IEC60870-5-103 Compact

Joachim Bürmann, *IFTOOLS GmbH*

September 17, 2020

The IEC60870-5 refers to a collection of standards produced by the International Electrotechnical Commission, or IEC , to provide an open standard for the transmission of SCADA telemetry control and information. The companion standard IEC 60870-5-103 specifies the SCADE transmission protocol especially for the informative interface of protection equipment.

Message structure

IEC60870-5-103 or IEC103 uses the FT1.2 frame format (defined in IEC60870-5-1) similar to IEC60870-5-101. There are three kinds of frames:

- Single characters used for acknowledge
- Frames with fixed length for commands
- Frames with variable lengths for exchanging data

Single control character

The single control frame consists of only the character or byte 0xE5. It is exclusively used for short acknowledges without the need of further information.

0xE5

Table 1: *Single control character*

Fixed length frame

The fixed length frame is used for sending data link commands and acknowledges only. It never carries any user data! The complete information is carried in the control field. The address field consists of one or two bytes in a non-balanced transmission. It must be specified by a fixed system parameter. Altogether the fixed frame length is 5 (one address byte) or 6 byte (two address bytes).

Start 0x10
Control
Address
Address (optional)
Checksum
End 0x16

Table 2: *Fixed length frame*

Frame with variable length

Frames with variable length are used to transport certain user data organized as a so called application service data unit, in short ASDU.

Start 0x68
Length field
Length field repeated
Start 0x68 repeated
Control
Address
Address (optional)
Link user data (ASDU)
Checksum
End 0x16

Table 3: *Frame with variable length*

The size of the ASDU block is specified in the length field whereas the length includes the control, the address(es) and the ASDU block. Less the first two the ASDU is limited to a maximum length of 253 bytes (or 252 with two address fields). The maximum frame length is therefore 261 bytes or octets.
The length is repeated twice. Frames with unequal length fields will not accepted by the recipient.
The address is either one or two bytes specified by the system. The value 0xFF or 0xFFFF is defined as the broadcast address

Checksum

The checksum range starts with the control field (2th byte in frames with fixed length) or 5th byte in frames with variable lengths and ends with the last byte before the checksum field.
The checksum itself is the modulo 256 sum of all bytes in the checksum range. Here is the according Lua code:

```
function checksum(data)
  local sum = 0
  for i=1,#data do
    sum = (sum + data;byte(i))%256
  end
  return sum
end
```

Frame timing rules

It is stated in [1] that the time between two consecutive bytes within a frame must not exceed one idle bit time (meaning the start bit of the next byte must follow immediately after the stop bit).
Additional a idle time of 33 bits must be allowed after detecting an erroneous frame by the recipient before it reacts.

Balanced transmission

In balanced transmission only two participants exist on each side of the bus (point-to-point). In this special case the address field is obsolete and the recipient is clearly identified by the DIR bit in the control field, see table 5 and 6.

Non-Balanced transmission

In a non-balanced configuration only one primary or controlling station polls data from several secondary stations (nodes). This makes sure that only one bus participant can initiate transmissions to avoid collisions. The stations are not working on a peer-to-peer (or point-to-point) base, thus described as non-balanced.

The control field

The control field of a data frame (fixed and variable length) is essential for the processing of the telegram. It is almost identical to the control field used by DNP3. Both were developed from the same specification IEC60870-5-2.
The control field has a little different meaning for balanced and non-balanced transmission. Both are described in the following.

RES	1 PRM 0	FCB ACD	FCV DFC	Function Code			
Bit 8	7	6	5	4	3	2	1

Table 4: *Control field non-balanced transmissions*

DIR	1 PRM 0	FCB RES	FCV DFC	Function Code			
Bit 8	7	6	5	4	3	2	1

Table 5: *Control field balanced transmissions*

The following table shows the detailed meaning of the bits in the control field (both, balanced and non-balanced transmissions).

