

# IEC 870-5-104 Sinaut

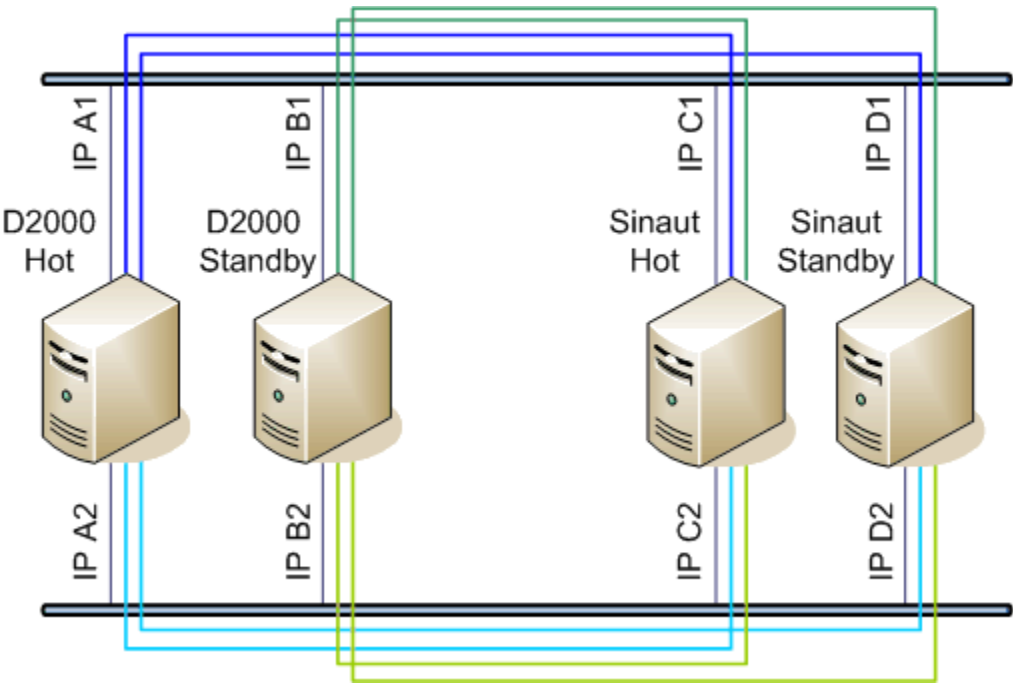
## IEC 870-5-104 Sinaut communication protocol

[Supported device types and versions](#)  
[Communication line configuration](#)  
[Communication station configuration](#)  
[Station protocol parameters](#)  
[I/O tag configuration](#)  
[Literature](#)  
[Document revisions](#)

### Supported device types and versions

The protocol is a modification of the protocol [IEC870-5-104](#) working on the basis of TCP network communication. The protocol has been modified specifically for redundant communication with the system **Siemens Sinaut Spectrum**. It supports the balanced mode and active and passive establishing the communication (connecting party and listening party) according to the [station protocol parameters](#), and therefore allows to interconnect not only D2000 system with Sinaut system but also two D2000 systems.

Picture: D2000 redundant system communicating with Sinaut redundant system in redundant network



The picture above shown TCP connections - each process [D2000 KOM](#)(D2000 Hot, D2000 StandBy) with eachSinaut (Sinaut Hot, Sinaut StandBy)

Implementation according to the standard IEC870-5-104 is following:

- **Originator ASDU address** - is 1 byte, it is defined as a line number.
- **ASDU address** - is 2 bytes, it is defined as station address. For each station on one line, there must be defined different ASDU address.  
**Note:** Because of Sinaut data model, the low and high address bytes are changed unlike the standard IEC 104 implementation, i.e. big endian instead of little endian.  
Example:  
station address=1, ASDU address is sent as 0, 1 bytes  
station address=513 (2\*256+1), ASDU address is sent as 2, 1 bytes  
For better orientation, station address may be defined in the form of ByteHI,ByteLO, i.e. address **2,1** is the same as **513**
- **Cause of transmission** - is 2 bytes (it also contains Originator ASDU address)
- **Information object address** - 3 bytes, it is defined as I/O tag address  
**Note:** Because of Sinaut data model, the low and high address bytes are changed unlike the standard IEC 104 implementation, i.e. big endian instead of little endian.  
Example:  
I/O tag address=1, ASDU address is sent as 0, 0, 1 bytes.  
I/O tag address=66051(1\*65536+2\*256+3), ASDU address is sent as bytes 1, 2, 3.  
For better orientation, I/O tag address may be defined in the form of ByteLO,ByteMIDDLE,ByteHI, i.e. address **1,2,3** is sent as bytes 1, 2, 3.

