SIEMENS

**SIMATIC S7-1500
TIM 1531 IRC V2.3
Protocol IEC 60870-5-101**

**Interoperability list
V1.4**

SIEMENS

1 VERSION HISTORY

Version	Date	Author	Review	Remarks
1.0	08.02.2018	Joerg Hahn		First draft
1.1	08.22.2018	Joerg Hahn		Release before conformance test
1.2	11.05.2018	Joerg Hahn		Release after conformance test
1.3	13.09.2021	Joerg Hahn		Change max. frame length from 253 to 252
1.4	27.03.2023	Joerg Hahn		Additional parameters for IEC 60870-5-7 (supported as of TIM 1531 IRC V2.3), support of master function, support of RS485

SIEMENS

2 SCOPE OF THIS DOCUMENT

The scope of this document is to describe in a detailed way the implementation of the IEC 60870-5 communication interface as indicated in the first page. It contains a default template as in IEC 60870-5-101Ed.2 that shows the minimum information to describe 101 function, which is integrated in a customized way by additional sections, notes, figures and data that the manufacturer wants to show to whoever it may concern.

3 OBJECTIVE OF THIS DOCUMENT

The objective is:

For a Manufacturer PID: to provide utilities, system integrators, and whoever is interested in using/purchasing this implementation, the necessary information to evaluate quality, features, and interoperability risks when the product is integrated in a given multi-vendor network or substation.

For an Utility PID: provide manufacturers which are the minimum requirements for their devices to be integrated into the utility network and guarantee interoperability in a multi-vendor network (this latter still to be verified by dedicated interoperability testing). This document can be used as a technical specification during a tender process.

4 PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS)

IMPORTANT

The Protocol Implementation Conformance Statement (PICS) in this paragraph is the basis for the applicable test cases in Chapter 5.This PICS gives an overview of the tested protocol implementation, but this isn't a guarantee that the complete function or ASDU, as enabled in the PICS, is tested and supported. Partial testing is possible and the completeness of the tests for the specific function or ASDU should be consulted in Chapter 5.

The selected parameters should be marked in the white boxes as follows:

☐   Function or ASDU is not used

☒   Function or ASDU is used as standardized (default)

R   Function or ASDU is used in reverse mode

B   Function or ASDU is used in standard and reverse mode

The possible selection (blank, X, R, or B) is specified for each specific clause or parameter.

NOTE: In addition, the full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

4.1 System or device

(System-specific parameter, indicate the definition of a system or a device by marking one of the following with '**X**').

SIEMENS

☐	System definition
☒	Controlling station definition
☒	Controlled station definition

4.2 Network configuration

(Network-specific parameter, all configurations that are used are to be marked '**X**').

☒	Point-to-point	☒	Multipoint-partyline
☐	Multiple point-to-point	☒	Multipoint-star

4.3 Physical layer

(Network-specific parameter, all interfaces and data rates that are used are to be marked '**X**').

Transmission speed (control direction)

Unbalanced interchange RS232	Unbalanced interchange RS232	Unbalanced interchange RS485	
☐ 100 bit/s	☒ 2 400 bit/s	☒ 1200 bit/s	☒ 115 200 bit/s
☐ 200 bit/s	☒ 4 800 bit/s	☒ 2400 bit/s	☐
☐ 300 bit/s	☒ 9 600 bit/s	☒ 4800 bit/s	☐
☐ 600 bit/s	☒ 19 200 bit/s	☒ 9600 bit/s	
☒ 1 200 bit/s	☒ 38 400 bit/s	☒ 19 200 bit/s	
☐	☒ 115 200 bit/s	☒ 38 400 bit/s	

Transmission speed (monitor direction)

Unbalanced interchange RS232	Unbalanced interchange RS232	Unbalanced interchange RS485	
☐ 100 bit/s	☒ 2 400 bit/s	☒ 1200 bit/s	☒ 115 200 bit/s
☐ 200 bit/s	☒ 4 800 bit/s	☒ 2400 bit/s	☐
☐ 300 bit/s	☒ 9 600 bit/s	☒ 4800 bit/s	☐
☐ 600 bit/s	☒ 19 200 bit/s	☒ 9600 bit/s	
☒ 1 200 bit/s	☒ 38 400 bit/s	☒ 19 200 bit/s	
☐	☒ 115 200 bit/s	☒ 38 400 bit/s	

4.4 Link layer

(Network-specific parameter, all options that are used are to be marked 'X'. Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the type ID and COT of all messages assigned to class 2.)

