Description and analysis of IEC 104 Protocol

Technical Report

Petr Matoušek

FACULTY OF INFORMATION TECHNOLOGY

Technical Report no. FIT-TR-2017-12

Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic

December , 2017

Abstract

IEC 60870-5-104 protocol (aka IEC 104) is a part of IEC Telecontrol Equipment and Systems Standard IEC 60870-5 that provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation. Telecontrol means transmitting supervisory data and data acquisition requests for controlling power transmission grids.

IEC 104 provides the network access to IEC 60870-5-101 (aka IEC 101) using standard transport profiles. In simple terms, it delivers IEC 101 messages as application data (L7) over TCP, port 2404. IEC 104 enables communication between control station and a substation via a standard TCP/IP network. The communication is based on the client-server model.

In this report we give a short overview of related standards and describe IEC 104 communication model. The main part of this report is description of the IEC 104 protocol, especially APCI and ASDU format. As other monitoring protocols, IEC 104 transmits ASDU containing information objects and information elements which build the basic part of IEC 104 monitoring. The report is a part of IRONSTONE[1] research project focused on security monitoring of IoT networks.

[1] IRONSTONE - IoT monitoring and forensics, Technological Agency of the Czech Republic, 2016-2019, no. TF03000029, see http://www.fit.vutbr.cz/~matousp/grants.php.en?id=1101.

Table of Contents

1 IEC 60870-5 Communication

1.1 Introduction to IEC 60870-5 standard

The International Electrotechnical Commission (IEC) defines IEC 60870 standards for telecontrol (supervisory control and data acquisition) in electrical engineering and power system automation applications. Part 5 provides a communication profile for sending basic telecontrol messages between a central telecontrol station and telecontrol outstations, which uses permanent directly connected data circuits between the central station and individual outstations.

IEC 60870-5 consists of the following parts, under the general title Telecontrol Equipment and Systems – Part 5: Transmission protocols:

- *IEC 60870-5-1 Transmission Frame Formats*
  - This describes the operation of the physical and data link layers. It provides a choice of four data link frame types FT1.1, FT1.2, FT2 and FT3 with fixed and variable length.
- *IEC 60870-5-2 Link Transmission Procedures*
  - It describes service primitives and transmission procedures: the unbalanced and balanced transmission. It also describes whether transmission can be initiated only by a master station, or by any station.
- *IEC 60870-5-3 General Structure of Application Data*
  - It specifies the general structure of data at the application level, rules for forming application data units, etc.
- *IEC 60870-5-4 Definition and Coding of Application Information Elements*
  - It provides the definition of information elements and defines a common set of information elements used in telecontrol applications. These include generic elements such as signed or unsigned integers, fixed or floating point numbers, bit-strings, and time elements.
- *IEC 60870-5-5 Basic Application Functions*
  - It describes the highest level functions of the transmission protocol that include station initialization, methods of acquiring data, clock synchronization, transmission of commands, totalizer counts, and file transfer.
- *IEC 60870-5-6 Guidelines for conformance testing for the IEC 60870-5 companion standards*

IEC also generated companion standards for basic telecontrol tasks, transmission of integrated totals, data exchange and network access:

- IEC TS 60870-5-7 Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)
- IEC 60870-5-101 (1995) Transmission Protocols - Companion standards for basic telecontrol tasks
- IEC 60870-5-102 (1996) Transmission Protocols - Companion standard for the transmission of integrated totals in electric power systems

- IEC 60870-5-103 (1997) Transmission Protocols - Companion standard for the informative interface of protection equipment
- IEC 60870-5-104 (2000) Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles
- IEC TS 60870-5-601 Transmission protocols - Conformance test cases for the IEC 60870-5-101 companion standard
- IEC TS 60870-5-604 Conformance test cases for the IEC 60870-5-104 companion standard

The IEC 60870-5 protocol stack is based on the reduced reference model called Enhanced Performance Architecture (EPA) that includes three layers of ISO OSI model: application layer (L7), link layer (L2), and physical layer (L1), see Table 1.

Enhanced Performance Architecture (EPA)	
Selected application functions of IEC 60870-5-5	User process
Selected application information elements of IEC 60870-5-4	Application Layer (L7)
Selected application service data units of IEC 60870-5-3	
Selected link transmission procedures of IEC 60870-5-2	Link Layer (L2)
Selected transmission frame formats of IEC 60870-5-1	
Selected ITU-T recommendations	Physical Layer (L1)

Table 1: EPA stack

- *Physical layer* defines the hardware-dependent specifications of the IEC 60870-5-101/IEC 60870-5-104 communication interfaces. It includes definition of communication interfaces (V.24/V.28 FSK, V.24/V.28 Modem, X.24/X.27 Synchronous), network configurations (point-to-point, multiple point-to-point, multi-point star, multi-point-party line, multi-point-ring).
- *Data link layer* specifies frame formats (FT1.2 with fixed or variable length), bit order of information (starting with the LSB and ending with the MSB), and transmission procedures (balanced or unbalanced mode, primary or secondary stations, SEND/NO REPLY, SEND/CONFIRM, REQUEST/RESPOND services, link initialization), see Section 1.2.
- *Application layer* defines the information elements for structuring application data and the communication service functions. It defines overall message structure, ASDU structure (see Section 2.2), message addressing and routing, information elements, and set of ASDUs.

1.2 Transmission

IEC 60870-5-101 provides a communication profile for sending basic telecontrol messages between a central telecontrol station (master, controlled station) and telecontrol outstations (slave, controlling station), which uses permanent directly connected data circuits between the central station and individual outstations, see Figure 1.

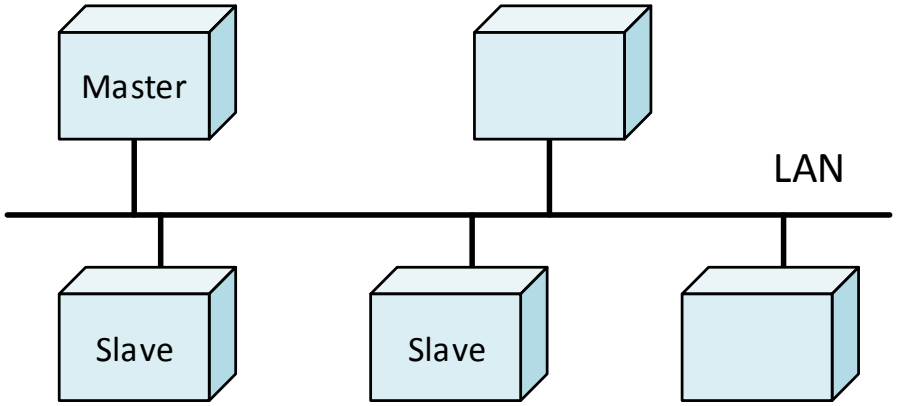


Figure 1: Network topology

The IEC 104 specification combines the application layer of IEC 60870-5-101 and the transport functions provided by a TCP/IP (Transmission Control Protocol/Internet Protocol).

IEC 101 allows two alternative transmission procedures [2]:

- *Unbalanced transmission* – the controlling station controls the data traffic by polling the controlled outstations sequentially. It initiates all the message transfers while the controlled outstations only respond to these messages. The following services are supported:
  - SEND/NO REPLY – for global messages and for cyclic set-point commands
  - SEND/CONFIRM – for control commands and set-point commands
  - REQUEST/RESPOND – for polling data from the controlled outstations
- *Balanced transmission* – in this mode, each station can initiate message transfer. The stations can act simultaneously as controlling stations and controlled stations (they are called combined stations). The balanced transmission is restricted to point-to-point and to multiple point-to-point configurations. Supported services are:
  - SEND/CONFIRM
  - SEND/NO REPLY – this can be initiated only by a controlling station with a broadcast address in a multiple point-to-point configuration

Figure 2 shows a topology of IEC 104 router connected with 104 SCADA monitoring systems using IEC 104 protocol over TCP/IP, and IEC 101 sensors communicating via Modbus RTU with the router.

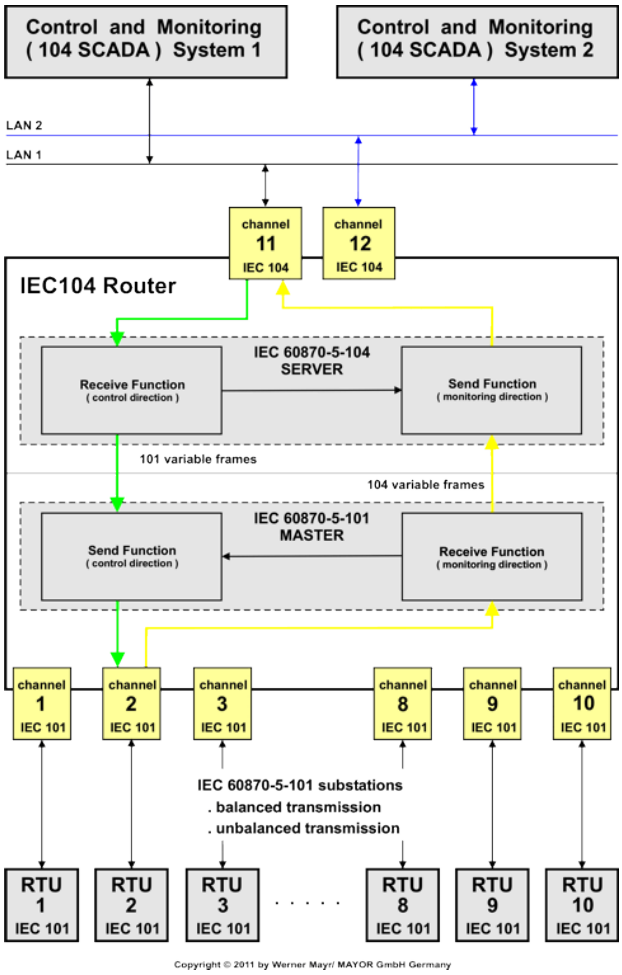


Figure 2: Network topology of SCADA monitoring system

1.3 Communication

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.

