Siemens-PU (AS511)

Table of Contents

5.1 Siemens PU 5.1-3
5.1.1 General Information 5.1-3
5.1.2 Technical Description 5.1-4
5.1.3 Protocol Parameters Siemens PU 5.1-4
5.1.3.1 Interface Parameters of the PLC 5.1-5
5.1.3.2 Parameter Maximum Waiting Time for Response 5.1-5
5.1.3.3 Parameter Delay Until Connection Setup 5.1-5
5.1.3.4 Parameter Fast Data Block Access 5.1-5
5.1.4 Data Type Structure 5.1-5
5.1.4.1 Data Types 5.1-7
5.1.4.2 Special Simatic Data Formats 5.1-8
5.1.5 Data Block Cache within the Siemens PU Protocol 5.1-8
5.1.6 Additional Functions 5.1-9
5.1.7 Physical Interfacing 5.1-11
5.1.7.1 Connecting Cable TTY / 20 mA - Siemens PU 5.1-12
5.1.7.2 Connecting Cable Universal Interface SER1 TTY / 20 mA - Siemens PU 5.1-13
5.1.8 Error Messages 5.1-14
5.1.9 Guidance for the Employment of CPUs with 2 PU Interfaces 5.1-15

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

Siemens-PU (AS511)

Siemens-PU (AS511)

5.1 Siemens PU

5.1.1 General Information

The operating terminals can be conveniently connected to the Siemens PLCs S90 - S155 thus making the operating terminals the perfect man-machine-interface for your Siemens PLC.
The operating terminal is connected to the PU (programming unit) interface of the PLC. An additional communications module is not necessary. The data communication on the interface is handled by the PU protocol AS511.
Connections to the following Simatic S5 PLC types are supported:

SIMATIC S5-90U (8-bit CPU)
SIMATIC S5-95U (8-bit CPU)
SIMATIC S5-100U
CPU 100 (8-bit CPU)
CPU 102 (8-bit CPU)
CPU 103 (8-bit CPU)
SIMATIC S5-115U
CPU 941 (8-bit CPU)
CPU 942 (8-bit CPU)
CPU 943 (8-bit CPU)
CPU 944 (8-bit CPU)
CPU 945 (8-bit CPU with 20-bit address range)
SIMATIC S5-135U
CPU 922 (16-bit CPU)
CPU 928 (16-bit CPU)
CPU 928B (16-bit CPU)
SIMATIC S5-155U
CPU 948 (20-bit CPU)

Connection to the following Simatic S5 PLC type is **not supported**:

SIMATIC S5-135U
CPU 921 (16-bit CPU)

The software components of the system are fully adapted to the parameters and marginal conditions of the PU interface.

This offers the user the following advantages:

– Random read and write access to all data within the PLC. Data from existing PLC programs can be displayed and modified directly on the operating terminal. Since the communication data do not need to be stored in a specified address area or data type area, it is not necessary to adapt the PLC program to the operating terminal in any respect.

– The operating terminal automatically polls the freely definable data areas for cyclic data.

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

- Use of a PU multiplexer allows simultaneous connection of the operating terminal and Siemens programming unit (PU).

- No configuration required within the PLC.

- The PU protocol is handled entirely by the firmware of the PLC. A PLC program (function blocks, etc.) in the PLC is not required to handle the communication.

- The protocol provides error control. Transmission errors are detected and, if possible, eliminated by repeating the transmission. An electrically isolated, noise-immune interface hardware in accordance with the 20 mA current loop interface standard permits the application even in a harsh industrial environment.

- The parameters of the interface SER1 are assigned in the programming software in a protocol-specific manner and are stored in the application description. The parameters can also be modified in the setup mask or any other I/O mask of the terminal.

- The programming system provides a maximum of support to the operator in programming the operating terminal. The definitions (abbreviations) used here are identical with the definitions used within the PLC program.

5.1.2 Technical Description

The PU protocol is used to connect the operating terminal to the Siemens PLCs.
The PU protocol AS511 allows random read and write access to all PLC data. Any byte-structured data types can also be accessed in bit-mode. The size of the address area depends on the respective PLC.

Access to the individual bytes of a data word within a data block is also possible.

A read access must be performed before individual bits or bytes of a data word within a data block can be accessed for a write operation. Subsequently, a write access is possible to the entire data structure. When accessing individual bits or bytes, special care needs to be taken to ensure that neither the terminal nor the PLC modify individual bits within one byte (or individual bits within one data word, respectively).

5.1.3 Protocol Parameters Siemens PU

To ensure proper communication, the parameters must **not** be altered.

