the link, and one or more controlled stations act as secondary stations. The stations are not peer-to-peer at the link level, and so are unbalanced in their functionality.

This is the situation in Figure 8.8 for each of the two communications links. In this configuration the controlling station must acquire data from the controlled stations by polling each in turn for data. This is because they cannot initiate transmissions on their own. The advantage of unbalanced communication is that there is no possibility of collisions between controlled stations attempting to transmit information at the same time.

Balanced transmission refers to the configuration where any station on a link may act as a primary, which means it can initiate communications. This configuration is also known as peer-to-peer communications.

Under IEC 60870-5-101, only point-to-point (that is two station) links can be balanced. Multi-point links must be unbalanced. This is in contrast to DNP3, which uses balanced transmission only, and therefore has to have procedures to overcome collisions which can occur when more than one outstation commences communications simultaneously.

A balanced communications link is shown in Figure 8.9. In this case a master station is connected via a point-to-point link to a sub-master station. Note that each station can act as a primary and a secondary at the ports for this link. These may in fact be thought of as two separate processes within each station, which in fact is how they are logically within the stations. Station A has a primary process and a secondary process operating simultaneously for that link, and Station B has the same.

Figure 8.9
Balanced communications

Figure 8.10 shows the primary and secondary processes for unbalanced transmission. The processes are represented by circles identified as primary (P) or secondary (S). The primary station implements the primary process only, and the secondary stations each implement a secondary process only. Note that in effect there is a separate logical link for each secondary station and it is necessary for the primary to keep a record of the state of each link.

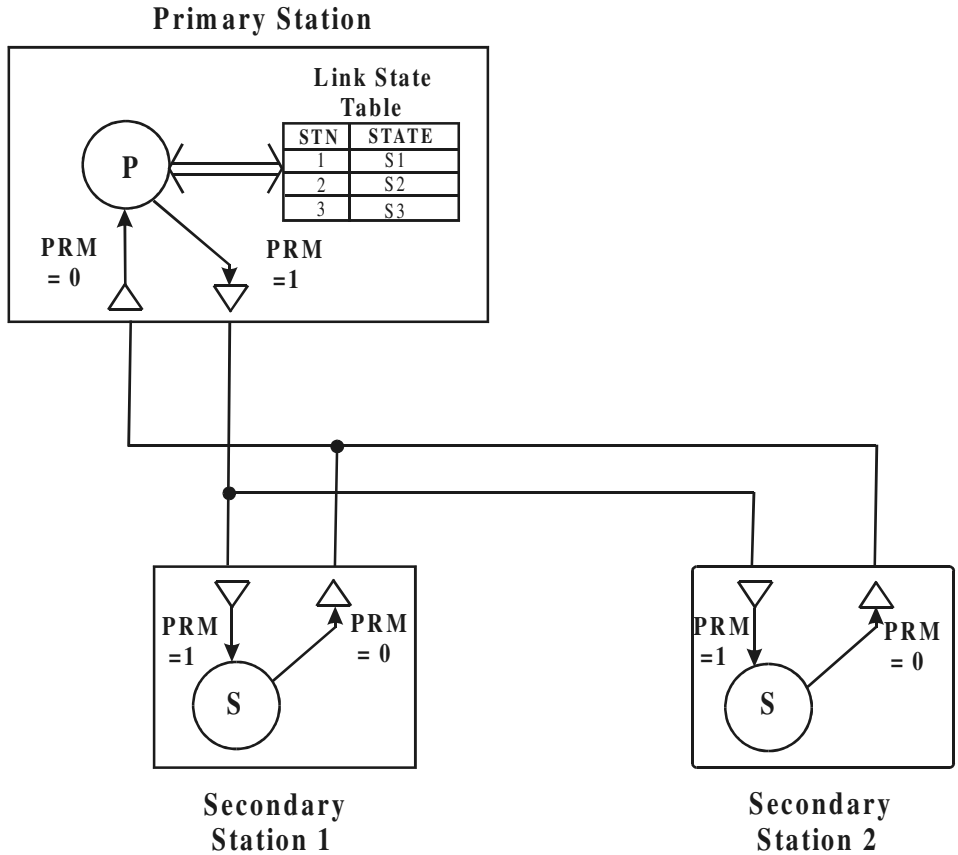


Figure 8.10
Unbalanced transmission processes

Figure 8.11 shows the processes for balanced transmission. In this case there is a primary and secondary process for each station.

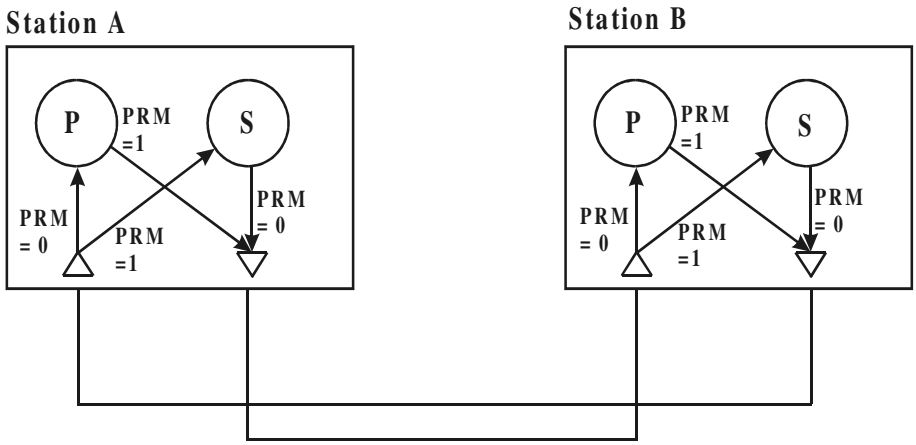


Figure 8.11
Unbalanced transmission processes

8.4.6 Service procedures

The term 'services' is descriptive of the function of the link layer, it provides specific services to the user, which is the application layer, to carry out the transmission of data.

There are three main types of services provided by the data link layer, which have the following names:

- Send/no reply
- Send/confirm
- Request/respond

The send/no reply service is used to send a message or command for which no reply is required from the addressed station. It is used for sending broadcast messages and for messages for which receipt confirmation is not important. The send/confirm service is used to send a command or data which must be reliably transmitted. For this service a confirmation response is required. The request/respond service is used to obtain data from the controlled station. In this case the controlled station responds not with a confirmation, but with the required data.

These services are illustrated in Figure 8.12. This shows the link layer of two stations on a communication channel, and a time-sequence diagram of the service interactions. At each side are shown the commands, data, and responses that are passed between the link layer and the service user, which is the application layer. These are termed the 'service primitives'. In the centre the message transmission is labelled with the transmission procedure name.

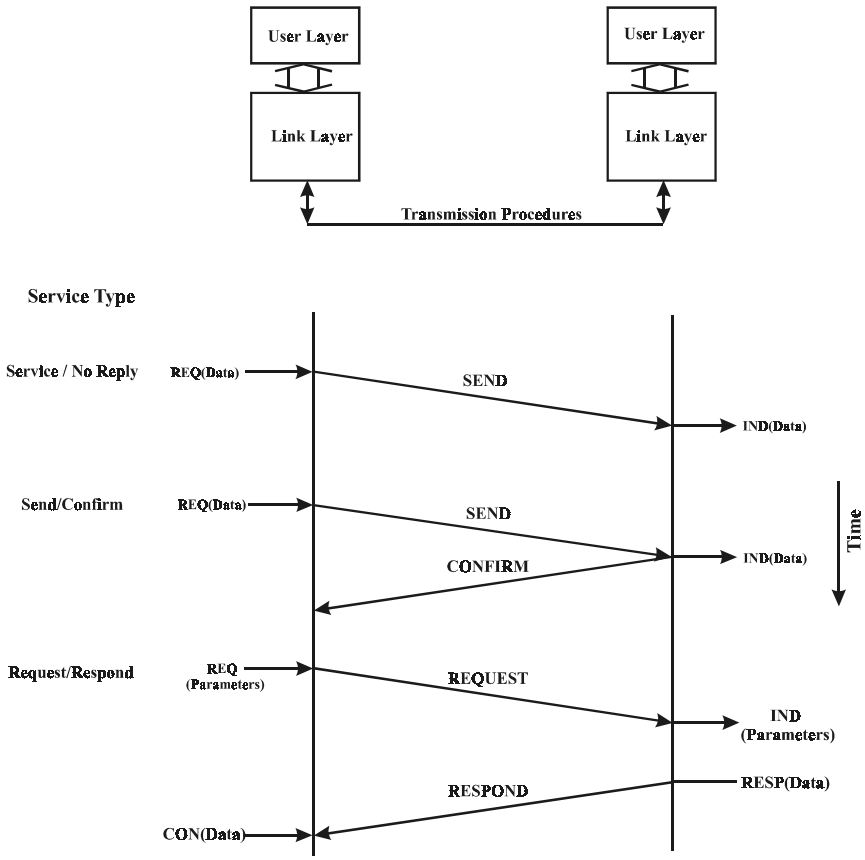


Figure 8.12
Link layer services

The transmission procedures are a set of rules that ensure that transmissions are successfully carried out in response to link user requests. They must be able to cope with errors on the transmission channel that may introduce errors, or cause information to be lost. The transmission procedures are different for unbalanced and balanced links, and described for each in the following sections.

8.4.7 Link initialization

Link initialization is a data link service carried out after a station has been off-line and first becomes available again. While the slave station is off-line the master periodically sends link status request functions until a status of link response is obtained. The sequences are shown following for both unbalanced and balanced modes.

Station / link initialization, unbalanced mode:

- Master sends link status request until status of link received
- Master sends link reset
- Link is active on receipt of ACK
- Slave generates station initialization complete event

Station/link initialization, balanced mode:

- Each station sends link status request until status of link received
- Each station sends link reset
- Link is active on receipt of ACK at each station
- One or both may generate station initialization complete event

8.4.8 Unbalanced transmission procedures

Unbalanced transmission procedures are required for links other than point-to-point, that is multi-point links. For these links the controlling station must control the data traffic by polling the outstations for data. Only when the controlling or primary station on a link polls a particular secondary station may that station respond.

8.4.9 The control field

The control field of the data frame is central to the operation of the transmission procedures. This field is almost identical to that used by the DNP3 protocol because it was derived from the same source document, IEC 60870-5-2 1992. The interpretation of the control field is dependent on whether the communication is a primary or secondary message. Figure 8.13 shows the control field for unbalanced transmission procedures, including the short descriptions of the meanings of the function codes for primary and secondary messages.

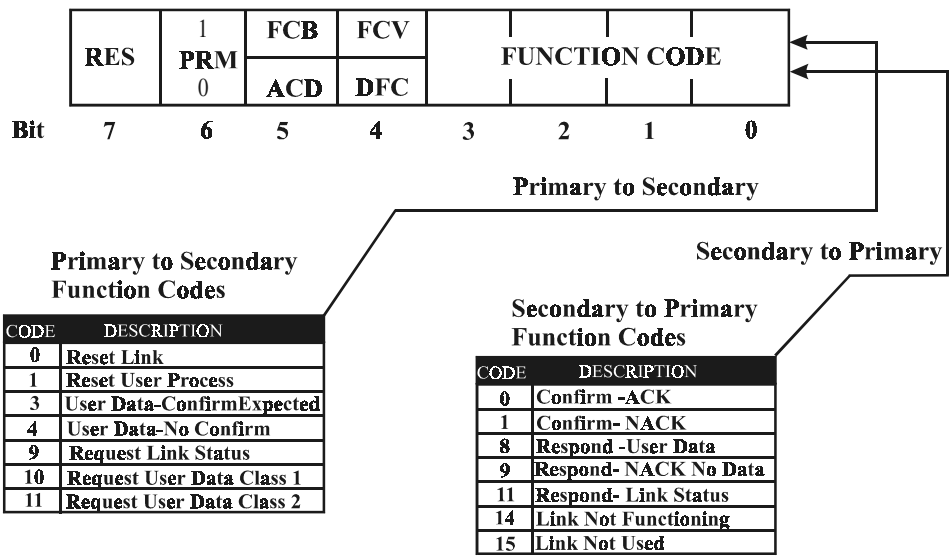


Figure 8.13
Control field – unbalanced transmission

Code	Meaning	Description
PRM	Primary Message	1 => Frame from primary or initiating station
FCB	Frame Count Bit	Alternates between 0 and 1 for sequential frames
FCV	Frame Count Valid	1 => FCB is valid 0 => ignore FCB
RES	Reserved	= 0
DFC	Data Flow Control Bit	Set to 1 by secondary station if further send of user data will cause buffer overflow
ACD	Access Demand Bit	Set to 1 if there is Class 1 data available

Table 8.6
Control field bit meanings – unbalanced transmission

The tables below show the detailed meanings for the function codes in the control field. The meanings are different depending on whether the message is a primary or a secondary transmission. The frame count bit is used in the primary direction only, and is only valid for certain functions. This is indicated by the state of the frame count valid bit.

Function codes from primary station

Function Codes	Frame Type	Service Function	FCV Bit
0	SEND – CONFIRM expected	Reset of remote link	0
1	SEND – CONFIRM expected	Reset of user process	0
2	SEND – CONFIRM expected	Reserved	–
3	SEND – CONFIRM expected	User data	1
4	SEND – NO REPLY expected	User data (unconfirmed)	0
8	REQUEST – RESPOND expected	Request for access demand	0
9	REQUEST – RESPOND expected	Request status of link	0
10	REQUEST – RESPOND expected	Request user data class 1	1
11	REQUEST – RESPOND expected	Request user data class 2	1

Codes 5–7, 12–15 are reserved.

Function codes from secondary station

Function Code*	Frame Type	Service Function
0	CONFIRM	ACK – positive acknowledgment**
1	CONFIRM	NACK – Message not accepted, link busy
8	RESPOND	User data
9	RESPOND	NACK – Requested data not available
11	RESPOND	Status of link (DFC = 0 or 1) or access demand
14		Link service not functioning
15		Link service not used or implemented

*Codes 2–7, 10, 12–13 are reserved **Note that control code 0xE5 may be used in place of the FC0 or FC9 frames.

Table 8.7
Function codes – unbalanced transmission

The functions of the control bits are explained in more detail in the following paragraphs.

Primary bits

The PRM bit is set if the frame is primary (initiating) or a secondary (responding). This is used directly by the link layer in interpreting the function code.

Frame count bits

These are the frame count bit (FCB) and the frame count valid bit (FCV). These bits are only used for primary messages. The frame count bit is used to detect losses or duplication of frames to a secondary station. The frame count valid bit enables the use of the FCB. When the FCV bit is true, the FCB is toggled for each successful SEND–CONFIRM transaction between the same primary and secondary stations.

How they work is like this:

- Following data link startup or a failed transaction, a secondary station will not accept any primary SEND–CONFIRM frames with FCV=1 until a reset transaction is completed. This means it will only accept either a RESET link or a RESET user process command
- After a secondary station receives a RESET link frame from a primary and it responds with a CONFIRM, that link will be operational until a frame transmission error occurs.
- The secondary station will expect the next frame to contain FCV=1 and FCB=1
- The next primary SEND–CONFIRM message will have FCV=1 and FCB=1. The secondary station will accept this as the FCB is valid and is set, as expected.
- Each subsequent primary SEND–CONFIRM message will have the FCB cleared or set in turn.

Data flow control bit

The data flow control bit (DFC) is included in secondary frames. The secondary station will set DFC = 1 if a further SEND of user data will cause its buffer to overflow. On receipt of a frame with DFC = 1 a primary station will cease to send data, but will request link status until DFC = 0.

Access demand bit

There are two classes of data defined, class 1 and class 2. Class 1 data has higher priority than class 2 data. The ACD bit is a means for the secondary station to indicate to the primary that there is class 1 data available.

Address field

The address field of the link layer frame is one or two octets in length, set as a fixed system parameter. This field contains the link address of the secondary station. A frame transmitted by the primary station on a link contains the link address of the secondary station to which the message is directed. A frame transmitted by a secondary station to the primary contains its own link address. By this means the primary station can identify which secondary station the message is from.

Transmission procedures

In this section the procedures are discussed briefly. The procedures are very similar to those used by the DNP3 protocol. This may be referred to for further illustration of the concepts presented.

Note that in the following procedures, no new procedure is commenced until the previous procedure is terminated. It is for this reason that a single-bit frame count bit is sufficient for protection against frame sequence number errors; there is a frame window of exactly one.

SEND/NO REPLY procedures

The frame is transmitted, and a minimum line-idle time of 33 bit-times is required before any further transmissions by the primary. On receipt of the message at the secondary, it is checked for error by comparison with the checksum octet, and if valid it is notified to the service user.

SEND/CONFIRM procedures

The primary station will transmit the message. If a confirmation is not received from the secondary station within a configured time-out period, it will re-transmit the message up until a configured number of retries.

If the secondary station receives the message, it will respond with either a positive or negative confirmation, function code 0 or 1. FC=0 means the message is correctly received and accepted, and in this case the procedure terminates. FC=1 means the secondary cannot accept the message, because its buffer is full or some other reason. In this case the primary will retry, up until a configured number of retries.

This procedure makes use of the frame count bit (FCB) to ensure that the message sequence is not disturbed. The FCB is toggled with each SEND/CONFIRM transmission from the primary station, and an expected FCB flag is maintained by the secondary station. If a message sent by the primary is not confirmed by the secondary, it is retransmitted with the FCB unchanged. Thus a message lost or corrupted in the primary to secondary transmission direction would when retransmitted still have the expected FCB value. Alternatively, if the problem was that the confirmation from the secondary station was lost or corrupted, the secondary station would be able to recognize receipt of a retransmitted message from the primary by the unchanged FCB bit. In this case it retransmits the original confirmation message.

As an alternative to sending a confirmation frame, which is a minimum of six octets in length (that is if single-octet address is used), the single control character response (hexadecimal 0xE5) is allowed. This option may be used to improve transmission efficiency when there is no need to transmit any other information back to the primary station.

REQUEST/RESPOND procedures

This procedure is similar to the SEND/CONFIRM except instead of receiving a confirmation back from the secondary station, a frame containing data is returned, or a negative response is returned indicating that no data is available. In the case of a negative response, either a frame with FC=9, or the single control character (0xE5) may be returned.

