Siemens S7 Plus Devices Connector

S7 300/400/1200/1500

- Name: **SiemensPlus**
- Version: 2.2.2.5
- Protocol: Proprietary
- Interface: TCP/IP
- Runtime: .NET 2.0 (Multiplatform)
- Configuration:
    - Devices / Protocols

Overview
Channel Configuration
Node Configuration
Points Configuration
Error Code Reference
Driver Revision History

Overview

Communication Driver Information	
Driver name	SiemensPlus
Assembly Name	T.ProtocolDriver.SiemensPlus
Assembly Version	2.2.2.5
Available for Linux	True
Devices supported	S7 300/400/1200/1500
Third-party libraries	S7.Net.dll.
Manufacturer	Siemens
Protocol	Proprietary over TCP/IP
PC Requirements	Ethernet port

Channel Configuration

Protocol Options

The SiemensPlus connector exposes a Respect User Config Data Type option that controls how the driver resolves the data type for bit-addressable bytes.

RespectUserConfigDataType

A checkbox in the channel's Protocol Options. Controls whether the driver honors the user-configured Data Type on the Communication Point instead of overwriting it from the parsed address suffix.

- **Default:** `false` — driver overrides Data Type based on the parsed address suffix (back-compatible behavior).
- **When set to `true`:** driver keeps the Point's configured Data Type. Required for accurate bit extraction when reading a single bit from a byte whose other bits are also active.

Example — reading a single bit with Data Type = Byte

A read-only tag pointing to bit 0 of a byte (e.g. `DB1.DBB10.0`) can misreport its value when another bit of the same byte is set. To read it correctly:

1. Enable **Respect User Config Data Type** in the channel's Protocol Options.
2. On the Communication Point, set **Data Type** to `Byte`.

Field	Value
Address	`DB1.DBB10.0`
Data Type	`Byte`
Respect User Config Data Type (channel)	checked

With this configuration, when the PLC byte holds `0x80` (bit 7 ON, bit 0 OFF), the bit-0 tag correctly reads **FALSE**. Without it, the same tag would incorrectly read TRUE.

BlockSize

Defines the maximum amount of items per group, the default value is **512**. Some devices support larger blocks, increase it to improve performance, or lower it if the PLC rejects the request.

Node Configuration

Station Configuration

Station syntax: *<IP Address> ; <Rack>; <Slot>;<S7 Family>*

- <**IP Address**>: IP address of the slave device in the Siemens network
- <**Rack**>: Rack of the device
- <**Slot**>: Slot of the device
- <**S7 Family**>: Model of the device. The options are:

  300/400: Support for PLC Siemens S7-300 and S7-400 Series

  1200: Support for PLC Siemens S7-1200 and S7-1500 Series

Points Configuration

Symbol names. This connector always communicates by absolute address (for example DB1.DBW0). To keep the PLC symbol names, import the tags from a TIA Portal XML export: each tag gets the symbol name and its resolved absolute address. Symbol tables from STEP 7 (SIMATIC Manager) are not imported. Optimized data blocks on S7-1200/1500 need the Siemens S7-1200 and S7-1500 Symbolic Connector.

Address

The syntax for the Siemens communication points is: ***<Type><Format><Address>.<Bit or String Length>***

For DataBlock type: ***DB<DB Group>.<DB Format><Address>.<Bit or String Length>***

There is no separator between the register type and the format. The only separators are the dot after the **DB Group** number and the dot before the optional **Bit or String Length**.

Where:

- ***<Type>*** is the register type. Valid values are:
  - **M**=Flags
  - **T**=Timers
  - **C**=Counters
  - **I**=Inputs
  - **Q**=Outputs
  - **DB**=Data Blocks.
- ***<DB Group>*** is the group number of the configured Data Block type.
- ***<Address>*** is the device address.
- ***<Format>*** is the format to treat the value from or to the device. The valid tokens depend on the register type — Data Blocks require the DB-prefixed tokens, every other area requires the plain tokens. Do not mix the two sets:
  - For **M**, **T**, **C**, **I** and **Q**: **B**=Byte, **W**=Word, **DW**=Dword, **F**=Float, **ST**=String, **C**=Counter, **T**=Timer
  - For **DB**: **DBB**=Byte, **DBW**=Word, **DBDW**=Dword, **DBF**=Float, **DBSTR**=String, **DBST**=Short String
- ***<Bit or String Length>*** is the bit number. This parameter is optional. If you use the String type, it represents the String length.