Baud rate: 300, 600, 1200, 2400, 4800, **9600**, 19200, 38400, 375000, 500000 Baud
Parity: none, **even**, odd
Data bits: 5, 6, 7, **8**
Stop bits: 1, 1.5, **2**
Handshake: **no handshake**, Hardware, Software

The default settings are printed in **bold**.

5.1.3.1 Interface Parameters of the PLC

The operating terminal adapts to the default parameters of the PU interface. It is therefore **not** necessary to modify the interface parameters in the PLC. This allows communication between the operating terminal and Siemens PLC without requiring any configuration.

5.1.3.2 Parameter Maximum Waiting Time for Response

This timer indicates the length of time that the operating terminal (master) waits for the response from the PLC (slave).
Permitted values are in the range of 0 ms to 65535 ms.
The default value is 500 ms.

This value must be increased when using a CPU with two PU interfaces (see „Guidance for the employment of CPUs with 2 PU interfaces“).

5.1.3.3 Parameter Delay Until Connection Setup

Specifies the period of time that the terminal allows to elapse after an unsuccessful attempt to establish the connection and before making another attempt.
Permitted values are in the range of 0 ms to 65535 ms.
The default value is 10000 ms.

5.1.3.4 Parameter Fast Data Block Access

The base address for each data block being used is determined only once and this information is stored temporarily in a local buffer with 10 positions. Any subsequent accesses continue to operate with the information stored in the local buffer. The information in the buffer is erased upon restarting the terminal or upon a resynchronization after a communication error.

Important:
In this case, do not modify the size of data blocks or compress the PLC memory while the connection between the terminal and the PLC is still being established!
If a terminal and a programming unit are simultaneously connected to the PLC by means of a multiplexer, then any value of the data block that is altered via the programming unit and transferred into the PLC, also results in a change of the address location of the data block. In this case, the cache should be deactivated.

5.1.4 Data Type Structure

a) Alphanumerical Texts
Are stored in the memory byte for byte in ascending address order.

b) Counter
A distinction is made between variables which have been assigned a counter address and variables which have been assigned another PLC address.

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

Counter address
When accessing counter addresses, the count value is interpreted in the binary format and the control bits of the counter are masked out. Therefore, to avoid control bits from being erased, counter addresses should be accessed in the **read-mode** only.

All other addresses
The count value is interpreted in BCD-code. This allows transfer of this value within the PLC program to the counter by means of the accumulator. This service should be used for indirect write-operations of count values since the values are available in the Siemens conforming format.

c) Timer
Timer functions consist of a time value and a time base. The terminal operates with imaginary unsigned 4-byte variables even though the data stored in the PLC comprise only 2 bytes.

When read-accessing timers, the terminal converts the time value and time base into a terminal-internal unsigned 4-byte variable which represents the time value in reference to the time base of 0.01 second.

Example : A range of 10 (time base is 1.0 second) and a time value of 999 are represented or edited in the terminal by the value 99900. Scaling of this value to other value ranges is possible by specifying a factor and divisor within the variable definition.

Before writing a timer variable to the PLC, a terminal-internal unsigned 4-byte value is converted to a time value and the smallest possible time base.
In addition, a distinction is made between variables which have been assigned a timer address or another PLC address.

Timer address
When accessing timer addresses, the time value is interpreted in binary format. To avoid timer control bits from being erased, this service should be used in the **read-mode** only.

All other addresses
The time value is interpreted BCD-coded. Because the values are available in the Siemens conforming format, this service should be used for indirect write-operations of time values.

d) Floating Point Number
The data are interpreted in the Siemens floating point format.

e) Binary Variables with a Length of 1, 2 or 4 Bytes
Data with a length of 2 bytes are interpreted in the PLC-conforming byte order for words.
Data with a length of 4 bytes are interpreted in the PLC-conforming byte order for long words.

5.1.4.1 Data Types

Direct accessing of the following data types is possible:

Type	Description	Access
E	Input Bits	Bit Access, Read Only
A	Output Bits	Bit Access
M	Flag Bits	Bit Access
EB	Input Bytes	Byte Access, Read Only
AB	Output Bytes	Byte Access
MB	Flag Bytes	Byte Access
EW	Input Word	Word Access, Read Only
AW	Output Word	Word Access
MW	Flag Word	Word Access
ED	Input Double Word	Double Word Access, Read Only
AD	Output Double Word	Double Word Access
MD	Flag Double Word	Double Word Access
DW	Data Word	Word Access
DL	Data Word, Left-hand (High)	Word Access
DR	Data Word, Right-hand (Low)	Word Access
DD	Data Double Word	Double Word Access
T	Timer	Word Access, Read Only
Z	Counter	Word Access, Read Only

Table 5.1-1: Data types

The size of each data area depends on the CPU of the PLC.

