SIEMENS

SIMATIC S5

Special Driver for CP 521 BASIC / SI

Adaptation MODBUS Protocol RTU-Format

S5 is Slave

Operating Instructions

Part No. for Special Driver Submodule and S5-Function Blocks:
6ES5 897 - 8QA01

Version	Submodule:	02
	S5-FB's:	02

Index

1. General Comments

The Special Driver Submodule for the Communications Processor CP521 BASIC/SI creates a data link between "modbus capable" control systems (e.g. Modicon-controllers or Honeywell TDC 3000) and U Series SIMATIC S5-devices (95U, 100U with CPU 103).
The used transmission protocol is GOULD - MODICON - MODBUS with **RTU-Format** . Data transmission is carried out following the Master-Slave-Principle. The **Master** has the initiative during the transmission, the CP521 operates as the Slave.
Function Codes 01, 03, 04, 05, 06, 08 and 16 can be used for communication between the CP and the host system.
In the S5, data can be read from data blocks, flags, inputs, outputs, counters and timers. Data can be written to data blocks, flags, inputs, outputs, counters and timers. In all instances the address information from the master is interpreted in an "S5 manner". The structure of the address field may be found in the description for the function codes, Chapter 6.

> Any warranty obligation is forfeited in the event of any manipulation carried out to the submodule or to the function blocks.
> No compensation will be granted for subsequent damages.

1.1. Parameter Assignment of the Special Driver

Please find below a list of parameters and operating modes for the special driver which may be set by the user:

- Slave Address of the CP
- Operating Mode (Normal, Modem)
- DB-Number for Work-DB
- with/without Error Code 06
- Multiplication Factor for the Character Delay Time
- Baudrate, Parity and Interface
- Waiting Times when using V24-Auxiliary Signals

1.2. Special Features CP521 BASIC

The RUN/PRG switch has no influence on the program.

The RxD and TxD-LED functions are reversed, i.e. TxD-LED lights in the middle during reception, during transmission RxD-LED lights at the top.

1.3. Versions Special Driver and S5-Function Blocks

The version of the S5 function blocks can be identified by means of the Directory Number. For Output Status 02 the function blocks must have the following Directory Numbers:

FB 220, 221	20065
FB 222, 224, 225, 226, 229	13045

The version number of the special driver submodule can be found on the submodule itself. Providing it has not been running on a back-up battery it will also appear on initial start up of the CP, as date and time.

Date	:	Date generated, e.g. 29.06.95
Time	:	Hour contains Version number e.g. 02.

After starting the CP, the clock continues with the specified values.

2. Commissioning

The supplied memory submodule contains the special driver which realises the MODBUS-protocol. Plug it into the appropriate slot on the CP521 BASIC or CP521 SI. Please ascertain that the CP is in MAINS OFF status.

> Once the memory submodule complete with special driver has been inserted in CP521, all standard protocols are inoperative and the CP can only run with the MODBUS protocol.

The supplied floppy disk contains the following directories and files:
\MANUAL\ENGLISH\S5S8QA02.DOC
➨ Operating Instructions for Special Driver
\STEP_5\ENGLISH\S5S8QAST.S5D
➨ Function Blocks and Sample Program

Copy the S5 Program S5S8QAST.S5D to a programming unit which had the S5 package already installed. The following pages explain how to proceed from here.

Hardware-Pre-requisites:

The function blocks can only be used on the SIMATIC PLC95U and on the CPU103 of PLC100U. The CPU-Type is read from the system data of the PLC.

3. Physical Interface

The procedure is asynchronous, half duplex, code transparent und can run on a 20mA (TTY, line current)-or V24(RS232) interface.

Connect the serial interface of CP521 to that of the link partner. Assignment values for the CP521 interface can be found in the

CP521 SI Manual
6ES5 998-1UD21
Para. 2.3.

The procedure parameters are preset with 8 data bits and 1 stop bit. Parity and baud rate may be parameterised in accordance with the system configuration.

4. Function Blocks in PLC

4.1. General

In addition to the CP521 SI/BASIC, communication between a MODBUS-Master and a SIMATIC-PLC also requires S5-blocks in the PLC. The S5S8QAST.S5D file contains the necessary function blocks (FB's). They are also called in the sample-PB's and OB's..

Organsation blocks OB1, OB21 and OB22, as well as program blocks PB220 and PB221 have been added as examples - they may be changed as required.

In order to test the data link carry out an overall reset of the PLC followed by a transfer of the entire file into the PLC.