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	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 when it cannot handling more data (buffer overflow)
ACD	Access Demand Bit	Set to 1 if Class 1 data is available

Table 6: *Control field bit meanings*

The interpretation of the control function field is different for requests (primary messages) and responses (secondary message). Bit 7 (PRM or Primary) in the control field (table 4 and 5) indicates the kind of message.
It also has slight different entries for balanced and non-balanced transmissions.

PRM	Code	Non-Balanced	Balanced
1	0	Reset Link	Reset Link
1	1	Reset User Process	Reset User Process
1	2		Test Link Function
1	3	User Data-Confirm Expected	User Data-Confirm Expected
1	4	User Data-No Confirm	User Data-No Confirm
1	9	Request Link Status	Request Link Status
1	10	Request User Data Class 1	
1	11	Request User Data Class 2	

Table 7: *Primary (Request) message*

PRM	Code	Non-Balanced	Balanced
0	0	Confirm - ACK	Confirm - ACK
0	1	Confirm - NACK	Confirm - NACK
0	8	Respond - User Data	
0	9	Respond - NACK No Data	
0	11	Respond - Link Status	Respond - Link Status
0	14	Link Not Functioning	Link Not Functioning
0	15	Link Not Used	Link Not Used

Table 8: *Secondary (Response) message*

The address field

The address field in a non-balanced transmission (with more than two bus participants) consists of one or two bytes (specified by a fixed application parameter).
In a balanced transmission (point-to-point) with only one node on each end the address field is obsolete and can be left out since the recipient is always clear (using the DIR bit in the control field). This too has to be specified by the application.

Application Service Data Unit

or in short ASDU. The ASDU block is the container for all data transmitted between a primary and secondary. It is segmented into two main sections: The Data Unit Identifier block and the data itself, consisting of one or more Information Objects.
Note that only one ASDU is allowed per frame.

Data Unit Identifier	ASDU Type Identifier
	Variable Structure Qualifier
	Cause of Transmission
	Common Address of ASDU
Information Object	Function Type
	Information Number
	Information Element(s)

Table 9: *ASDU structure*

Data Unit Identifier

The Data Unit Identifier specifies which data type is transported in the following information object(s). This covers: How many information elements are included, the cause of transmission and the data location inside the accessed device or station.

ASDU Type Identifier

The first octet of the Data Unit Identifier indicates the type of data (Type identification Code). The code has a special meaning depending on the direction, either in monitor or control direction.

7 0
Type Code

IEC60870-5-103 only supports a subset of types in comparison with IEC60870-5-101. These are:

ID	Description
1[1]	Time-tagged message (M_TTM_TA_3)
2[1]	Time-tagged message with relative time (M_TMR_TA_3)
3[1]	Measurands I (M_MEI_NA_3)
4[1]	Time-tagged measurands with relative time (M_TME_TA_3)
5[2]	Identification (M_IRC_NA_3)
6[2]	Time synchronisation (M_SYN_TA_3)
6[3]	Time synchronisation (C_SYN_TA_3)
7[3]	General interrogation (C_IGI_NA_3)
8[2]	Termination of general interrogation (M_TGI_NA_3)
9[1]	Measurands II (M_MEII_NA_3)
10[2]	Generic data (M_GD_XA_3)
10[3]	Generic data (C_GD_XA_3)
11[2]	Generic identification (M_GI_XA_3)
Continued on next page	

Continued from previous page

ID	Description
20[3]	General command (C_GRC_NA_3)
21[3]	Generic command (C_GC_NA_3)
23[1]	List of recorded disturbances (M_LRD_TA_3)
24[3]	Order for disturbance data transmission (C_ODT_NA_3)
25[3]	Acknowledgement for disturbance data transmission (C_ADT_NA_3)
26[1]	Ready for transmission of disturbance data (M_RTD_TA_3)
27[1]	Ready for transmission of channel (M_RTC_NA_3)
28[1]	Ready for transmission of tags (M_RTT_NA_3)
29[1]	Transmission of tags (M_TOT_NA_3)
30[1]	Transmission of disturbance values (M_TOV_NA_3)
31[1]	End of transmission (M_EOT_NA_3)

Table 10: *ASDU Type IDs*

1: Process Information in monitoring direction
2: System Information in monitoring direction
3: System Information in control direction

Variable Structure Qualifier

The second byte in the Data Unit Identifier is the variable structure qualifier or VSQ. It specifies the number of information objects and how they are addressed.