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

5.1.4.2 Special Simatic Data Formats

The following data formats are supported in the editors:

KB 0 to 255
Variable in byte format

KF -32768 to +32767
Variable in 16-bit fixed point number format

KH 0000 to FFFF
Variable in 4-digit hexadecimal number format

DH 00000000 to FFFFFFFF
Variable in 8-digit hexadecimal number format

KC !! to zz (2 ASCII-characters each)
Variable represented by 2 characters in ASCII format

KT 000.0 to 999.3
Variable represented as a time value

KZ 000 to 999
Variable represented as a count value

KG ±1.2*10-38 to .±3.4*10+38
Variable in 32-bit floating point number format

KM 00000000 00000000 to 11111111 11111111
Variable in bit pattern format

5.1.5 Data Block Cache within the Siemens PU Protocol

Data blocks are not stored in a fixed address area, unlike other data types (e.g. flags).

In order to access the data of these data blocks, it is necessary to determine their current base address.

a) Data block cache is inactive
Prior to every access to a data block, the current base address of this data block is determined. This reduces the access speed to data, however, ensures that the address is updated if a change has occured.

b) Data block cache is active
The base address for each data block being used, is determined only once and this information is stored temporarily in a local buffer with 10 positions. Any following accesses continue to operate with the information stored in the local buffer. The information in the buffer is erased upon restarting the terminal or upon a resynchronization after a communications error.

Please note carefully:
In this case, do not modify the size of data blocks or compress the PLC memory while the communication between the terminal and the PLC is still in process!

If a terminal and a programming unit are simultaneously connected to the PLC by means of a multiplexer, then any value of the data block that is altered via the programming unit and transferred into the PLC, also results in a change of the adress location of the data block. In this case as well, the cache should be deactivated.

5.1.6 Additional Functions

In addition to the random read and write access to PLC variables, a 11-byte memory area is specified in the application description as a poll area. The location of this memory area can also be specified in the application description.

The only marginal conditions regarding this memory area is that the PLC must be able to access in bit-mode and the terminal in byte-mode and the memory area must be contiguous.

Access modes of the PLC to the poll area are:

Byte-structured Memory Mapping
The maximum size for the data area is 11 bytes.
Example:
The cyclic poll area is set to flag byte (MB) 12 in the programming system.

Byte Address	Reference	Description
Byte Address + 0	MB12	Write Coordination Byte
Byte Address + 1	MB13	Message Channel High Byte
Byte Address + 2	MB14	Message Channel Low Byte
Byte Address + 3	MB15	Function Keys LED 1 to 4
Byte Address + 4	MB16	Function Keys LED 5 to 8
Byte Address + 5	MB17	Function Keys LED 9 to 12
Byte Address + 6	MB18	Function Keys LED 13 to 16
Byte Address + 7	MB19	Function Keys LED 17 to 20
Byte Address + 8	MB20	Function Keys LED 21 to 24
Byte Address + 9	MB21	Function Keys LED 25 to 28
Byte Address + 10	MB22	Function Keys LED 29 to 32

Table 5.1-2: Byte-structured poll area

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

Word-structured Memory Mapping
The maximum size for the data area is 6 words or 12 bytes.
Example:
The cyclic data area is set to DW21 in the programming system.

Word Address	Reference	High Byte	Low Byte
Word Address + 0	DW21	Write Coordination Byte	Reserved
Word Address + 1	DW22	Message Channel High Byte	Message Channel Low Byte
Word Address + 2	DW23	Function Keys LED 1 to 4	Function Keys LED 5 to 8
Word Address + 3	DW24	Function Keys LED 9 to 12	Function Keys LED 13 to 16
Word Address + 4	DW25	Function Keys LED 17 to 20	Function Keys LED 21 to 24
Word Address + 5	DW26	Function Keys LED 25 to 28	Function Keys LED 29 to 32

Table 5.1-3: Word-structured poll area

5.1.7 Physical Interfacing

Pin	Designation	Function
1	Shield	Shielding
2	T+	Transmit Data, Positive Polarity
3	S1+	Power Source 1, Positive Polarity
4	R+	Receive Data, Positive Polarity
5	S2+	Power Source 2, Positive Polarity
6	T-	Transmit Data, Negative Polarity
7	S1-	Power Source 1, Negative Polarity
8	R-	Receive Data, Negative Polarity
9	S2-	Power Source 2, Negative Polarity