There are implemented the following ASDU types in the direction of logging (from Sinaut system to D2000 system and also vice-versa in balanced mode):

**Table 1**

ASDU type	I/O tag types
1 - Single-point information	Di, Qi (On/Off), Ai, Ci
2 - Single-point information with time tag	Di, Qi (On/Off), Ai, Ci
3 - Double-point information	Qi, Ai, Ci
4 - Double-point information with time tag	Qi, Ai, Ci
5 - Step position information	Ci, Ai *
6 - Step position information with time tag	Ci, Ai *
7 - Bitstring of 32 bits	Ci, Ai
8 - Bitstring of 32 bits with time tag	Ci, Ai
9 - Measured value, normalized value	Ai
10 - Measured value, normalized value with time tag	Ai
11 - Measured value, scaled value	Ci, Ai
12 - Measured value, scaled value with time tag	Ci, Ai
13 - Measured value, short floating point value	Ai
14 - Measured value, short floating point value with time tag	Ai
15 - Integrated totals	Ci, Ai
16 - Integrated totals with time tag	Ci, Ai
17 - Event of protection equipment with time tag	Ci, Ai, TiR **
18 - Packed start events of protection equipment with time tag	Ci, Ai, TiR ***
20 - Packed single-point information with status change detection	Ci, Ai
21 - Measured value, normalized value without quality descriptor	Ai
30 - Single-point information with time tag CP56Time2a	Di, Qi (On/Off), Ai, Ci
31 - Double-point information with CP56Time2a tag	Qi, Ai, Ci
32 - Step position information with CP56Time2a tag	Ci, Ai *
33 - Bitstring of 32 bits with CP56Time2a tag	Ci, Ai
34 - Measured value, normalized value with CP56Time2a tag	Ai
35 - Measured value, scaled value with CP56Time2a tag	Ci, Ai
36 - Measured value, short floating point value with time tag CP56Time2a	Ai
37 - Integrated totals with time tag CP56Time2a	Ci, Ai
38 - Event of protection equipment with time tag CP56Time2a	Ci, Ai, TiR **
39 - Packed start events of protection equipment with time tag CP56Time2a	Ci, Ai, TiR ***
40 - Packed output circuit information of protection equipment with time tag CP56Time2a	Ci, Ai, TiR ***

**Note:** The individual bites of the byte that inform us on quality (SIQ for ASDU 1,2,30; DIQ for ASDU 3,4,31; QDS for 5..14,20,32..36) are mapped to the flags FLA (0.bit),FLB (1.bit) ..FLH (7.bit).

For example:

**for ASDU 4:** FLA=DPI bit 0, FLB=DPI bit 1, FLC=0, FLD=0, FLE=BL bit, FLF=SB bit, FLG=NT bit,FLH=IV bit.

**for ASDU 16:** FLA..FLE Sequence number bity 0..4, FLF=CY bit, FLG=CA bit, FLH=IV bit

Moreover:

- if a bit is set to IV (Invalid), the value state will be Invalid
- if some of the bits are set to NT (Not topical), SB (Substituted), BL (Blocked), OV (Overflow), CA (Counter adjusted), CY (Counter overflow) for corresponding ASDU types, the value state will be Weak.

\* - T-bit of the value of these ASDUs is in the flag FI, a number within -64 .. +63 is in a variable of Ci/Ai type

\*\* - **ASDU 17** and **38**: SEP byte is in the flags FLA (0.bit),FLB (1.bit) ..FLH (7.bit), following 2 bytes (CP16Time2a) are in a variable of Ci/Ai type as a positive number (0-60 000) or they are in a variable of TiR type as a relative time (0-60 seconds)

The following ASDU types are implemented in the control course (from D2000 system to Sinaut system and vice-versa in balanced mode):