The address is a **single concatenated string** with this structure: `<Block><DBNumber>.<DataType><Address>.<BitOrStringLength>`. The `<DBNumber>` and the dot that follows it appear only for `DB` addresses. Examples:

- `MB0` — Flag (Merker) byte at address 0
- `MW0` — Flag (Merker) word at address 0
- `IB0` — Input byte at address 0
- `QB4` — Output byte at address 4
- `DB1.DBW0` — Data Block 1, Word at address 0
- `DB1.DBDW0` — Data Block 1, DWord at address 0
- `DB5.DBB10` — Data Block 5, Byte at address 10
- `DB1.DBF8` — Data Block 1, Float at address 8
- `DB1.DBB0.3` — Data Block 1, Byte at address 0, bit 3
- `DB1.DBSTR0.52` — Data Block 1, String at address 0, `STRING[50]` (52 total bytes, see below)
- Block prefixes: `M` (Flag/Merker), `T` (Timer), `C` (Counter), `I` (Input), `Q` (Output), `DB` (Data Block)

- Data types: `B` (ByteChar), `W` (WordShort), `DW` (DWordInteger), `F` (FloatSingle), `ST` (StringASCII), `C` (CounterShort), `T` (TimerShort) for non-DB areas; `DBB` (DB Byte), `DBW` (DB Word), `DBDW` (DB DWord), `DBF` (DB Float), `DBSTR` / `DBST` (DB String) for DB areas, always written immediately after the dot that follows the DB number

A DB address written without that dot (`DB1DW0`), or with a colon in place of it (`DB1:DW0`), is not the accepted form. A plain token used inside a DB area (`DB3.ST12.50`) is invalid as well — use `DB3.DBSTR12.50`.

String Layout (DBSTR / DB String)

When an address uses the `DBSTR` or `DBST` format token, the value on the PLC occupies **N+2 bytes**: a 2-byte header followed by N data bytes. The first header byte holds the declared maximum length, the second holds the current length, and the remaining N bytes hold the ASCII characters. This matches the Siemens S7 native `STRING` type. The length you write after the final dot is the **total** byte count, so for a `STRING[N]` you configure `N + 2`. For example, `DB1.DBSTR0.52` addresses a `STRING[50]` starting at byte offset 0, and `DB1.DBSTR16.26` addresses a `STRING[24]` starting at byte offset 16. Reserve those `N + 2` bytes in the Data Block when sizing memory.

Adjacent tags: the next address starts after the N+2 bytes

Those `N + 2` bytes are the field's real footprint inside the Data Block, so the next tag must be configured at the first byte after them. `DB21.DBSTR0.26` occupies bytes **0 through 25**, which makes byte 26 the first free offset in DB21 — `DB21.DBW26`:

Address	Bytes occupied	Content
`DB21.DBSTR0.26`	0 – 25	Byte 0 = declared length, byte 1 = current length, bytes 2 – 25 = up to 24 characters (`STRING[24]`)
`DB21.DBW26`	26 – 27	Next tag — first offset free after the string

If the following tag is configured at an offset that falls inside the string range — `DB21.DBW24`, for example — every write to the string also lands on that tag's address and replaces its value. Nothing writes to the numeric tag itself: the string write is what changes it.

> **Symptom to look for**
>
> A numeric tag that drops back to `0` on its own, intermittently, with no write ever issued to its address, usually means a `STRING` tag is configured immediately before it in the same Data Block and the two byte ranges overlap. Recalculate the string footprint as `N + 2` and move the following tag to the first byte after it.

> **Migration**
>
> Solutions built on prior driver versions that emitted raw N-byte string addresses are migrated automatically on first load with the 2.2.2.x driver. The driver re-resolves the layout at runtime; no user action is required and existing addresses continue to work without edits.

Error Code Reference

Hex	Decimal (signed)	Description
0x00000000	0	No error
0x00000001	1	No error, job still in process
0xFFF00000	-1048576	Function not implemented
0xFFF00001	-1048575	Parameter error when calling function
0xFFF00002	-1048574	Invalid device number
0xFFF00003	-1048573	Invalid PLC number
0xFFF00004	-1048572	Invalid parameter type
0xFFF00005	-1048571	Insufficient memory
0xFFF00006	-1048570	Device already opened
0xFFF00007	-1048569	Device not opened
0xFFF00008	-1048568	Job already removed
0xFFF00009	-1048567	Invalid job number
0xFFF0000A	-1048566	Function not supported
0xFFF0000B	-1048565	Adapter not initialized