IEC 101/104 communication is exchanged between the controlled and the controlling station.

- *Controlled station* is monitored or commanded by a master station (RTU)
  - It is also called outstation, remote station, RTU, 101-Slave, or 104-Server.
- *Controlling station* is a station where a control of outstations is performed (SCADA)
  - Typically, it is a PC with SCADA system, can be also a RTU32.

IEC 101/104 defines several modes of direction:

- *Monitor Direction* is a direction of transmission from controlled station (RTU) to the controlling station (PC).
- *Control Direction* is a direction of transmission from controlling station, typical a SCADA system to the controlled station, typical an RTU.

- *Reversed Direction* is a direction when monitored station is sending commands and controlling station is sending data in monitor direction.

1.4 Application data objects

IEC 60870-5 has information on a set of information objects that are suited to both general SCADA applications, and electrical system applications in particular. Each different type of data has a unique type identification number (see Section 2.2 and Appendix C.1). Only one type of data is included in any one Application Service Data Unit (ASDU). The type is the first field in the ASDU. The information object types are grouped by direction (monitoring or control direction) and by the type of information (process info, system info, parameter, file transfer).

- An example of process information in monitoring direction is a measured value, e.g., a bit or an analog. In control direction it can be a command to set a bit or a value.
- An example of system information in monitoring direction is initiation flag, in the control direction it can be interrogation command, reset, etc.

Thus, application data is carried within the ASDU within one or more information objects. Depending on the variable structure flag (SQ, see Section 2.2) 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.

1.5 Addressing

IEC 101 defines addressing both at the link and at the application level. The link address (or device address) and ASDU address (or common address) are provided for identification of the end station:

- The *device address* is the identification number of the device.
    - The link address field may be 1 or 2 octets for unbalanced, and 0, 1 or 2 octets for balanced communication. As balanced communication are point-to-point the link address is redundant, but may be included for security.
    - The value range depends on the link address length that can be one byte, i.e., range 1 – 255, or two bytes, i.e. range 1 – 65 535. Typical values are 1 for IEC 101 and 2 for IEC 104.
    - The link address FF or FFFF is defined as a broadcast address, and may be used to address all stations at the link level.
- Each device on the communication network has a *Common Address of ASDU (COA or ASDU address)*. The common address of the ASDU combined with the information object address contained within the data itself combine to make the unique address for each data element.
    - COA is typically the application address of the client (logical station) that must match the address defined in the client configuration. This is defined as the address of the controlling station in the control direction.

- In the monitoring direction, however, the common address field contains the address of the station returning the data (controlled station). This is required so that the data can be uniquely identified and mapped to the right points in system data images.
- The maximum value depends on the ASDU address length that is one or two bytes similarly to the device address. Typical values are 1 for IEC 101 and 2 for IEC 104. The length of COA is fixed per system.

2 IEC 104 Protocol

IEC 60870-5-104 Protocol (aka IEC 104) is a standard for telecontrol equipment and systems with coded bit serial data transmission in TCP/IP based networks for monitoring and controlling geographically widespread processes. Protocol standard defines the transferred data entities in the station object as equal to the ones used in the IEC 60870-5-101 protocol. The implementation of the IEC 104 protocol uses the same as station objects (STA) as the IEC 101 implementation. IEC 104 is designated according to a selection of transport functions given in the TCP/IP Protocol Suite (RFC 2000). Within TCP/IP various network types can be utilized including X.25, Frame Relay, ATM, ISDN, Ethernet and serial point-to-point (X.21), see Figure 3.

<table>
<tr><th>Selected application functions</th><th>User process</th></tr>
<tr><td>Selection of Application Service Data Units (ASDU) of IEC 60870-5-101 and 104</td><td rowspan="2">Application Layer (L7)</td></tr>
<tr><td>Application Protocol Control Information (APCI)</td></tr>
<tr><td rowspan="4">Selection of TCP/IP Protocol Suite (RFC 2200)</td><td>Transport Layer (L4)</td></tr>
<tr><td>Network Layer (L3)</td></tr>
<tr><td>Link Layer (L2)</td></tr>
<tr><td>Physical Layer (L1)</td></tr>
</table>

Figure 3: Protocol stack with IEC 104

2.1 APCI format

Each APCI (Application Protocol Control Information) starts with a start byte with value 0x68 followed by the 8-bit length of APDU (Application Protocol Data Unit) and four 8-bit control fields (CF). APDU contains an APCI or an APCI with ASDU, see Figure 4. Generally, the length of APCI is 6 bytes.

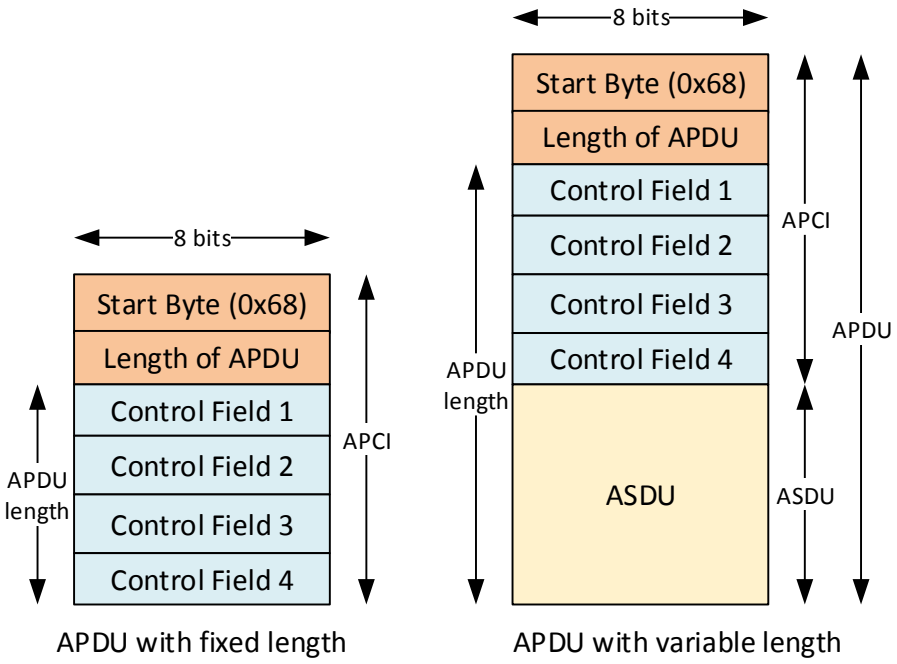


Figure 4: APCI frame format

There are packets with fixed length and with variable length containing Application Service Data Unit (ASDU, also called telegram) [4].

The frame format is determined by the two last bits of the first control field (CF1). The standard defines three frame formats, see Figure 5.

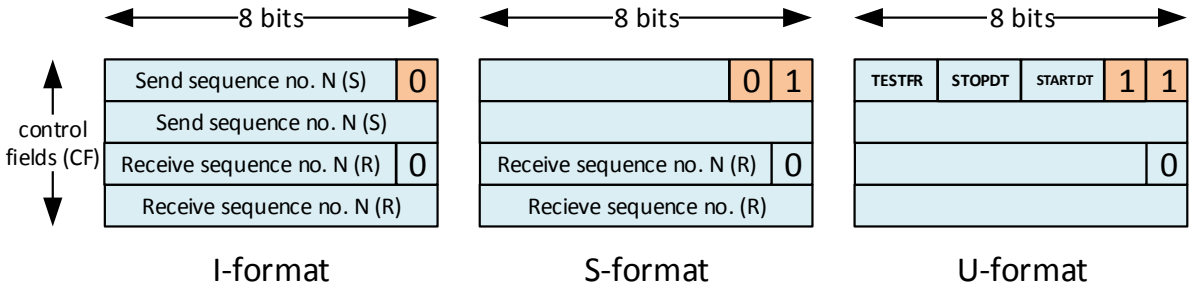


Figure 5: APCI frame types

- *I-format (information transfer format), last bit of CF1 is 0*
  - It is used to perform numbered information transfer between the controlling and the controlled station. It has variable length.
  - I-format APDUs contains always an ASDU.
  - Control fields of I-formats indicates message direction. It contains two 15-bit sequence numbers that are sequentially increased by one for each APDU and each direction.
    - The transmitter increased the Send Sequence Number N(S) and the receiver increases the Receive Sequence Number N(R). The receiver station acknowledges each APDU or a

number of APDUs when it returns the Receiver Sequence Number up to the number whose APDUs are properly received.
- The sending station holds the APDU or APDUs in a buffer until it receives back its own Send Sequence Number as a Receive Sequence Number which is valid acknowledge for all numbers less or equal to the received number.
- In case of a longer data transmission in one direction only, an S format has to be sent in the other direction to acknowledge the APDUs before buffer overflow or time out.
- The method should be used in both directions. After the establishment of a TCP connection, the send and receive sequence numbers are set to zero.
- The standard case studies of sequence number acknowledgement is shown in Appendix A.

- The right interpretation of sequence numbers depends on the position of LSB (Least Significant Bit) and MSB (Most Significant Bit), see Figure 6. Notice that the fixed bits (white background) on the most right position are not used for sequence numbers. Thus, sequence numbers of I-format have 15 bits only.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Send sequence no. N (S) *LSB*							0
MSB Send sequence no. N (S)							
Receive seq. no. N (R) *LSB*							0
MSB Receive sequence no. N (R)							

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

Figure 6: Interpretation of sequence numbers

For example, sequence 0x06 0x00 0x02 0x00 (see above, right table) will be interpreted as N(S) = 3 and N(R) = 1, e.g., the third APDU sent by the source and waiting for the first APDU from the destination.

- *S-format (numbered supervisory functions), last bits of CF1 are 01*
  - It is used to perform numbered supervisory functions. It has fixed length.
  - S-format APDUs always consist of one APCI only.
  - In any cases where the data transfer is only in a single direction, S-format APDUs have to be send in other direction before timeout, buffer overflow or when it has crossed maximum number of allowed I format APDUs without acknowledgement.