For general information on function blocks please refer to the S5 file in the #READ.ME doc file.

4.2. SIMATIC-Blocks

Organisation Blocks

OB1	Cyclic Program		1)
OB21	Cold Re-Start		1)
OB22	Warm Re-Start		1)

Program Blocks

PB220	Initial Start	Call only in OB21,OB22	1)
PB221	Cyclic Program	Call only in OB1	1)

Function Blocks

FB220	Initial Start	Call in OB21,OB22 (PB220)
FB221	Cyclic Program	Call in OB1 (PB221)
FB222	Read Bits	Call in FB221
FB224	Read Words/Registers	Call in FB221
FB225	Write Bits	Call in FB221
FB226	Write Words/Registers	Call in FB221

FB229	PAE/PAA-Trace		Call in OB1 (PB221)	2)

Data Blocks

DB220	Work-DB Modbus	A-DB	DB3...DB255	3)
DB229	Trace-DB	PAEA	DB3...DB255	3)

Flags

The FB's use flag area FY240 to FY255 as scratch flags. Therefore this area is not available for "Fixed Flags".

The following must be noted during **alarm processing**:

- If flags from the area FY240 to FY255 are being used during alarm processing, these flags must be saved at the start of the alarm processing and be re-loaded at the end of alarm processing.
- Accesses to CP521 from the alarm program are not allowed.

Timers

Timers are not used in the FB's. The only exception being the timer used during parameter assignment of FB220 for monitoring of initialisation.

Counters

The blocks do not use counters.

Notes:

1) The OB's and PB's are only added as examples - these blocks may be changed as required.
2) FB229 and DB PAEA are required only for diagnostic purposes. FB229 is used to protocol data traffic between the CP and CPU in DB PAEA.
3) The data blocks may be parameterised in the area from DB3 to DB255.

4.3. Parameter Assignment of Initialisation FB FB220

FB220 may only be called in the Initialisation OB's (OB21, OB22). Prior to calling FB220 it is essential to create the Work-DB with a minimum length of 140 DW. If the DB does not exist, or if it is too short, the PLC reverts to stop in FB220.

FB220 reads the CPU Identifier from the system area. If in this instance neither "CPU103" nor "PLC95" is read, the following error message appears: "Illegal CPU".
Otherwise the memory addresses and the initialisation parameter blocks are now entered into the Work DB and the monitoring time is started.

Parameter Assignment FB220

Parameter	Format	Meaning	
ST/T	KY	CP-Slot, Monitoring Time INIT	
T-AN	KT	Value Monitoring Time	
BITS	KM	INIT-Bits	
DB,R	KY	Work-DB, Reserved (=0)	
S,ZV	KY	Slave-Address, Factor Character Delay Time	
F:VB	KY	Enable Flags:	from, to
I:VB	KY	Enable Inputs:	from, to
Q:VB	KY	Enable Outputs:	from, to
T:VB	KY	Enable Timers:	from, to
C:VB	KY	Enable Counters:	from, to
D:VB	KY	Enable Data:	from, to
T1	KF	Send Delay	10 ms Intervals
T2	KF	ON Delay	10 ms Intervals
T3	KF	OFF Delay	10 ms Intervals

4.3.1. CP-Slot

Indicates the slot for CP521. Values 0 (direcly next to the CPU) to 7 are allowed.

4.3.2. Monitoring Time for Initialisation

A free time must be specified here. It is used to monitor the initialisation of the CP. Timers 0 to 127 are allowed.

4.3.3. Value Monitoring Time

Indicates the time value to monitor initialisation of the CP.   If this time is exceeded , the following error message appears in DW16 of the work-DB: "Monitoring Time CP-Start-Up Exceeded".

4.3.4. INIT-Bits

The INIT-Bits are used to parameterise the interface of the CP. The bits are assigned as follows (the Default-setting of the program example is printed in bold):

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
SS	F6	PE	P	B3	B2	B1	B0	AT	R	R	R	M3	M2	M1	M0

SS	Interface	1:	**Use V24 Interface**
		0:	Use TTY Interface
F6	Error Code 06	1:	**with Error Code 06 Output**
		0:	without Error Code 06 Output
PE	Parity-Enable	1:	**Parity Check is enabled**
		0:	do not carry out parity check / do not generate parity bit
P	Parity	1:	uneven parity
		0:	**even parity**
B3-B0	Baudrate	0000:	invalid
		0001:	invalid
		0010:	150 Baud
		0011:	300 Baud
		0100:	600 Baud
		0101:	1200 Baud
		0110:	2400 Baud
		0111:	4800 Baud
		1000:	**9600 Baud**
		1001:	19200 Baud
AT	reserved		reserved
R	reserved		reserved
M3-M0	Mode	0000:	**Normal-Operating Mode**
		0001:	Modem with V24 Auxiliary Signals

with/without Error Code 06

Due to the fact that some units cannot process Error Code 06, it is possible to suppress output of this error message.