Frame format FT 1.2, single character 1 and the fixed time out interval are used exclusively in this companion standard.

Link transmission

☐ Balanced transmission

X Unbalanced transmission

Address field of the link

☐ not present (balanced transmission only)

X One octet

X Two octets

Frame length

`252` Maximum length L[1] (control dir.)

`252` Maximum length L[1] (monitor dir.)

☐ Structured

X Unstructured

When using an unbalanced link layer, the following ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission:

☐ The standard assignment of ASDUs to class 2 messages is used as follows:

Type identification	Cause of transmission
9, 11, 13, 21	<1>

☐ A special assignment of ASDUs to class 2 messages is used as follows:

Type identification	Cause of transmission

Note: In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available.

---

[1] L in the frame from the Control field octet 1, therefore excluding START and L fields itself, max 253

SIEMENS

4.5 Application layer

Transmission mode for application data

Mode 1 (least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

(system-specific parameter, all configurations that are used are to be marked '**X**').

☐ One octet   ☒ Two octets

Information object address

(system-specific parameter, all configurations that are used are to be marked '**X**').

☐ One octet   ☐ Structured

☐ Two octets   ☒ Unstructured

☒ Three octets

Cause of transmission

(system-specific parameter, all configurations that are used are to be marked '**X**').

☐ One octet   ☒ Two octets (with originator address) Originator address is set to zero if not used

Selection of standard ASDUs

Process information in monitor direction

(station-specific parameter, mark each type ID '**X**' if it is only used in the standard direction, '**R**' if only used in the reverse direction, and '**B**' if used in both directions).

☒ <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

[X]	<9>	:=	Measured value, normalized value	M_ME_NA_1
[ ]	<10>	:=	Measured value, normalized value with time tag	M_ME_TA_1
[X]	<11>	:=	Measured value, scaled value	M_ME_NB_1
[ ]	<12>	:=	Measured value, scaled value with time tag	M_ME_TB_1
[X]	<13>	:=	Measured value, short floating point value	M_ME_NC_1
[ ]	<14>	:=	Measured value, short floating point value with time tag	M_ME_TC_1
[X]	<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
[X]	<30>	:=	Single-point information with time tag CP56Time2a	M_SP_TB_1
[X]	<31>	:=	Double-point information with time tag CP56Time2a	M_DP_TB_1
[X]	<32>	:=	Step position information with time tag CP56Time2a	M_ST_TB_1
[X]	<33>	:=	Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
[X]	<34>	:=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
[X]	<35>	:=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
[X]	<36>	:=	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1

X	<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

Either ASDUs of the set <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <17>, <18>, <19> or of the set <30 –40> are used.

Process information in control direction

(station-specific parameter, mark each type ID '**X**' if it is only used in the standard direction, '**R**' if only used in the reverse direction, and '**B**' if used in both directions).

X	<45>	:= Single command	C_SC_NA_1
X	<46>	:= Double command	C_DC_NA_1
X	<47>	:= Regulating step command	C_RC_NA_1
X	<48>	:= Set point command, normalized value	C_SE_NA_1
X	<49>	:= Set point command, scaled value	C_SE_NB_1
X	<50>	:= Set point command, short floating point value	C_SE_NC_1
X	<51>	:= Bitstring of 32 bit	C_BO_NA_1

System information in monitor direction

(station-specific parameter, mark '**X**' if it is only used in the standard direction, '**R**' if only used in the reverse direction, and '**B**' if used in both directions)

X	<70>	:= End of initialization	M_EI_NA_1

System information in control direction

(station-specific parameter, mark each type ID '**X**' if it is only used in the standard direction, '**R**' if only used in the reverse direction, and '**B**' if used in both directions)

X	<100>	:= Interrogation command	C_IC_NA_1
X	<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_1

Parameter in control direction

(station-specific parameter, mark each type ID 'X' if it is only used in the standard direction, 'R' if only used in the reverse direction, and 'B' if used in both directions)

☐ <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 value   P_ME_NC_1

☐ <113>:= Parameter activation   P_AC_NA_1

File Transfer

(station-specific parameter, mark each type ID 'X' if it is only used in the standard direction, 'R' if only used in the reverse direction, and 'B' if used in both directions)

☐ <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 {blank or X, only available in monitor (standard) direction}   F_DR_TA_1

☐ <127>:= Query log – Request archive file   F_SC_NB_1

Type identifier and cause of transmission assignments

(station-specific parameters)

Shaded boxes are not defined in this companion standard and shall not be used.