**Table 2**

ASDU type	I/O tag type
45 - Single command	Dout
46 - Double command	Dout, Co
47 - Regulating step command	Dout
48 - Set point command, normalised value	Ao
49 - Set point command, scaled value	Co
50 - Set point command, short floating point value	Ao
51 - Bitstring of 32 bit	Co
58 - Single command with time tag CP56Time2a	Dout
59 - Double command with time tag CP56Time2a	Dout, Co
60 - Regulating step command with time tag CP56Time2a	Dout
61 - Set point command, normalised value with time tag CP56Time2a	Ao
62 - Set point command, scaled value with time tag CP56Time2a	Co
63 - Set point command, short floating point value with time tag CP56Time2a	Ao
64 - Bitstring of 32 bit with time tag CP56Time2a	Co

To set the bites of "status" (SCO for ASDU 45,58; DCO for ASDU 46,59; RCO for ASDU 47,60; QOS for ASDU 48..50,61..63), there are used the flags FLA (0.bit),FLB (1.bit) ..FLH (7.bit) except the bites, which are directly set by the variable value ( SCO bit 0, DCO and RCS bites 0-1). Having received a response (positive/negative), the flags FLA..FLH are set according to the bites of the "status" byte.

When sending commands (ASDU 45-64), the value of 6 [Activation] is used as CauseOfTransmission. Expecting a response from the controlled station depends on the parameter **CMDC**. There are the following possibilities:

- write is successful, if there is a packet with RSN confirming the SSN packet with the log
- write is finished, if there is a response with CauseOfTransmission=7 [Activation Confirmation] and/or 10 [Activation Termination]. Success /Unsuccess depends on the setting of the P/N bite in CauseOfTransmission.

## Redundant communication with Siemens Sinaut system - Basic features:

- One communication line of *CP Redundant* type communicates with two redundant partners Sinaut, where one of them is HOT, the other is STANDBY.
- Communication to each of the partners is performed through two redundant networks (i.e. there are created two TCP connections for each Sinaut, together four TCP connections).
- Sending new values and replying to ASDU 100 [Interrogation Command] is allowed just HOT partner (D2000 eventually Sinaut). Having established the connection, STANDBY partner only sends confirmations (S-frames) and test frames. STANDBY partner may also send ASDU 100 [Interrogation Command].
- Each partner communicates to the other just through one TCP connection. It sends new values, command confirmations, ASDU 1000 and replies to ASDU 100 through the connection. Second connection is standing (except sending test frames through it) and is used when a failure on first connection is detected.

## Establishing connection:

- In the active mode, the process **D2000 KOM** connects to specified TCP ports. It sends to each of the ports an U-frame StartDT Act, and waits for StartDT Con as reply.
- In the passive mode, the process **D2000 KOM** waits on specified TCP port (see the parameters **SP**, **SH**). When the clients are connected, the process waits for an U-frame StartDT Act, and sends StartDT Con as reply.
- Further communication is completely symmetrical one. Both partners can send ASDU 100 [Interrogation Command] in order to read all current values and then the partners receive and sends changed values and commands.

Having established the connection, a partner may send I-frame with ASDU 100 [Interrogation Command] with CauseOfTransmission=6 [Activation] and with ASDUAddress=FFFF, whereby requests the values of I/O tags for all stations. As a replay, the partner waits for:

- receiving an I-frame with ASDU 100 [Interrogation Command] and with CauseOfTransmission= 7 and ASDUAddress=FFFF
- receiving the current values of all I/O tags
- receiving an I-frame with ASDU 100 [Interrogation Command] and with CauseOfTransmission= 10 and ASDUAddress=FFFF

Forced disconnection: If all [communication stations](#) on the line are in the simulation mode or the communication is disabled for them, the [communication line](#) will be disconnected (closing communication sockets). If the simulation mode is not enabled and communication is not disabled for at least one [station](#) (the tab [Parameters](#) of object of [Station](#) type), the line will be reconnected (and Interrogation Command eventually Counter Interrogation Command will be send to the station). Then after enabling each next station, there is send an Interrogation Command or Counter Interrogation Command to the station; see the next point.

Forced sending Interrogation Command or Counter Interrogation Command: If a [station](#) is in the status, that it is not in the simulation mode and the communication is not disabled (the tab [Parameters](#) of object of [Station](#) type), the process [D2000 KOM](#) sends Interrogation Command and/or Counter Interrogation Command (see the parameters [OIC](#), [OCIC](#)).