"Normal"-Operation

In this operating mode the errors listed under paragraph "Transmission Procedure" result in the appropriate error message in the condition code word of the triggered Send Job.

The end criterion is Character Delay Time, if the received slave address is unequal to the parameterised slave address and unequal to the broadcast address, the message is not evaluated but ignored.

"Modem"-Operation

The CP does not recognize a message from the master until after it receives the first correct character which tallies with the slave address or the broadcast address.
Message end is determined by function code and bytecount, further reception while the character delay time is running out at message end, is not interpreted as an error but the characters are ignored.

Handling of the the V24-Auxiliary Signals is carried out as described in the CP521 SI Manual Part No. 6ES5 998-1UD21 (EWA 4NEB 812 6072-01a) on pages 6-3 and 6-4.

4.3.5. Work-DB

The number of the work-DB for the Modbus-blocks must be specified here. The user must create this DB prior to calling FB220. This DB must also be specified for FB220 and for FB229 with parameter "A-DB" - permitted DB's are DB3 to DB255

To ensure consistent access to data, the appropriate messages of the master are saved temporarily prior to entering them into the specified area and/or before they can be transferred to the CP. For this purpose it is essential to specify a data block which can be used as the work area.

When received, the data is temporarily saved in the work-DB, until all data has been transferred completely and without error from the CP to the CPU. It is then entered into the destination data area by the function block during the

PLC cycle.
During transmission (reading function by the master) the data is read from the user area during a PLC cycle, is saved temporarily in the work-DB and then transferred to the CP.

4.3.6. Reserved

This Byte is reserved and must be defaulted with 0.

4.3.7. Slave-Address

This is where the MODBUS-Slave adrdess is indicated. It is the address to which the CP521 should send its replies.

4.3.8. Factor Character Delay Time

This multiplication factor is used to increase the character delay time which is calculated from the set baudrate. The multiplication values may range from 1 to 9. The standard setting is factor 1 which means three and a half times the character delay time according to the MODBUS-specification.

The character delay time should only be increased if the link partner cannot keep the required times. This can be determined with intermittent error entries such as "message length incorrect" or "incorrect CRC-Check".

4.3.9. Enabling the Data Areas

Enable Flags:	from, to
Enable Inputs:	from, to
Enable Outputs:	from, to
Enable Timers:	from, to
Enable Counters:	from, to
Enable Data:	from, to

The data areas in the PLC which can be accessed by means of the Modbus functions, are defined here. This applies for both writing and reading accesses. The maximum values listed below must not be exceeded.

Request messages from the master which are outside these areas are not transferred to the CPU by the CP.

Example: F:VB :   KY 120,159
Access is only possible to flags F120.0 to F159.7.

Example: D:VB :   KY 200,204
Access is only possible to data blocks DB200 to DB204 .

Limit Values

Data Area	Min-Value	Max-Value
Flags	0	239
Inputs	0	127
Outputs	0	127
Timers	0	127
Counters	0	127
Data Block	3	255

4.3.10. Waiting Times when Using V24 Auxiliary Signals

The delay times T1, T2 and T3 described in the following 3 Chapters are evaluated **only in the "MODEM" Operating Mode** when using the V24 interface.

The standard settings for the CP are operation without Send Delay T1, without RTS-ON Delay T2 and with an RTS-OFF Delay of 10 to 20 milliseconds, which corresponds to settings T1 = 0, T2 = 0 and T3 = 2.

Should your Modem require any other time requirements it is possible to change the timers accordingly.

