S5-LAN-LINK protocol

Version 1.0

The S5-LAN-LINK protocol is handled via the set S5 server port in the LAN module. Currently, only one connection can be connected to the LAN module at the same time. The module acts as a TCP / IP server, which means that it is in the "Listen" state. The protocol is based on the request / response principle. The client (PC) sends a request block to the module via TCP / IP (as described below). If the PC wants to read from the PLC, only the request block is sent. If the PC writes data, the data is written together with the request block. A job is then triggered in the S5 LAN module. During this time, no new request should be sent. After the LAN module has completed the communication with the PLC. Responds with the response block. This has the same format as the request. The success of the action can be checked via the Err field.

Read data from the PLC

1. Fill out the request block and send it to the LAN module.
2. Waiting for response may take several seconds, depending on the number of data required. Time approx. 50 ms + Number of bytes * 1.5 ms vgl.
3. Evaluate the response block (check the Err field).
4. If the desired data could be read, the read data is followed by the response block.
5. If byte-wise read, this are the bytes in the requested order.
6. If the word was read in words, the data is in the low byte format high byte (in PC-friendly format).

Write data to the PLC

1. Fill out the request block, provide data. If words are to be written, attention must be paid to the transmitter sequence low byte, high byte.
2. Send the requestblock and data preferably in one piece to the LAN module.
3. Waiting for response may take several seconds, depending on the number of data required. Time approx. 50 ms + Number of bytes * 1.5 ms
4. Evaluate response block (check Err field).
5. There is no data, only the response block in response.

Request block / Response block.

Byte = 8 bits
WORD = 18 bits
Integer = 16 bit with sign

Data type	**Name**	**r/w**	**Function**
BYTE	PLCType	r/w	PLC type
WORD	Interface	r/w	Interface number
BYTE	PLCNo	r/w	PLC address
BYTE	HdLen	r/w	Length of this header in bytes
BYTE	Cmd	r/w	Command type, e.g. 'R' = read
BYTE	DataType	r/w	Data type related to # "Cmd"
BYTE	DataArea	r/w	Data area in the PLC
WORD	DBNo	r/w	Block number
WORD	Start	r/w	Start byte / Start word
WORD	Count	r/w	Number of data types
integer	Err	r	Error code
WORD	VersionNo	r	version number
BYTE * 4	UserCode	r/w	code, can be used by the user
BYTE * 4	Reserved	r	4 bytes reserved for future expansion
BYTE * n	Data block	r/w	optional Data dependent, whether reading or writing

The fields in detail

PLCType

Specifies the PLC type to be addressed. Must be set to '5'.

interface

Set to zero is used in later versions.

PLCNo

Set to zero is used in later versions. Is for example provided for S7-MPI.

HdLen

Is the length of the request block (without data) in bytes. Currently 26 bytes.

Cmd

The type of the command is defined here.
'R' or 'r' = read
Write 'W' or 'w' =

Data Type

Selects the data type:

'B'	byte (8 bits)
'W'	word (16 bits)

Data Area

Specifies the data area in the PLC:

'M'	flag
'A','O'	process image outputs
'E','I'	process image outputs
'T'	timer (word-by-word only)
'Z','C'	counter (word-by-word only)
'D'	data block (only word-by-word)
'X'	DX block (only word-by-word)

DBNo

Number of the data block or the DX block. We only evaluated DataArea DB or DX.

Start

Start byte or start word number. Depends on DataType.

Count

Number of Units

Err

0	Action successful. The data follows in the case of a read job.
2	Data area not existent in the PLC. For example, Desired DB does not exist.
6	LAN module has detected incorrect request format
3	Desired range too small (e.g., DB too short)
7	An attempt is made to send too much data to the module max. 2048 bytes
9	Timeout with PLC
10	The module has received too little data

VersionNr

Version number of the firmware of the module.
e.g. with version 1.04 is displayed 104 here

User code

These 4 bytes can be used for your own purposes.

Reserved

Reserved for future extensions.

Data block

The user data is displayed here. For example, Read DB 10 from DW5 20 words. Then there are 40 bytes of user data (low byte / high byte order).