Variable Structure Qualifier

7	6 0
SQ	Number N

Bit 7 (the SQ flag) distinguish between a single or sequential number of information objects. The lower 7 bits contain the number of information objects.

Cause of Transmission

The cause of transmission field (COT) is a single byte indicating the cause of a data transmission like spontaneous or cyclic.

COT	Description
1	Spontanous data
2	Cyclic data
3	Reset FCB bit
4	Reset communication unit
5	Start/Restart
6	Power on
7	Test mode
8	Time synchronisation
9	General interrogation
10	Termination of general interrogation
11	Local operation
12	Remote operation
20	Positive ack of command
21	Negative ack of command
31	Transmission of disturbance values
40	Positive ack of generic write command
41	Negative ack of generic write command
42	Valid data response to genric read command
43	Invalid data response to generic read command
44	Confirmation of generic write

Table 11: *COT Types*

Common Address of ASDU

A single byte which denotes separate segments and its address inside a device.

Information Object

The Information Object follows immediately to the Data Unit Identifier and differs from IEC60870-5-101 in several ways. First: IEC60870-5-3 only allows one information object whereas 101 can have multiple ones. Also the information object address in 101 is divided in a function type and information number.

Function Type

The function type is a single octet and provides the function type clarification of the used protection equipment. The following types are supported by 103 (reserved types are grayed out):

Type	Description
0..127	Reserved (private area)
128	Distance protection
129	Not used (compatible area)
130..143	Reserved (private area)
144..145	Not used (compatible area)
146..159	Reserved (private area)
160	Overcurrent protection
161	Not used (compatible area)
162..175	Reserved (private area)
176	Transformer differential protection
177	Not used (compatible area)
178..191	Reserved (private area)
192	Line dirrerential protection

Continued on next page

Continued from previous page	
Type	**Description**
193	Not used (compatible area)
194..207	Reserved (private area)
208	Not used (compatible area)
209	Not used (compatible area)
210..223	Reserved (private area)
224	Not used (compatible area)
225	Not used (compatible area)
226..239	Reserved (private area)
240	Not used (compatible area)
241	Not used (compatible area)
242..253	Reserved (private area)
254	Generic function (GEN)
255	Global function (GLB)

Table 12: *Function Types*

Function Number

The function number differs between monitor and control direction. First the monitor direction:

Number	Description
0..15	System functions
16..31	State
32..47	Control
48..63	Earth faults
64..127	Short-circuit faults
128..143	Automatic reclose
144..159	Operating measured values
160..239	Not used
240..255	Generic functions

Table 13: *Function Number - Monitor direction*

The function numbers in control direction:

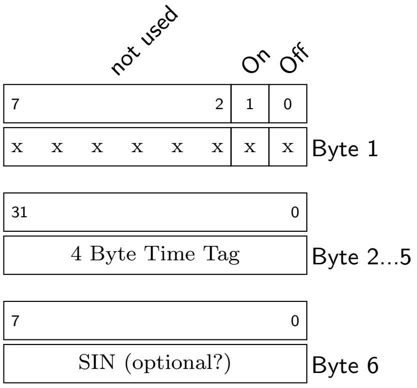
Number	Description
0..15	System functions
16..31	General commands
32..239	Not used
240..255	Generic functions