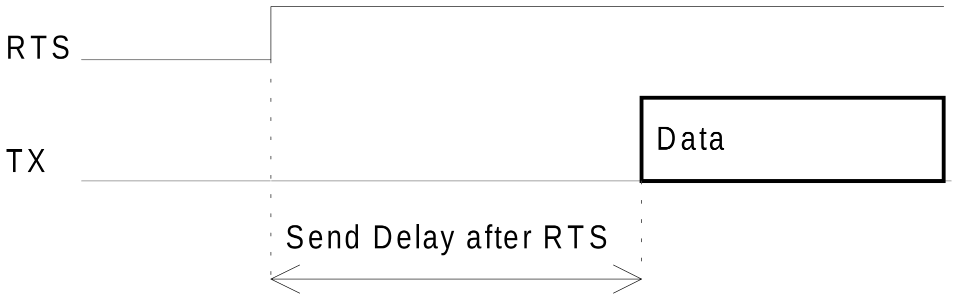
All three timers can be set in 10 millisecond intervals, whereby the set value corresponds to the maximum waiting time. The minimum waiting time is 10 milliseconds lower (e.g. Tx = 9 corresponds to a waiting time of 80 to 90 ms).

The Tx = 0 setting means that operation is without waiting time and the CP continues the send sequence straight away.
The Tx = 1 is not recommended , in this instance the driver assumes Tx = 2 .

4.3.11. Send Delay T1 after RTS

When operation is without send delay T1, the CP activates the "RTS" output and immediately waits for input "CTS" to be activated.

When using send delay T1 the CP activates output "RTS" and starts time T1. After this TIME-OUT the CP checks input "CTS" and commences data output immediately once it is activated.

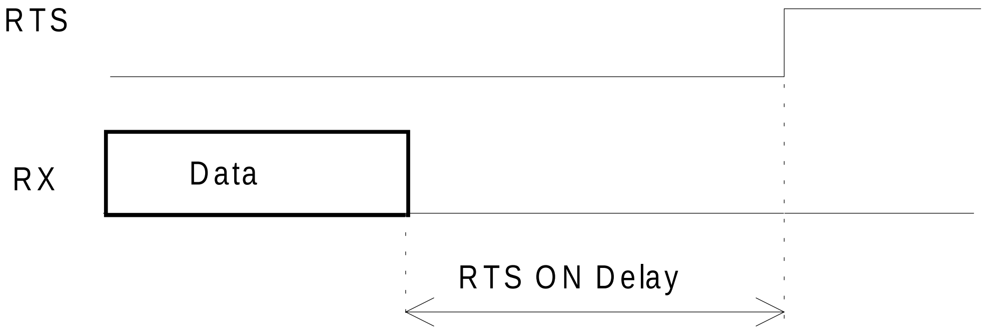


4.3.12. RTS ON Delay T2

For operation without RTS-ON Delay, CP521 activates output RTS - following a send request without time delay independent of how much time has elapsed after receiving the data.

For operation with RTS-ON Delay, CP521 starts time T2 after receiving a request message from the master. After this time period has elapsed the CP checks whether in the meantime the reply message has been generated and whether it is ready for transmission. RTS is set providing send data is available.

If the T2 time was parameterised in such a way that it takes longer to generate the answer than the RTS ON delay, it may be possible for the pause between the request message end and the setting of RTS to exceed T2. This means that the RTS-ON delay defines the minimum pause between message end and RTS.

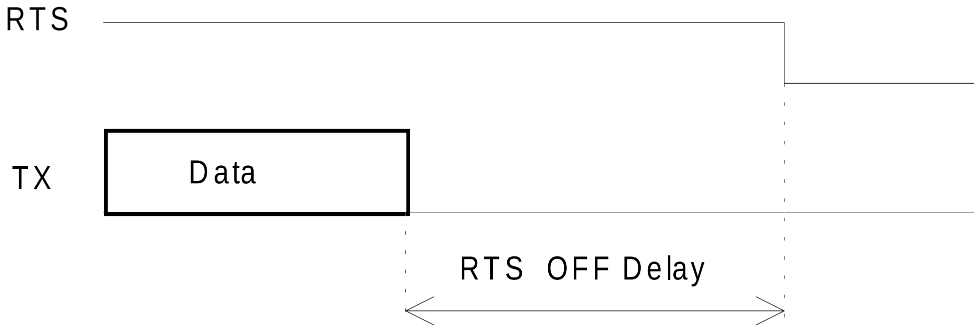


4.3.13. RTS-OFF Delay T3

If operation is without RTS-OFF delay, the "RTS" output is de-activated by the CP521 as soon as the last character is output.

If operation is with RTS-OFF delay, the time T3 time is started by CP521 as soon as the last character is output. The "RTS" output is de-activated once this time has elapsed.

If operation is without OFF delay there is a danger that the link partner no longer recognizes the last character.