As for the SEND/CONFIRM procedures, the frame count bit is toggled at each end for each message transmission, and this is used to detect errors in the transmission in either direction. Basically, when both primary and secondary have incremented their frame count bits and they agree, the procedure is complete.

Philosophy of transmission

For unbalanced transmission only the controlling or primary station on a link can initiate transmissions. Because of this it is necessary that a polling system is implemented by the primary station in order to determine if there is change data available at each secondary station.

To accomplish this the controlling station will poll each secondary station on a cyclic basis for data. It will typically poll for class 2 user data using the request–respond function code 10. The secondary station will then return any class 2 data that it has available, and at the same time it will indicate if there is any class 1 data available by setting the access demand bit (ACD). Typically analog values will be assigned to class 2 and be updated during the cyclic scan, and all other data such as events will be assigned to class 1.

Note that although the polling operation is carried out by the link layer, the polling sequence itself is implemented by a higher level of the protocol, the user process level. The higher level generates services requests using service primitives to specify the polling actions to be carried out by the link layer.

8.4.10 Balanced transmission procedures

Balanced transmission procedures may only be used for point-to-point links equipped with duplex channel communication. Under balanced transmission each station can act as both a primary and a secondary station simultaneously. The control field and transmission procedures are modified slightly from the unbalanced case to accommodate this operation.

The control field

There are two modifications to the data link control field for balanced transmission. The first is that the access demand (ACD) bit is not required, because either station can initiate transmissions. The second is the inclusion of a direction bit (DIR). This indicates the direction of transmission of a message between the two stations. The control field for balanced transmission is shown in Figure 8.14.

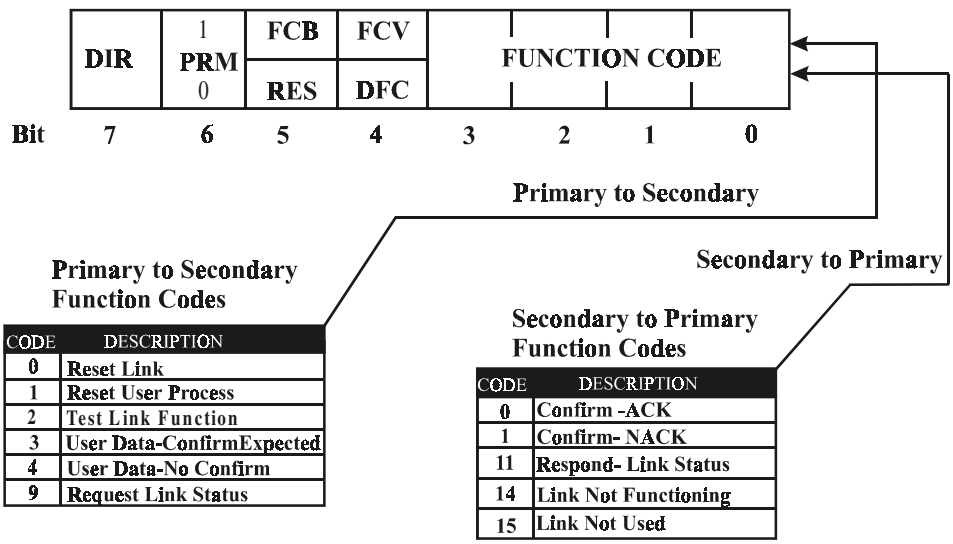


Figure 8.14
Control field – balanced transmission

Code	Meaning	Description
DIR	Direction of Message	1 => A to B 0 => B to A
PRM	Primary Message	1 => Frame from primary or initiating station
FCB	Frame Count Bit frames	Alternates between 0 and 1 for sequential
FCV	Frame Count Valid	1 => FCB is valid 0 => ignore FCB
RES	Reserved	= 0
DFC	Data Flow Control Bit	Set to 1 by secondary station if further send of user data will cause buffer overflow

Table 8.8
Control field bit meanings – balanced transmission

The tables below show the detailed meanings for the function codes in the control field. The changes from the codes for unbalanced transmission are shown in italics.

Function codes from primary station

Function Code	Frame Type	Service Function	FCV Bit
0	SEND – CONFIRM expected	Reset of remote link	0
1	SEND – CONFIRM expected	Reset of user process	0
2	SEND – CONFIRM expected	*Test for function of link*	1
3	SEND – CONFIRM expected	User data	1
4	SEND – NO REPLY expected	User data (unconfirmed)	0
8		*Used by unbalanced only*	–
9	REQUEST – RESPOND expected	Request status of link	0
10		*Used by unbalanced only*	1
11		*Used by unbalanced only*	1

Codes 5–7, 12–15 are reserved.

Function codes from secondary station

Function Code*	Frame Type	Service Function
0	CONFIRM	ACK – positive acknowledgment**
1	CONFIRM	NACK – Message not accepted, link busy
8		*Used by unbalanced only*
9		*Used by unbalanced only*
11	RESPOND	Status of link (DFC = 0 or 1)
14		Link service not functioning
15		Link service not used or implemented

*Codes 2–7, 10, 12–13 are reserved.
**Note that control code 0xE5 may be used in place of the FC0.

Table 8.9
Function codes – balanced transmission

The changes in functions from unbalanced transmission are:

- A test link primary function code FC=2 has been added
- Requests for access demand and for user data class 1 or 2 have been removed (primary function codes FC = 8, 10, 11)
- Secondary respond function codes FC = 8, 9 have been removed

These changes reflect the changes to the way data is transmitted. Under balanced transmission the request/respond service is not used for transmission of user data, but only for checking the status of the link. User data is transmitted directly by the link layer using the send service.

8.4.11 Address field

The address field for balanced communications may be zero, one or two octets. Thus there is the option of having no address field under balanced communications. This is the case because as there is only one station at each end of the link, there is no need for the secondary process at either end to verify the address.

In effect, for a balanced link, the direction (DIR) bit substitutes for the address, making the inclusion of the link address redundant.

Transmission procedures

The transmission procedures for balanced transmission are the same as those for unbalanced transmission. The only difference is that there are both primary and secondary processes operating simultaneously at each station. This is similar to two unbalanced links operating in parallel. These processes maintain a separate frame count bit sequence for each primary–secondary link and use these to detect and recover from errors in the same way as a single unbalanced primary–secondary link operates.

Philosophy of transmission

For balanced transmission either station on the link can initiate transmission. Therefore there is no need for a station to be polled for data as it can send it directly when it is available. This changes the services used at the link layer from the case for unbalanced transmission. Where unbalanced transmission makes use of the request/respond service to obtain user data from the secondary station, for balanced transmission the station with the data just uses the send/confirm service directly. Comparison of Figures 8.13 and 8.14 shows that the secondary codes for responding with user data FC8 and FC9 are not available for balanced transmission. Instead, primary function codes FC3 or FC4 are used to send the data directly.

8.4.12 Data link security

IEC 60870-5-101 and DNP3 utilize the FT1.2 and FT3 frame formats specified by IEC 60780-5-1 respectively. These formats differ in their security provisions as shown in Table 8.6. IEC 60870-5-101 uses an 8-bit checksum and a maximum frame size of 255 bytes. DNP uses a 16-bit cyclic redundancy code (CRC) for every 16 bytes of user data contained in the body of its frame.

Protocol	IEC 60870-5 Frame Type	Security Method	Hamming Distance Error Bits	Maximum Secured Length in Bytes
IEC 60870-5-101	FT1.2	8 bit checksum	4	255
DNP 3.0	FT3	16 Bit CRC	6	16

Table 8.10
Link layer error security

The effect of these differences in security is often quoted in terms of the 'Hamming distance'. This is equal to the minimum number of single bit errors that are required to allow an incorrect message to be mistakenly accepted as a good message, that is for the security system to fail. These are 4 and 6 for methods used by FT1.2 and FT3. However, these figures ignore the effect of the ratio of security code bits to message bits, which in the case of DNP is higher due to the inclusion of CRC codes within the body section of the FT3 frame format.

8.4.13 Link versus application data

There is a distinction between link data and application level data that is subtle and can be difficult to grasp at first sight. It derives from the fact that the application level messages are treated simply as data at the link layer level, and may be best illustrated by example.

Take the case where an unbalanced link is operating between primary station A and secondary station D. Suppose that the application level of station D requires some particular data from A. This is in the reverse direction to most data traffic, which is generally from the secondary station to the primary. In this case the application level request from D will generate a class 1 access demand at the link level. This will have to wait until that station

is polled for data by the primary station A. At this point, if class 2 data has been polled for it will respond with any class 2 data, or with an FC9 'NACK – no data' frame, but in either case with the ACD (access demand) bit set. The primary station A will then poll for the class 1 data from station D, and at this point D will be able to transmit its class 1 data. This will contain the application level request by D, for the primary station to send the application level data that it requires.

The link layer frame that was requested by polling from primary A, carried an application level request from station D. This resulted in the application layer of A using the send service to return the requested data to station D. Note that a link layer request in direction A to D (the poll) has resulted in an application level request from D to A.

In the following sections dealing with the application layer and above, the operation of the link layer can be generally seen as a message transport mechanism that can be assumed to just transport the application level messages as required. However, awareness of the transport mechanism is important to understanding the response times, as these will depend on the transmission mode, and polling frequency for the unbalanced mode.

8.5 Application layer

The remaining sections of Chapter 8 describe the operation of the application layer and above of the IEC 60870-5 protocol. Most of this section is applicable to both the non-networked and networked versions of the protocol, IEC 60870-5-101 and IEC 60870-5-104. The areas that are different are discussed in the following chapter under Advanced considerations of IEC 60870-5.

This information is presented in the following sequence:

- Overall message structure
- ASDU structure
- Message addressing and routing
- Information elements
- Set of ASDUs

8.5.1 Overall message structure

In the preview, the overall message structure under IEC 60870-5 was presented. This is represented in Figure 8.15. This shows the application layer application service data unit or ASDU, and shows how this is carried as link user data by the data link layer under IEC 60870-5-101. For the networked version IEC 60870-5-104 the ASDU is carried by the TCP/IP protocols instead of the T101 link layer and so the link frame shown below does not apply to this case.

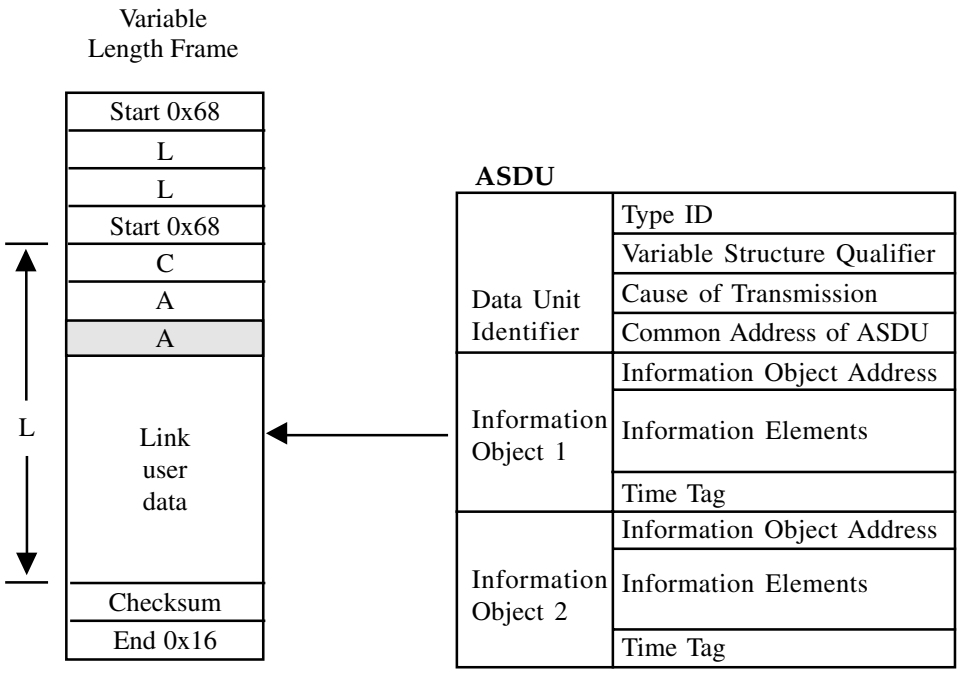


Figure 8.15
Message structure under IEC 60870-5-101

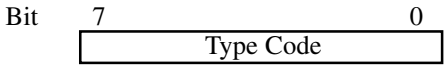
The only important point to note about the relationship between the ASDU and the link layer frame is that a maximum of just one ASDU is allowed per frame. This sets an upper limit for the size of the ASDU at 255 octets, minus 2-3 octets for the link control and address fields.

8.5.2 ASDU structure

The structure of the ASDU is in two main sections. These are the data unit identifier, and the data itself, made up of one or more information objects. The data unit identifier defines the specific type of data, provides addressing to identify the specific identity of the data, and it includes additional information in the cause of transmission field. The fields of the ASDU are now discussed in turn.

Type identification

The type identification field is a single-octet unsigned integer field. Its content is interpreted as a code in the ranges shown below.



Code Range	Purpose
<1..127>	Standard type definitions
<128..135>	Reserved for message routing – private
<136..255>	For special use – private

Figure 8.16
Type identification field

The following notes apply to these codes:

- The value <0> is not used
- The range <128..255> is not defined by the standard, and may be used by particular vendors for system specific roles. However this has implications for interoperability

In the range of the standard type definitions, there are presently 58 specific types defined. These are grouped as shown in Table 8.11 which shows the overall groups and numbers of type identification codes that are defined.

Defined Type codes	**Group**
<1..40>	Process information in monitor direction
<45..51>	Process information in control direction
<70>	System information in monitor direction
<100..106>	System information in control direction
<110..113>	Parameter in control direction
<120..126>	File transfer

Table 8.11
Defined type code groups

It is important to note that the type identification applies to the whole ASDU, therefore if there are multiple information objects contained in the ASDU, they are all of the same type.

Table 8.13 provides a full list of the ASDU types. The table is broken into the code groups shown in Table 8.11. Full details of each individual ASDU type are given under 'Set of ASDUs' later in this text.

Table 8.13 also includes information code references which may be encountered. These references are defined by IEC 60870-5-5. They provide a hierarchical reference system using the following structure:

Level	**Symbol**	**Description**
1	M_ C_ P_ F_	Monitored information Control information Parameter File transfer
2	Various	see actual usages
3	_Nx _Tx _xA _xB _xC _xD	Not time tagged Time tagged Type A: status and normalized, with quality Type B: scaled, with quality Type C: short floating point, with quality Type D: normalized without quality

Table 8.12
Reference information code structure

For example, M_ME_TA_1 is monitored information, a measured value, with time tag, and type A, which is a normalized value with quality.

Type No.	Description	Reference
<0>	not defined	
<1>	single-point information	M_SP_NA_1
<2>	single-point information with time tag	M_SP_TA_1
<3>	double-point information	M_DP_NA_1
<4>	double-point information with time tag	M_DP_TA_1
<5>	step position information	M_ST_NA_1
<6>	step position information with time tag	M_ST_TA_1
<7>	bitstring of 32 bit	M_BO_NA_1
<8>	bitstring of 32 bit with time tag	M_BO_TA_1
<9>	measured value, normalized value	M_ME_NA_1
<10>	measured value, normalized value with time tag	M_ME_TA_1
<11>	measured value, scaled value	M_ME_NB_1
<12>	measured value, scaled value with time tag	M_ME_TB_1
<13>	measured value, short floating point number	M_ME_NC_1
<14>	measured value, short floating point number with time tag	M_ME_TC_1
<15>	integrated totals	M_IT_NA_1
<16>	integrated totals with time tag	M_IT_TA_1
<17>	event of protection equipment with time tag	M_EP_TA_1
<18>	packed start events of protection equipment with time tag	M_EP_TB_1
<19>	packed output circuit information of protection equipment with time tag	M_EP_TC_1
<20>	packed single-point information with status change detection	M_PS_NA_1
<21>	measured value, normalized value without quality descriptor	M_ME_ND_1
<22..29>	reserved for further compatible definitions	

Table 8.13a
ASDU types – process information in monitoring direction

Table 8.13b shows types that were added to this category with amendment 2 of IEC 60870-5-101. These provide for a longer time tag format.

Type No.	Description	Reference
<30>	single-point information with time tag CP56Time2a	M_SP_TB_1
<31>	double-point information with time tag CP56Time2a	M_DP_TB_1
<32>	step position information with time tag CP56Time2a	M_ST_TB_1
<33>	bitstring of 32 bits with time tag CP56Time2a	M_BO_TB_1
<34>	measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
<35>	measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
<36>	measured value, short floating point number with time tag CP56Time2a	M_ME_TF_1
<37>	integrated totals with time tag CP56Time2a	M_IT_TB_1
<38>	event of protection equipment with time tag CP56Time2a	M_EP_TD_1
<39>	packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
<40>	packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1
<30>	single-point information with time tag CP56Time2a	M_SP_TB_1
<31>	double-point information with time tag CP56Time2a	M_DP_TB_1
<32>	step position information with time tag CP56Time2a	M_ST_TB_1
<33>	bitstring of 32 bits with time tag CP56Time2a	M_BO_TB_1
<34>	measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
<35>	measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
<36>	measured value, short floating point number with time tag CP56Time2a	M_ME_TF_1
<37>	integrated totals with time tag CP56Time2a	M_IT_TB_1
<38>	event of protection equipment with time tag CP56Time2a	M_EP_TD_1
<39>	packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
<40>	packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1
<41..44>	reserved for further compatible definitions	

Table 8.13b
ASDU types – process information in monitoring direction cont'd

Type No.	Description	Reference
<45>	single command	C_SC_NA_1
<46>	double command	C_DC_NA_1
<47>	regulating step command	C_RC_NA_1
<48>	set point command, normalized value	C_SE_NA_1
<49>	set point command, scaled value	C_SE_NB_1
<50>	set point command, short floating point number	C_SE_NC_1
<51>	bitstring of 32 bits	C_BO_NA_1

Table 8.13c
ASDU types – process information in control direction

Type No.	Description	Reference
<70>	end of initialization	M_EI_NA_1
<70..99>	reserved for further compatible definitions	

Table 8.13d
ASDU types – system information in monitor direction

Type No.	Description	Reference
<100>	interrogation command	C_IC_NA_1
<101>	counter interrogation command	C_CI_NA_1
<102>	read command	C_RD_NA_1
<103>	clock synchronization command	C_CS_NA_1
<104>	test command	C_TS_NA_1
<105>	reset process command	C_RP_NA_1
<106>	delay acquisition command	C_CD_NA_
<107..109>	reserved for further compatible definitions	

Table 8.13e
ASDU types – system information in control direction

Type No.	Description	Reference
<110>	parameter of measured value, normalized value	P_ME_NA_1
<111>	parameter of measured value, scaled value	P_ME_NB_1
<112>	parameter of measured value, short floating point number	P_ME_NC_1
<113>	parameter activation	P_AC_NA_1
<114..119>	reserved for further compatible definitions	

Table 8.13f
ASDU types – parameter in control direction

Type No.	Description	Reference
<120>	file ready	F_FR_NA_1
<121>	section ready	F_SR_NA_1
<122>	call directory, select File, call File, call section	F_SC_NA_1
<123>	last section, last segment	F_LS_NA_1
<124>	ack File, ack section	F_AF_NA_1
<125>	segment	F_SG_NA_1
<126>	directory	F_DR_TA_1
<127>	reserved for further compatible definitions	

Table 8.13g
ASDU types – file transfer

Variable structure qualifier

The variable structure qualifier is a single-octet that specifies the number of information objects or information elements, and how they are addressed. It contains a seven-bit binary number, and a 1-bit field that indicates which of two different possible information structures are used. Figure 8.17 shows the variable structure qualifier field, followed by a detail of the two information structures.