Blank = function or ASDU is not used.

Mark type identification/cause of transmission combinations:

'**X**' if only used in the standard direction
'**R**' if only used in the reverse direction
'**B**' if used in both directions

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1			X											X					
<2>	M_SP_TA_1																			
<3>	M_DP_NA_1			X											X					
<4>	M_DP_TA_1																			
<5>	M_ST_NA_1			X											X					
<6>	M_ST_TA_1																			
<7>	M_BO_NA_1			X											X					
<8>	M_BO_TA_1																			
<9>	M_ME_NA_1			X											X					
<10>	M_ME_TA_1																			
<11>	M_ME_NB_1			X											X					
<12>	M_ME_TB_1																			
<13>	M_ME_NC_1			X											X					
<14>	M_ME_TC_1																			
<15>	M_IT_NA_1			X												x				
<16>	M_IT_TA_1																			
<17>	M_EP_TA_1																			
<18>	M_EP_TB_1																			
<19>	M_EP_TC_1																			
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X																
<31>	M_DP_TB_1			X																
<32>	M_ST_TB_1			X																
<33>	M_BO_TB_1			X																
<34>	M_ME_TD_1			X																
<35>	M_ME_TE_1			X																
<36>	M_ME_TF_1			X																
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X							X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X							X	X	X	X

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<47>	C_RC_NA_1						X	X	X	X	X							X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X							X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X							X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X							X	X	X	X
<51>	C_BO_NA_1						X	X			X							X	X	X	X
<70>	M_EI_NA_1				X																
<100>	C_IC_NA_1						X	X	X	X	X							X	X	X	X
<101>	C_CI_NA_1						X	X			X							X	X	X	X
<102>	C_RD_NA_1																				
<103>	C_CS_NA_1						X	X										X	X	X	X
<104>	C_TS_NA_1						X	X										X	X	X	X
<105>	C_RP_NA_1																				
<106>	C_CD_NA_1																				
<110>	P_ME_NA_1																				
<111>	P_ME_NB_1																				
<112>	P_ME_NC_1																				
<113>	P_AC_NA_1																				
<120>	F_FR_NA_1																				
<121>	F_SR_NA_1																				
<122>	F_SC_NA_1																				
<123>	F_LS_NA_1																				
<124>	F_AF_NA_1																				
<125>	F_SG_NA_1																				
<126>	F_DR_TA_1*																				

*) blank or X only

NOTE: Cause of transmission (COT) 44 shall only be marked for Type identifications which are not supported

4.6 Basic application functions

Station initialization

(station-specific parameter, mark 'X' if function is used).

☐ Remote initialization

Cyclic data transmission

(station-specific parameter, mark 'X' if function is used only in the standard direction, 'R' if used only in the reverse direction, and 'B' if used in both directions).

☐ Cyclic data transmission

SIEMENS

Read procedure

(station-specific parameter, mark 'X' if function is used only in the standard direction, 'R' if used only in the reverse direction, and 'B' if used in both directions).

☐ Read procedure

Spontaneous transmission

(station-specific parameter, mark '**X**' if function is used only in the standard direction, '**R**' if used only in the reverse direction, and '**B**' if used in both directions).

☒ Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

(station-specific parameter, mark each information type 'X' where both a type ID without time and corresponding type ID with time are issued in response to a single spontaneous change of a monitored object).