- *U-format (unnumbered control functions), last bits of CF2 are 11*
  - It is used to perform unnumbered control functions. It has fixed length.
  - U-format APDUs always consist of one APCI only. Only one of functions TESTFR (Test Frame), STOPDT (Stop Data Transfer) or STARTDT (Start Data Transfer) can be activated at the same time. The binary values of CF1 are in Figure 7.

U-Frame Function	7	6	5	4	3	2	1	0	Hexa Value
Test Frame Activation	0	1	0	0	0	0	1	1	0x43
Test Frame Confirmation	1	0	0	0	0	0	1	1	0x83
Stop Data Transfer Activation	0	0	0	1	0	0	1	1	0x13
Stop Data Transfer Confirmation	0	0	1	0	0	0	1	1	0x23
Start Data Transfer Activation	0	0	0	0	0	1	1	1	0x07
Stop Data Transfer Confirmation	0	0	0	0	1	0	1	1	0x0B

Figure 7: U-Frame functions and their codes

- U-format is used for activation and confirmation mechanism of STARTDT, STOPDT and TESTFR.
- STARTDT and STOPDT are used by the controlling station to control the data transfer from a controlled station.
  - When the connection is established, user data transfer is not automatically enabled, e.g., default state is STOPDT. In this state, the controlled station does not send any data via this connection, except unnumbered control functions and confirmations. The controlling station must activate the user data transfer by sending a *STARTDT act* (activate). The controlled station responds with a *STARTDT con* (confirm). If the STARTD is not confirmed, the connection is closed by the controlling station.
  - Only the controlling station sends the STARTDT. The expected mode of operation is that the STARTDT is sent only once after the initial establishment of the connection. The connection then operates with both controlled and controlling station permitted to send any message at any time until the controlling station decides to close the connection with a STOPDT command.
  - Example of start and stop data transfer procedures is shown in Appendix B.

- The controlling and/or controlled station must regularly check the status of all established connections to detect any communication problems as soon as possible. This is done by sending TESTFR frames.
  - Open connections may be periodically tested in both directions by sending test APDUs (TESTFR=act) which are confirmed by the receiving station sending TESTFR=con.
  - Both stations may initiate the test procedure after a specific period of time in which no data transfer occur (time out).

2.2 ASDU format

The ASDU contains two main sections: the data unit identifier (with the fixed length of six bytes), 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 includes additional information as cause of transmission. Each ASDU can transmit maximum 127 objects. The format of ASDU is in Fig. 8.

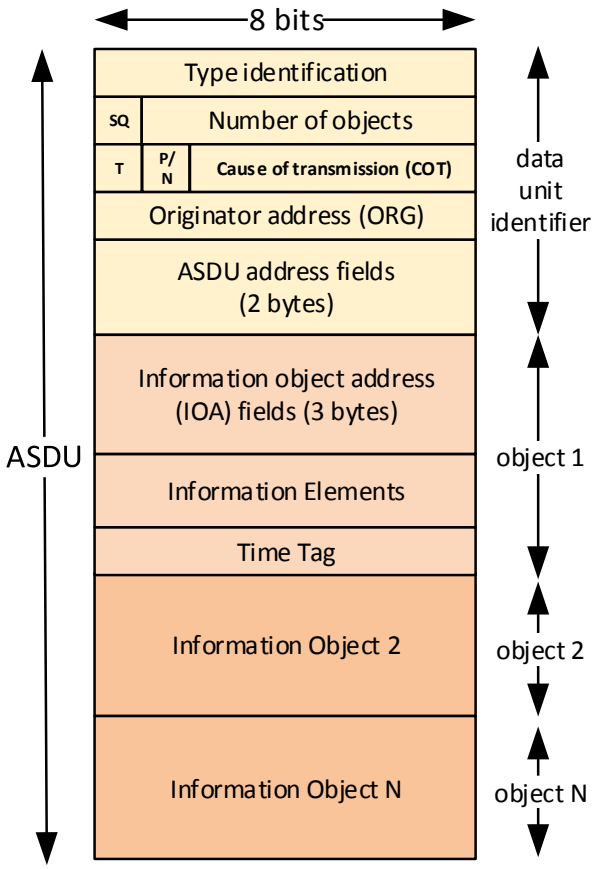


Figure 8: ASDU Format

ASDU[2] contains the following fields:

- *Type identification (TypeID, 1 byte)*
  - 0 is not used, 1-127 is used for standard IEC 101 definitions, 128-135 is reserved for message routing and 136-255 for special use.
  - In the range of standard IEC 101 definitions, there are presently 58 specific types defined. These types form following groups, see Table 2.

Type ID	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 2: Defined type code groups

[2] Fields and values of ASDU dissector in Wireshark are described in https://www.wireshark.org/docs/dfref/1/104asdu.html (last access in June 2017).

- 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.
- The standard values of TypeID are listed in Appendix C.1.

- *SQ (Structure Qualifier)* bit specifies how information objects or elements are addressed.
  - SQ=0 (sequence of information objects): addressing of individual single information elements or combination of information elements in a number of information objects (IO) of the same type, see Figure 8.
    - Each single element or a combination of elements is addressed by the information object address. The ASDU may consist of one or more than one equal information object. The number of objects is binary coded (number of objects) and defines the number of the information objects.
    - SQ=0 implies a *sequence of information objects* where each object has its own information object address. The number of information objects is given by the seven-bit value in the date unit identifier (field number of objects, see Figure 7). Therefore there can be up to 127 information objects in this ASDU. [7]
  - SQ=1 (just one information object): addressing of a sequence of single information elements or equal combinations of information elements of *a single object per ASDU*, see Figure 9.
    - A sequence of equal information objects (e.g. measured values of identical format) is addressed by the information object address. The information object address specifies the associated address of the first information element of the sequence. The following information elements are identified by numbers continuously by + 1 from this offset. The number of objects is binary coded (number of elements) and defines the number of the information elements. In case of a sequence of information elements only one information object per ASDU is allocated.
    - When SQ=1, the structure contains a *sequence information elements within one information object*. All information objects are of the same format, such as a measured value. There is just one information object address, which is the address of the first information element.

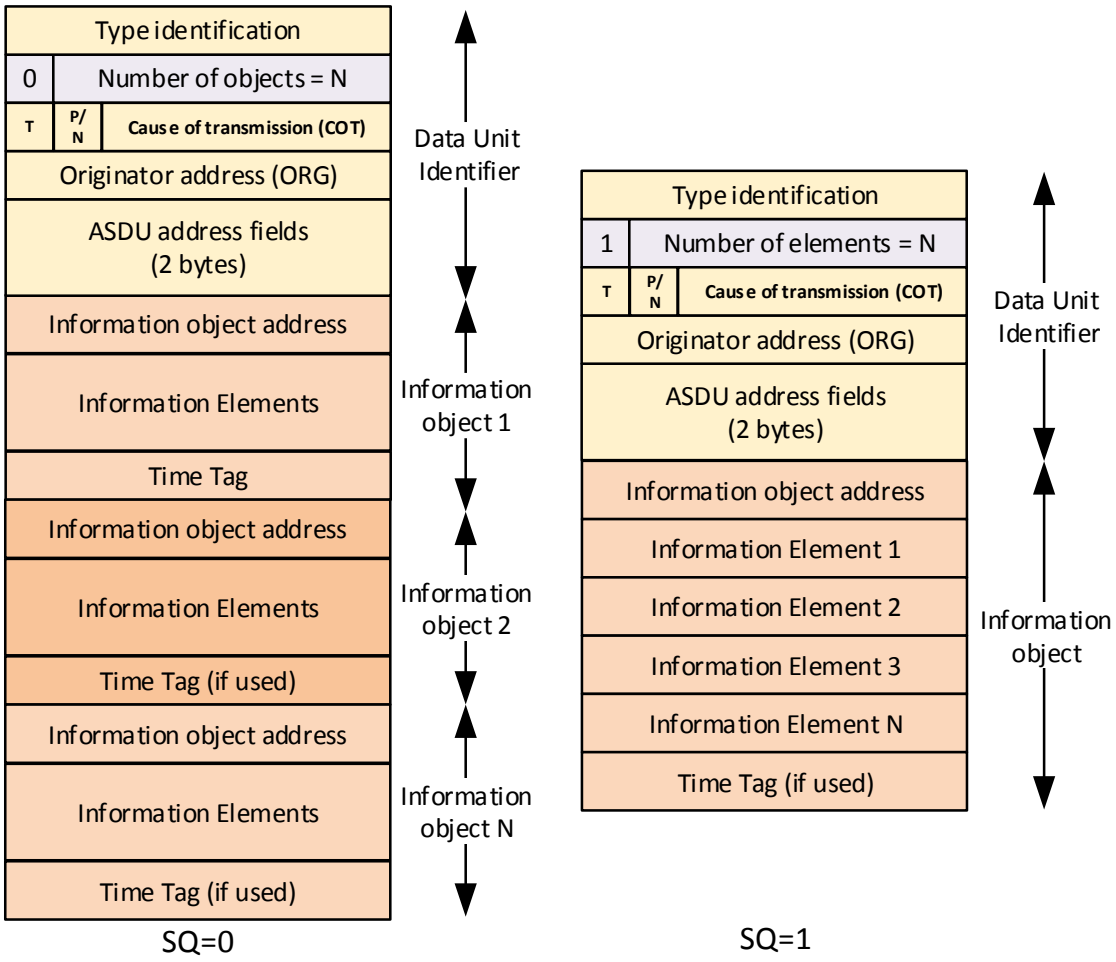


Figure 9: The structure of ASDU with SQ=0 and SQ=1

- *Number of objects/elements*
  - Uses range 0 – 127
  - 0 means ASDU contains no information object (IO)
  - 1-127 defines no. of information objects or elements

- *T (test) bit* defines ASDUs which were generated during test conditions and not intended to control the process or change the system state.
  - T=0 (no test), T=1 (test)

- *P/N (positive/negative) bit* indicates the positive or negative confirmation of an activation requested by a primary application function.
  - P/N = 0 (positive confirm), P/N = 1 (negative confirm).
  - P/N is meaningful when used with control commands. The 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 set to zero.