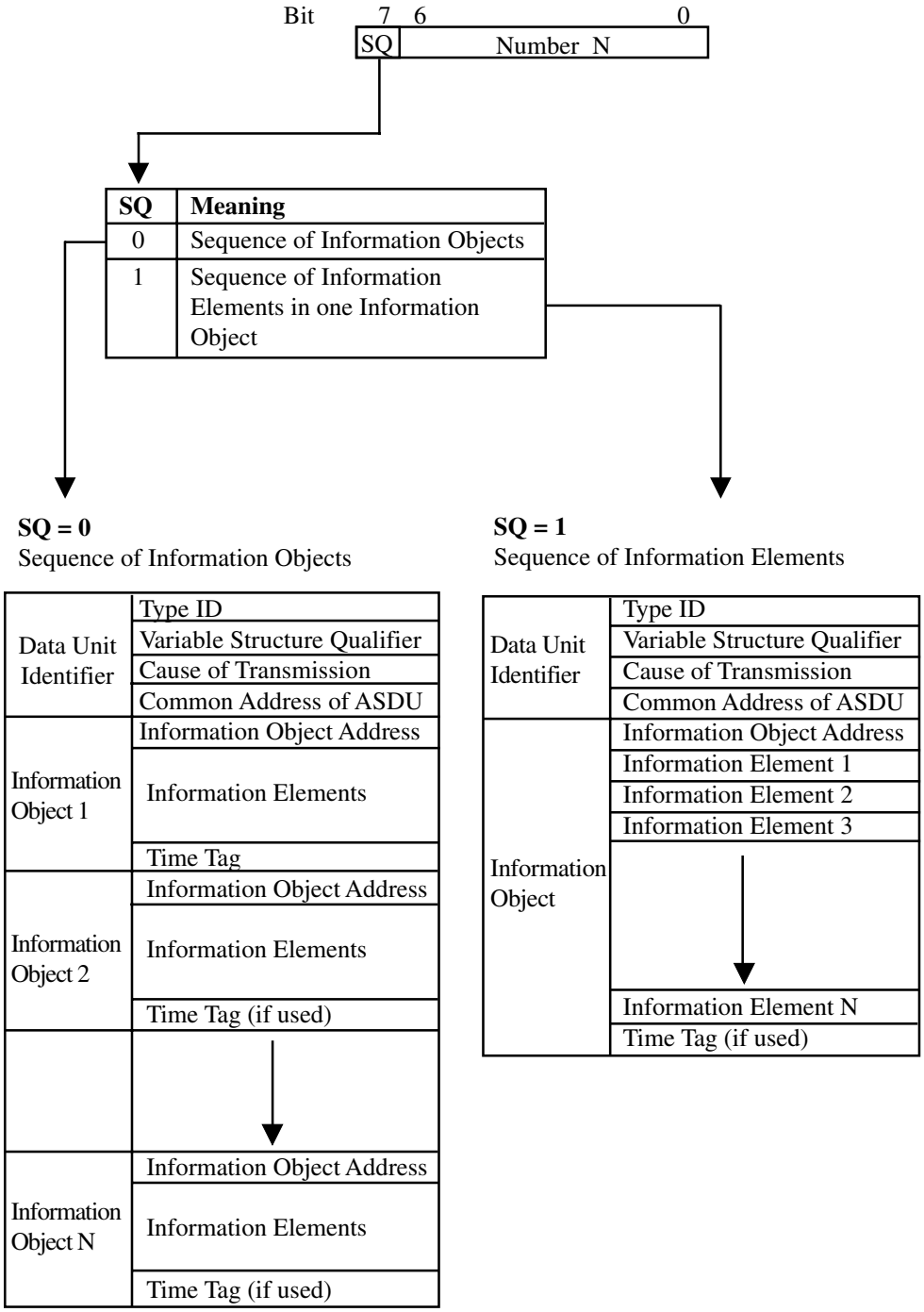


Figure 8.17
Variable structure qualifier and structures

It may be seen from Figure 8.17 that there are two different structures, depending on the state of the most significant bit of the variable structure qualifier. This is termed the SQ bit, which may be thought of as the structure qualifier bit.

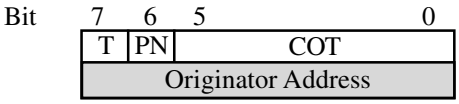
When SQ = 0, the structure is a sequence of information objects. Each information object carries its own address, and therefore the information elements contained do not need to have sequential addresses. The number of information objects is given by the seven-bit value N. Therefore there can be up to 127 information objects in this ASDU.

When SQ = 1, the structure contains just one information object, but this may contain multiple information elements, all of the same format, such as a measured value. In this case there is only one information object address, and only one time tag (if used).

The effect of the SQ bit is that for each type identification number, there may effectively be two ASDUs. This is seen in the sub-section presenting the set of ASDUs, where it will be seen that some types have both variations (SQ=0 and SQ=1), and others have only one of these.

Cause of transmission

The cause of transmission (COT) field is used to control the routing of messages both on the communications network, and within a station, by directing the ASDU to the correct program or task for processing. This sub-section will initially look at the structure and meaning of the sub-fields within the COT, and then look at how these are used.



Key:

COT	Cause of Transmission <0..63>
PN	Positive / Negative Confirm bit
T	Test bit
OA	Originator Address <0..255>

Figure 8.18
Cause of transmission field

The cause of transmission or COT is a six-bit code which is used in interpreting the information at the destination station. The codes are shown in Table 8.14. Each defined ASDU type has a defined sub-set of the codes which are meaningful with it, and these are given in the section presenting the set of ASDUs.

The PN bit is the positive/negative confirmation bit. This is meaningful when used with control commands. This bit is used when the control command is mirrored in the monitor direction, and it provides indication of whether the command was executed or not. When the PN bit is not relevant it is cleared to zero.

The T or test bit is set when ASDUs are generated for test purposes and are not intended to control the process or change the system state. It is used for testing of transmission and equipment.

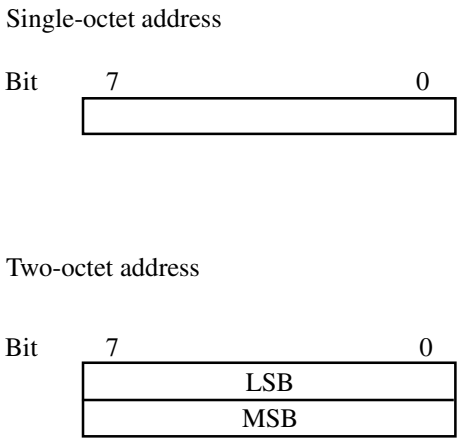
The originator address is optional on a system basis. It provides a means for a controlling station to explicitly identify itself. This is not necessary when there is only one controlling station in a system, but is required when there is more than one controlling station, or some stations are dual-mode stations. These are stations that act both as controlled and

controlling stations. In these circumstances the originator address can be used to direct command confirmations back to the particular controlling station that issued the command, rather than to the whole system. The one exception to this is the originator address of zero <0>. This has the same effect as if there was no originator address. It is termed the default address and its effect is that the message is transmitted to all stations. The use of the originator address is discussed in greater detail under message addressing and routing.

COT code	Cause of Transmission
0	Not used
1	Periodic, cyclic
2	Background scan
3	Spontaneous
4	Initialized
5	Request or requested
6	Activation
7	Activation confirmation
8	Deactivation
9	Deactivation confirmation
10	Activation termination
11	Return information caused by a remote command
12	Return information caused by a local command
13	File transfer
14–19	Reserved for future definitions
20	Interrogated by station interrogation
21–36	Interrogated by group (1–16) interrogation
37	Requested by general counter request
38–41	Requested by group (1–4) counter request
42–43	Reserved for future definitions
44	Unknown type identification
45	Unknown cause of transmission
46	Unknown common address of ASDU
47	Unknown information object address

Table 8.14
Cause of transmission codes (COT)

8.5.3 Common address of ASDU



Address Range	Purpose
<0>	Not used
<1..254> or <1..65534>	Station Address
<255> or <65535>	Global Address

Figure 8.19
Common address of ASDU

The common address of the ASDU is either one or two octets in length, fixed on a per-system basis. The address is called a common address because it is in common to all of the data contained within the ASDU. This is normally interpreted as a station address, however it can be structured to form a station/sector address where individual stations are broken up into multiple logical units. The address <0> is not used.

The highest address 0xFF or 0xFFFF is global. This means that an ASDU with this address will be interpreted by all stations. Use of the global address is restricted to the ASDUs listed below. These are used when the same application function must be initiated simultaneously.

Type	Description	Purpose
100	Interrogation command	Reply with particular system data snapshot at common time
101	Counter interrogation command	Freeze totals at common time
103	Clock synchronization command	Synchronize clocks to common time
105	Reset process command	Simultaneous reset

Information object address

The information object address is the first field of the information object. It identifies the particular data within a defined station. The information object address may be one, two, or three octets in length. However, the case of three octets is provided only to allow for structured address systems, and one station is allowed only 65 536 different information

object addresses, as for two-octet addressing. The information object address of zero is reserved for the case when the address is not relevant. The information object address is shown in Figure 8.20.

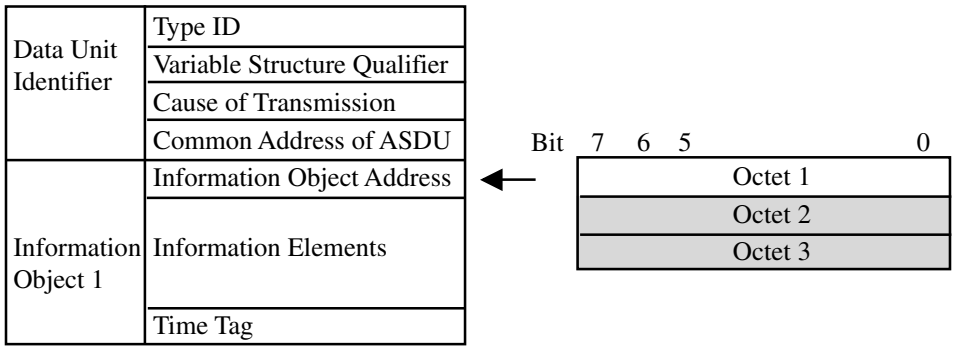


Figure 8.20
Information object address

On a system basis, specific data is uniquely identified by the combination of the common address and the information object address.

An example of how this might work in practice is where there are a number of identical intelligent electronic devices IEDs connected to a sub-master RTU, which is in turn connected to a master station. These could be re-closers on a distribution system. Each IED will have an identical data structure internally, as determined by the device manufacturer. Most likely this will be some tens of information elements or data points, which could be addressed by a one-octet information object address. However, as the system includes RTUs that have many more data points, two-octet addressing is used across the system. At a system configuration level, there will be a single model for that type of re-closer, and configuration of each device into the system database will be a matter of using the standard point-mapping for that device type and adding the station number to form unique point references.

8.5.4 Message addressing and routing

Control and monitor directions

An important concept in understanding addressing under IEC 60870-5 is the difference between control and monitor directions. It is an assumption that the overall system has a hierarchical structure involving centralized control. Under the protocol, every station is either a controlling station or a controlled station. The communications network structure will normally be aligned with this, and for unbalanced communications links the controlling stations will be primaries, and the controlled stations will be secondaries at the link level. This follows naturally from the fact that a hierarchical structure involves multiple controlled stations, controlled by one or at least few controlling stations.

In such a system, control messages such as commands or interrogations are transmitted by the controlling station, and these result in actions and return information transmitted by the controlled station.

Addressing of ASDUs

Messages are addressed in the control direction by the common address field of the ASDU. This address field is one or two octets, and defines the station (or logical station)

to which the ASDU is being addressed. In the monitor direction, however, the common address field contains the address of the station returning the data. This is required so that the data can be uniquely identified and mapped to the right points in system data images.

In some cases a station that is generally a controlled station may itself act as a controlling station, perhaps to interrogate the master station for data, or to initiate an action in another controlled station. This is called reverse direction operation. A station that can act in both the forward and the reverse direction is called a dual-mode or combined station. When a dual-mode station issues a control ASDU to another station, it must set the controlled station's address as the common address of the ASDU. This is necessary, as for any control direction ASDU, so that the intended station can recognize the message as being directed at it. When the action is carried out, further communication will be necessary with the controlling station to send an action confirmation message, and possibly an execute message if two-phase operation is being used. But as monitor direction messages carry the address of the controlled station, this cannot be used to route the communications back to the controlling station. Instead, the originator address octet of the cause of transmission field is used for this purpose. Its operation is described in the following paragraphs and drawing.

When a control direction ASDU is transmitted by a dual-mode station that is not the system master station, that station must include a non-zero value in the originator address octet of the cause of transmission field. This has no effect in the control direction of the ASDU, but is used in the monitoring direction to route action confirmation and action termination messages back to the originator. When the controlled station returns an action confirmation or other message arising from this control ASDU, it includes the originator address from the control direction ASDU in the monitoring direction response. It is the responsibility of any intermediate routing devices to recognize a non-zero originator address in a monitor direction ASDU, and to route it back to that originator.

As the originator address sub-field is only one octet in length, and common addresses may be two octets, it is clear that either any dual-mode stations on a system must either be numbered within the range <1..256>, or a mapping must be used between originator addresses and common addresses if these are not in that range.

It should be noted that also arising from the control action may be some changes within the controlled station that need to be conveyed to the master station rather than the dual-mode station that initiated the control action. These would typically be to convey the changed system state, and might also include time-tagged events. The monitor direction ASDUs that carry this information need to be directed to the master station, and possibly to other areas of the network if required. These ASDUs are given an originator address value of zero. Thus, in a system which contains dual-mode stations, it is necessary to use the originator address sub-field, and all monitor direction messages going back to the master station will have this field set to zero.

These concepts are illustrated in Figure 8.21. This shows a system with intermediate RTUs acting as controllers and data concentrators, and multiple controlled stations linked to these. One of these issues a command to a peer station. Both action confirmation and change data messages are generated, and are routed to their correct destinations by the use of the originator address field.