Table 14: *Function Number - Control direction*

ASDU Type Identifier

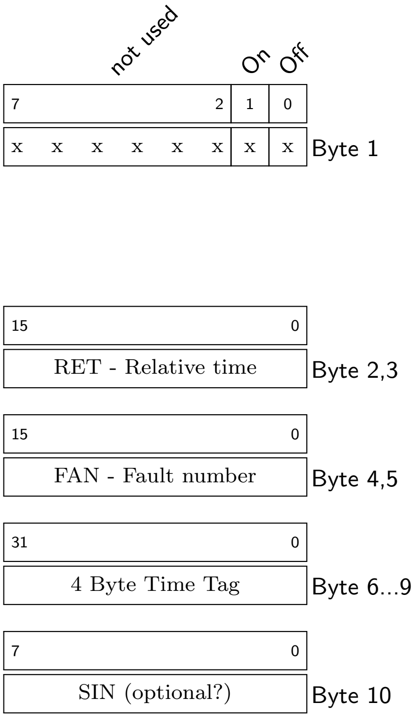
Type ID 1 - Time-tagged messages

Time-tagged messages with each data point represented by two bits in the first byte. The following four bytes contains the time tag. Byte 6 (Supplementary Information or SIN) may be optional.



Type ID 2 - Time-tagged message with relative time

Time-tagged messages with relative time. Each data point represented by two bits in the first byte. The next two bytes specify the relative time as a 16 bit value. Byte 4 and 5 have to interpret also as a 16 bit value containing a fault value.
Byte 6 to 9 contain the 4 octet time tag. The last byte is the supplementary information and may be optional.



Type ID 3 - Measurands I

Measurands with quality descriptor. Two octets forming a 16 bit value with low byte first. Bit 0-2 represented status information. The upper 13 bits contained a signed, 12-bit number. This data type will return from 1 to 4 values. The number of words dependants on the information object number and the slave device.

Measurand with quality descriptor

sign	value	Reserved	Invalid	Overflow
15	14 3	2	1	0
x	x x x x x x x x x x x x	x	x	x

Type ID 4 - Time-tagged measurands with relative time

Time-tagged measurands with relative time. The measurand value is packet as 4 octets representing a single floating-point number with the format IEEE754, low byte first.

31 0	
Short floating number	Byte 1...4
15 0	
RET - Relative time	Byte 5,6
15 0	
FAN - Fault number	Byte 7,8
31 0	
4 Byte Time Tag	Byte 9...12

Type ID 5 - Identification

Identification data composed of 12 bytes. The first eight bytes contain ASCII characters, the last four bytes are defined by the manufacturer and could be either ASCII or bytes.
Some specifications also indicates a leading COL byte containing the compatibility level (2 or 3) which would increase the data to 13 bytes.

Byte	COL	1	2	3	4	5	6	7	8	9	10	11	12
	COL	ASCII characters								Vendor			

Type ID 6 - Time synchronization

Transports seven bytes representing a 56 bit (7 octets) binary time format.

55 0	
Time-tag 56 bit	Byte 1...7

Type ID 7 - General interrogation

The primary station uses the general interrogation function after an initialization procedure or when the primary station detects a loss of information. The message consists of only one byte, the SCN or scan number (0...255).

7 0	
scan number	Byte 1

Type ID 8 - Termination of General interrogation

Terminates a general interrogation. The message consists of only one byte, the SCN or scan number (0...255).

7 0	
scan number	Byte 1

Type ID 9 - Measurands II

Measurands with quality descriptor. Two octets forming a 16 bit value with low byte first. Bit 0-2 represented status information. The upper 13 bits contained a signed, 12-bit number (range from -4096 to +4095). This data type will return from 1 to 9 values (some slaves will return up to 16 values). The number of words dependants on the information object number and the slave device.

Measurand with quality descriptor

sign	value	Reserved	Invalid	Overflow
15	14 3	2	1	0
x	x x x x x x x x x x x x	x	x	x

Type ID 10 - Generic Data

Used to transport a variable length of different data.