- *Cause of transmission (COT)*
  - COT field is used to control the routing of messages both on the communication network, and within a station, directing by ASDU to the correct program or task for processing. ASDUs in control direction are confirmed application services and may be mirrored in monitor direction with different causes of transmission.
  - COT is a six-bit code which is used in interpreting the information at the destination station. Each defined ASDU type (see Appendix C.1, valid COTs) has a defined subset of the codes which are meaningful with it.
  - 0 is not defined, 1-47 is used for standard definitions of this companion standard (compatible range), see Appendix C.2, 48-63 is for special use (private range).

- *Originator Address (ORG)*
  - 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. In this case the originator address can be used to direct command confirmations back to the particular controlling station rather than to the whole system.
  - The originator address directs mirrored ASDUs and interrogated ASDUs in monitor direction (e.g. interrogated by a general interrogation) to the source that activated the procedure.
  - If the originator address is not used (bits are set to zero) and there is more than one single source in a system defined, the ASDUs in monitor direction have to be directed to all relevant sources of the system. In this case the specific affected source has to select its specific ASDUs.

- *ASDU Address Field (Common Address of ASDU, COA),* see also Section 1.5
  - The address is called common address because it is associated with all objects 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.
  - COA is either one or two octets in length, fixed on a per-system basis.
  - The global address is a broadcast address directed to all stations of a specific system (broadcast address). ASDUs with a broadcast address in control direction have to be answered in monitor direction by the address that is the specific defined common address (station address). According to the standard this parameter consists of 2 octets.
  - Value 0 is not used, range 1 – 65 534 means a station address, value 65 535 (0xFFFF) means global address.
  - Global address is used when the same application function must be initiated simultaneously. It is restricted to the following ASDUs:
    - Type=100 (Interrogation command): reply with particular system data snapshot at common time

- Type=101 (counter interrogation command): freeze totals at common time
- Type=103 (clock synchronization command): synchronize clocks to common time
- Type=105 (reset process command): simultaneous reset

2.2.1 Information Objects

ASDU transmits information objects within its structure. Each information object is addressed by *Information Object Address (IOA)* which identifies the particular data within a defined station. Its length is 3 bytes for IEC 104. The address is used as destination address in control direction and as source address in monitor direction.

- The third byte of IOA is only used in case of structuring the information object address in order to define unambiguous addresses within a specific system. In all cases the maximum number of different object addresses is limited to 65 535 (as for two bytes).
- If the information object address is not relevant (not used) in some ASDUs, it is set to zero.

All information objects transmitted by one ASDU must have the same ASDU type (e.g., 5, step position information, see Appendix C.1). If there are more objects of different types to be transmitted, they are inserted in several ASDUs.

For each defined ASDU type, the IEC 104 standard defines the format of the information object, i.e., what information elements form such object and how they are structured.

- Figure 10 shows an example of information object Single-point information without time (ASDU type=1). The object format has two forms: one for SQ=0 and one for SQ=1. Valid COT for this objects are: 2 (background scan), 3 (spontaneous), 5 (requested), 11, 12 (feedback), 20 +G (interrogated by station interrogation), see Appendix C.1.

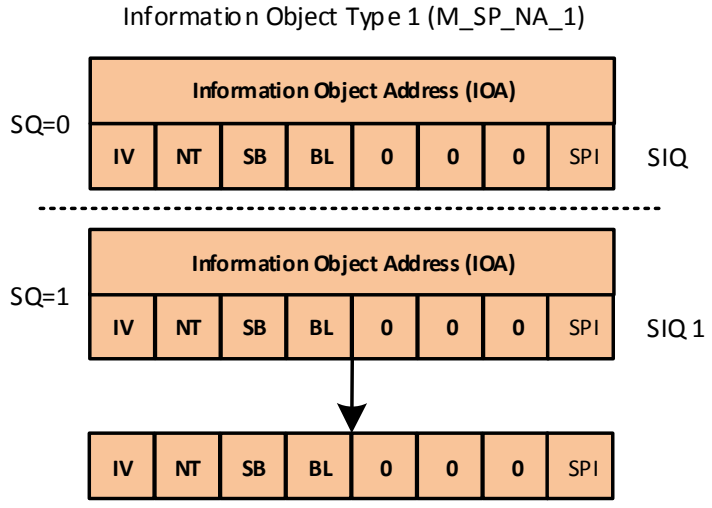


Figure 10: Example of information object Single-point information without time (type=1)

- Some information objects contain several information elements. For example, Figure 11 shows information object of type 10 (measured value, normalized with time tag). This object is defined only for SQ=0 and contains three information elements: normalized value NVA (2 bytes), quality descriptor (1 byte), and binary timestamp (3 bytes). For this type of object, valid causes of transmission are spontaneous (code 3) or requested (code 5, see Appendix C.2).

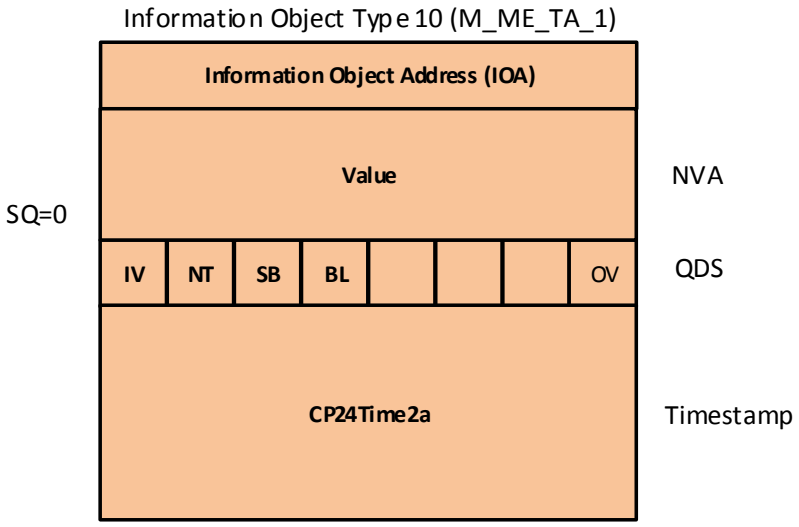


Figure 11: Example of information object Measured normalized value with the timestamp (type=10)

The number of information objects and information elements within the ASDU is the *Number of objects* given in the second byte of ASDU header (see also above).

2.2.2 Information Elements

Information elements are building blocks used to transmit information. Format and length of each information element differs and is given by the standard. The standard also describes how encoded values are interpreted.

A list of available information elements is given in Appendix C.3. The list also gives the length of the element and object types where it is used.

- The interpretation of values transmitted by an information element is also given by the standard and can be found in [7]. Figure 11 shows a format of three information elements: SIQ (single point of information), VTI (value with transient state indication) and SVA (scaled value). SIQ contains a set quality bits (see interpretation in Appendix C.4), VTI contains a seven-bit value from the range <-64..+63>. SVA contains a 16-bit value in the range <-32 768..32 767> which represents a fixed decimal point number. However, the position of the decimal point is not transmitted by the value but it is 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.

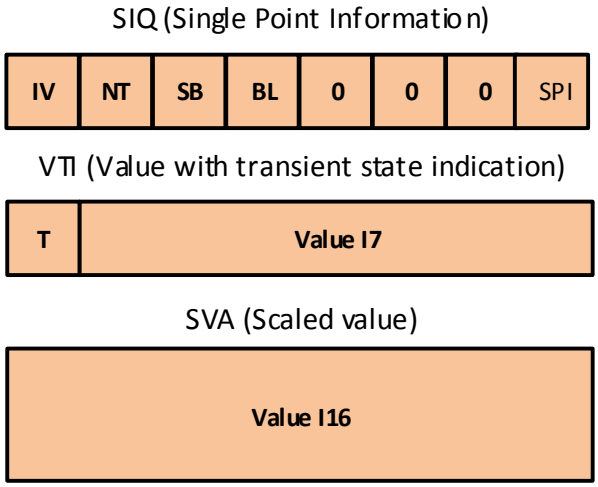


Figure 11: Example of three information elements: SIQ, VTI and SVA

For SQ=1, the number of information elements within the information object is given in the *Number of objects* field of the ASDU header. The structure of the information object contains:

- *Information object address* (3 bytes)
- *A set of information elements of the same type*
  - The number of the elements is given in the ASDU header.
  - The format of the element is given by the standard and depends on the ASDU type.
  - The length of information object can be computed using APDU length, e.g., information *object_length* (bytes) = *APDU_length – ADPU_control_fields* (4 bytes) – *ASDU_header* (6 bytes) – *IOA* (3 bytes) = *APDU_length* – 13 bytes.
  - The length of each information element within this object is given by *object_length / number_of_objects*.
- Please, remind that each of the elements belongs to one information objects which IOA is given by offset from the IOA in the ASDU, e.g., +1 for the second element, +2 for the third element, etc.

For SQ=0, the number of information objects is given in the *Number of objects* field of the ASDU header. The format of the object, e.g., from which elements the object is built, is fixed by the standard. The structure of ASDU data part is following:

- *Information object address of object no.1* (3 bytes)
- *A set of information elements of object no. 1*
- *Information object address of object no.2* (3 bytes)
- *A set of information elements of object no. 2*
- …
- *Information object address of object no.N* (3 bytes)
- *A set of information elements of object no. N*
  - The number of the objects is given in the ASDU header.
  - All of the objects are of the same type and thus have the same length.

- The length of the information object can be computed as follows: *object_length* (bytes) = (*APDU_length* – *ADPU_control_fields* (4 bytes) – *ASDU_header* (6 bytes)) / *number_of_objects* – *IOA* (3 bytes) = (*APDU_length* – 10 bytes) / *number_of_objects* – 3 bytes

2.3 IEC 104 Analysis

IEC 104 examples in this part are taken from [5].