4.4. Parameter Assignment of Cyclic FB221

FB221 must be called in the cyclic program (OB1). It must not be called in the alarm program or on initial start (OB21/22). After cold or warm re-start the initialisation parameters are transferred to the CP by the block. After initialisation the input data is read by the CP and it is checked whether data is to be transferred.

During data transfer from CP to CPU the data is entered initially into the input buffer. The CPU acknowledges each data block from the CP. Immediately after transmission of the last data block, the data is entered into the destination area of the CPU.

When data is requested by the CP, it is entered into the send buffer in the current S5-cycle and the first data message is transferred to the CP. The CP outputs the data on the interface upon receipt of the last block from the CPU.

Parameter Assignment FB221

Parameter	Format	Meaning
A-DB	B	Work-DB

A-DB
The work-DB for the function blocks is specified here. It is required to specify the same DB as for Parameter "DB,R" of FB220.

4.5. Parameter Assignment of FB229 - CP-TRACE

FB229 is not required for the Modbus data link. It exists for diagnostic purposes only. The FB lists the input data from the CP (PAE) and the output data to the CP (PAA) in data block "PAEA".

Input to the DB is carried out only when the control word (Bytes 0 and 1) in PAE or in PAA is diffferent. The "PAEA" data block must be created by the user program on initial start having a minimum length of 256 data words (see example - PB220).

The "PAEA" data block is organised as a ring buffer. DW1 of the DB points to the data word from which the next block is to be entered. At the end of the DB the pointer is re-set to the first block (DW9).

A block contains the identifier input data (EE) or output data (AA), the cycle counter and the input/output bytes of the CP.

Parameter Assignment FB229

Parameter	Format	Meaning
A-DB	B	Work-DB
PAEA	KF	No. of DB with PAE/PAA-Trace

A-DB

The work DB for the function blocks is specified here**.** It is required to specify the same DB as for Parameter "DB,R" of FB220 and for Parameter "A-DB" of FB221.

PAEA

DB for PAE/PAA-Trace - permitted DB3 ... DB255. However, the number of the work-DB ("A-DB") must not be specified.

4.6. Special Functions

Read Clock

The CP transfers the clock data to the CPU , when there are no job data to be transferred. The clock data is entered into the work-DB of DW90 to DW92 in BCD-format.

By means of the clock data it is possible to check whether the communication between CP and CPU is running. The clock time is counted in intervals of seconds.

Set Clock

It is also possible to set the clock data from PLC. For this purpose it is required to enter the data from the user program into the work DB DW85 to DW87 in BCD-format. This is followed by setting the transfer bit D0.14 in the work-DB. FB221 transfers the clock data to the CP and resets the transfer bit.

5. Transmission Procedure

The used procedure is code transparent, and asynchronous.

Data transfer is without handshake.

The Master initiates the transmission and after outputting a request message it waits for a reaction message from the CP (=Slave). Message traffic from slave to slave is not possible.

The data exchange "Master-Slave" and/or "Slave-Master" begins with the slave address (0 - 255), followed by the function code (01, 03, 04, 05, 06, 08 or 16), the address field, the data and a CRC-check sum.

The entire message received by the CP always consists of 8 bytes for function codes 01 to 08; and of a maximum of 45 bytes for function codes 15 and 16 , whereby the length depends on the specified bytecount.

Due to the low transmission rate from CP to CPU and vice versa the following **maximum values** have been specified: **36 Bytes** corresponds to **288 Bit**.

The CP recognizes message end, when no transmission takes place during the time period required for the transmission of three and a half characters (see MODBUS Protocol Reference Guide). Therefore this TIME-OUT is baud rate-indepedent.

The maximum time which may elapse between reception of two characters (= character delay time ZVZ), is also equivalent to the time required for the transmission of thee and a half characters. If the CP receives no further characters within this time the part message received so far is considered to be invalid. If the link partner does not adhere to the required times, the ZVZ can be adjusted the following multiplication factor (can be parameterised):

The CRC check character may be calculated by the following Polynominal:

$\mathbf{x^{16} + x^{15} + x^{2} + 1}$

The result is added to the message during transmission (first the Low-Byte, then the High-Byte). On reception all data is subjected to the same CRC-check. If transmission was correct, the received CRC sum and the internally generated CRC sum tally, and an action is initiated. In the event of an incorrect CRC-word the CP does not reply to the message from the master.