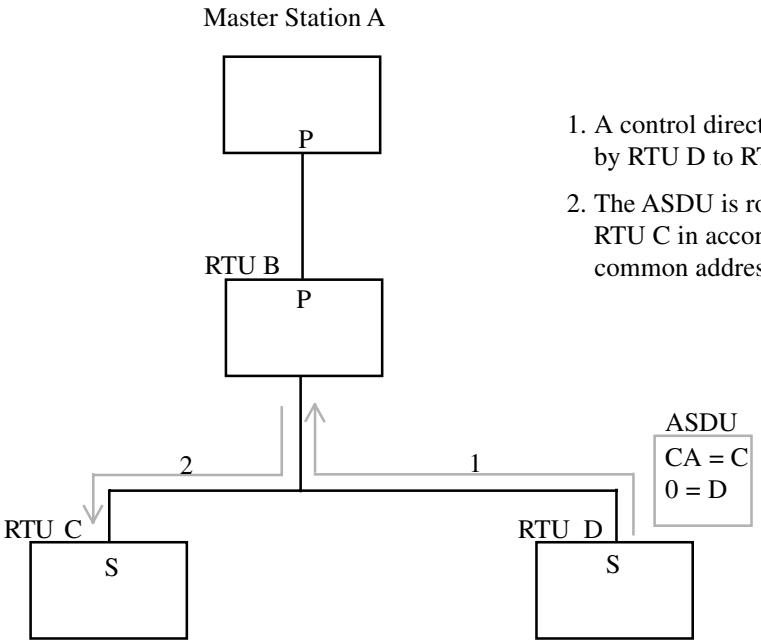


Figure 8.21
Control command issued from dual-mode RTU

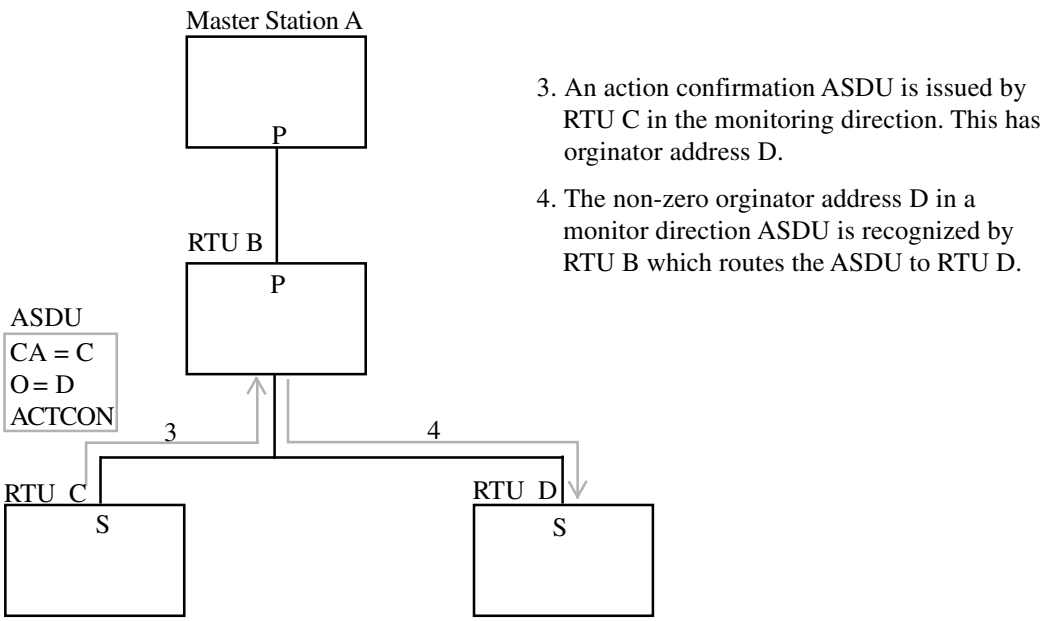


Figure 8.22
Activation confirmation ASDU returned to dual-Mode RTU

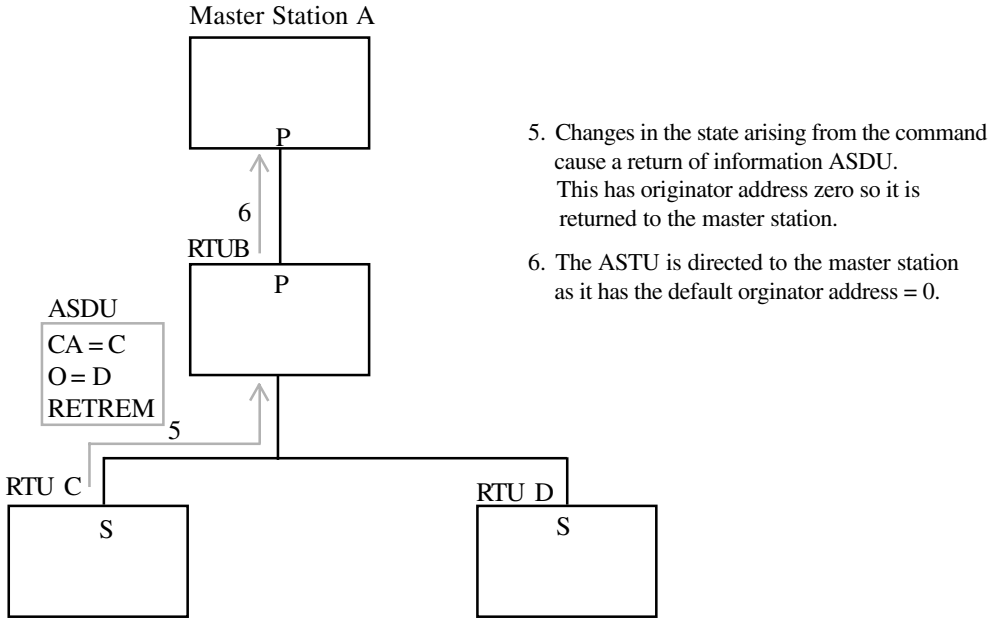


Figure 8.23
Monitoring information returned to SCADA master

8.6 Information elements

As has been shown in the preceding sections on ASDU structure, application data is carried within the ASDU within one or more information objects. Depending on the variable structure flag there may be multiple information objects each containing a defined set of one or more information elements, or there may be just one information object containing a number of identical information elements. In either case, the information element is the fundamental component used to convey information under the protocol. The information elements are used as building blocks in the definition of the set of ASDUs under the protocol.

In this section this set of information building blocks is presented. These are referred to in the following section when the set of ASDUs are defined.

In the following definitions, these interpretation rules should be noted:

- Key descriptions give the logical state for a set bit, i.e. bit = 1
- Blank bit positions are reserved and must be cleared, i.e. bit = 0
- Bit positions have been numbered <0..7> for consistency within this text and the powers of 2 the positions represent. Note that the IEC documents actually use <1..8>. This is a matter of definition only and does not change the meaning

The set of information elements is listed in Table 8.15. This is followed by representations of each of the data elements, grouped by general type.

General Type Symbol	Description
Process	
SIQ	Single-point information with quality descriptor
DIQ	Double-point information with quality descriptor
BSI	Binary state information
SCD	Status and change detection
QDS	Quality descriptor
VTI	Value with transient state indication
NVA	Normalized value
SVA	Scaled value
R32-IEEE STD 754	Short floating point number
BCR	Binary counter reading
Protection	
SEP	Single event of protection equipment
SPE	Start events of protection equipment
OCI	Output circuit information of protection equipment
QDP	Quality descriptor for events of protection equipment
Commands	
SCO	Single command
DCO	Double command
RCO	Regulating step command
Time	
CP56Time2a	Seven octet binary time
CP24Time2a	Three octet binary time
CP16Time2a	Two octet binary time
Qualifiers	
QOI	Qualifier of interrogation
QCC	Qualifier of counter interrogation command
QPM	Qualifier of parameter of measured values
QPA	Qualifier of parameter activation
QRP	Qualifier of reset process command
QOC	Qualifier of command
QOS	Qualifier of set-point command
File Transfer	
FRQ	File ready qualifier
SRQ	Section ready qualifier
SCQ	Select and call qualifier
LSQ	Last section or segment qualifier
AFQ	Acknowledge file or section qualifier
NOF	Name of file
NOS	Name of section
LOF	Length of file or section
LOS	Length of segment
CHS	Checksum
SOF	Status of file
Miscellaneous	
COI	Cause of initialization
FBP	Fixed test bit pattern, two octets

Table 8.15
Information elements

Quality bits

Quality bits are not information elements in themselves, but appear as individual bits within information elements. These are defined in this section.

Note that quality bits are set or cleared independently of each other. Examination of these shows that these may be used to differentiate between different types of situation or problem that may be affecting the data. Whether all are used will depend on the system. A simple approach would be to interpret any of the quality bits being set as 'bad value', whereas more sophisticated approaches may differentiate based on the actual bit(s) set. Their individual meanings are explained further below.

Blocked (BL)

This means that the value of the point is as it was prior to being blocked. Blocking prevents updating of the value of the point.

Substituted (SB)

This is where a value has been substituted or forced by manual entry or otherwise. It means that the value is not derived from the normal measurement.

Not topical (NT)

This means that the value was not updated successfully at the last time it was due to be updated.

Invalid (IV)

This indicates that the value cannot be used because it may be incorrect due to a fault or other abnormal condition.

Overflow bit (OV)

This means that a value is out of a defined range. It is used primarily with analog or counter values.

Elapsed time invalid (EI)

This is used with events of protection equipment. If set it means that the elapsed time interval value is invalid. This means that for some reason the elapsed time value cannot be relied upon and should be ignored.

8.6.1 Process related information elements

The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
SIQ	Single-point information with quality descriptor
DIQ	Double-point information with quality descriptor
BSI	Binary state information
SCD	Status and change detection
QDS	Quality descriptor
VTI	Value with transient state indication
NVA	Normalized value
SVA	Scaled value
R32-IEEE STD 754	Short floating point number
BCR	Binary counter reading

Table 8.15 Extract A
Process related information elements

SIQ Single point information

SIQ is single point information with quality descriptor. The status bit itself is bit 0. The 4 highest bits provide the quality information per the key below.

7	6	5	4	3	2	1	0
IV	NT	SB	BL				SPI

Key	
SPI	Status ON
BL	Blocked
SB	Substituted
NT	Not topical
IV	Invalid

DIQ Double-point information

The DIQ is double-point with quality. The quality bits are as previously defined, and the four states of the two status bits are given in the key following.

7	6	5	4	3	2	1	0
IV	NT	SB	BL			DPI	

Key – DPI Code

<0> Indeterminate or intermediate state

<1> OFF

<2> ON

<3> Indeterminate state

Key – Status Bits

BL Blocked

SB Substituted

NT Not topical

IV Invalid

BSI Binary state information

This is a 4-octet, 32-bit set of independently assigned bits.

7	6	5	4	3	2	1	0
7							0
15							8
23							16
31							24

SCD Status change detection

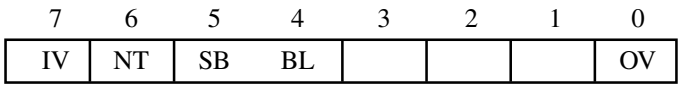
This is a 4-octet information element containing the states of 16 independent bits, plus change status for each.

7	6	5	4	3	2	1	0	
7							0	Status bits
15							8	
23							16	Change bits
31							24	

Bits <0..15> are the status bits, and bits <16..31> are the corresponding change bits. A change bit is set if at least one change has occurred to the bit since last reported.

QDS Quality descriptor

The quality descriptor may be used to provide the same quality information for analog and counter values as is included with the single or double-point with quality information elements. In addition it has an overflow bit OV.

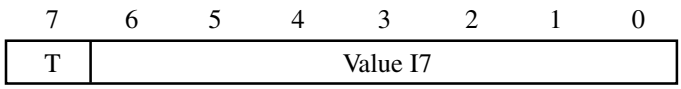


Key – Bit

OV	Overflow
BL	Blocked
SB	Substituted
NT	Not topical
IV	Invalid

VTI Value with transient state indication

This information element may be used for step position for transformers and other devices with step positions.

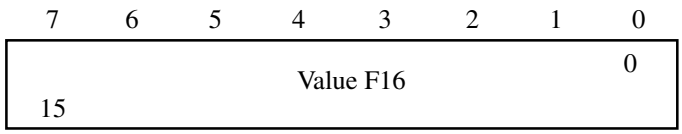


Key

I7	Value I7[1..7] <−64..+63>
T	Transient state

NVA Normalized value

A normalized value is a number in the range of −1.0 to 1.0, or as close as can be represented by the length of number used. If the resolution of the measuring device is less than that provided by the normalized value, then the lower significant bits are cleared to zero.

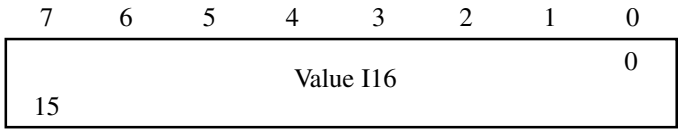


Key

F16	Value F16[0..15] <−1..+1−2^{-15}>

SVA Scaled value

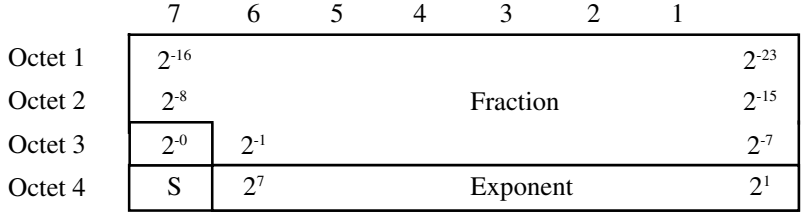
This is used to transmit values where a fixed decimal point position is defined. Values are in the range −32 768 to +32 767. The range and the position of the decimal points are fixed parameters, set in the system database. For example, a value of 39.5 amps may be transmitted as 395 where the resolution is fixed at 0.1 amp.



Key		
I16		Value I16[0..15] <2^{15}..+1−2^{-15}>

R32 short floating point number

The short floating point number is a 4-octet number defined by IEEE Standard 754. It is made up of a fraction, an exponent or power of 2, and a sign bit.



Key		
F	Fraction	UI23[0..22] <0..1−2^{-23}>
E	Exponent	UI[23..30] <0..255>
S	Sign	0= Positive, 1 = Negative

Interpretation

Case	**Interpretation**
F=<0>, E=<0>	Value = <0>
F non-zero, E=<0>	Non-normalized number Value = $(-1)^S \times 2^{E-126} \times (0.F)$
F non-zero, E <1..254>	Normalized number Value = $(-1)^S \times 2^{E-127} \times (1.F)$
F=<0>, E=<255>	Value = $(-1)^S \times$ infinity
F non-zero, E=<255>	Not a valid number

Note that a normalized number is one which has been scaled to the form 0.1xxxx so that it falls between 0.1 and 1.0, and then multiplied by 2 to give 1.xxxx. This removes the leading '1' to the right of the radix point, which is redundant because it is always a 1.

BCR Binary counter reading

	7	6	5	4	3	2	1	0
Octet 1	7							0
Octet 2	15			Counter I32				8
Octet 3	23							16
Octet 4	31							24
Octet 5	IV	CA	CY	SQ				

Key

I32 Counter value I32[0..31] <$-2^{31}..+2^{31}-1$>

SQ Sequence number UI5[32..36] <0..31>

CY Carry

CA Counter adjusted

IV Counter valid

Counter adjusted (CA): This means that the counter value has been adjusted since the last reading.

Sequence number (SQ): This number is incremented with each counter read operation.

Protection relay information elements

The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
SEP	Single event of protection equipment
SPE	Start events of protection equipment
OCI	Output circuit information of protection equipment
QDP	Quality descriptor for events of protection equipment

Table 8.15 Extract B
Protection relay information elements

SEP Single event of protection equipment

7	6	5	4	3	2	1	0
IV	NT	SB	BL	EI		ES	

Key – Event state ES <0..3>

<0> Indeterminate state

<1> OFF

<2> ON

<3> Indeterminate state

Key

EI	Elapsed time invalid
BL	Blocked
SB	Substituted
NT	Not topical
IV	Invalid

SPE Start events of protection equipment

7	6	5	4	3	2	1	0
		SRD	SIE	SL3	SL2	SL1	GS

Key

GS	General start of operation
SL1	Start of operation phase L1
SL2	Start of operation phase L2
SL3	Start of operation phase L3
SIE	Start of operation IE (earth current)
SRD	Start of operation in reverse direction

OCI Output circuit information

7	6	5	4	3	2	1	0
				CL3	CL2	CL1	GC

Key

GC	General start of operation
CL1	Start of operation phase L1
CL2	Start of operation phase L2
CL3	Start of operation phase L3

QDP Quality descriptor for events of protection equipment

7	6	5	4	3	2	1	0
IV	NT	SB	BL	EI			

Key

EI	Elapsed time invalid
BL	Blocked
SB	Substituted
NT	Not topical
IV	Invalid

8.6.2 Command information elements

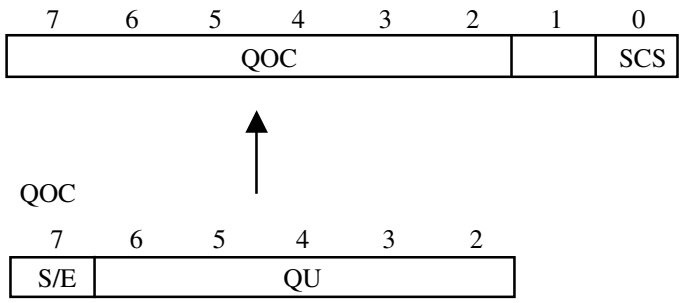
The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
SCO	Single command
DCO	Double command
RCO	Regulating step command

Table 8.15 Extract C
Command information elements

SCO Single command

This is a command to operate a single output. Bits 2 to 7 are the Qualifier of Command sub-field. This is used for other commands also.



Key – Command

SCS Single command state BS1[0] <0..1>
<0> = Command OFF
<1> = Command ON

Key – QOC Qualifier of command

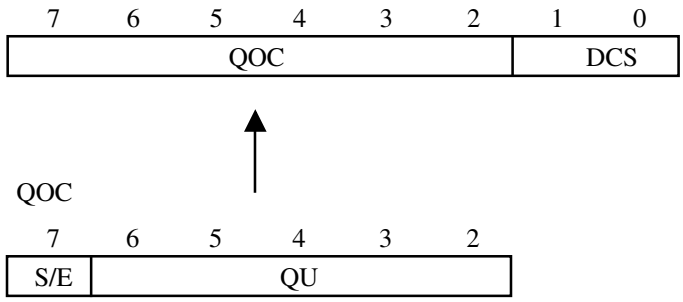
QU Qualifier UI5[2..6] <0..31>
<0> = No additional definition
<1> = Short pulse duration
<2> = Long duration pulse
<3> = Persistent output
<4..8> = Reserved for further standard definitions
<9..15> = Reserved for selection of other predefined functions
<16..31> = Reserved for special use (private range)

S/E Select/Execute BS1[7] <0..1>
<0> = Execute
<1> = Select

An important feature of this command is that it has two forms depending on bit 7, the select and the execute form. The select form is used when select before execute operation is required. This is also known as two-phase command operation.

DCO Double command

The double command state is used when two physical outputs are used to command operation. This is used to provide higher security against false operation due to equipment failure or transmission error. The qualifier of command sub-field is the same as for the single command.