Sample 1:

- 68 0E 4E 14 7C 00 65 01 0A 00 0C 00 00 00 00 05

LPDU bytes	Explanation
68	Start byte
0E	Length of the APDU = 14 bytes
4E	Send sequence number N(S) LSB, bit 0 = 0 => I-Format
14	Send sequence number N(S) MSB
7C	Receive sequence number N(R) LSB
0	Receive sequence number N(R) MSB
65	Type identification: C_CI_NA_1 (counter interrogation command)
1	Number of objects = 1
0A	Cause of transmission = 10 (activation termination)
0	Originator address = 0
0C 00	Common ASDU address (2 octets) = 12 dec.
00 00 00	Object address (3 octets)
5	Counter interrogation request qualifier = 5 (general counter interrogation)

Sample 2:

- 68 34 5A 14 7C 00 0B 07 03 00 0C 00 10 30 00 BE 09 00 11 30 00 90 09 00 0E 30 00 75 00 00 28 30 00 25 09 00 29 30 00 75 00 00 0F 30 00 0F 0A 00 2E 30 00 AE 05 00

LPDU bytes	Explanation
68	Start byte
34	Length of the APDU = 52 bytes
5A	Send sequence number N(S) LSB, bit 0 = 0 => I-Format
14	Send sequence number N(S) MSB
7C	Receive sequence number N(R) LSB
0	Receive sequence number N(R) MSB
0B	Type identification: M_ME_NB_1(measured value, scaled value)
7	Number of objects = 7
3	Cause of transmission = 3 (spontanous)
0	Originator address = 0
0C 00	Common ASDU address (2 octets) = 12 dec.
10 30 00	Object address (3 octets) of **first** information object
BE 09 00	Scaled value + QDS (quality descriptor) of **first** information object
11 30 00	Object address (3 octets) of **second** information object
90 09 00	Scaled value + QDS (quality descriptor) of **second** information object
0E 30 00	Object address (3 octets) of **third** information object
75 00 00	Scaled value + QDS (quality descriptor) of **third** information object
28 30 00 25 09 00	Object address + Scaled value + QDS (quality descriptor) of information object four to seven
29 30 00 75 00 00	
0F 30 00 0F 0A 00	
2E 30 00 AE 05 00	

Sample 3:

- 68 04 01 00 7E 14

LPDU bytes	Explanation
68	Start byte
4	Length of the APDU = 4
1	bits 2..7 reserved, bit 0 = 1 and bit 1 = 0 => S-Format
0	reserved
7E	Receive sequence number N(R) LSB
14	Receive sequence number N(R) MSB

2.4 Basic application functions

Following application functions are implemented in IEC 101 communication [2]:

- *Data acquisition* – collecting data cyclically, upon change, or upon request
  - In unbalanced transmission, the controlled outstation must always wait for a request from the controlling station.
  - When balanced transmission is used, the buffered data is transmitted by the controlled outstation to the controlling station without a delay.
- *Even acquisition*
  - Events occur spontaneously at the application level of the controlled outstation. The transmission in balanced or unbalanced mode is similar to the data acquisition.
- *Interrogation* – used for updated the controlling station after an internal initialization
  - The controlling station requests the controlled outstations to transmit the actual values of all their process variables.
- *Clock synchronization*
  - After system initialization, the clocks are initially synchronized by the controlling station. After, the clocks are periodically resynchronized by transmission of a clock synchronization command.
- *Command transmission* – used to change the state of operational equipment.
  - A command may be initiated by an operator or by automatic supervisory procedures in the controlling station.
  - Two standard procedures for command transmission:
    - *Direct command* – used by the controlling station to immediately control operations in the controlled outstations. Permission and validity of the command is checked by the outstation
    - *Select and execute command* – a two-step command that prepares a specified control operation in a control outstation, checks that the correct control operation is prepared, and execute the command. The preparation is checked by an operator or by an application procedure. The controlled outstation does not start the control operation until it has received the correct execute indication.
- *Transmission of integrated totals*
  - Transmits values that are integrated over a specific time period using two methods:
    - *Freeze-and-Read*: acquisition of integrated totals
    - *Clear-and-Read*: acquisition of incremental information
- *Changes in protocol and link parameters* – when the link parameters are changed
- *Acquisition of transmission delay* – needed for time correction

2.5 Transactional view on IEC 104 communication

For security monitoring, it is better to group individual IEC 104 packets into transactions. Considering master-slave transactions we can divide the communication on transactions as depicted in the following table:

Master (10.20.102.1) < --- > Slave (10.20.100.108) communication				
No.	**Direction**	**object**	**Cause of transmission (COT)**	**Setting values of the information element**
1	**---->**	IOA=0	activation	interrogation command
	<----	IOA=0	activation confirmation	interrogation command
	<----	IOA=0	interrogation command	
		IOA=1-4	interrogation command	SIQ=0, DIQ=0
	<----	IOA=1-4	interrogation command	step position = 0
		IOA=1-4	interrogation command	bitstring = 0
		IOA=1-4	interrogation command	normalized value = 0
		IOA=1-4	interrogation command	scaled value = 0
		IOA=1-4	interrogation command	short float = 0
		IOA=11-14	interrogation command	SIQ=0, DIQ=0 with time tag
		IOA=11-14	interrogation command	step position = 0 with time tag
		IOA=11-14	interrogation command	bitstring = 0 with time tag
	<----	IOA=11-14	interrogation command	normalized value = 0 with time tag
		IOA=11-14	interrogation command	scaled value = 0 with time tag
		IOA=11-14	interrogation command	short float = 0 with time tag
		IOA=0	activation termination	interrogation command
		IOA=0	activation confirmation	interrogation command
		IOA=1-4	interrogation command	SIQ=0, DIQ=0
		IOA=1-4	interrogation command	step position = 0
		IOA=1-4	interrogation command	bitstring = 0
		IOA=1-4	interrogation command	normalized value = 0
		IOA=1-4	interrogation command	scaled value = 0
		IOA=1-4	interrogation command	short float = 0
	<----	IOA=11-14	interrogation command	SIQ=0, DIQ=0 with time tag
		IOA=11-14	interrogation command	step position = 0 with time tag
		IOA=11-14	interrogation command	bitstring = 0 with time tag
		IOA=11-14	interrogation command	normalized value = 0 with time tag
		IOA=11-14	interrogation command	scaled value = 0 with time tag
		IOA=11-14	interrogation command	short float = 0 with time tag
		IOA=0	activation termination	interrogation command
2	**---->**	IOA=13	activation	single command ON
	<----	IOA=13	activation confirmation	single command ON
		IOA=13	activation termination	single command ON

		IOA=13	spontaneous	SIQ=0x01 (SPI=ON) with time tag
3	**---->**	IOA=2	activation	single command ON
	<----	IOA=2	activation confirmation	single command ON
		IOA=2	activation termination	single command ON
		IOA=2	spontaneous	SIQ=0x01 (SPI=ON)
4	**---->**	IOA=1	activation	double command ON
	<----	IOA=1	activation confirmation	double command ON
	<----	IOA=1	activation termination	double command ON
		IOA=1	spontaneous	DIQ=0x01 (DPI=OFF)
5	**---->**	IOA=14	activation	double command ON
	<----	IOA=14	activation confirmation	double command ON
		IOA=14	activation termination	double command ON
		IOA=14	spontaneous	DIQ=0x02 (DPI=ON) with time tag
6	**---->**	IOA=1	activation	regulating step cmd: UP
	<----	IOA=1	activation confirmation	regulating step cmd: UP
		IOA=1	activation termination	regulating step cmd: UP
		IOA=1	spontaneous	step position = 1
	<----	IOA=12	activation confirmation	regulating step cmd: DOWN
		IOA=12	activation termination	regulating step cmd: DOWN
		IOA=12	spontaneous	step position = -1 with time tag

The table shows logical transactions exchanged between the master and slave. Arrow represents direction: master to slave (--->) or slave to master (<---). A transaction usually concerns one information object with its address (IOA). Only exception is transaction no. 1 which summarizes initialization of the system. Following transactions are initiated by the master station that sends activation command (COT=6) which is responded by the slave station using a sequence of messages with COT=7 (activation confirmation), COT=10 (activation termination) and COT=3 (spontaneous).

In the table, we can noticed some specific features of IEC 104 communication:

- Destination is addressed on L7 by common ASDU address (COA) which is 10 in this case (address of the slave station). Then, each destination contains several objects addressed by the information object address (IOA). Usually, the controlling station sends or retrieves data from the specific information object identified by its IOA.
- Special destination address 0 does not refer to a specific information object but to the configuration of the whole slave system. Thus, initialization of the slave is addressed using IOA=0.
- The transaction 1 sends an activation message with the interrogation command which enforces a sequence of interrogation answers from object 1-4 and 11-14 transmitting the actual settings of their values.
- We can notice that one object with a given IOA can contain several types of information elements. E.g., object 1 has elements of type SIQ, DIG, step position, bitstring, normalized value, scaled value, or short floating point.

- Some responses can be divided into several TCP packets, e.g., the response on transaction no. 4 is sent in two packets: one contains ActCon ASDU, the other ActTerm ASDU and Spon ASDU. This is different to transaction no. 3, where the response is sent via one TCP packet that contains three ASDUs: ActCon, ActTerm and Spon.
- Some objects (e.g., 11-14) returns values with timestamp, others (1-4) do not use them.
- One TCP packet can transmit a sequence of ASDUs of several objects. E.g, the third response from slave in the transaction 1 transmits ASDUs with objects IOA=1-4 and IOA=11-14.
- We can also see that some ASDUs contain one information element and some a sequence of information elements. This number is specified in the Number of Objects field in the ASDU header.