0xFFF0000C	-1048564	No free connections available
0xFFF0000D	-1048563	Device not configured or not supported
0xFFF0000E	-1048562	Hardware not found
0xFFF0000F	-1048561	Error when reading parameters
0xFFF00010	-1048560	Error when writing parameters
0xFFF00011	-1048559	Demo period expired
0xFFF00012	-1048558	Wrong character in text. Conversion not possible
0xFFF00013	-1048557	Buffer is not long enough
0xFFF00014	-1048556	File not found
0xFFF00015	-1048555	Error when calling configuration program
0xFFF00016	-1048554	Error when loading DLL dynamically
0xFFF00017	-1048553	Could not create file
0xFFF50000	-720896	No free job buffer available
0xFFF50001	-720895	Invalid packet
0xFFF50002	-720894	No connection to PLC
0xFFF50003	-720893	Connection closed
0xFFF50004	-720892	Timeout
0xFFF50005	-720891	Invalid context
0xFFF50006	-720890	PLC memory error
0xFFF50007	-720889	Invalid operating state
0xFFF50008	-720888	Invalid address on PLC
0xFFF50009	-720887	Invalid mode
0xFFF5000A	-720886	No data available e.g. DB is missing
0xFFF5000B	-720885	Priority class associated to OB does not exist
0xFFF5000C	-720884	Empty blocklist
0xFFF5000D	-720883	Block size error
0xFFF5000E	-720882	Invalid block number
0xFFF5000F	-720881	Protection level of function not sufficient
0xFFF50010	-720880	Unknown SSL-ID (e.g. access to CP instead of PLC)
0xFFF50011	-720879	Unknown SSL-index (e.g. access to CP instead of PLC)
0xFFF50012	-720878	Information currently not ascertainable
0xFFF50013	-720877	Unknown error message from PLC (please report!)
0xFFF50014	-720876	Hardware error e.g. not available periphery
0xFFF50015	-720875	Object access not allowed
0xFFF50016	-720874	Context not supported
0xFFF50017	-720873	Type (data type) not supported
0xFFF50018	-720872	Internal error, please report
0xFFF50019	-720871	Error rebooting PLC
0xFFF5001A	-720870	Error restarting PLC
0xFFF5001B	-720869	Connection end received
0xFFF5001C	-720868	PLC not found

0xFFF5001D	-720867	Too many data for this version of ACCON-AGLink
0xFFF5001E	-720866	PLC does not support this function
0xFFF5001F	-720865	Wrong Password
0xFFF50020	-720864	Connection already legitimated
0xFFF50021	-720863	Legitimation already released
0xFFF50022	-720862	Password not neccessary
0xFFF50023	-720861	At least one variable address invalid
0xFFF50024	-720860	Job does not exist
0xFFF50025	-720859	Invalid job state
0xFFF50026	-720858	Invalid cycle time
0xFFF50027	-720857	No more cyclic job possible
0xFFF50028	-720856	Function not posible for this job (invalid state)
0xFFF50029	-720855	Function abort (overload)
0xFFF5002A	-720854	No data for this variable
0xFFF5002B	-720853	Wrong time format
0xFFF5002C	-720852	Unknown PI name
0xFFF5002D	-720851	File transfer canceled by NCK
0xFFF5002E	-720850	Response too large for PDU size
0xFFF5002F	-720849	No H-PLC found
0xFFF50030	-720848	Data not changed
0xFFF30000	-852968	Error when reading device information
0xFFF30001	-852967	Error when reading bus parameters
0xFFF30002	-852966	Error when writing bus parameters
0xFFF30003	-852965	No resources available on device
0xFFF30004	-852964	Invalid device
0xFFF30005	-852963	Adapter not found
0xFFF30006	-852962	Needed device driver not found
0xFFF20000	-917504	The desired adapter address already exists
0xFFF20001	-917503	Invalid HSA (smaller than biggest active participant)
0xFFF20002	-917502	Adapter is not in the logical ring
0xFFF20004	-917500	Received package has wrong content
0xFFF20006	-917498	Unknown error number from adapter
0xFFF20007	-917497	Unknown error number from device driver
0xFFF20008	-917496	Communications adapter has been removed
0xFFF20009	-917495	Modem has been removed
0xFFF2000A	-917494	No directly connected PLC found
0xFFF20313	-916717	Invalid speed on MPI bus
0xFFF20314	-916716	Address is bigger than HSA
0xFFF20315	-916715	The desired adapter address already exists
0xFFF2031A	-916710	No other active bus participants found
0xFFF2031C	-916708	Bus is jammed