Key – Command

DCS Double command state BS2[0..1] <0..3>

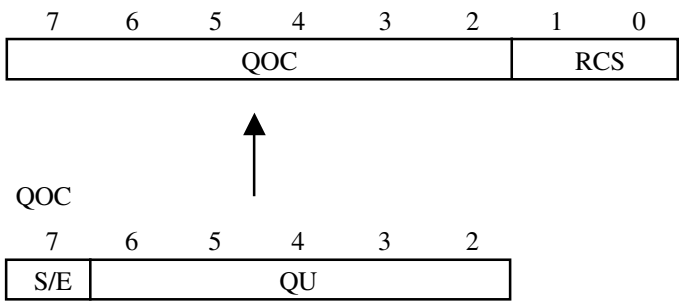
<0> = Not permitted

<1> = Command OFF

<2> = Command ON

<3> = Not permitted

RCO Regulating step command



Key – Command

RCS Single command state BS2[0..1] <0..3>

<0> = Not permitted

<1> = Next step LOWER

<2> = Next step HIGHER

<3> = Not permitted

8.6.3 Time information elements

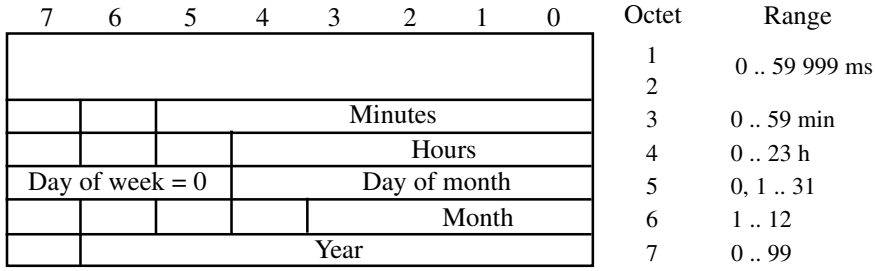
The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
CP56Time2a	Seven octet binary time
CP24Time2a	Three octet binary time
CP16Time2a	Two octet binary time

Table 8.15 Extract D
Command information elements

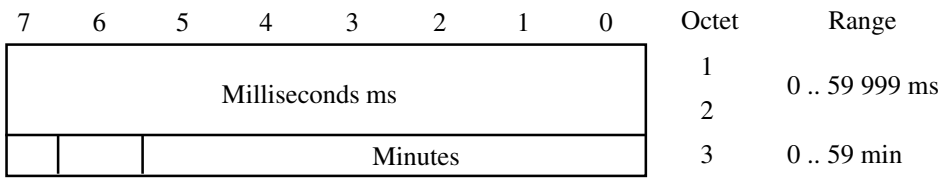
CP56Time2a – Seven-octet binary time

Seven-octet binary time is used for clock synchronization. Note that although days of the week are defined, these are not used and are set to zero.



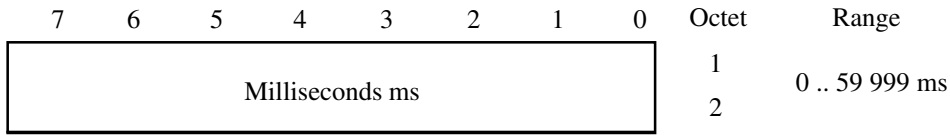
CP24Time2a – Three-octet binary time

This is typically used for time tags of information objects. It is the first three octets of the seven-octet binary time element.



CP16Time2a – Two-octet binary time

This is used for elapsed times such as for relay operating time. It is the first two octets of the seven octet-binary time element.



8.6.4 Qualifier information elements

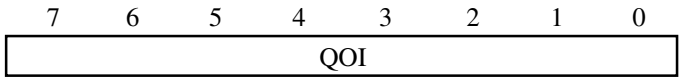
The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
QOI	Qualifier of interrogation
QCC	Qualifier of counter interrogation command
QPM	Qualifier of parameter of measured values
QPA	Qualifier of parameter activation
QOC	Qualifier of command
QRP	Qualifier of reset process command
QOS	Qualifier of set-point command

Table 8.15 Extract E
Command information elements

Qualifiers are information elements used in combination with other information elements in the definition of ASDUs.

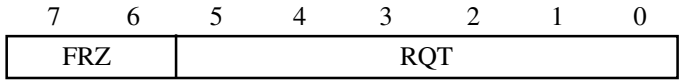
QOI Qualifier of interrogation



Key

QOI Qualifier of command UI8[1..7] <0..255>
- <0> = Not used
- <1..19> = Reserved for future standard definitions
- <20> = Station interrogation – global
- <20+N> = Interrogation of group G, where G = <1..16>
- <37..63> = Reserved for future standard definitions
- <64..255>= Reserved for special use (private range)

QCC Qualifier of counter interrogation command



Key

RQT Request UI6[0..5] <0..63>
- <0> = Not used
- <0+N> = Request counter group G, where G = <1..4>
- <5> = General request counter
- <6..31> = Reserved for future standard definitions
- <32..63> = Reserved for special use (private range)

FRZ Freeze UI2[6..7] <0..3>
- <0> = Read without freeze or reset
- <1> = Freeze without reset
- <2> = Freeze with reset
- <3> = Reset

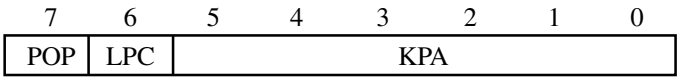
Note that the action specified by FRZ is applied to the group selected by the RQT code.

The four values of freeze code FRZ each specify a different operation immediately following the counter read. These are:

<0> Continue to count from value. The read is just a snapshot
<1> Stop counting and hold value as read
<2> Clear the count to zero and stop counting
<3> Clear the count and continue counting from zero

QPM Qualifier of parameter of measured values

This information element is used in setting local parameters of measured values. The KPA code defines the type of parameter, and the other bits determine whether local changes are permitted, and whether the parameter is to be activated.



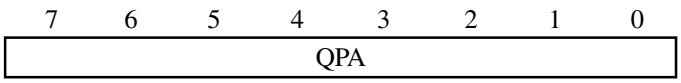
Key

KPA Kind of Parameter UI6[0..5] <0..63>
- <0> = Not used
- <1> = Threshold value
- <2> = Smoothing factor (filter time constant)
- <3> = Low limit for transmission of measured values
- <4> = High limit for transmission of measured values
- <5..31> = Reserved for future standard definitions
- <32..63> = Reserved for special use (private range)

LPC Local parameter change BS1 [6] <0..1>
- <0> = No change
- <1> = Change

POP Parameter in operation BS1[7] <0..1>
- <0> = Operation
- <1> = Not in operation

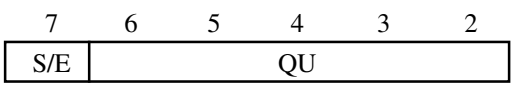
QPA Qualifier of parameter activation



Key

QPA UI8[0..7] <0..255>
- <0..2> = Not used
- <3> = Activation of cyclic transmission of object
- <4..127> = Reserved for future standard definitions
- <128..255> = Reserved for special use (private range)

QOC Qualifier of command



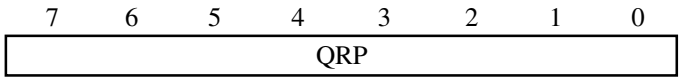
Key – QOC Qualifier of command

QU Qualifier UI5[2..6] <0..31>
<0> = No additional definition
<1> = Short pulse duration
<2> = Long duration pulse
<3> = Persistent output
<4..8> = Reserved for further standard definitions
<9..15> = Reserved for selection of other predefined functions
<16..31> = Reserved for special use (private range)

S/E Select/Execute BS1[7] <0..1>
<0> = Execute
<1> = Select

Note that code <0> may be used when the control function performance is fixed and not affected by the command qualifier.

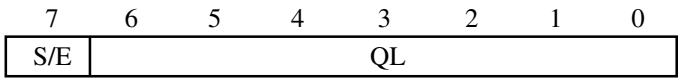
QRP Qualifier of reset process command



Key

QRP UI8[0..7] <0..255>
<0> = Not used
<1> = General reset of process
<2> = Clear time tagged information from event buffer
<3..127>= Reserved for future standard definitions
<128..255>= Reserved for special use (private range)

QOS Qualifier of set-point command



Key

QL Qualifier UI7[0..6] <0..127>
<0> = Default
<1..63> = Reserved for further standard definitions
<64..127> = Reserved for special use (private range)

S/E Select/Execute BS1[7] <0..1>
<0> = Execute
<1> = Select

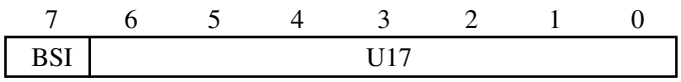
8.6.5 File transfer information elements

The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
FRQ	File ready qualifier
SRQ	Section ready qualifier
SCQ	Select and call qualifier
LSQ	Last section or segment qualifier
AFQ	Acknowledge file or section qualifier
NOF	Name of file
NOS	Name of section
LOF	Length of file or section
LOS	Length of segment
CHS	Checksum
SOF	Status of file

Table 8.15 Extract E
Command information elements

FRQ File ready qualifier

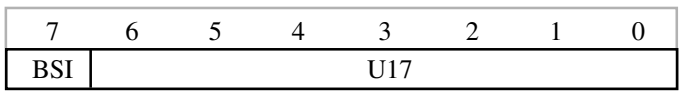


Key

UI7 Qualifier Code UI7[0..6] <0..127>
<0> = Default
<1..63> = Reserved for further standard definitions
<64..127> = Reserved for special use (private range)

BS1 Non-confirmation BS1[7] <0..1>
<0> = Positive confirmation of select, request, deactivate or delete
<1> = Negative confirmation

SRQ Section ready qualifier

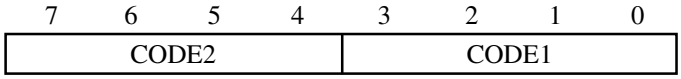


Key

UI7 Qualifier Code UI7[0..6] <0..127>
<0> = Default
<1..63> = Reserved for further standard definitions
<64..127> = Reserved for special use (private range)

BS1 Not Ready BS1[7] <0..1>
<0> = Section ready to load
<1> = Section not ready to load

SCQ Select and call qualifier

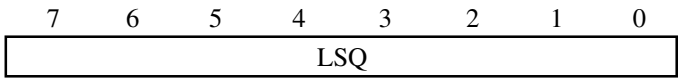


Key

CODE1 Selection Code UI4[0..3] <0..15>
- <0> = Default
- <1> = Select file
- <2> = Request file
- <3> = Deactivate file
- <4> = Delete file
- <5> = Select section
- <6> = Request section
- <7> = Deactivate section
- <8..10> = Reserved for further standard definitions
- <11.15> = Reserved for special use (private range)

CODE2 Fault Code UI4[4..7] <0..15>
- <0> = Default
- <1> = Requested memory space not available
- <2> = Checksum failed
- <3> = Unexpected communication service
- <4> = Unexpected name of file
- <5> = Unexpected name of section
- <6..10> = Reserved for further standard definitions
- <11.15> = Reserved for special use (private range)

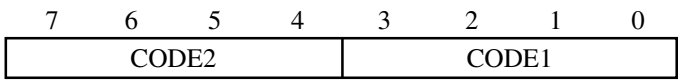
LSQ Last section or segment qualifier



Key

LSQ Selection Code UI8[0..7] <0..255>
- <0> = Not used
- <1> = File transfer without deactivation
- <2> = File transfer with deactivation
- <3> = Section transfer without deactivation
- <4> = Section transfer with deactivation
- <5..127> = Reserved for further standard definitions
- <128.255> = Reserved for special use (private range)

AFQ Acknowledge file or section qualifier

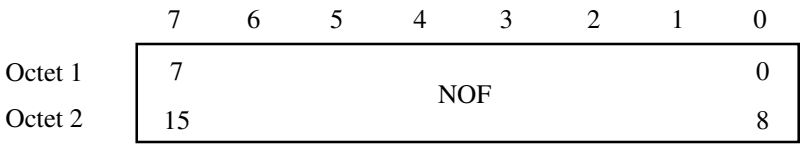


Key

CODE1 Selection Code UI4[0..3] <0..15>
- <0> = Not used
- <1> = Positive acknowledge of file transfer
- <2> = Negative acknowledge of file transfer
- <3> = Positive acknowledge of section transfer
- <4> = Negative acknowledge of section transfer
- <5..10> = Reserved for further standard definitions
- <11.15> = Reserved for special use (private range)

CODE2 Fault Code UI4[4..7] <0..15>
- <0> = Default
- <1> = Requested memory space not available
- <2> = Checksum failed
- <3> = Unexpected communication service
- <4> = Unexpected name of file
- <5> = Unexpected name of section
- <6..10> = Reserved for further standard definitions
- <11.15> = Reserved for special use (private range)

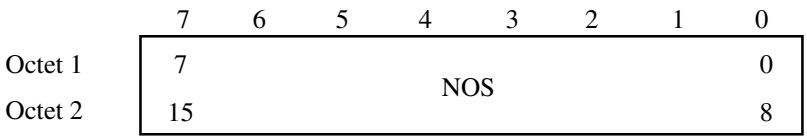
NOF Name of file



Key

NOF Name of File UI16[0..15] <0..65535>
- <0> = Default
- <1..65535> = Name of file

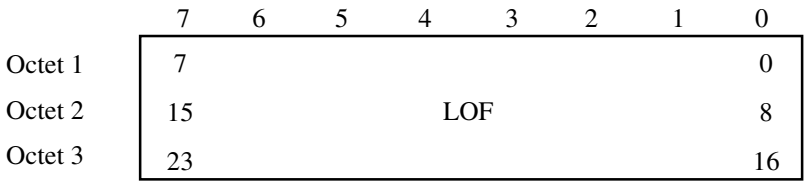
NOS Name of section



Key

NOS Name of Section UI16[0..15] <0..65535>
- <0> = Default
- <1..65535> = Name of section

LOF Length of file

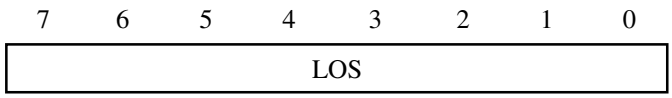


Key

LOF Length of File UI24[0..23] <0..16777215>
<0> = Not used
<1..16777215> = Length of file

The length is that of the complete file or section in octets.

LOS Length of segment

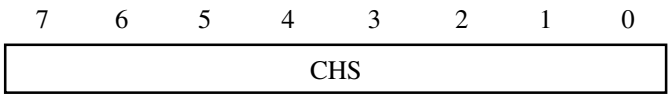


Key

LOS Length of Segment UI8[0..7] <0..255>
<0> = Not used
<1..N> = Number of octets in segment

The length N ranges between 1 and a maximum number which is determined by the maximum length of the data link user data field, the data unit identifier and the information object address. The maximum value of N taking these into account is between 234 and 240.

CHS Checksum

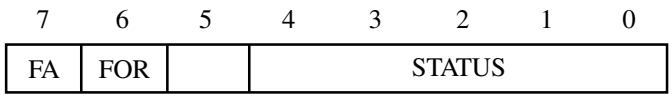


Key

CHS Checksum UI8[0..7] <0..255>
<0..255> = Arithmetic sum modulo 256

When used in a last segment ASDU the checksum is the modulo 256 sum over all the octets of the section. When used in a last section ASDU, the checksum applies to the whole file. This allows verification on a per-section basis, and finally on the complete file.

SOF Status of file



Key

STATUS Status of File UI5[0..4] <0..32>
<0> = Default
<1..15> = Reserved for further standard definitions
<16..32> = Reserved for special use (private range)

FOR File Origin BS1[6] <0..1>
<0> = Name defines file
<1> = Name defines subdirectory

FA File Active BS1[7] <0..1>
<0> = File waits for transfer
<1> = Transfer of this file is active

8.6.6 Miscellaneous information elements

The following information elements from Table 8.15 are presented in this sub-section.

Symbol	Description
COI	Cause of initialization
FBP	Fixed test bit pattern, two octets

Table 8.15 Extract F
Command information elements

COI Cause Of initialization

7	6	5	4	3	2	1	0
BSI	U17						

Key

UI7 Qualifier UI7[0..6] <0..127>
<0> = Local power switch on
<1> = Local manual reset
<2> = Remote reset
<3..31> = Reserved for future standard definitions
<32..127> = Reserved for special use (private range)

BS1 Select/Execute BS1[7] <0..1>
<0> = Initialization with unchanged local parameters
<1> = Initialization after changed local parameters

FBP **Fixed test bit pattern, two octet**

7	6	5	4	3	2	1	0
1	0	1	0	1	0	1	0
0	1	0	1	0	1	0	1

Key

Pattern Fixed Value UI16[1..16] <0x55AA>

8.7 Set of ASDUs

This section presents the set of application service data units or ASDUs defined under IEC 60870-5-101. ASDUs are the application level units of data that are used to convey SCADA information between controlling stations and controlled stations. Thus, there are ASDUs for each type of information carrying, such as sending control parameters, sending set-points, sending commands to set or clear particular status points, and for sending data such as measured analog values or counter values.

In Figure 9.17, the overall structure of the ASDUs was presented. This showed that each ASDU is made up of a data unit identifier followed by one or more information objects. The reader will recall that there are two types of structures that can be used, and these depend on the state of SQ bit of the variable structure qualifier field, which is in the data unit identifier. If the SQ bit is zero, then multiple information objects are allowed, between 1 and 127.

The two structures are shown in simplified form in Figures 8.24 and 8.25 following.

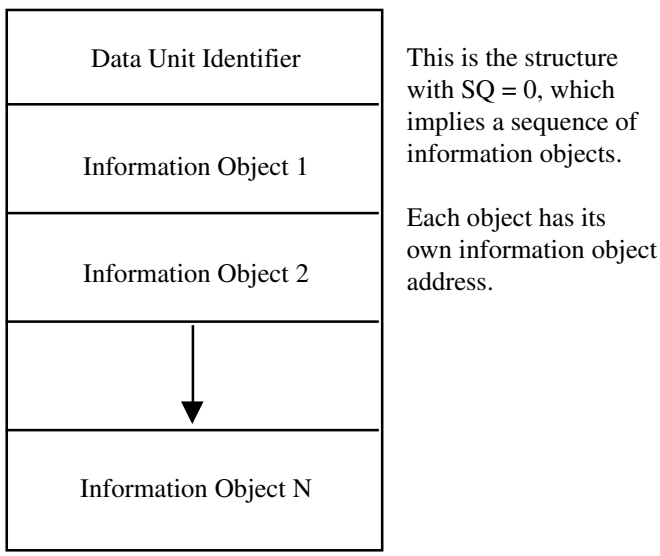
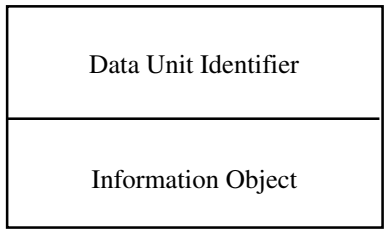


Figure 8.24
Simplified structure of ASDU with SQ=0



This is the structure with SQ = 1, which implies a sequence of information elements within one information object.