2.6 Observation of IEC 104 communication

After detailed analysis of the several PCAP sample of IEC 104 communication, we can make the following observations:

1) One TCP stream transmits several types of IEC format frames: U-frames, S-frames, I-frames. These frames have different format and usage for IEC communication. From point of view of network monitoring, it can be useful to keep statistics that include no. of packets, bytes, etc. for each of the frame formats.
2) It is better to monitor transactions related to objects than individual packets. Each informational object is addressed by an IP address of the controlled station (on L3), by a controlled station address on L7 (common ASDU address, COA), and an object address (IOA). Thus, the transaction can be identified using a target address (COA+IOA) and action (COT, cause of transmission). Each transaction gets values or sets values of information elements that are part of the referred object. The standard defines which object type contains what kind of information elements.
3) Transactions are build by exchanges of ASDU messages between the slave and the controlling station. There is no transaction ID, thus slave and master have to check transactions based on COA, COT and OUI. If a message is lost, the loss is detected by L7 via ASDU sequence numbers and re-sent.
4) One ASDU can transmits several objects, however, these objects must have the same COT.
5) One TCP packet can contain several ASDUs with same or different COTs.

3 IEC 104 Security Monitoring

This part discusses how flow monitoring approached can be applied on IEC 104 communication.

3.1 Security issues of IEC 104

When analyzing IEC 104, we can notice several similarities with SNMP monitoring. SNMP manager sends short commands to SNMP agent in order to set variables or retrieve their values. The same is IEC 104 master station. Unlike SNMP, IEC 104 does not define any security as access passwords (via community string in SNMPv1 and SNMPv2), authentication (using RSA) or encryption (using SHA) as supported by SNMPv3.

This forms a serious vulnerability against IEC 104 communication, especially when transmitted over unsecure IP layer. Possible attacks on IEC 104 communication may include:

- changing the value of an ASDU transmitted in the IEC 104 packet,
- inserting spoofed ASDU messages into the network,
- providing DDoS attacks on IEC 104 master or slave stations,
- inserting a rogue control station into the network,
- interception of the transmitted data,
- etc.

These vulnerabilities and possible attacks are also discussed in [8] and [9]. We can mitigate possibility of these threats by hardening the access to IEC 104 communication which is sometimes not feasible, or we can provide security monitoring with anomaly detection. This can be implemented using Netflow monitoring.

3.2 Recommended monitoring approach

In case of flow monitoring, IEC communication is composed of one IP flow transmitting values and action related to a range of different objects. Such a large set of useful data can be hardly incorporated in IP flow records. One solution is to look at IEC communication via transactions described above rather than classical IP flows. This can be implemented by creating several virtual flows out of one IP flow with IEC 104 PDUs.

Then, the monitoring can be similar to other request-response communication, for example DNS. DNS communication sends requests over UDP. A DNS client queries the DNS server which sends a response in one packet.

IEC 104 has similar behavior: IEC 104 transactions are directed to an information object at the controlled station using ASDUs. IEC 104 communicates in control mode (master to slave) or monitoring mode (slave to master). Each transaction has its type (COT, cause of transmission); this can be parallel to the type of DNS request (A, PTR, etc.). A requested object identified by IOA can be compared with the requested DNS query (like www.fit.vutbr.cz).

As flow analysis of DNS combines DNS requests and responses based on the transaction ID, IEC 104 monitoring can combine IEC 104 transactions identified by a sequence of COA, COT and IOA. For each transaction, we can monitor metadata (e.g., no. of transmitted ASDUs, packets, bytes), or direct values of information elements transmitted in ASDUs.

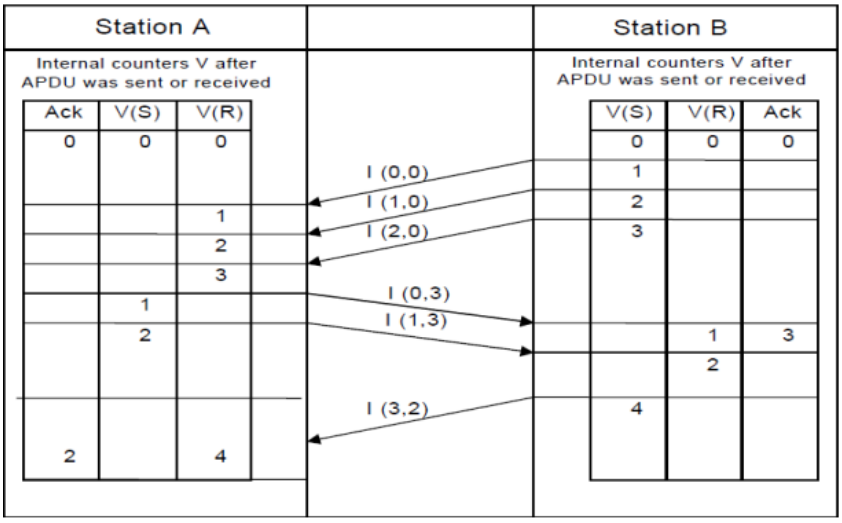
The implementation will be part of the further phase of the IRONSTONE project.

References

1. IEC 60870-5-104:2006(E): *Network access for IEC 60870-5-101 using standard transport profiles*, IEC, 2006.
2. ABB: RER620. IEC 60870-5-101/104 Communication Protocol Manual. 2010. Retrieved from https://library.e.abb.com/public/7801b90da654ce61c125795d003c7b26/RER620_ANSI_IEC101-104prot_306892_ENb.pdf in June 2017.
3. ABB: MicroSCADA Pro. IEC 60870-5-104 Master Protocol. 2006. Retrieved from https://library.e.abb.com/public/5fd0e08edecd7651c1257ab80041c671/SYS600_IEC%2060870-5-104%20Slave%20Protocol_756654_ENb.pdf in June 2017.
4. Werner Mayer: Manual LIAN 98. IEC 60870-5-104: Telegram structure, 2011. Retrieved from http://www.mayor.de/lian98/doc.en/html/u_iec104_struct.htm in June 2017.
5. Backhoff Information System: IEC 60870-5-104 telegram structure. Retrieved from https://infosys.beckhoff.com/english.php?content=../content/1033/tcplclibiec870_5_104/html/tcplclibiec870_5_104_telegrammstructure.htm&id= in June 2017.
6. Kamjoo Bayat: SCADA Protocols Introduction. Retrieved from http://www.pbscontrol.com/pdf/SCADAProtocols.pdf in June 2017.
7. G. Clarke, D. Reynders, E. Wright: *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*, Elsevier, 2004.
8. Y. Yang, K. McLaughlin, S. Sezer, Y.B. Yuan, W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security", PES General Meeting | Conference & Exposition 2014 IEEE, pp. 1-5, 2014.
9. Peter Maynard, Kieran McLaughlin, and Berthold Haberler. 2014. Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. In *Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014* (ICS-CSR 2014). BCS, , UK, 30-42. DOI: https://doi.org/10.14236/ewic/ics-csr2014.5

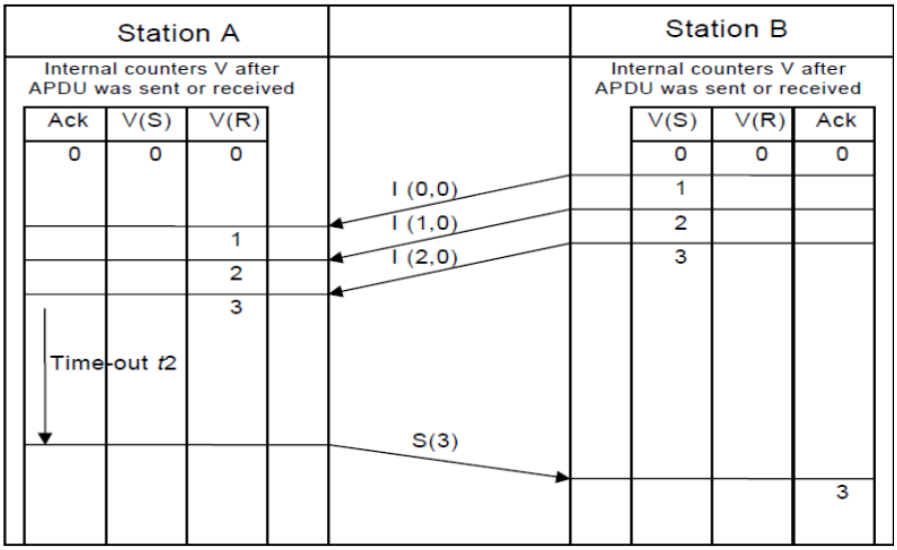
Appendix A: APDU Sequence Numbers

1. Undisturbed sequences of numbered I format APDUs

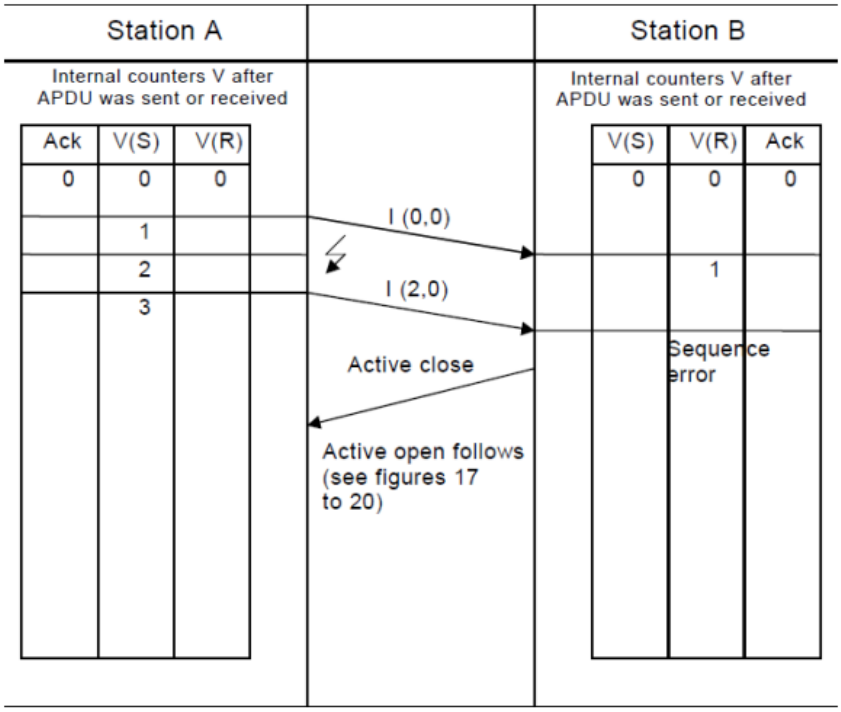


V(S) = Send state variable (see ITU-T X.25);
V(R) = Receive state variable (see ITU-T X.25);
Ack = Indicates that the DTE has received correctly all I format APDUs numbered up to and including this number;
I(a,b) = Information format APDU with a = send sequence number and b = receive sequence number;
S(b) = Supervisory format APDU with b = receive sequence number;
U = Unnumbered control function APDU.