Table 5.1-4: Pin assignment X2 TTY / 20 mA

Pin	Designation	Function
10	T+	Transmit Data, Positive Polarity
12	S1+	Power Source 1, Positive Polarity
13	R+	Receive Data, Positive Polarity
14	R-	Receive Data, Negative Polarity
16	S2+	Power Source 2, Positive Polarity
19	T-	Transmit Data, Negative Polarity
21	S1-	Power Source 1, Negative Polarity
24	S2-	Power Source 2, Negative Polarity

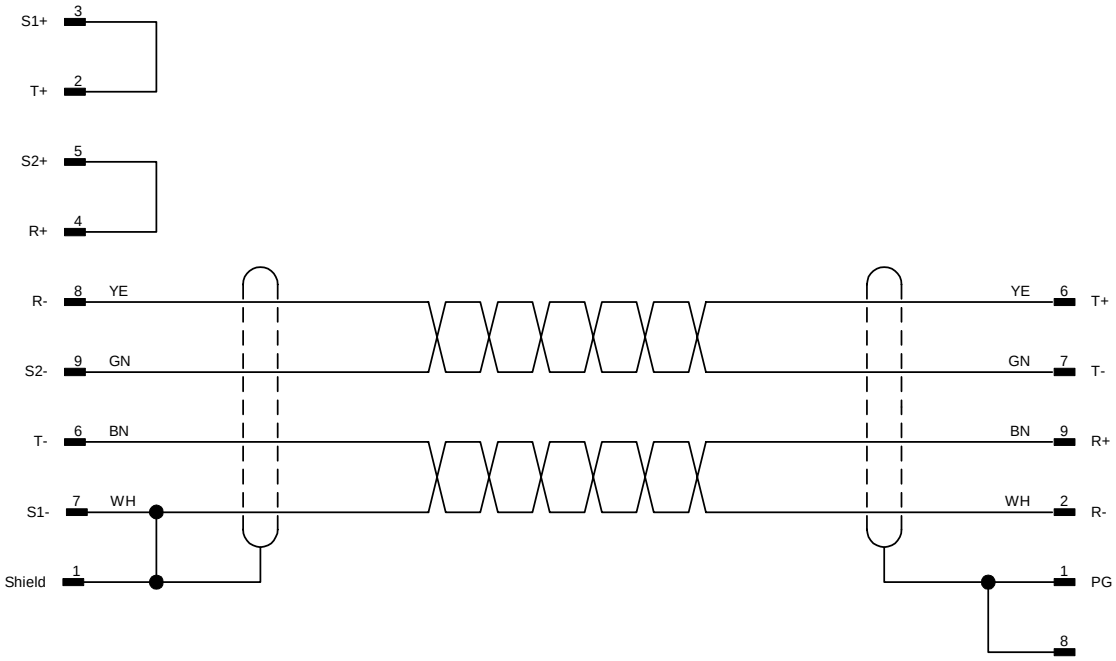
Table 5.1-5: Pin assignment universal interface SER1 TTY / 20 mA

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

5.1.7.1 Connecting Cable TTY / 20 mA - Siemens PU

The following wiring diagram does not apply to terminals with universal interface.

TesiMod	Siemens
Operating Terminal	Simatic S5 - PU Interface
Transmitter active	Transmitter passive
Receiver active	Receiver passive



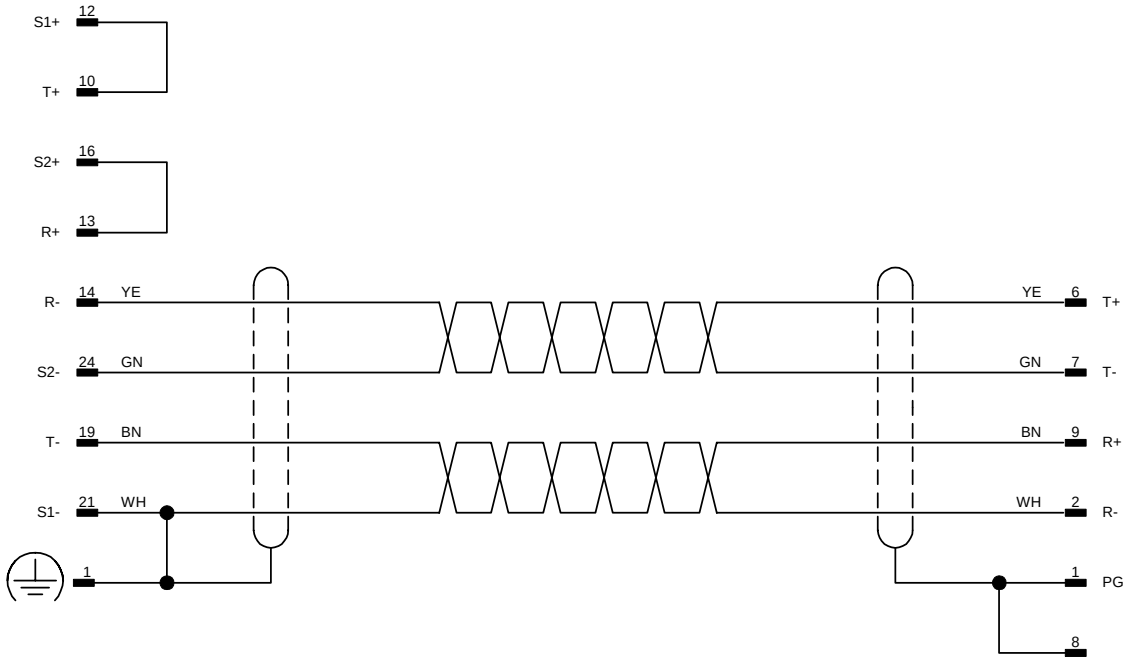
D-Subminiature	D-Subminiature
Male Connector	Male Connector
9-pin	15-pin