0xFFF2031D	-916707	Bus is jammed
0xFFF2031E	-916706	Automatic detection of bus profile doesn't work, missing bus parameter telegram
0xFFF20337	-916681	Legitimation missing
0xFFF10000	-983040	COM-Port already used
0xFFF10001	-983039	Modem not found
0xFFF10002	-983038	Modem not onhook
0xFFF10003	-983037	Modem not offhook
0xFFF10004	-983036	Error in basic initialisation
0xFFF10005	-983035	Error in Initstring 1
0xFFF10006	-983034	Error in Initstring 2
0xFFF10007	-983033	Error in Initstring 3
0xFFF10008	-983032	Error in Initstring 4
0xFFF10009	-983031	Error in dialtype sequence
0xFFF1000A	-983030	Error in dialtone sequence
0xFFF1000B	-983029	Error in autoanswer sequence
0xFFF1000C	-983028	Modem has been removed
0xFFF1000D	-983027	Connection could not be established
0xFFF1000E	-983026	Login denied. Unknown user.
0xFFF1000F	-983025	Login denied. Wrong password.
0xFFF10010	-983024	Login denied. Callback number defined in adapter.
0xFFF10011	-983023	Error while dialing
0xFFF80000	-524288	Function not allowed
0xFFF80001	-524287	Invalid project handle
0xFFF80002	-524286	Error opening project
0xFFF80003	-524285	Error creating program instance of project
0xFFF80004	-524284	Error closing project
0xFFF80005	-524283	No resp. no more programs found
0xFFF80006	-524282	Program not found
0xFFF80007	-524281	At least one of the specified parameters is invalid
0xFFF80008	-524280	Runtime has expired (demo version)
0xFFF8000A	-524278	No resp. invalid data specified
0xFFF8000B	-524277	The program selected has no symbol table
0xFFF8000C	-524276	Symbol table already opened
0xFFF8000D	-524275	No resp. no more symbol entry found
0xFFF8000E	-524274	Error reading symbol entry
0xFFF8000F	-524273	Symbol not found
0xFFF80010	-524272	Operand not found
0xFFF80011	-524271	Invalid symbol
0xFFF80012	-524270	Invalid operand
0xFFF80013	-524269	Invalid filter string
0xFFF80014	-524268	Data block (DB) not present

0xFFF80015	-524267	Error reading DB block data
0xFFF80016	-524266	Error parsing DB block data
0xFFF80017	-524265	An opened DB is already present
0xFFF80018	-524264	No opened DB present
0xFFF80019	-524263	No resp. no more DB component found
0xFFF8001A	-524262	Specified DB component not found
0xFFF8001B	-524261	Specified DB component is invalid
0xFFF8001C	-524260	Specified DB component not matching
0xFFF8001E	-524258	Invalid constant
0xFFF8001F	-524257	Invalid constant size or format
0xFFF80020	-524256	Object type initialization failed
0xFFF80021	-524255	Invalid version of message configuration
0xFFF80022	-524254	Error opening message configuration
0xFFF80023	-524253	Error closing message configuration
0xFFF80024	-524252	No resp. no more message entry found
0xFFF80025	-524251	No resp. no more language found
0xFFF80026	-524250	Database access error
0xFFF80027	-524249	Invalid signal number
0xFFF80028	-524248	Invalid add. value specification
0xFFF80029	-524247	Add. value number invalid
0xFFF8002A	-524246	Element type of add. value invalid
0xFFF8002B	-524245	Add. value data length invalid
0xFFF8002C	-524244	Format specification missing
0xFFF8002D	-524243	Format specification invalid
0xFFF8002E	-524242	No resp. no more text library found
0xFFF8002F	-524241	No resp. no more text library entry found

Driver Revision History

Siemens Revision History	
Version	**Notes**
2.2.2.2	Initial release on new documentation standards.
2.2.2.3	Configurable BlockSize. STRING write correction: the driver no longer adds the 2-byte S7 header on top of the configured length, so a `DBSTR` / `DBST` write stays inside its `N + 2` footprint and no longer overwrites the address that follows it in the Data Block. Available from FrameworX 10.1 Update 5d (build 2093) — earlier builds also report driver 2.2.2.3, so on this version check the product build number as well.
2.2.2.4	Assembly version raised so that a build carrying the STRING write correction above can be identified by the driver version alone. No functional change over the corrected 2.2.2.3.
2.2.2.5	Tag import from TIA Portal now sets STRING tag addresses to the full byte length, so the last two characters of a string are no longer lost on write; string tags imported earlier must be re-imported or corrected.

In this section...