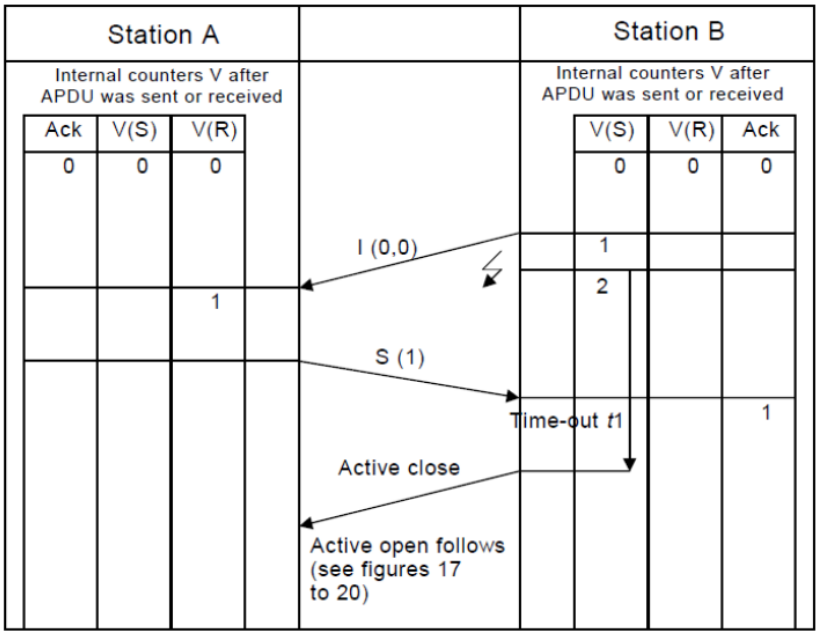
2. Undisturbed sequences of numbered I format APDUs acknowledged by an S format APDU



3. Disturbed sequence of numbered I format APDUs

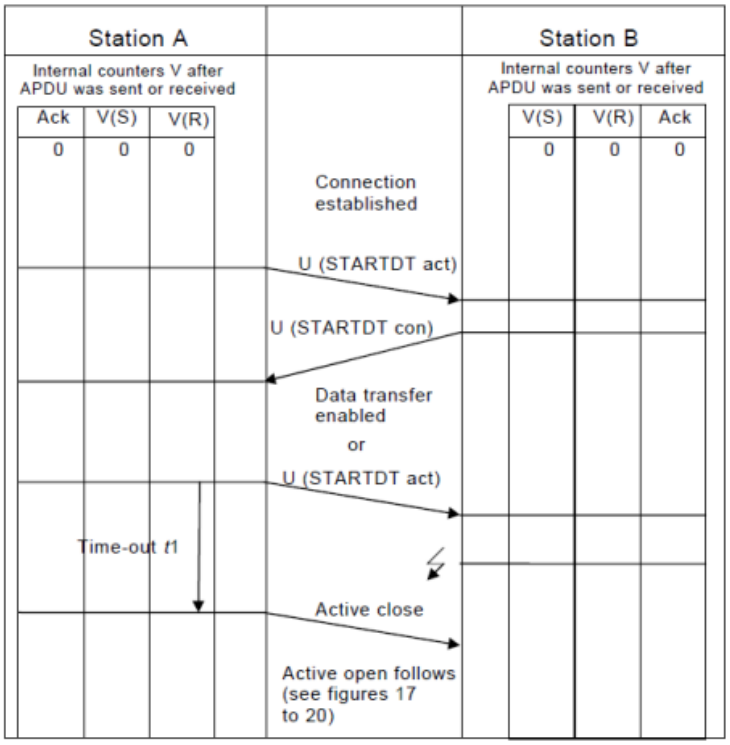


4. Time-out in case of a not acknowledged last I format APDU

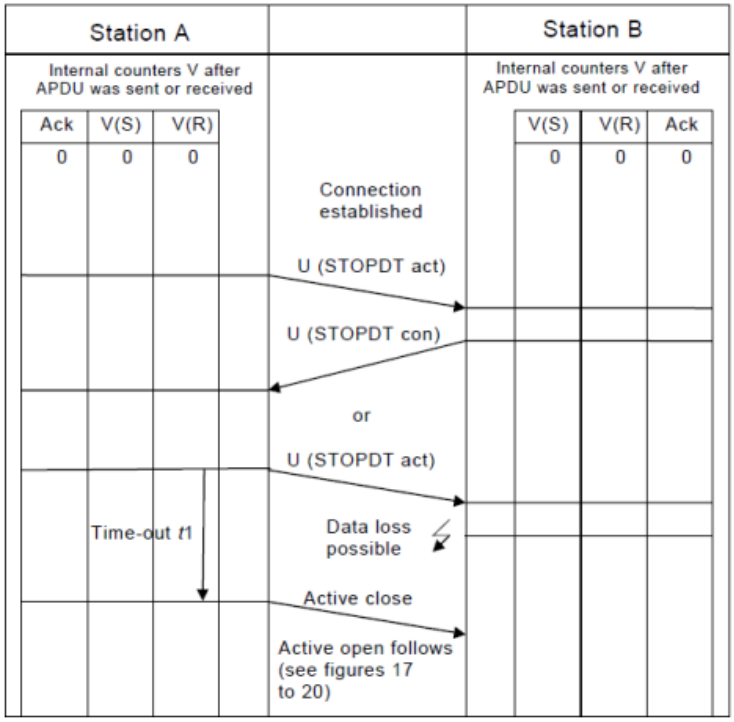


Appendix B: Start and stop data transfer procedures

1. Start Data Transfer Procedure



2. Stop Data Transfer Procedure



Appendix C.1: IEC 104 ASDU types and their description

Type	Description	Reference	Format	Valid COTs
Process information in monitor direction :				
1	Single point information	M_SP_NA_1	SIQ	2,3,5,11,20,20+G
2	Single point information with time tag	M_SP_TA_1	SIQ + CP24Time2a	3,5,11,12
3	Double point information	M_DP_NA_1	DIQ	2,3,5,11,12,20,20+G
4	Double point information with time tag	M_DP_TA_1	DIQ + CP24Time2a	3,5,11,12
5	Step position information	M_ST_NA_1	VTI + QDS	2,3,5,11,12,20,20+G
6	Step position information with time tag	M_ST_TA_1	VTI + QDS + CP24Time2a	2,3,5,11,12
7	Bit string of 32 bit	M_BO_NA_1	BSI + QDS	2,3,5,11,12,20,20+G
8	Bit string of 32 bit with time tag	M_BO_TA_1	BSI + QDS + CP24Time2a	3,5
9	Measured value, normalized value	M_ME_NA_1	NVA + QDS	2,3,5,11,12,20,20+G
10	Measured value, normalized value with time tag	M_ME_TA_1	NVA + QDS + CP24Time2a	3,5
11	Measured value, scaled value	M_ME_NB_1	SVA + QDS	2,3,5,11,12,20,20+G
12	Measured value, scaled value with time tag	M_ME_TB_1	SVA + QDS + CP24Time2a	3,5
13	Measured value, short floating point value	M_ME_NC_1	IEEE STD 754 + QDS	2,3,5,11,12,20,20+G
14	Measured value, short floating point value with time tag	M_ME_TC_1	IEEE STD 754 + QDS + CP24Time2a	2,3,5,11,12,20,20+G
15	Integrated totals	M_IT_NA_1	BCR	2,37,37+G
16	Integrated totals with time tag	M_IT_TA_1	BCR + CP24Time2a	3,37,37+G
17	Event of protection equipment with time tag	M_EP_TA_1	CP16Time2a + CP24Time2a	3
18	Packed start events of protection equipment with time tag	M_EP_TB_1	SEP + QDP +C P16Time2a + CP24Time2a	3
19	Packed output circuit information of protection equipment with time tag	M_EP_TC_1	OCI + QDP + CP16Time2a + CP24Time2a	3
20	Packed single-point information with status change detection	M_PS_NA_1	SCD+QDS	2,3,5,11,12,20,20+G
21	Measured value, normalized value without quality descriptor	M_ME_ND_1	NVA	1,2,3,5,11,12,20,20+G
Process telegrams with long time tag (7 octets) :				
30	Single point information with time tag CP56Time2a	M_SP_TB_1	SIQ + CP56Time2a	3,5,11,12
31	Double point information with time tag CP56Time2a	M_DP_TB_1	DIQ + CP56Time2a	3,5,11,12