The protocol IEC870-5-104 Sinaut supports the **balanced mode** described in the communication protocol [IEC 870-5-104](#) - it is server in part, so the rules of [server protocols](#) are valid for it.

## Communication line configuration

- Communication line category: [TCP/IP-TCP Redundant](#)
- TCP parameters:
  - Host: string containing at most 80 characters – two comma-separated server IP addresses in the form of a.b.c.d  
In the active mode, they are the addresses of the server, where the process [D2000 KOM](#) is connecting to.  
In the passive mode (see the parameters [SP](#), [SH](#)), they are the IP addresses of a client, which are accepted by the process [D2000 KOM](#) (if the client is connecting from other IP address, will be disconnected).
  - Port: TCP port number (0...65535)  
In the active mode, it is the server port, where the process [D2000 KOM](#) is connecting to.  
In the passive mode (see the parameters [SP](#), [SH](#)), the parameter will be ignored (but must be set, e.g. to the value of 0).
  - Line number: is used as Originator ASDU address (1 byte, 0-255).

## Communication station configuration

- Communication protocol: [IEC870-TCP Sinaut](#).
- Station address is a decimal number within the range of 0 až 65535, defines the ASDU address.  
For better orientation, station address may be defined in the form of ByteHI,ByteLO, i.e. address **2,1** is the same as **513** ( $2 \cdot 256 + 1$ ). See [a note about ASDU address](#).

**Note:** The protocol supports sending long time stamps (CP56Time2a tag) in local time or UTC time with defined offset (see the parameter [Use monotonic UTC time +](#)).

## Station protocol parameters

[Station configuration](#) dialog box - tab **Protocol parameters**.

They influence some of optional protocol parameters. There can be defined the following station protocol parameters:

**Table 3**

Full name	Meaning	Unit	Default value
Command Confirm	Confirmation of control ASDUs. If CMDC=0, the process <a href="#">D2000 KOM</a> is not waiting for confirmation of control ASDUs from the partner station using backward sending ASDU with other CauseOfTransmission, ASDU is consider to be confirmed when a packet containg corresponding ReceiveSequenceNumber is received. If CMDC=1, the process <a href="#">D2000 KOM</a> is waiting for confirmation with CauseOfTransmission=7 (Activation Confirmation). If CMDC=2, the process <a href="#">D2000 KOM</a> is waiting for confirmation with CauseOfTransmission=10 (Activation Termination). If CMDC=3, the process <a href="#">D2000 KOM</a> is waiting for confirmation with CauseOfTransmission=7 or 10 (if both of them are received, just the first of them is taken into account). Having received the corresponding confirmation means that writing is finished (the <i>Transient</i> attribute of written value is evaluated and the WtN timeout stops elapsing). If there is received confirmation with other CauseOfTransmission as the process <a href="#">D2000 KOM</a> expect for, it will be ignored. Writing is successful if received ASDU contains the P/N bit set to 0. Otherwise, writing is unsuccessful. The value from a received ASDU is backwardly written into the corresponding I/O tag and is sent to the system. E.g. if an ASDU of type 50 (short floating point) with the value of 1200.0 is sent and the partner station sends an ASDU of type 50 as reply, P/N bit=0, value of 999.0 (e.g. due to physical limitations of the given parameter), the the value is to be send by the process <a href="#">D2000 KOM</a> to the system.	-	3
Debug Input	It is a mask for a debug level of the input data. A meaning of the bits: <ul style="list-style-type: none"> <li>• 1. bit - number of points received within General Interrogation</li> <li>• 2. bit - a received values of I/O tags</li> <li>• 3. bit - balanced mode: Interrogation command was received</li> </ul>	0 .. 255	0
Debug Output	It is a mask for a debug level of the output data. A meaning of the bits: <ul style="list-style-type: none"> <li>• 1.bit - balanced mode: a number of points sent within General Interrogation</li> <li>• 2.bit - it shows a sent values of I/O tags</li> </ul>	0 .. 255	0