5.1. Parameter "Slave-Address"

The CP only replies to messages where the received slave address corresponds to the its own parameterised address. Messages to other slaves are not checked and are not answered.

5.1.1. Broadcast Message (Slave-Address 0)

Due the fact that all slaves on the bus are addressed with slave address 0, the CP does not send a reaction message to the master after execution of the function code.

Broadcast-Messages are only permitted in conjunction with writing **function codes 05, 06, and/or 16**.

Function codes unequal to the above are ignored with Slave address 0. The interface between CP and S5-CPU only allows a limited data throughput, which also depends on the cycle time of the user program. Therefore it is impossible to ensure that broadcast messages in quick succession can be processed. Appropriate error messages are transferred to the S5-CPU.

5.2. Parameter "Function Code"

The function code describes the function to be carried out. **The CP processes function codes 01, 03, 04, 05, 06, 08 and 16.**

If any other function codes are received, the CP replies with an error message number 01: "Illegal Function Code".

The function codes are defined as follows:

Function-Code	General Description	Function as per MODBUS-Specification	Function in S5
01	Read Bits	Read Coil Status	Read from area unequal DB bit by bit
03	Read Registers	Read Holding Registers	Read from area unequal DB word by word
04	Read Registers	Read Input Registers	Read Data Word(s) from DB
05	Write 1 Bit	Modify Coil Status	Write one Bit in areas unequal DB
06	Write 1 Register	Modify Register Content	Write on to one data word in DB
08	Check Message	Loop Back Test	
16	Write serveral Registers	Preset Multiple Registers	Write on to several data words in DB

The areas "unequal DB" may be any of the following memory locations within the S5:

- Flags
- Inputs
- Outputs
- Counters
- Timers

6. Function Codes

6.1. Function Code 01 - Read Flags Bit by Bit (Read Output Status)

This function allows the reading of individual bits by the master in the S5 areas listed below. The address specified by the master is interpreted as follows: -

Bit 15 Bit 0

T	T	T	T	B	B	B	B	A	A	A	A	A	A	A	A

- T = Type of Memory Location in PLC
- B = Bit Number
- A = Address of Byte / Word

Type	Identifier (Bit 12 to 15) = TTTT	Address = AA..AA	organised in
Flags	0	0 to 255	Bytes
Inputs	1	0 to 127	Bytes
Outputs	2	0 to 127	Bytes

Bit numbers B from 0 to 7 are permitted. Address A ranges from 0 to 127 for inputs and outputs and from 0 to 255 for flags.

Amount of Bits may range from **1** to **288**. The CP-CPU interface imposes a limitation on the maximum permissible amount of bits.

Example:
Address 0480H corresponds to Flag 128.4
Address 0580H corresponds to Flag 128.5
Address 1203H corresponds to Input 3.2
Address 2010H corresponds to Output 16.0

6.2. Function Code 03 - Read Output Registers

This function allows the reading of words (registers) by the master in the S5 areas listed below. The address specified by the master is interpreted as follows: -

Bit 15															Bit 0
T	T	T	T	X	X	X	X	A	A	A	A	A	A	A	A

- T = Type of Memory Location in PLC
- X = not used, should be 0
- A = Address of Byte / Word

Type	Identifier (Bit 12 to 15) = TTTT	Address = AA..AA	organised in
Flags	0	0 to 255	Bytes
Inputs	1	0 to 127	Bytes
Outputs	2	0 to 127	Bytes
Timers	5	0 to 255	Words
Counters	6	0 to 255	Words

It is possible to read **a maximum of 18 slave registers** (1 Register = two Bytes) with one message.

Example:
Address 0011H corresponds to Flag Word 17
Address 0012H corresponds to Flag Word 18
Address 1004H corresponds to Input Word 4
Address 2040H corresponds to Output Word 64
Address 5032H corresponds to Timer 50
Address 607FH corresponds to Counter 127

6.3. Functions Code 04 - Read Input Registers

This function allows the reading of data words from a data block. The address specified by the master is interpreted as follows: -

Bit 15	Bit 0
Data Block	Data Word

- Number of Data Block 3 to 255 (System-DB's are not allowed)
- Number of Data Word 0 to 255

Example:
Address 0410H corresponds to DB 4, DW 16
Address 0411H corresponds to DB 4, DW 17
Address 1208H corresponds to DB 18, DW 8

6.4. Function Code 05 - Force Single Coil

This function allows the change of a bit by the master in the S5 areas listed below. The address specified by the master is interpreted as follows: -

Bit 15 Bit 0

T	T	T	T	B	B	B	B	A	A	A	A	A	A	A	A

- T = Type Of Memory Location in PLC
- B = Bit Number
- A = Address of Byte / Word

Type	Identifier (Bit 12 to 15) = TTTT	Address =AA....AA	organised in
Flags	0	0 to 255	Bytes
Outputs	2	0 to 127	Bytes

Address A ranges from 0 to 127 for outputs, from 0 to 255 for flags. Bit numbers B from 1 to 7 are permitted.