32	Step position information with time tag CP56Time2a	M_ST_TB_1	VTI + QDS + CP56Time2a	2,3,5,11,12
33	Bit string of 32 bit with time tag CP56Time2a	M_BO_TB_1	BSI + QDS + CP56Time2a	3,5
34	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1	NVA + QDS + CP56Time2a	3,5
35	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1	SVA + QDS + CP56Time2a	3,5
36	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1	IEEE STD 754 + QDS + CP56Time2a	2,3,5,11,12,20,20+G
37	Integrated totals with time tag CP56Time2a	M_IT_TB_1	BCR + CP56Time2a	3,37,37+G
38	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1	CP16Time2a + CP56Time2a	3
39	Packed start events of protection equipment with time tag CP56time2a	M_EP_TE_1	SEP + QDP + CP16Time2a + CP56Time2a	3
40	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1	OCI + QDP + CP16Time2a + CP56Time2a	3
Process information in control direction :				
45	Single command	C_SC_NA_1	SCO	6,7,8,9,10,44,45,46,47
46	Double command	C_DC_NA_1	DCO	6,7,8,9,10,44,45,46,47
47	Regulating step command	C_RC_NA_1	RCO	6,7,8,9,10,44,45,46,47
48	Setpoint command, normalized value	C_SE_NA_1	NVA + QOS	6,7,8,9,10,44,45,46,47
49	Setpoint command, scaled value	C_SE_NB_1	SVA + QOS	6,7,8,9,10,44,45,46,47
50	Setpoint command, short floating point value	C_SE_NC_1	IEEE STD 754 + QOS	6,7,8,9,10,44,45,46,47
51	Bit string 32 bit	C_BO_NA_1	BSI	6,7,8,9,10,44,45,46,47
Command telegrams with long time tag (7 octets) :				
58	Single command with time tag CP56Time2a	C_SC_TA_1		
59	Double command with time tag CP56Time2a	C_DC_TA_1		
60	Regulating step command with time tag CP56Time2a	C_RC_TA_1		
61	Setpoint command, normalized value with time tag CP56Time2a	C_SE_TA_1		
62	Setpoint command, scaled value with time tag CP56Time2a	C_SE_TB_1		
63	Setpoint command, short floating point value with time tag CP56Time2a	C_SE_TC_1		
64	Bit string 32 bit with time tag CP56Time2a	C_BO_TA_1		

System information in monitor direction :				
70	End of initialization	M_EI_NA_1	COI	4
System information in control direction :				
100	(General-) Interrogation command	C_IC_NA_1	QOI	6,7,8,9,10,44,45,46,47
101	Counter interrogation command	C_CI_NA_1	QCC	6,7,8,9,10,44,45,46,47
102	Read command	C_RD_NA_1	null	5
103	Clock synchronization command	C_CS_NA_1	CP56Time2a	3,6,7,44,45,46,47
104	(IEC 101) Test command	C_TS_NB_1	FBP	6,7,44,45,46,47
105	Reset process command	C_RP_NC_1	QRP	6,7,44,45,46,47
106	(IEC 101) Delay acquisition command	C_CD_NA_1	CP16Time2a	6,7,44,45,46,47
107	Test command with time tag CP56Time2a	C_TS_TA_1		
Parameter in control direction :				
110	Parameter of measured value, normalized value	P_ME_NA_1	NVA + QPM	6,7,9,10,20,20+G,44,45,46,47
111	Parameter of measured value, scaled value	P_ME_NB_1	SVA + QPM	6,7,20,20+G,44,45,46,47
112	Parameter of measured value, short floating point value	P_ME_NC_1	IEEE STD 754 + QPM	6,7,20,20+G,44,45,46,47
113	Parameter activation	P_AC_NA_1	QPA	6,7,8,9,44,45,46,47
File transfer:				
120	File ready	F_FR_NA_1	NOF + LOF + FRQ	13
121	Section ready	F_SR_NA_1	NOF + NOS + LOF + SRQ	13
122	Call directory, select file, call file, call section	F_SC_NA_1	NOF + NOS + SCQ	5,13
123	Last section, last segment	F_LS_NA_1	NOF + NOS + LSQ + CHS	13
124	Ack file, Ack section	F_AF_NA_1	NOF + NOS + AFQ	13
125	Segment	F_SG_NA_1	NOF + NOS + LOS + segment	13
126	Directory	F_DR_TA_1	NOF + LOF + SOF + CP56Time2a	3,5
127	QueryLog – Request archive file	F_SC_NB_1		

- M_ (monitored information), C_ (control information, P_ (parameter), F_ (file), _Nx (not time tagged), _Tx (time tagged), _xA (type A: status and normalized, with quality), _xB (type B: scaled, with quality), _xC (type C: short floating point, with quality), _xD (type D: normalized without quality)
- Format defines a sequence of information elements that are valid for the given type. Depending on SQ parameter and number of object there can be a several instances of defined information elements
- Valid COTs contains a list of valid cause of transmission codes associated with this type

Appendix C.2: Cause of Transmission (COT) values

Code	Cause of Transmission	Abbreviation
1	periodic, cyclic	per/cyc
2	background interrogation	back
3	spontaneous	spont
4	initialized	init
5	interrogation or interrogated	req
6	activation	act
7	confirmation activation	actcon
8	deactivation	deact
9	confirmation deactivation	deactcon
10	termination activation	actterm
11	feedback, caused by distant command	retrem
12	feedback, caused by local command	retloc
13	data transmission	file
14-19	reserved for further compatible definitions	
20	interrogated by general interrogation	inrogen
21	interrogated by interrogation group 1	inro1
22	interrogated by interrogation group 2	inro2
23	interrogated by interrogation group 3	inro3
24	interrogated by interrogation group 4	inro4
25	interrogated by interrogation group 5	inro5
26	interrogated by interrogation group 6	inro6
27	interrogated by interrogation group 7	inro7
28	interrogated by interrogation group 8	inro8
29	interrogated by interrogation group 9	inro9
30	interrogated by interrogation group 10	inro10
31	interrogated by interrogation group 11	inro11
32	interrogated by interrogation group 12	inro12
33	interrogated by interrogation group 13	inro13
34	interrogated by interrogation group 14	inro14
35	interrogated by interrogation group 15	inro15
36	interrogated by interrogation group 16	inro16
37	interrogated by counter general interrogation	reqcogen
38	interrogated by interrogation counter group 1	reqco1
39	interrogated by interrogation counter group 2	reqco2
40	interrogated by interrogation counter group 3	reqco3
41	interrogated by interrogation counter group 4	reqco4
...		
44	type-Identification unknown	uknown_type
45	cause unknown	uknown_cause
46	ASDU address unknown	unknown_asdu_address
47	Information object address unknown	unknown_object_address

Appendix C.3: Information Elements

Element Type	Description	Length (B)	Used with the following Information Object Type(s)
Process information in monitor direction			
SIQ	Single-point information with quality descriptor	1	1, 2, 30
DIQ	Double-point information with quality descriptor	1	3
BSI	Binary state information	4	7, 8, 33, 51
SCD	Status and change detection	4	20
QDS	Quality descriptor	1	5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 20, 32, 33, 34, 36
VTI	Value with transient state indication	1	5, 6, 32
NVA	Normalized value	2	9, 10, 21, 34, 48, 110
SVA	Scaled value	2	11, 12, 49, 111
IEEE STD 754	Short floating point number	4	13, 14, 36, 50, 112
BCR	Binary counter reading	5	15, 16, 37
Protection			
SEP	Single event of protection equipment	1	17, 38
SPE	Start events of protection equipment	1	18, 39
OCI	Output circuit information of protection equipment	1	19, 40
QDP	Quality descriptor for events of protection equipment	1	18, 19, 39, 40
Commands			
SCO	Single command	1	45
DCO	Double command	1	46
RCO	Regulating step command	1	47
Time			
CP56Time2a	Seven octet binary time	7	4, 6, 8, 10, 12, 14, 16, 17, 18, 19, 31, 32, 33, 34, 36, 37, 38, 39, 40, 103, 126
CP24Time2a	Three octet binary time	3	4, 5, 6, 8, 10, 12, 14, 16, 17, 18, 19, 31, 32, 33, 34, 36, 37, 38, 39, 40
CP16Time2a	Two octet binary time	2	17, 18, 19, 38, 39, 40, 106
Qualifiers			
QOI	Qualifier of interrogation	1	100
QCC	Qualifier of counter interrogation command	1	101
QPM	Qualifier of parameter of measured values	1	110, 112
QPA	Qualifier of parameter activation	1	111, 113
QRP	Qualifier of reset process command	1	105
QOC	Qualifier of command	1	45, 46, 47, 48, 49, 50
QOS	Qualifier of set-point command	1	48, 49, 50
File Transfer			
FRQ	File ready qualifier	1	120
SRQ	Section ready qualifier	1	121
SCQ	Select and call qualifier	1	122

LSQ	Last section or segment qualifier	1	123
AFQ	Acknowledge file or section qualifier	1	124
NOF	Name of file	2	120, 121, 122, 123, 124, 125, 126
NOS	Name of section	2	121, 122, 123, 124, 125
LOF	Length of file or section	3	120, 121
LOS	Length of segment	1	125
CHS	Checksum	1	123
SOF	Status of file	1	126
Miscellaneous			
COI	Cause of initialization	1	70
FBP	Fixed test bit pattern, two octets	2	104

Appendix C.4: Quality bits

IV = VALID (0) / INVALID (1)

- A value is valid if it was correctly acquired. After the acquisition function recognizes abnormal conditions of the information source (missing or non-operating updating devices) the value is then marked invalid. The value of the information object is not defined under this condition.
- The mark invalid is used to indicate to the destination that the value may be incorrect due to a fault or other abnormal condition, and cannot be used.

NT = TOPICAL (0) / NOT TOPICAL (1)

- A value is topical if the most recent update was successful. It is not topical if it was not updated successfully during a specified time interval or if it is unavailable.

SB = NOT SUBSTITUTED (0) / SUBSTITUTED (1)

- The value of the information object is provided by the input of an operator (dispatcher) or by an automatic source.
- It means that the value is not derived from the normal measurement.

BL = NOT BLOCKED (0) / BLOCKED (1)

- The value of information object is blocked for transmission; the value remains in the state that was acquired before it was blocked. Blocking prevents updating of the value of the point.
- Blocking and deblocking may be initiated for example by a local lock or a local automatic cause.

SPI = OFF (0) / ON (1)

- Single Point Information
- The value reported in the SPI of the Information Object is derived from the current state of the binary point. SPI=1 means status ON, SPI=0 means status OFF.

OV = NO OVERFLOW (0) / OVERFLOW (1)

- The value of the information object is beyond a predefined range of value (mainly applicable to analog values).
- It is used primarily with analog or counter values.

DPI = Double Point Information

- indeterminate or intermediate state (0) / determined state OFF (1) / determined state (ON) / indeterminate state (3)

EI = 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.