ICCP compatible flags	It allows a flag mapping which is compatible to Sinaut Spectrum <a href="#">ICCP OPC communication</a> . For more information see <a href="#">ICCP compatible flag mapping</a> .	YES /NO	NO
Ignore Unknown Addresses	If IUA=TRUE, the process <a href="#">D2000 KOM</a> will not show an error on its console or write it into log files in case that incoming value has the address not matching any of the addresses of I/O tags defined in the D2000 system.	-	False
Interrogation Covers Counter Interrogation	As a reply to Interrogation, there are also sending ASDU 15,16,37 (Integrated Totals), which are standard requested by ASDU 101 [Counter Interrogation].	-	True
K (max outstanding I APDUs)	Sending window size i.e. packet quantity, which is sent by the process <a href="#">D2000 KOM</a> without receiving a confirmation (S-frame or I-frame). According to the standard, the default value is 12.	-	12
No Flags	If the parameter is True, then the status bit of incoming ASDUs is ignored and not saved into the flags FA...FH. Flags of output I/O tags are also ignored and they not set the status bit.	-	False
Order of IC	Order for sending ASDU 100 [Interrogation Command] when the station initializes to communicate or when creating a new station. If OIC<OCIC, ASDU 100 will be send before ASDU 101. If OIC=0, ASDU 100 will not be sent. The parameter can be set extra for each station.	-	1
Order of Counter IC	Order of sending ASDU 101 [Counter Interrogation Command] when initializing the connection. OCIC<OIC, ASDU 101 will be sent before ASDU 100. If OCIC=0, ASDU 101 will not be sent. The parameter can be set extra for each station.	-	0
Ping Count	Number of repetitions, after which the IP address not responding to ping is to be known as non-functional. See the parameter PTO.	-	3
Ping TimeOut	If the parameter is other than zero, then defines the timeout (in milliseconds) of server response for ping (ICMP echo) packet. In the background, the process <a href="#">D2000 KOM</a> sends ping packets to all defined IP addresses. If some of the addresses does not respond for PCNT-times, it is designated as non-functional and connection is terminated. If the parameter PTO= 0, sending ping packet to IP addresses is disabled.	-	0
Post Start Delay	When initializing the connection, delay between receiving StartDT Con response and sending Interrogation Command and/or Counter Interrogation Command.	ms	0
Send Ssequence Number	Initial SSN. According to the standard, after establishing the connection the SSN is set to 0, other than zero could be appropriate e.g. for testing.	-	0
Server Port, Server Host	The port number and IP address of the interface, where the process <a href="#">D2000 KOM</a> is to be listening. If both the parameters are defined, the process <a href="#">D2000 KOM</a> is working as passive (is waiting for connecting Sinaut clients). If the process should listen on all network interfaces, there must be set <i>SH=ALL</i> .	-	
Standby Keep Open	If True, after changing the status of process <a href="#">D2000 Server</a> (the process <a href="#">D2000 KOM</a> is connected to) from Hot into Standby state (redundant system), connection with partner will not be closed.	-	True
Station Communication Error	Number of unsuccessful attempts to connect after communication breakdown. The station status is changed into the state St_CommErr after reaching the number. For redundant lines, the communication must be either failed for both TCP connections or a TCP connection with standby-server must be functioning (see the parameters ICF3 and IT), i.e. data from the server are ignored.	-	2
Station Hard Error	Number of unsuccessful attempts to connect after communication breakdown. The station status is changed into the state St_HardErr after reaching the number. For redundant lines, communication must be either failed for both TCP connections or working a TCP connection with standby-server must be functioning (see the parameters ICF3 and IT), i.e. data from the server are ignored.	-	5
Strict Redundancy Connection Signalisation	Number of TCP connections, which must be opened so that the line could be considered as OK. There are 4 connections (2x Sinaut, each of them has 2 network addresses).	-	4
Tcp Keep Init	The parameter is implemented for use on OpenVMS platforms only. If it is other than zero, then defines the timeout (in seconds) for opening a new connection to server. For OpenVMS, the default value is 75 seconds, for Windows it is 20 seconds.	-	0
TCP NoDelay	TND parameter sets a low-level parameter of TCP_NODELAY sockets which switch off a default packet linking.		
W (ack after receiving W APDUs)	Quantity of received packets, after which the process <a href="#">D2000 KOM</a> sends an S-frame confirmation. According to the standard, the default value is 8. There must be true $W < K$ , the standard recommends $W = 2/3 * K$ .	-	8
Wait Timeout T1	Timeout for receiving the confirmation of a I-frame sent (either the confirmation within the I-frame or the S-frame itself) or a U-frame. If the process <a href="#">D2000 KOM</a> does not get the confirmation in the time WT1, it closes the TCP connection. According to the standard, the WT1 default value is 15000 ms.	ms	15 000