There is just one information object address, which is the address for the first information element.

Figure 8.25
Simplified structure of ASDU with SQ=1

For each defined type identification, there are either one or two forms of the ASDU depending on whether one or both variable structure codes are allowed. The ASDUs are made of components that have all been introduced and described in the preceding sections. These are summarized below.

ASDU components:

- Data unit identifier
  - Type identification
  - Variable structure qualifier
  - Cause of transmission
  - Common address of ASDU
- Information object
  - Information object address
  - One or more information elements
  - Time tag if used
- Additional information objects (if SQ = 0)
  - Information object address
  - One or more information elements
  - Time tag if used

The following sub-sections show the ASDUs organized by type numbers and groups. To avoid unnecessary repetition, for each ASDU only the information objects are shown. The reader must remember that the complete ASDU has the data unit identifier prior to the information object or objects.

Also, note that only one information object is shown for each of SQ = 0 and SQ = 1. In the case of SQ = 0, which implies a sequence of information objects the reader must be aware that although only one information object is presented, multiple information objects may be used to form the ASDU.

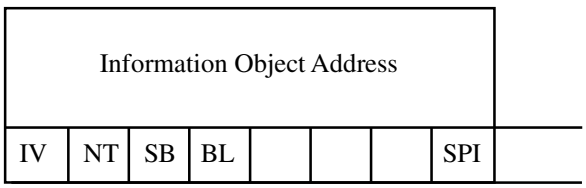
In the case of SQ = 1, which implies a sequence of information elements within one information object, there is of course only the one information object. For these note that there is only one information object address and one time tag, if used. The information object addresses for sequential information elements within the ASDU are obtained by incrementing from the address of the first information element. Thus for the i^{th} information element, the address is given by IOA + I − 1. The time tag therefore applies to all of the information elements within the ASDU.

8.7.1 Process information in monitor direction

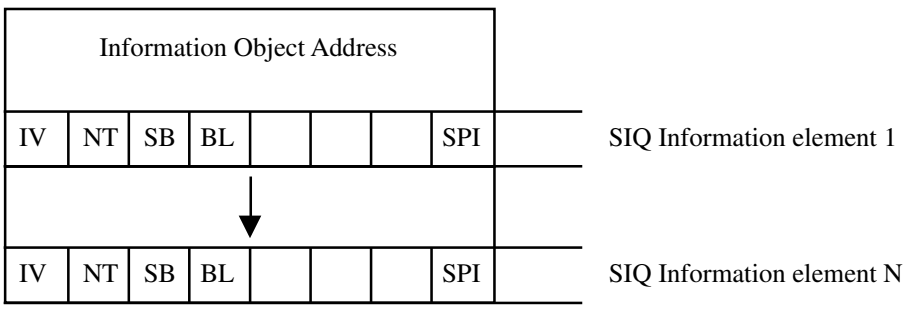
Type 1 Single-point without time

INFORMATION OBJECT TYPE:	1
CODE:	M_SP_NA_1
DESCRIPTION:	Single point information without time tag
VALID WITH SQ:	0, 1

Information object for SQ = 0 (sequence of Information Objects)



Information object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

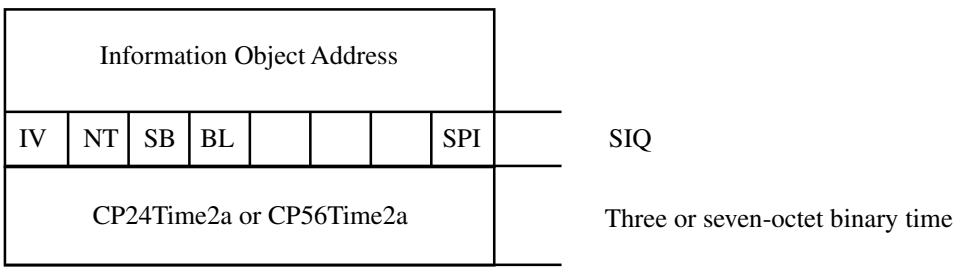
Notes

SIQ is single point information with quality

Types 2, 30 Single-point with time

INFORMATION OBJECT TYPE:	2, 30
CODE:	M_SP_TA_1, M_SP_TB_1
DESCRIPTION:	Single-point information with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Valid cause of transmission codes

<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command

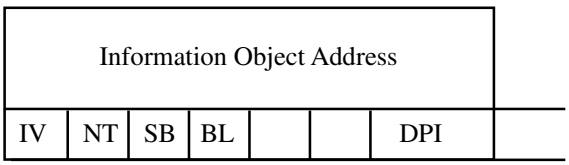
Notes

SIQ – Single-point information with quality descriptor
Type 2 has three-octet time. Type 30 has seven-octet time

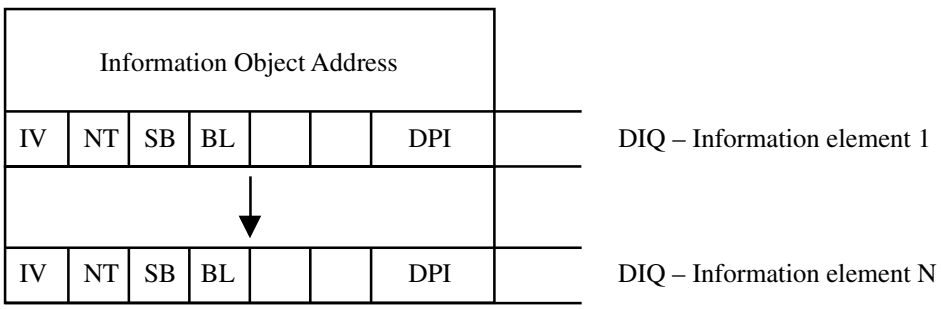
Type 3 Double-point without time

INFORMATION OBJECT TYPE:	3
CODE:	M_DP_NA_1
DESCRIPTION:	Double-point information without time tag
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

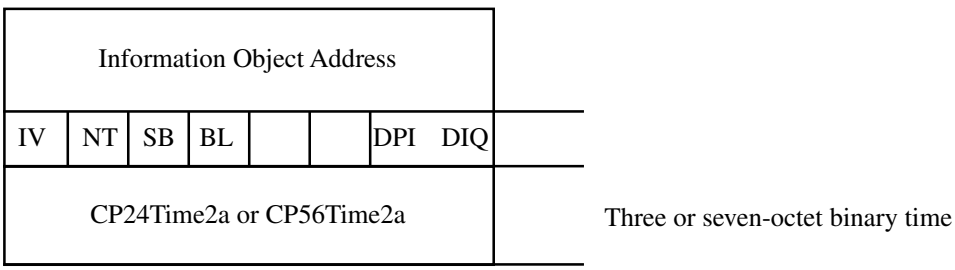
Notes

DIQ – Double-point information with quality descriptor

Types 4, 31 Double-point with time

INFORMATION OBJECT TYPE:	4, 31
CODE:	M_DP_TA_1, M_DP_TB_1
DESCRIPTION:	Double-point information with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Valid cause of transmission codes

<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command

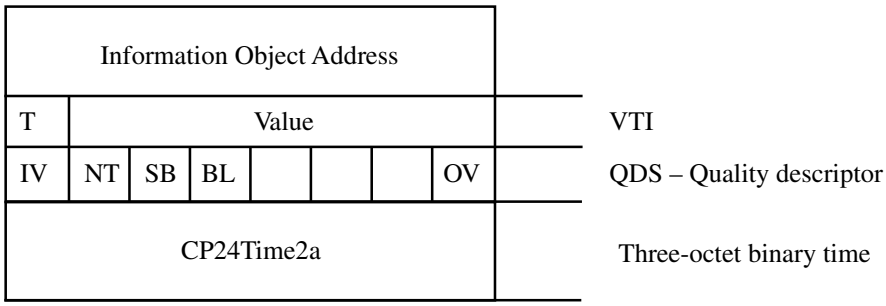
Notes

DIQ – Double-point information with quality descriptor
Type 4 has three-octet time. Type 31 has seven-octet time

Type 5, Step position information

INFORMATION OBJECT TYPE:	5
CODE:	M_ST_NA_1
DESCRIPTION:	Step position information
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)
Single information object only.



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

Notes

VTI – Value with transient state indication

Type 6, 32 Step position with time

INFORMATION OBJECT TYPE:	6, 32
CODE:	M_ST_TA_1, M_ST_TB_1
DESCRIPTION:	Step position information with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)
Single information object only.

Information Object Address									
T	Value								VTI
IV	NT	SB	BL				OV		QDS – Quality Descriptor
CP24Time2a or CP56 Time 2a									Three or Seven-octet binary time

Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command

Notes

VTI – Value with transient state indication
Type 6 has three-octet time. Type 32 has seven-octet time

Type 7, Bit-string of 32 bits

INFORMATION OBJECT TYPE:	7
CODE:	M_BO_NA_1
DESCRIPTION:	Bit-string of 32 bits
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)
Information Object Address

Information Object Address								
						O		
								BSI
31								
IV	NT	SB	BL			OV		QDS – Quality Descriptor

Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

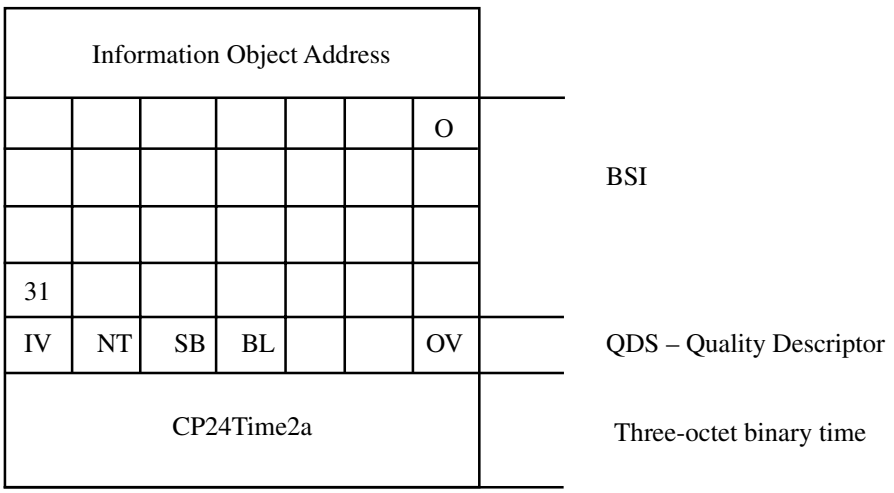
Notes

BSI – Binary state information, 32-bit

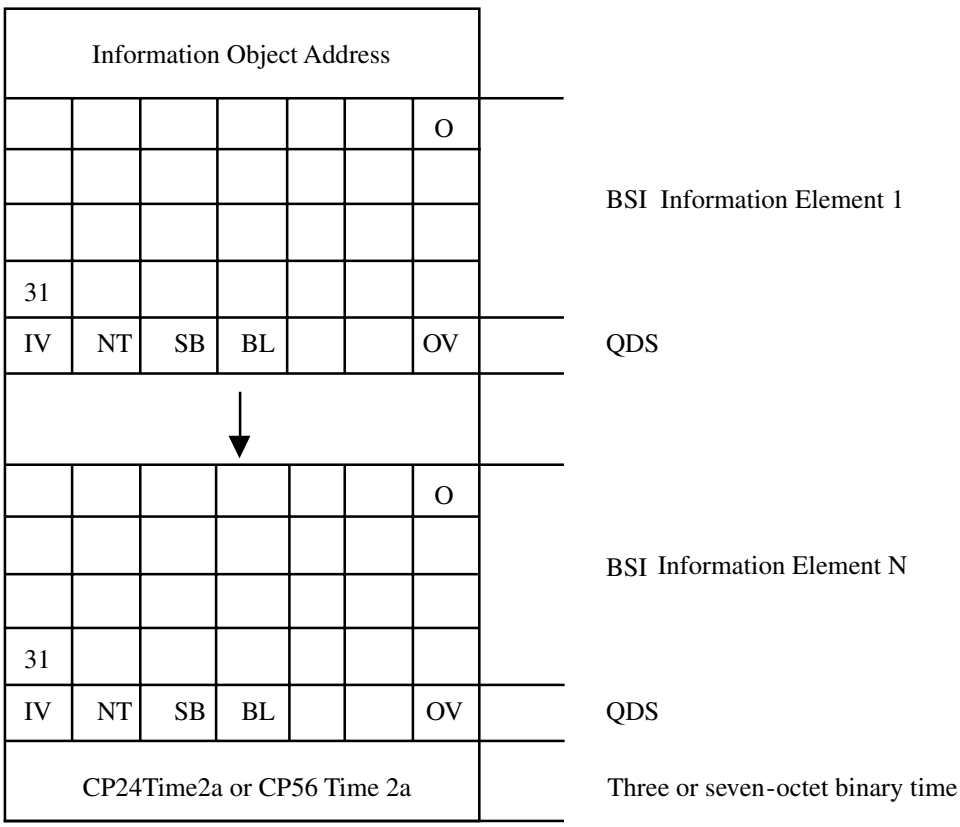
Types 8, 33 Bit-string of 32 bits with time

INFORMATION OBJECT TYPE:	8, 33
CODE:	M_BO_TA_1, M_BO_TB_1
DESCRIPTION:	Bit-string of 32 bits with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<3>	Spontaneous
<5>	Requested

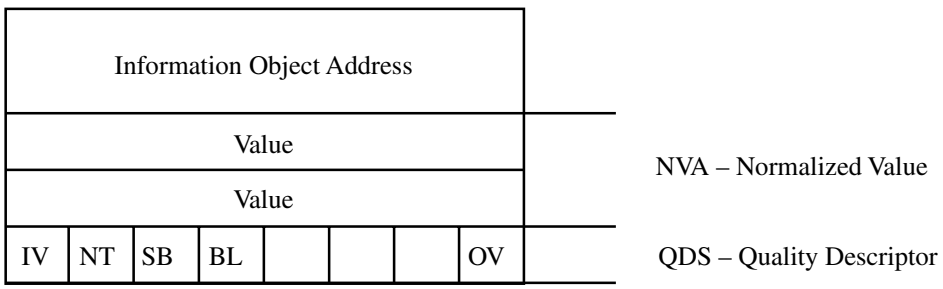
Notes

BSI – Binary state information, 32-bit.
Type 8 has three-octet time. Type 33 has seven-octet time.

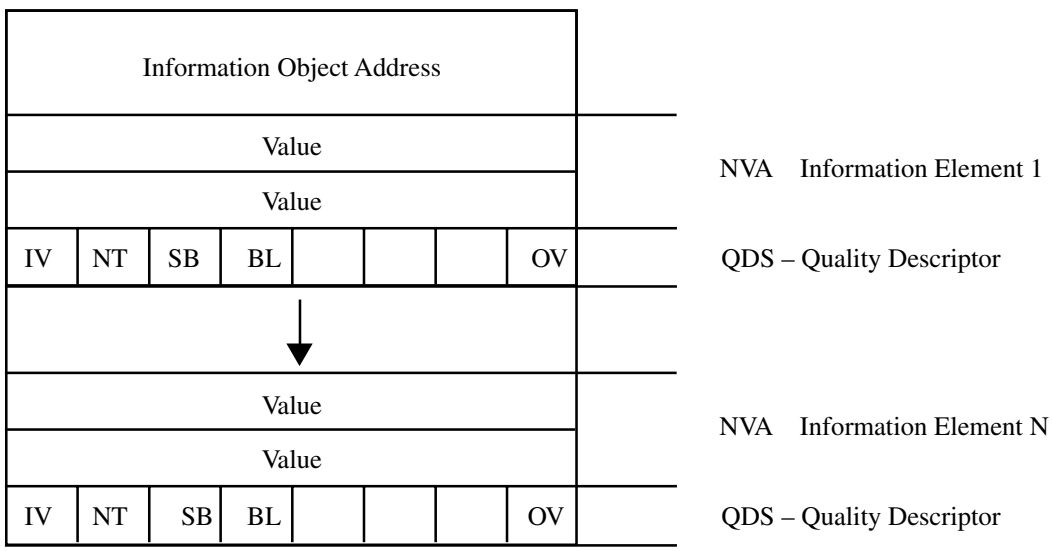
Type 9, Measured, normalized value

INFORMATION OBJECT TYPE:	9
CODE:	M_ME_NA_1
DESCRIPTION:	Measured value, normalized value
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

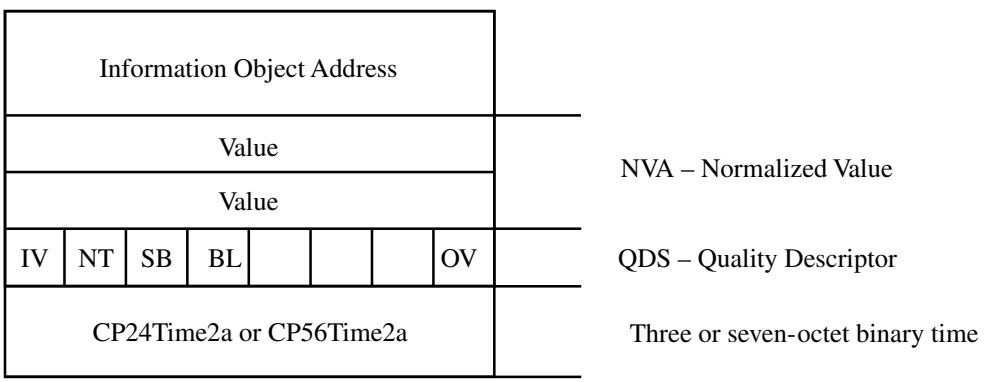
Notes

NVA – Normalized value

Types 10, 34 Measured, normalized value with time

INFORMATION OBJECT TYPE:	10, 34
CODE:	M_ME_TA_1, M_ME_TD_1
DESCRIPTION:	Measured value, normalized value with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Valid cause of transmission codes