Example:
Address 0480H corresponds to Flag 128.4
Address 0580H corresponds to Flag 128.5
Address 2010H corresponds to Output 16.0

6.5. Functions Code 06 - Write a Data Word (Preset Single Register)

This function allows overwriting of a data word of a data block with a new value. The address specified by the master is interpreted as follows: -

Bit 15	Bit 0
Data Block	Data Word

- Number of Data Block 3 to 255 (System-DB's are not allowed)
- Number of Data Word 0 to 255

Example:
Address 0410H corresponds to DB 4, DW 16
Address 0411H corresponds to DB 4, DW 17
Address 1208H corresponds to DB 18, DW 8

6.6. Function Code 08 - Loop Back Diagnostic Test

This function serves to monitor the connection between MODBUS Master and MODBUS Slave (here CP521 SI/BASIC).

This function code only supports **Subcode 00**!

This function has no effect on the S5-CPU and the user programs and data. The received message is independently returned by the CP to the master.

6.7. Function Code 16 - Preset Multiple Registers

This function allows the overwriting of up to **18 data words** of a data block with new values with one request message. The address specified by the master is interpreted as follows: -

Bit 15 Bit 0

Data Block	Data Word

- Number of Data Block 3 to 255 (System-DB's are not allowed)
- Number of Data Word 0 to 255

It is possible to overwrite **a maximum of 18 Registers (1 Register = 2 Bytes)** with one message..

Example:
Address 0410H corresponds to DB 4, DW 16
Address 0411H corresponds to DB 4, DW 17
Address 1208H corresponds to DB 18, DW 8

6.8. Error Messages from Slave

If the slave recognizes an **error in the request message** (e.g. register address illegal), it sets the highest ranking bit in the function code and sends an error message to the master. This error message is structured as follows: -

Error Message from Slave:

Meaning	
Slave-Address 5	05H
Function Code 05	85H
Error Code (1-7)	02H
CRC-Check Code "Low"	xxH
CRC-Check Code "High"	xxH

The following error codes are sent by CP521:

Error Code	Reason
1	Illegal Function Code
2	Address area not available or disabled
3	Length greater 288 Bit or 18 Registers or Data Field not FF00 or 0000 with FC05
4	Error during Data Transfer CP↔CPU
6	CP not ready to receive (Init-job from CPU recognized)

7. Error Messages

7.1. Error Messages from PLC

When the PLC recognizes an error, an error message is entered into DW16 of the Work-DB. The error number is retained until it is overwritten by a new error message. The initial start-FB (FB220) resets the error number.

If an error (Error 1 ... 4) is recognized by the initial start-FB (FB220), there can be no communication between CP and CPU.

Errors which are recognized in the cyclic program (by FB's FB221 ... FB226), result in a negative acknowledgement of the job to the CP. However, transfer of a new job is possible straight away. An acknowledgement of the errors by the user program is not required and is not possible.

Error Number	**Function Code**	**Error Description**	**used in FB**
1		Wrong PLC - only PLC95 and CPU103 allowed	FB220
2		Slave Number = 0	FB220
3		Slot > 7	FB220
4		Monitoring Time > 127	FB220
7		Monitoring Time CP-Initial Start exceeded	FB221
8		Received Block Number in Data Message> 6	FB221
9		Function not supported by PLC	FB221
12	1	Amount of Bits illegal (permitted 1...288)	FB222
13	1	Bit-No. > 7	FB222
15	1	Last F-Address > 255.7	FB222
16	1	Last I/Q Address > 127.7	FB222
31	4	DB-Number = 0	FB224
32	3, 4	Amount of Words illegal (permitted 0..18)	FB224
33	4	DB not available	FB224
34	4	DB too short	FB224

35	3	Last Flag Byte Address > 255	FB224
36	3	Last Input/Output Byte Address > 127	FB224
37	3	Last Timer/Counter Address > 127	FB224
55	5	Byte-Number > 239	FB225
56	5	Byte-Number > 127	FB225
57	5	Bit-Number > 7	FB225
60	6,16	DB-Number = Work-DB	FB226
61	6,16	DB-Number < 3	FB226
62	6,16	Amount of Words > 18	FB226
63	6,16	DB does not exist	FB226
64	6,16	DB too short	FB226
99	Emergency Brake (scratch flag word FY246 was overwritten). The scratch flags must be saved at the beginning of the alarm program and be re-loaded at the end of the alarm program.		