Wait Timeout T2	Timeout for sending the confirmation of a I-frame received. WT2 < WT1. If another I-frame (which confirms the I-frame received) is not sent in the time WT2 since the I-frame was received, so the process <b>D2000 KOM</b> sends an S-frame confirming the received I-frame to the partner. According to the standard, the WT2 default value is 10000 ms.	ms	10 000
Wait Timeout T3	Timeout for sending test frames (U-frame TEST ACT). If no data are sent in any direction for a long time, an U-frame TEST ACT will be sent to the process <b>D2000 KOM</b> after expiration of the WT3 time and there is expected (in the WT1 time after sending) receiving a U-frame TEST CON. If the WT3 on the partner side is set to a lower value, it sends the test frames and the process <b>D2000 KOM</b> replies to them. According to the standard, the WT2 default value is 20000 ms. Setting the value to 0 disables sending test frames.	ms	20 000
Wait Timeout N	Timeout for receiving the confirmation of a value sent. Receiving e.g. S-frame with RSN (Receive Sequence Number) confirming, that the other party received previous I-frame doesn't mean, that the I-frame was processed. In the WTn time, the process <b>D2000 KOM</b> waits for receiving the response (e.g. after sending ASDU with TypelIdentifier=45 [Single Command] with CauseOfTransmission=6 [Activation] there is expected receiving Single Command with CauseOfTransmission=7 [Activation Confirmation]. After the expiration of the WTn time, the process <b>D2000 KOM</b> closes the TCP connection.	ms	60 000

The defined parameters, except for [Order of IC](#) and [Order of Counter IC](#), are valid for the entire line, i.e. they can be set only for one station on the line.

### ICCP compatible flag mapping

A status byte of ASDU, unlike [ICCP OPC](#) communication, enables the transmission only limited group of flags. In Table 4 you can see a conversion of bits of the status byte to the flags which are compatible with ICCP OPC communication.

**Table 4**

Bits of status byte					Description	ICCP OPC mapping
8 [IV invalid]	7 [NT non topical]	6 [SB substituted]	5 [BL blocked]	1 [OV overflow]		
1	x	x	x	x	INVALID	FH (NotValid)
0	x	0	0	x	VALID	FA (Actual)
0	x	0	1	x	BLOCKED	FD (Blocked)
0	x	1	0	x	SUBSTITUTED	FC (Entered)
0	x	1	1	x	SUBSTITUTED + BLOCKED	FF (Blocked Manual)

## IO tag configuration

Permitted I/O tag types: **Ai, Ao, Ci, Co, Di, Dout, Qi**

- I/O tag address is mapped to Information object address, i.e. contains 3 bytes and must be within the interval of 0...16777215. For better orientation, I/O tag address may be defined in the form of ByteHI,ByteMIDDLE,ByteLO, i.e. address **1,2,3** is the same as **66051** ( $1 \cdot 256 \cdot 256 + 2 \cdot 256 + 3$ ). See [a note about IOA address](#).
- Input I/O tags must have corresponding types (Ai, Ci, Di, Qi) for received ASDU, see the [table 1](#).
- For particular type of output I/O tag (Ao, Dout, Co), it is necessary to set an type of ASDU that should be used, see the [table 1](#) and [table 2](#).
- It is possible to configure one input I/O tag and more output I/O tags on the same address, while the output I/O tags have different ASDUs.

Example:

- I/O tag M1, Di type, address 1,
- I/O tag M2, Dout type, address 1, ASDU 1 (single-point information)
- I/O tag M3, Dout type, address 1, ASDU 45 (single command)

Configuration on partner's side:

- I/O tag P1, Dout type, address 1, ASDU 1 (single-point information)
- I/O tag P2, Di type, address 1

Writing into the I/O tag P1 from the partner's side gives a new value to the I/O tagM1. Writings of the I/O tags M2, M3 gives a new value to the I/O tag P2on the partner's side.

## Literature

-

## Document revisions

- Ver. 1.0 – December 15th, 2004
- Ver. 1.1 – February 21st, 2011



**Related pages:**

[Communication protocols](#)