<3>	Spontaneous
<5>	Requested

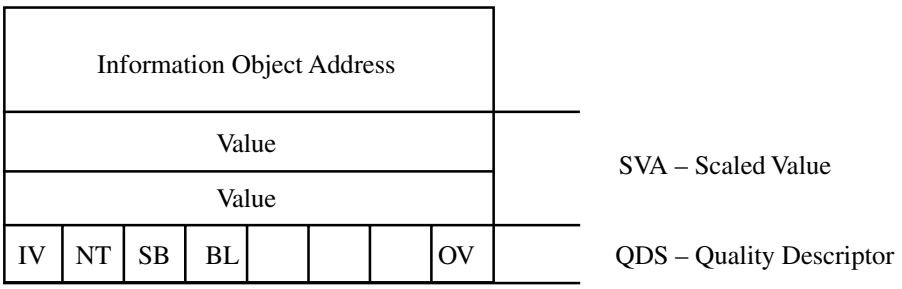
Notes

NVA – Normalized value
Type 10 has three-octet time. Type 34 has seven-octet time

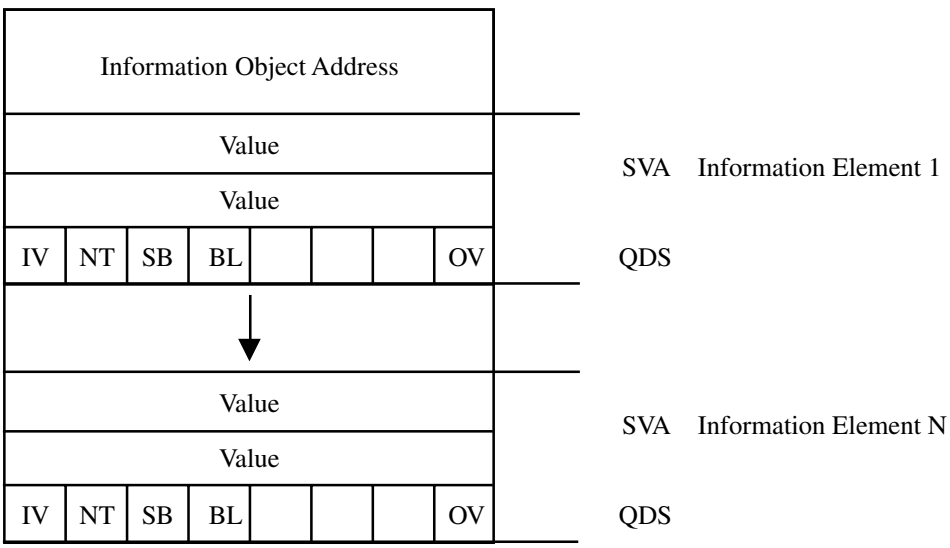
Type 11 Measured, scaled value

INFORMATION OBJECT TYPE:	11
CODE:	M_ME_NB_1
DESCRIPTION:	Measured value, scaled value
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

Notes

SVA – Scaled value

Types 12, 35 Measured, scaled value with time

INFORMATION OBJECT TYPE:	12, 35
CODE:	M_ME_TB_1, M_ME_TE_1
DESCRIPTION:	Measured value, scaled value with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Information Object Address								
Value								SVA – Normalized Value
Value								
IV	NT	SB	BL				OV	QDS – Quality Descriptor
CP24Time2a or CP56Time2a								Three or seven-octet binary time

Valid cause of transmission codes

<3>	Spontaneous
<5>	Requested

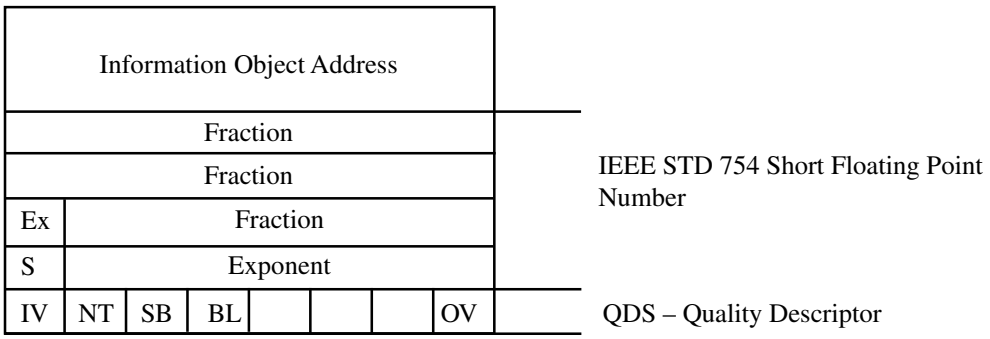
Notes

SVA – Scaled value
Type 12 has three-octet time. Type 35 has seven-octet time

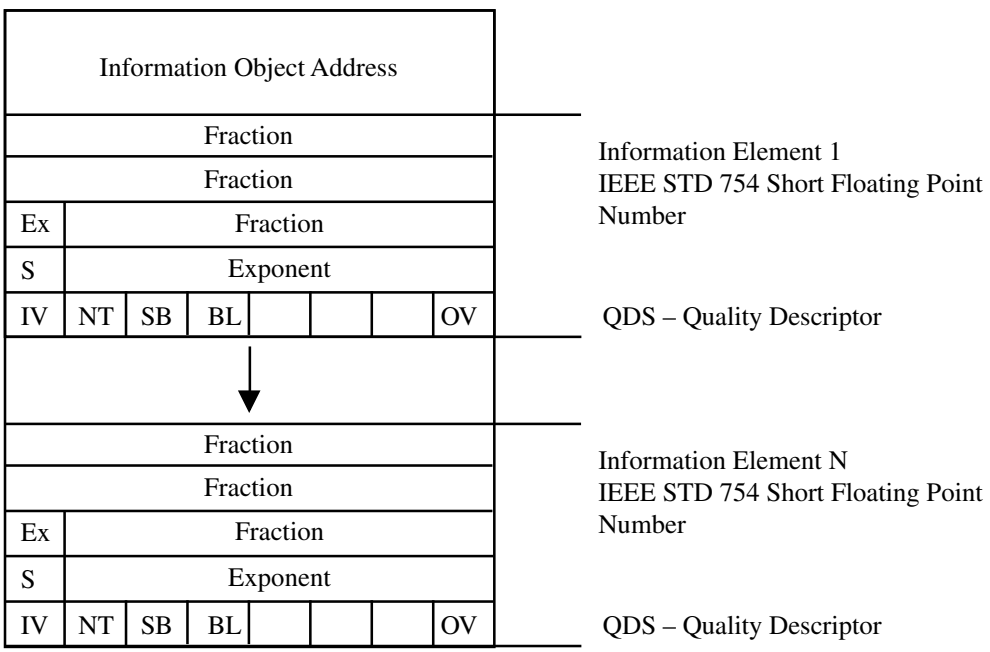
Type 13 Measured, short FP number

INFORMATION OBJECT TYPE:	13
CODE:	M_ME_NC_1
DESCRIPTION:	Measured value, short floating point number
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

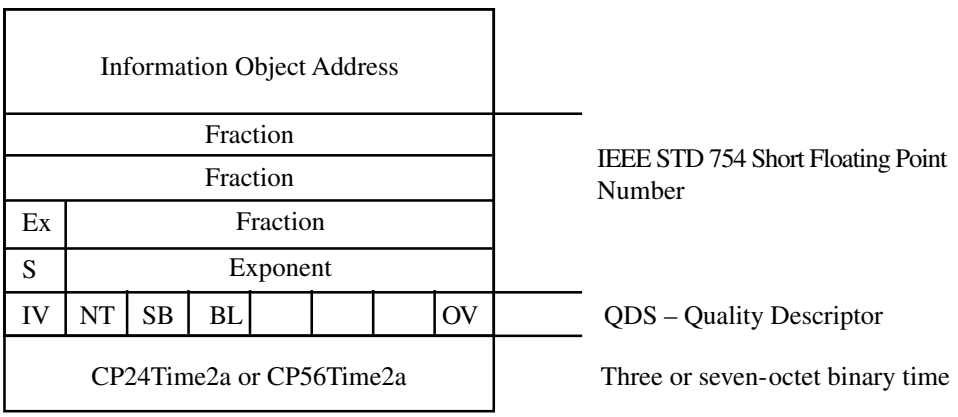
Notes

IEEE STD 754 – Short floating point number

Types 14, 36 Measured short FP number with time

INFORMATION OBJECT TYPE:	14, 36
CODE:	M_ME_TC_1, M_ME_TF_1
DESCRIPTION:	Measured value, short floating point number with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>

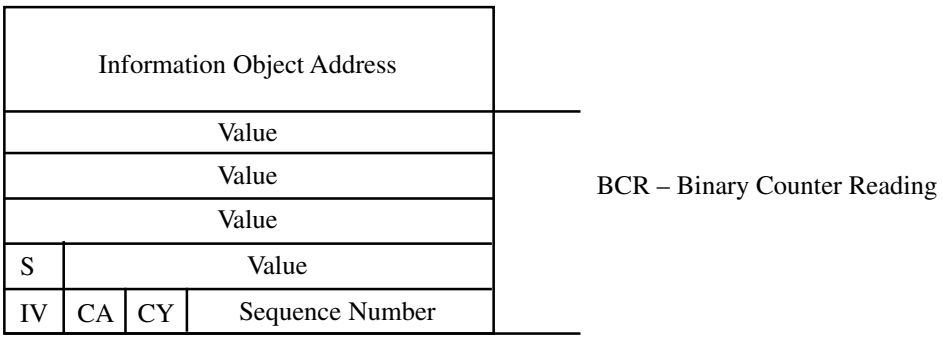
Notes

IEEE STD 754 – Short floating point number
Type 14 has three-octet time. Type 36 has seven-octet time

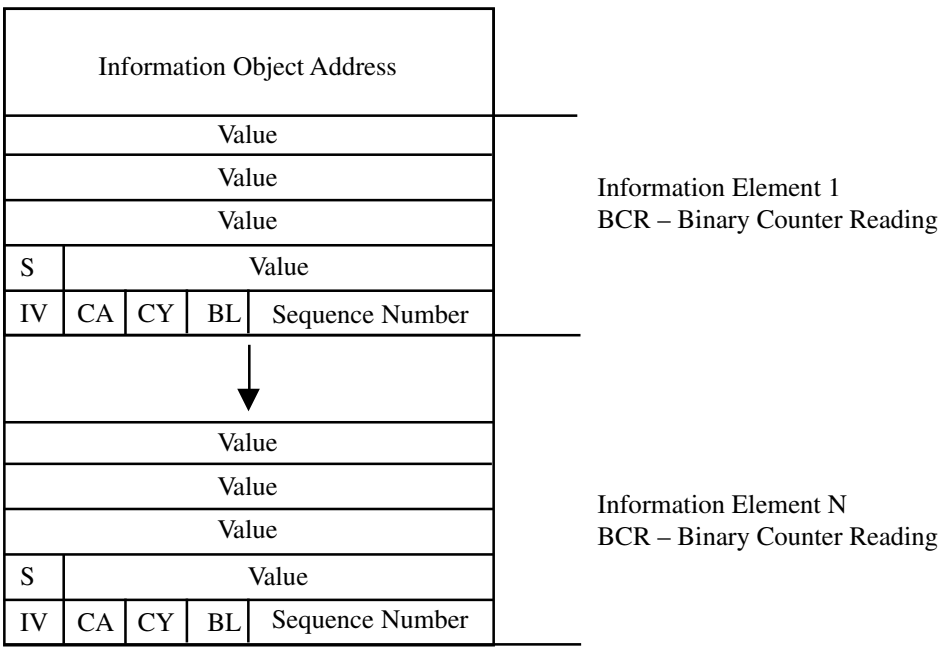
Type 15 Integrated totals

INFORMATION OBJECT TYPE:	15
CODE:	M_IT_NA_1
DESCRIPTION:	Integrated totals
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<2>	Background scan
<37>	Requested by general counter request
<37 + G>	Requested by group G counter request G = <1..4>

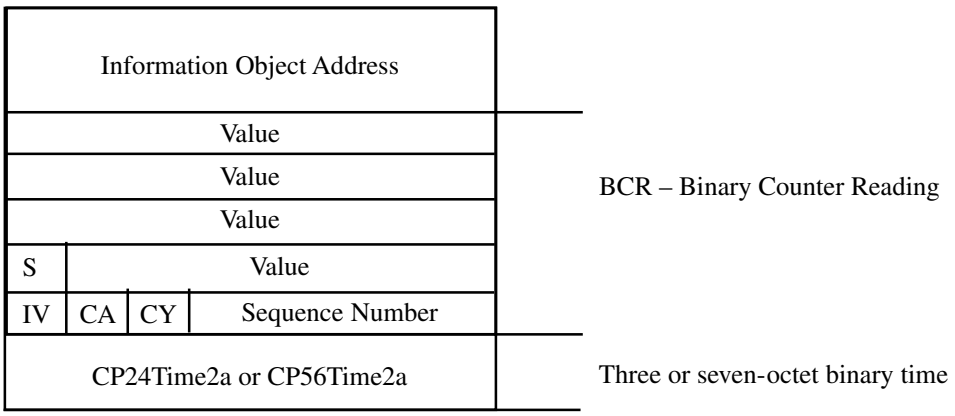
Notes

BCR – Binary counter reading

Types 16, 37 Integrated totals with time

INFORMATION OBJECT TYPE:	16,37
CODE:	M_IT_TA_1, M_IT_TB_1
DESCRIPTION:	Integrated totals with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Valid cause of transmission codes

<3>	Spontaneous
<37>	Requested by general counter request
<37 + G>	Requested by group G counter request G = <1..4>

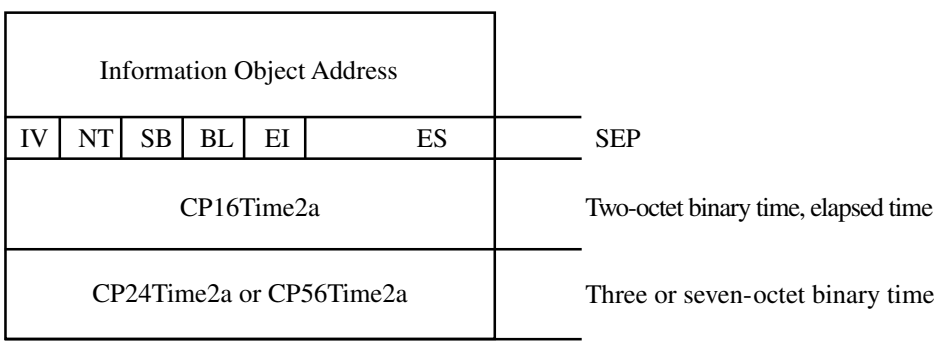
Notes

BCR – Binary counter reading
Type 16 has three-octet time. Type 37 has seven-octet time

Types 17, 38 Event of protection with time

INFORMATION OBJECT TYPE:	17, 38
CODE:	M_EP_TA_1, M_EP_TD_1
DESCRIPTION:	Event of protection equipment with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)



Valid cause of transmission codes

<3> Spontaneous

Notes

SEP – Single event of protection equipment
Type 17 has three-octet time
Type 38 has seven-octet time

Types 18, 39 Packed events of protection with time

INFORMATION OBJECT TYPE:	18, 39
CODE:	M_EP_TB_1, M_EP_TE_1
DESCRIPTION:	Packed start of events of protection equipment with time tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)
Single information object only.

Information Object Address									
		SRD	SIE	SL3	SL2	SL1	GS		SEP
IV	NT	SB	BL	EI					QDP
CP16Time2a									Two-octet binary time, relay duration time
CP24Time2a or CP56Time2a									Three or seven-octet binary time

Valid cause of transmission codes

<3> Spontaneous

Notes

SPE – Start event of protection equipment
QDP – Quality descriptor of protection equipment
Type 18 has three-octet time
Type 39 has seven-octet time

Types 19, 40 Packed output of protection with time

INFORMATION OBJECT TYPE:	19, 40
CODE:	M_EP_TC_1, M_EP_TF_1
DESCRIPTION:	Packed output circuit information of protection equipment with time-tag
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address									
				CL3	CL2	CL1	GC		OCI
IV	NT	SB	BL	EI					QDP
CP16Time2a									Two-octet binary time, relay operating time
CP24Time2a or CP56Time2a									Three or seven-octet binary time

Valid cause of transmission codes

<3> Spontaneous

Notes

OCI – Output circuit command of protection equipment
QDP – Quality descriptor of protection equipment
Type 19 has three-octet time
Type 40 has seven-octet time

Type 20 Packed single-point with status change detection

INFORMATION OBJECT TYPE:	20
CODE:	M_PS_NA_1
DESCRIPTION:	Packed single-point information with status change detection
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Information Object Address								
Status								SCD
Status								
Status Change detection								
Status Change detection								
IV	NT	SB	BL	EI			OV	QDS – Quality Descriptor

Valid cause of transmission codes

<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G = <1..16>

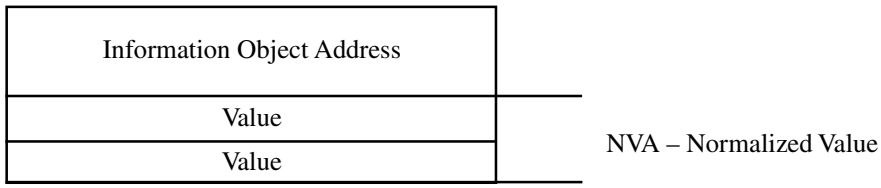
Notes

SCD – Status + status change detection, 32 bits

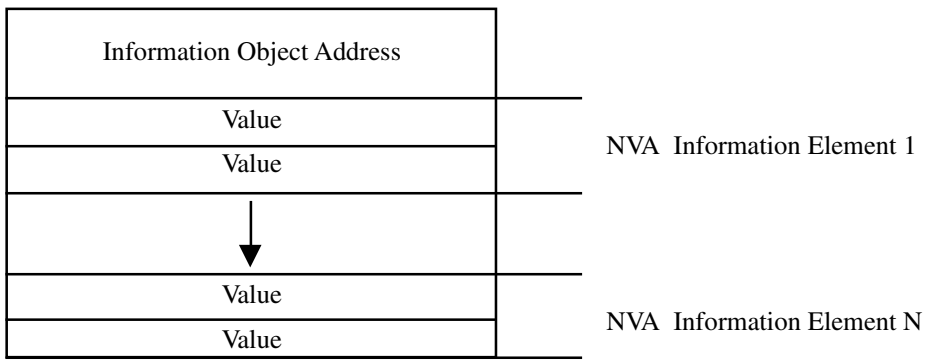
Type 21 Measured, normalized value without quality

INFORMATION OBJECT TYPE:	21
CODE:	M_ME_ND_1
DESCRIPTION:	Measured value, normalized value without quality descriptor
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)



Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<1>	Periodic / cyclic
<2>	Background scan
<3>	Spontaneous
<5>	Requested
<11>	Return of information caused by remote command
<12>	Return of information caused by local command
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G = <1..16>

Notes

NVA – Normalized value

Process Information in control direction

Type 45 single command

INFORMATION OBJECT TYPE:	45
CODE:	C_SC_NA_1
DESCRIPTION:	Single command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address				
S/E	QU		SCS	

SCO – Single Command

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

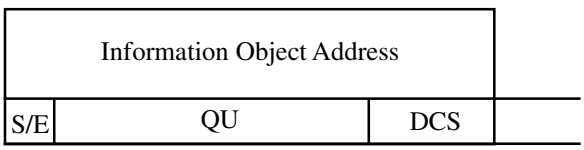
Notes

SCO – Single command

Type 46 Double command

INFORMATION OBJECT TYPE:	46
CODE:	C_DC_NA_1
DESCRIPTION:	Double command
VALID WITH SQ:	0, 1

Information Object for SQ = 0 (Sequence of Information Objects)
Single information object only.