Each end of the shield is connected to the metallic enclosure.

5.1.7.2 Connecting Cable Universal Interface SER1 TTY / 20 mA - Siemens PU

The following wiring diagram applies to operating terminals with universal interface only.

TesiMod	Siemens
Operating Terminal	Simatic S5 - PU Interface
Transmitter active	Transmitter passive
Receiver active	Receiver passive



D-Subminiature	D-Subminiature
Male Connector	Male Connector
25-pin	15-pin

Each end of the shield is connected to the metallic enclosure.

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

5.1.8 Error Messages

Code	1	E_SLAVE_NOT_READY	Slave not ready
	2	E_PROTOKOL	Sequence of the packets
	3	E_FRAME	Protocol frame error
	4	E_TIMEOUT	Timeout error
	6	E_PARITY	Parity error
	7	E_SEND_ABORT	Send process aborted
	8	E_REC_ABORT	Receive process aborted
	9	E_BUF_SIZE	Insufficient cyclic buffer
	10	E_NO_DEFINE	No cyclic data defined
	12	E_DEFINE	Cyclic data already defined
	15	E_NO_PROTOCOL	Selected protocol is not supported
	16	E_OVERRUN	Receive buffer overrun
	17	E_NAK	NAK from PLC despite repetition
	40	E_SYS_ADDRESS	Undefined system variable

Siemens-specific error messages:

50	E_BST_RANGE	Address outside of the range of the data block. The subcode indicates the number of the data block.
51	E_RECEIVE_COUNT	Wrong number of received data.
52	E_FUN_NOT_KNOWN	Unknown function.
53	E_WRONG_MODE	Wrong mode of operation.
54	E_DATA_BLOCK_NOT_KNOWN	Data block does not exist. The subcode indicates the number of the data block.
55	E_HIGH_LEVEL	Communication has reached higher level.
56	E_LOW_LEVEL	Communication has reached lower level.
57	E_MESSAGE_CONNECT	Invalid feedback received from the PLC during the connection setup phase. The subcode indicates the received data character.
58	E_MESSAGE_TRANSFER	Invalid feedback received from the PLC during the transfer phase. The subcode indicates the received data character.

59	E_MESSAGE_DISCONNECT	Invalid feedback received from the PLC during the disconnect phase. The subcode indicates the received data character.
60	E_CPU_TYP_921	A CPU of the type 921 has been detected. The operating terminal does not support this CPU type.
61	E_WRONG_ADDR	Wrong addressing used for job. The requested address level is not fully available.

5.1.9 Guidance for the Employment of CPUs with 2 PU Interfaces

CPUs with 2 PU interfaces (e.g. 928B with PU module) are used during system commissioning thus keeping the PU interface available for program debugging.

Please note that the interfaces are interacting (see Siemens CPU manual). For example, if a PLC program is analysed by means of the STATUS-function on the first interface of the CPU, this will cause the speed of protocol handling on the second interface to decrease significantly. With the STATUS-function, the PLC program can, so to speak, be operated in the single-step-mode, i.e. the result of every program line is displayed on the screen.

In order to maintain the connection, the timeout period must be increased to 5 seconds. Using the regular timeout period results in the terminal generating a communication error message.

In this case, each transmission requires 3-4 seconds, in contrast to a regular communication cycle which requires approximately 60 ms. This means a slow-down of the interface by a factor of 50!

/000-0322/ © Copyright by Sütron electronic GmbH
TESI_T_eng_V20.3005010QK0

Siemens-PU (AS511)