7 0	
RII	Byte 1

Cont	Count	NO	
7	6	5 0	
x	x	x x x x x x	Byte 2

Cont 0: No following ASDU with the same RII, 1: Following ASDU has the same RII

Count One bit counter for equal RII

NO Number of generic data sets

7 0	
GIN Group	Byte 3

7 0	
GIN Entry	Byte 4

7 0	
KOD	Byte 5

7 0	
DATATYPE	Byte 6

7 0	
DATASIZE	Byte 7

Cont	Number	
7	6 0	
x	x x x x x x x	Byte 8

Cont 0: No following ASDU with the same RII, 1: Following ASDU has the same RII

Number Number of following data block

7 0	
GID	Byte 9

---

7 0	
GIN Group	Byte 10

…

Type ID 11 - Generic Identification

Similar to the former Generic Data but used to transport special identification data.

7 0	
RII	Byte 1

7 0	
GIN Group	Byte 2

7 0	
GIN Entry	Byte 3

Cont	Count	NO	
7	6	5 0	
x	x	x x x x x x	Byte 4

Cont 0:No following ASDU with the same RII, 1:Following ASDU has the same RII

Count One bit counter for equal RII

NO Number of generic data sets

7 0	
KOD	Byte 5

7 0	
DATATYPE	Byte 6

7 0	
DATASIZE	Byte 7

Cont	Number	
7	6 0	
x	x x x x x x x	Byte 8

Cont 0: No following ASDU with the same RII, 1: Following ASDU has the same RII

Number Number of following data block

7 0	
GID	Byte 9

---

7 0	
KOD	Byte 10

…

Type ID 20 - General Command

General command to control a dual-point object. Each command issued by the module uses the values of two adjacent bits in the database or an override value specified by the user command.

Unused	DCS	
7 2	1 0	
x x x x x x	x x	Byte 1

DCS means Double Command State (sometimes also Dual Bit State) and defines the following states:
00 (0) : not used
01 (1) : off
10 (2) : on
11 (3) : not used

7 0	
RII	Byte 2

RII is the Return Information Identifier with a valid range of 0...255.

Type ID 21 - Generic Command

7	0	RII	Byte 1
7	0	NOG	Byte 2

NOG Number of generic data sets

Data Set 1

7	0	GIN Group	Byte 3
7	0	GIN Entry	Byte 4
7	0	KOD	Byte 5

Data Set 2

...

Type ID 23 - List of recorded disturbances

Data Set 1

15	0	FAN	Byte 1,2

RES		OTEV	Test	TM	TP	
7	4	3	2	1	0	
x		x	x	x	x	Byte 3

55	0	Time-Tag 56 bit	Byte 4...10

Data Set 2

...

Type ID 24 - Order for disturbance data transmission

7	0	TOO	Byte 1
7	0	TOV	Byte 2
15	0	FAN	Byte 3,4
7	0	ACT	Byte 5

Type ID 25 - ACK for disturbance data transmission

The same as Type ID 24, see above.

Type ID 26 - Ready for transmission of disturbance data

7	0	not used	Byte 1
7	0	TOV	Byte 2
15	0	FAN	Byte 3,4
15	0	NOF	Byte 5,6
7	0	NOC	Byte 7
15	0	NOE	Byte 8,9
15	0	INT	Byte 10,11
31	0	Time Tag 32	Byte 12..15

Type ID 27 - Ready for transmission of channel

7	0	not used	Byte 1
7	0	TOV	Byte 2
15	0	FAN	Byte 3,4
7	0	ACC	Byte 5
31	0	RPV	Byte 6..9

31	0	RSV	Byte 10..13
31	0	RFA	Byte 14..17

Type ID 28 - Ready for transmission of tags

7	0	not used	Byte 1
7	0	not used	Byte 2
15	0	FAN	Byte 3,4

Type ID 29 - Transmission of tags

15	0	FAN	Byte 1,2
7	0	NOT	Byte 3
15	0	TAP	Byte 4,5

Tag 1 ______________________________

7	0	Function Code Type	Byte 6
7	0	Information Number	Byte 7
8	3	0	Byte 8
1	0	DPI	

Tag 2 ______________________________

...