7.2. Error Messages from CP

Error messages from the CP are entered into the Work DB DW17 in format KY. The error group is listed in DL, the error number in DR.

Error Group	Error Number	Error Description
0		**Initialisation Error**
0	1	Modus incorrectly specified
0	2	illegal Baud rate
0	3	illegal number for the work-DB
0	4	Slave address 0 not allowed
0	5	illegal character delay time-factor
0	6	error during transfer of parameter assignment data from CPU
0	7	error during transfer of parameter assignment data from CPU
0	13	Function Code 1: Maximum Value for Inputs incorrect
0	15	Function Code 1: Maximum Value for Outputs incorrect
0	17	Function Code 1: Maximum Value for Timers incorrect
0	19	Function Code 1: Maximum Value for Counters incorrect
0	20	Function Code 2: DB-Number too small
0	33	Function Code 3: Maximum Value Inputs incorrect
0	35	Function Code 3: Maximum Value Outputs incorrect
0	40	Function Code 4: DB-Number too small
0	53	Function Code 5: Maximum Value Inputs incorrect
0	55	Function Code 5: Maximum Value Outputs incorrect
0	57	Function Code 5: Maximum Value Timers incorrect

0	59	Function Code 5: Maximum Value Counters incorrect
0	60	Function Code 6: DB-Number too small
0	153	Function Code 15: Maximum Value Inputs incorrect
0	155	Function Code 15: Maximum Value Outputs incorrect
0	160	Function Code 16: DB-Number too small
1		**Reception Errors**
1	1	BREAK
1	2	Character Delay Time elapsed
1	3	Buffer Overflow
1	4	Parity Error
1	5	Peripherals offline (DTR not available)
1	6	incorrect CRC-Check received
1	7	illegal function code received
1	8	wrong message length
1	20	Lower limit of data area infringed
1	21	Upper limit of data area infringed
1	22	Data type illegal
1	23	Amount of bits or registers too big
1	24	Bit number greater 7 requested and/or not 0
1	25	Data field contents illegal
1	26	wrong Sub-Code with Loop-Back-Test
1	27	Broadcast with read function received
1	255	internal Software error
2		**Errors during Transfer CPU → CP**
2	20	wrong job number
2	21	incorrect combination of status bits
2	22	wrong block number
2	23	wrong transfer length (too few blocks)
2	24	Error Message from CPU
3		**Send Errors**
3	1	BREAK
3	2	Reception during running job
3	5	Peripherals offline (DTR , CTS not available)

3	6	CTS not within 20 seconds

8. Hints on Commissioning

The special driver on the memory sub-module and the supplied S5-program work together which makes commissioning very easy. However, should you still have problems, the following tips should assist you in localising the error.

A common error is incorrect parameter assignment of the slot. In this instance the initialisation is completed with error (INIT-TIMEOUT = Error Number 7).

Does the specified slot tally with parameter assignment? It is possible to monitor the input area by means of the "Control Variable" function of the PG.
The CP reports to the FB by entering data.
The following slot allocation applies:

Slot	Input Word-No. yy
0	IW 64
1	IW 72
2	IW 80
3	IW 88
4	IW 96
5	IW 104
6	IW 112
7	IW 120

You should recognize a value unequal Zero in one of the Input Words:
In this instance the following values are possible:

KH 2xxx	Module not yet ready for data. This can only occur shortly after Mains-On.
KH 4xxx	
KH 5xxx	Module outputs time of day. After Mains-On without battery back-up the version date of the CP and the output status are displayed. IW yy+2: Day and Month for KH display IW yy+4: Year and Version number for KH-display.
KH 8xxx	
KH 9xxx	Module being parameterised.

Please note the error messages in DW 16 and DW 17 of the Work-DB.

Should you not succeed please use the supplied S5-programming package without your user blocks. In the event of correct parameter assignment the system should start and display the time of day and/or the version in the work DB from DW 90 to DW 92. Minutes and seconds are displayed in DW 92 . The values must constantly change here.

9. Notes