The following type identifications may be transmitted in succession caused by a single status change of an information object. The particular information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1

☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1

☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1

☐ Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project)

☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1

☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1

☐ Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and

Station interrogation

(station-specific parameter, mark '**X**' if function is used only in the standard direction, '**R**' if used only in the reverse direction, and '**B**' if used in both directions)

☒ global

☒ group 1	☒ group 7	☒ group 13
☒ group 2	☒ group 8	☒ group 14
☒ group 3	☒ group 9	☒ group 15
☒ group 4	☒ group 10	☒ group 16

X group 5	**X** group 11	
X group 6	**X** group 12	Information Object Addresses assigned to each group must be shown in a separate table

Clock synchronization

(station-specific parameter, mark '**X**' if function is used only in the standard direction, '**R**' if used only in the reverse direction, and '**B**' if used in both directions)

X Clock synchronization

☐ Day of week used

☐ RES1, GEN (Time tag substituted/not substituted) used

☐ SU-bit (summertime) used

Command transmission

(object-specific parameter, mark '**X**' if function is used only in the standard direction, '**R**' if used only in the reverse direction, and '**B**' if used in both directions)

X Direct command

X Direct set point command transmission

X Select and execute command (Only for the commands without timetag)

X Select and execute set point command (Only for the commands without timetag)

X C_SE ACTTERM used

X No additional definition

X Short pulse duration (duration determined by a system parameter in the outstation)

X Long pulse duration (duration determined by a system parameter in the outstation)

X Persistent output

Transmission of integrated totals

(station- or object-specific parameter, mark '**X**' if function is used only in the standard direction, '**R**' if used only in the reverse direction, and '**B**' if used in both directions)

X Mode A: Local freeze with spontaneous

X Mode B: Local freeze with counter

☐ Mode C: Freeze and transmit by counter interrogation

☐ Mode D: Freeze by counter interrogation command, frozen values reported

☒ Counter read

☐ Counter freeze without reset

☐ Counter freeze with reset

☐ Counter reset

☒ General request

☒ Request counter group 1

☒ Request counter group 2

☒ Request counter group 3

☒ Request counter group 4

Parameter loading

(object-specific parameter, mark 'X' if function is used only in the standard direction, 'R' if used only in the reverse direction, and 'B' if used in both directions)

☐ Threshold value

☐ Smoothing factor

☐ Low limit for transmission of measured

☐ High limit for transmission of measured

Parameter activation

(object-specific parameter, mark 'X' if function is used only in the standard direction, 'R' if used only in the reverse direction, and 'B' if used in both directions)

☐ Act/deact of persistent cyclic or periodic transmission of the addressed

Test procedure

(station-specific parameter, mark 'X' if function is used only in the standard direction, 'R' if used only in the reverse direction, and 'B' if used in both directions)

☒ Test procedure

—

File transfer

(station-specific parameter, mark '**X**' if function is used)

File transfer in monitor direction

☐ Transparent file

☐ Transmission of disturbance data of protection

☐ Transmission of sequences of events

☐ Transmission of sequences of recorded analogue values

File transfer in control direction

☐ Transparent file

Background scan

(station-specific parameter, mark '**X**' if function is only used in the standard direction, '**R**' if only used in the reverse direction, and '**B**' if used in both directions)

☐ Background scan

Acquisition of transmission delay

(station-specific parameter, mark '**X**' if function is only used in the standard direction, '**R**' if only used in the reverse direction, and '**B**' if used in both directions)

☐ Acquisition of transmission delay

SIEMENS

Support IEC 60870-5-7

Secure Authentication

Supports one user and use a pre-shared key as update key

MAC algorithms

- [X] HMAC-SHA-256 (required)
- [ ] Other

Key wrap algorithms

- [X] AES-256 Key Wrap (required)
- [ ] Other

Maximum Error messages sent

- [ ] Fixed at 2
- [X] Configurable

Use of Error messages

- [ ] Transmit Error messages
- [X] Configurable

Update Key Change Methods

- [X] None permitted
- [ ] Configurable

User Status Change

- [X] Non-certificate method (required)
- [ ] Use IEC/TS-62351-8 Certificates

Use aggressive mode

- [ ] Fixed
- [X] Configurable

Use security statistics

- [ ] Fixed
- [X] Configurable

List of supported critical functions:

Type identification		Description
< 46 >	C_DC_NA_1	Double command
< 47 >	C_RC_NA_1	Regulating step command
< 48 >	C_SE_NA_1	Set-point command, normalized value
< 49 >	C_SE_NB_1	Set-point command, scaled value
< 50 >	C_SE_NC_1	Set-point command, short floating-point number
< 51 >	C_BO_NA_1	Bitstring of 32-bit
< 103 >	C_CS_NA_1	Clock synchronization command

5   ADDITIONAL INFORMATION

Value range of Integrated totals is 0 - 0x7FFF FFFF, because only the positive part will be processed.