Type ID 30 - Transmission of disturbance values

7	0	not used	Byte 1
7	0	TOV	Byte 2
15	0	FAN	Byte 3,4
7	0	ACC	Byte 5
7	0	NDV	Byte 6
15	0	NFE	Byte 7,8
15	0	SDV 1	Byte 9,10
15	0	SDV 2	Byte 11,12
15	0	SDV 3	Byte 13,14

SDV n ______________________________

...

Type ID 31 - End of transmission

7	0	TOO	Byte 1
7	0	TOV	Byte 2
15	0	FAN	Byte 3,4
7	0	ACT	Byte 5

Data representation

The following section describes the internal data representation used in the several data types above in an alphabetic order.

ACC

One byte representing the actual channel in a range of 0...255.

DATATYPE

DATATYPE is used in Type ID 10 and 11 specifying the kind of data in the following data block.

Number	Description
0	No Data
1	OS8 ASCII
2	Packed Bit String
3	UI - Unsigned Integer
4	Integer
5	UF ?
6	F ?
7	R32 ?
8	R64 ?
9	Double Point Information
10	Single Point Information
11..22	not specified
23	Data Struct
24	Index
25..255	reserved

Table 15: *DATATYPE*

DATASIZE

8 Bit value specifying the data size in a generic data description (see Type ID 11 and 12).

DPI - Double Point Information

A 2-bit coded on/off information. A set bit 0 means off, a set bit 1 on.

FAN - Fault number

A 16 bit value (two bytes) specifying a valid range of 0...65335.

GIN Group - Generic Identification Number Group

A single byte or octet specifying the group identification (valid range is 0...255).

GIN Entry - Generic Identification Number Entry

A single byte or octet specifying the entry identification (valid range is 0...255).

INT - Interval

Specifies the interval for acquisition of the single information elements and is the same for all disturbance data. It is listed in microseconds (0...65535).

KOD - Kind of Description

Kind of description as used in Generic Data (Type ID 10) and Generic Identification (Type ID 119. The following values are defined:

Number	Description
0	no KOD specified
1	actual value
2	default value
3	range (min, max, step size)
4	reserved
5	precision
6	factor
7	% reference
8	enumeration
9	dimension
10	description
11	reserved
12	password entry
13	is read only
14	is write only
15..18	reserved
19	corresponding function type and information number
20	corresponding event
21	enumerated text array
22	enumerated value array
23	related entries
24..255	reserved

Table 16: *KOD - Kind of Description*

MEA - Measurand with quality descriptor

A 16 bit value whereas the three lowest bits indicating an invalid or overflow value. The remaining 13 bits representing a signed 12 bit value in the range of $-2^{12} ... + 2^{12}$ or -4096 to +4095.

sign	value	Reserved	Invalid	Overflow
15	14 ... 3	2	1	0
x	x x x x x x x x x x x x	x	x	x

NOC - Number of channels

A 8 bit value representing the number of channels (0...255).

NDV - Number of disturbance values

Number of relevant disturbance values per ASDU, valid range is 1..25.

NFE - Number of first information element

Number of the ASDU's first information element, a 16 bit value, valid range is 1...65535.

NOE - Number of information elements

of a channel. A 16 bit value (0..65335).

NOF - Number of grid faults

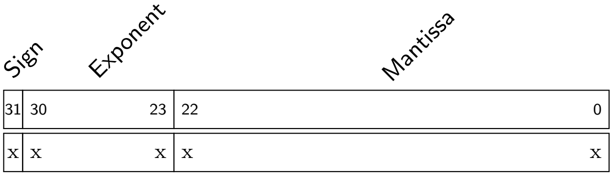
A 16 bit value (two bytes) specifying the number of grid faults (0..65335).

NOT - Number of tags

The number of following tags, one byte (0..255). 0 indicates not supported transmission of tags?

R32 - Short floating number

A four octet value representing a 32 bit floating number according to IEEE STD 754. Lowest byte first. Used in Type ID 4 for instance.