DCO – Double Command

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

DCO – Double command

Type 47 Regulating step command

INFORMATION OBJECT TYPE:	47
CODE:	C_RC_NA_1
DESCRIPTION:	Regulating step command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address			
S/E	QU	RCS	

RCO – Regulating Step Command

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

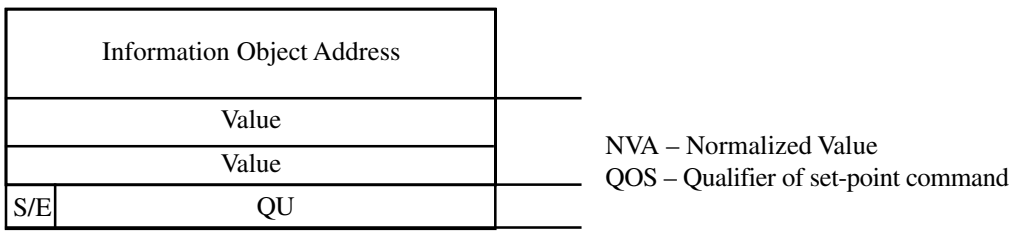
RCO – Regulating step command

Type 48 Set-point command, normalized value

INFORMATION OBJECT TYPE:	48
CODE:	C_SE_NA_1
DESCRIPTION:	Set-point command, normalized value
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.



Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

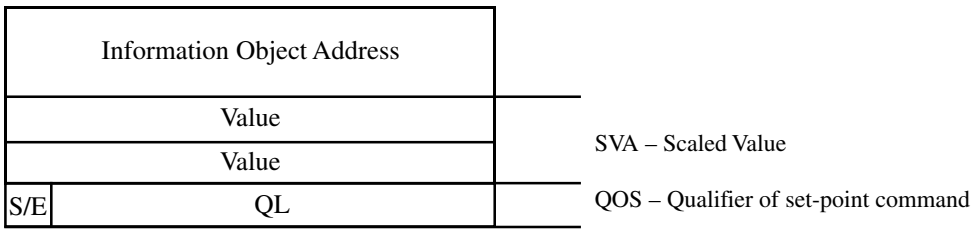
NVA – Normalized value
QOS – Qualifier of set-point command

Type 49 Set-point command, scaled value

INFORMATION OBJECT TYPE:	49
CODE:	C_SE_NB_1
DESCRIPTION:	Set-point command, scaled value
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.



Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

SVA – Normalized value
QOS – Qualifier of set-point command

Type 50 Set-point command, short FP number

INFORMATION OBJECT TYPE:	50
CODE:	C_SE_NC_1
DESCRIPTION:	Set-point command, short floating point number
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		
Fraction		IEEE STD 754 Short Floating Point Number
Fraction		
Ex	Fraction	
S	Exponent	
S/E	QL	QOS – Qualifier of set-point command

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

IEEE STD 754 – Short floating-point number
QOS – Qualifier of set-point command

Type 51 Bit-string of 32 bits

INFORMATION OBJECT TYPE:	51
CODE:	C_BO_NA_1
DESCRIPTION:	Bit-string of 32 bits
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address	
Bit-strings	BSI – Binary state information
Bit-strings	
Bit-strings	
Bit-strings	

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

BSI – Binary state information

System information in monitor direction

Type 70 End of initialization

INFORMATION OBJECT TYPE:	70
CODE:	M_EI_NA_1
DESCRIPTION:	End of initialization
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		IOA = 0
CP8		COI – Cause of Initialization

Valid cause of transmission codes

<4> Initialized

Notes

COI – Cause of Initialization

8.7.2 System information in control direction

Type 100 Interrogation command

INFORMATION OBJECT TYPE:	100
CODE:	C_IC_NA_1
DESCRIPTION:	Interrogation command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		IOA = 0
UI8		QOI – Qualifier of Interrogation

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

QOI – Qualifier of Interrogation

Type 101 Counter interrogation command

INFORMATION OBJECT TYPE:	101
CODE:	C_CI_NA_1
DESCRIPTION:	Counter interrogation command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		IOA = 0
CP8		QCC – Qualifier of counter command

Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

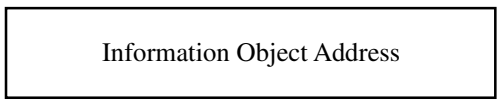
QCC – Qualifier of counter command

Type 102 Read command

INFORMATION OBJECT TYPE:	102
CODE:	C_RD_NA_1
DESCRIPTION:	Read command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.



Valid cause of transmission codes

<5> Request

Notes

There is only the information object address with the data unit identifier for this command.

Type 103 Clock synchronization command

INFORMATION OBJECT TYPE:	103
CODE:	C_CS_NA_1
DESCRIPTION:	Clock synchronization command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address	IOA = 0
CP56Time2a	Seven-octet binary time

Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<3>	Spontaneous
<7>	Activation confirmation
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

This command may be used in the monitor direction to transmit the outstation clock time. This enables messages stored at an outstation that span a change of hour to be interpreted without ambiguity. This arises because three-octet binary time provides only minutes and milliseconds up to one hour. Therefore, to interpret correctly time-tags from outstations, it is necessary to include outstation time hour changes within the messages. It is also necessary for the master station to keep a track of outstation hour whilst sequentially processing stored time-tagged data.

Type 104 Test command

INFORMATION OBJECT TYPE:	104
CODE:	C_TS_NA_1
DESCRIPTION:	Test command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address								
								IOA = 0
1	0	1	0	1	0	1	0	FBP – Fixed test pattern
0	1	0	1	0	1	0	1	

Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<7>	Activation confirmation
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

FBP – Fixed test pattern

Type 105 Reset process command

INFORMATION OBJECT TYPE:	105
CODE:	C_RP_NA_1
DESCRIPTION:	Reset process command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		IOA = 0
UI8		QRP – Qualifier of reset process cmd.

Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<7>	Activation confirmation
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

QRP – Qualifier of reset process command

Type 106 Delay acquisition command

INFORMATION OBJECT TYPE:	106
CODE:	C_CD_NA_1
DESCRIPTION:	Delay acquisition command
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		IOA = 0
CP16Time2a		Two-octet binary time

Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<7>	Activation confirmation
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

FBP – Fixed test pattern

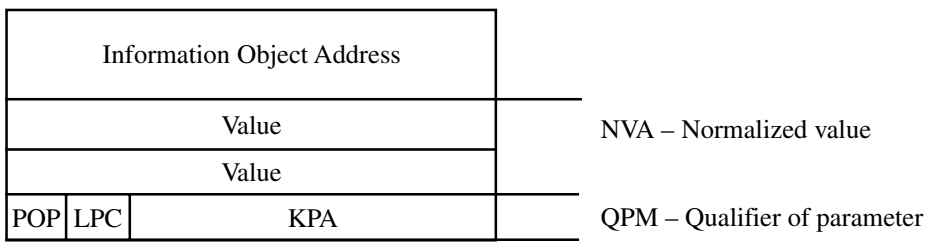
8.7.3 Parameter in control direction

Type 110 Parameter of measured, normalized value

INFORMATION OBJECT TYPE:	110
CODE:	PM_ME_NA_1
DESCRIPTION:	Parameter of measured values, normalized value
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.



Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>
<10>	Activation termination
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

QPM – Qualifier of parameter of measured values

Type 111 Parameter of measured, scaled value

INFORMATION OBJECT TYPE:	111
CODE:	PM_ME_NB_1
DESCRIPTION:	Parameter of measured values, scaled value
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address				
Value				SVA – Scaled value
Value				
POP	LPC	KPA		QPM – Qualifier of parameter

Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<7>	Activation confirmation
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G = <1..16>
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

QPM – Qualifier of parameter of measured values

Type 112 Parameter of measured, short floating point number

INFORMATION OBJECT TYPE:	112
CODE:	PM_ME_NC_1
DESCRIPTION:	Parameter of measured values, short floating point number
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address				
Fraction				IEEE STD 754 Short Floating Point Number
Fraction				
Ex	Fraction			
S	Exponent			
POP	LPC	KPA		QPM – Qualifier of parameter

Valid cause of transmission codes

In control direction

<6>	Activation

In monitor direction

<7>	Activation confirmation
<20>	Interrogated by station interrogation
<20 + G>	Interrogated by group G interrogation, G= <1..16>
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

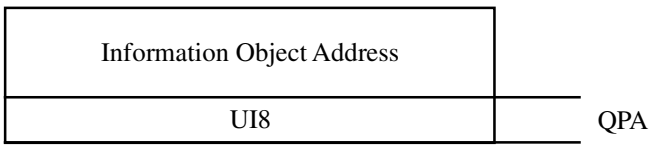
QPM – Qualifier of parameter of measured values

Type 113 Parameter activation

INFORMATION OBJECT TYPE:	113
CODE:	P_AC_NA_1
DESCRIPTION:	Parameter activation
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.



Valid cause of transmission codes

In control direction

<6>	Activation
<8>	Deactivation

In monitor direction

<7>	Activation confirmation
<9>	Deactivation confirmation
<44>	Unknown type identification
<45>	Unknown cause of transmission
<46>	Unknown common address of ASDU
<47>	Unknown information object address

Notes

QPA – Qualifier of parameter activation

8.7.4 File transfer

Type 120 File ready

INFORMATION OBJECT TYPE:	120
CODE:	F_FR_NA_1
DESCRIPTION:	File ready
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		
UI16		NOF – Name of file
UI24		LOF – Length of file
CP8		FRQ – File ready qualifier

Valid cause of transmission codes

<13> File transfer

Notes

NOF – Name of file
LOF – Length of file
FRQ – File ready qualifier

Type 121 Section ready

INFORMATION OBJECT TYPE:	121
CODE:	F_SR_NA_1
DESCRIPTION:	Section ready
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		
UI16		NOF – Name of file
UI8		NOS – Name of section
UI24		LOF – Length of file
CP8		SRQ – Section ready qualifier

Valid cause of transmission codes

<13> File transfer

Notes

NOF – Name of file
NOS – Name of section
LOF – Length of file

Type 122 Call directory

INFORMATION OBJECT TYPE:	122
CODE:	F_SC_NA_1
DESCRIPTION:	Call directory, select file, call file, call section
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		
UI16		NOF – Name of file
UI8		NOS – Name of section
CP8		SCQ – Select and call qualifier

Valid cause of transmission codes

<5>	Request (only for Call Directory)
<13>	File transfer (for all except Call Directory)

Notes

NOF – Name of file
NOF – Name of section
SCQ – Select and call qualifier

Type 123 Last section, last segment

INFORMATION OBJECT TYPE:	123
CODE:	F_LS_NA_1
DESCRIPTION:	Last section, last segment
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		
UI16		NOF – Name of file
UI8		NOS – Name of section
UI8		LSQ – Last section or segment qualifier
UI8		CHS – Checksum

Valid cause of transmission codes

<13> File transfer

Notes

NOF – Name of file
NOF – Name of section
LSQ – Last section or segment qualifier
CHS – Checksum

Type 124 ACK file, ACK section

INFORMATION OBJECT TYPE:	124
CODE:	F_AF_NA_1
DESCRIPTION:	ACK File, ACK Section
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.

Information Object Address		
UI16		NOF – Name of file
UI8		NOS – Name of section
CP8		AFQ – ACK file or section qualifier

Valid cause of transmission codes

<13> File transfer

Notes

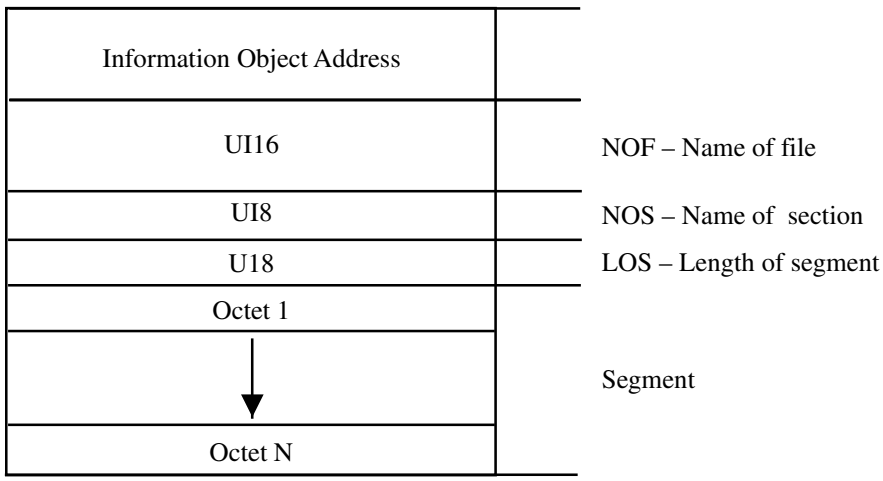
NOF – Name of file
NOS – Name of section
AFQ – ACK file or section qualifier

Type 125 Segment

INFORMATION OBJECT TYPE:	125
CODE:	F_SG_NA_1
DESCRIPTION:	Segment
VALID WITH SQ:	0

Information Object for SQ = 0 (Sequence of Information Objects)

Single information object only.



Valid cause of transmission codes

<13> File transfer

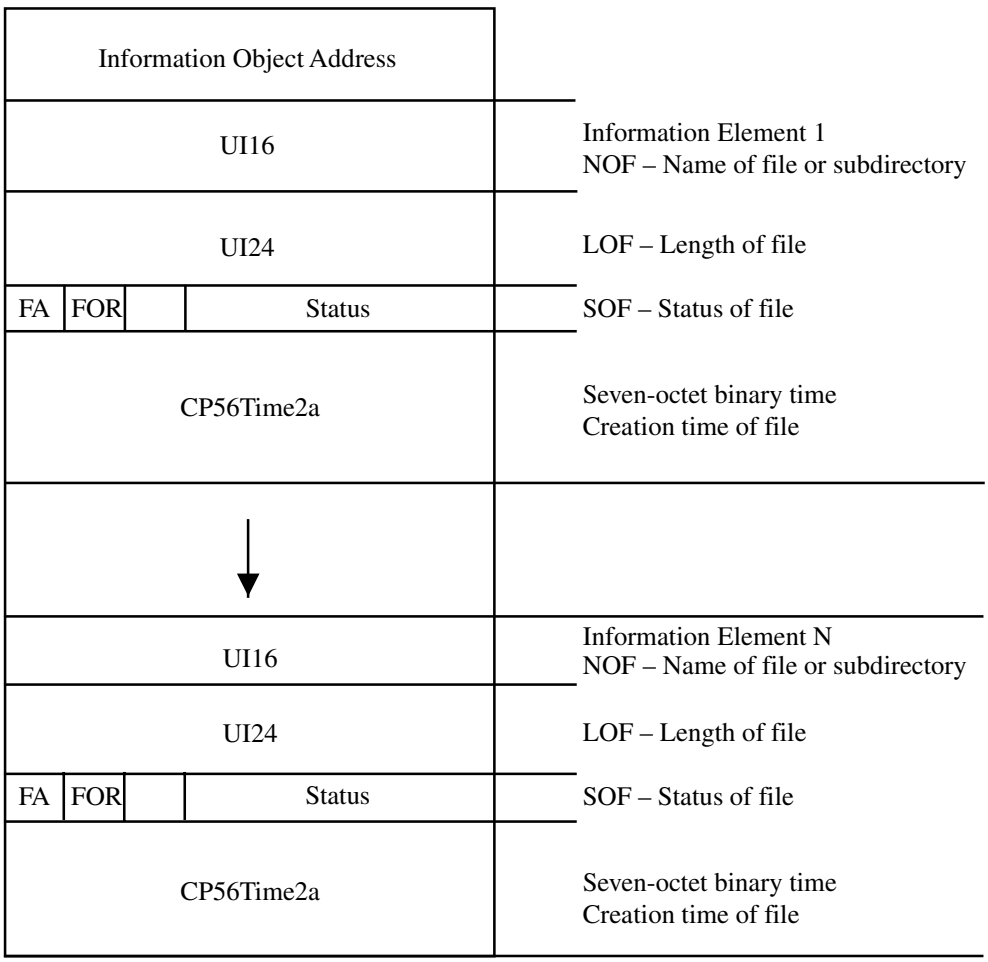
Notes

NOF – Name of file
NOS – Name of section
LOS – Length of segment

Type 126 Directory

INFORMATION OBJECT TYPE:	126
CODE:	F_DR_TA_1
DESCRIPTION:	Directory
VALID WITH SQ:	1

Information Object for SQ = 1 (Sequence of Information Elements)



Valid cause of transmission codes

<3>	Spontaneous
<5>	Requested

Notes

NOF – Name of file or subdirectory
LOF – Length of file
SOF – Status of file