Byte 1...4

RET - Relative Time

A 16 bit value (two bytes) specifying a valid range of 0..65335.

RFA - Reference Factor

A R32 value (32 bit short floating number).

RPV - Rated Primary Value

A R32 value (32 bit short floating number).

RSV - Rated Secondary Value

A R32 value (32 bit short floating number).

SCN - Scan Number

Used as return identifier in general interrogation responses. A single byte. Valid values are 0..255.

SDV - Single disturbance value

A signed 15 bit value (-32768...+32767).

SIN - Supplementary information

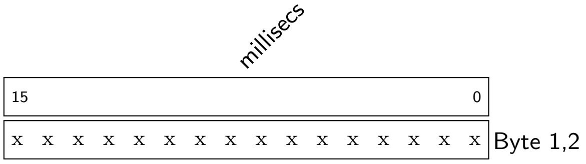
A single byte. Valid values are 0..255. It can be can be used as follows:
By general interrogation as a number of GI request or
By positive or negative acknowledgement of command as RII.

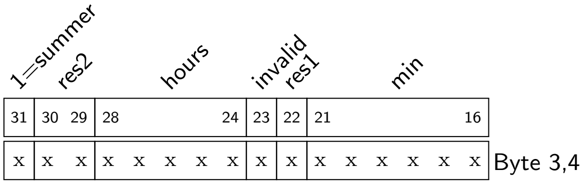
TAP - Tag position

A 16 bit value (0..65535). Some manufacturer preset it to 0, the meaning is not entirely clear.

Time-tag 32 Bit

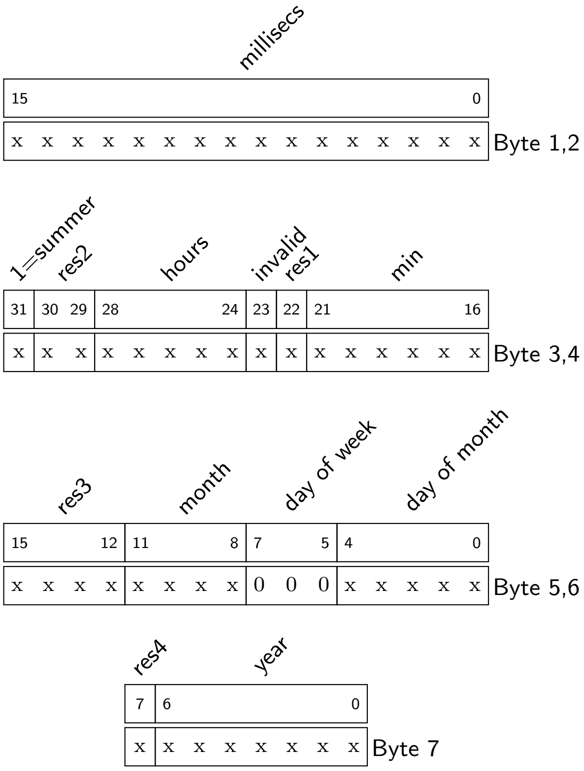
Four octets binary time tag used in several data types. The first two bytes contain the milliseconds in a range of 0...59999). The lower 6 bits in the third byte specifies the minutes (0...59).





Time-tag 56 Bit

A sequence of 7 bytes. The first four are equal with the 32 bit time tag. The additional three bytes hold information about the day of month, day of week (here not used and zero), the month and year.



TOO

One byte representing the type of order (valid values are 0...255).

TOV

Type of disturbance value, 1 byte, valid values are 0...255.

Further links

```
https://en.wikipedia.org/wiki/IEC_60870-5
https://infosys.beckhoff.com/content/1033/tf6500_tc3_iec60870_5_10x/9007200239043851.html?
id=6140844712604750394
```

References

[1] Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Gordon Clarke, Deon Reynders, Edwin Wright, 2004 IDC Technologies, ISBN 07506 7995