

# Siemens SIMATIC 3964(R) CW

## Siemens SIMATIC 3964(R) CW communication protocol

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

### Supported device types and versions

The protocol is an implementation of the Control Web "SIMATIC 3964R" protocol and was created to facilitate the replacement of Control Web applications with D2000 technology.

On the link layer, this protocol implements the Siemens SIMATIC 3964R protocol and uses it to read from and write to the PLC. The protocol only supports database block (DB) addressing 0-255.

The protocol contains the following header defined by Control Web:

| Byte | Name  | Description                                             |
|------|-------|---------------------------------------------------------|
| 1    | Id    | Zone identifier ('D' = data block)                      |
| 2    | DB    | Number of zone (data block)                             |
| 3-4  | DW    | Word address within a zone (lower byte, upper byte)     |
| 5    | Cmd   | Command ('R' - reading, 'W' - writing)                  |
| 6-7  | Count | Number of read / written words (lower byte, upper byte) |

The protocol supports reading data from control PLC automats of Siemens SIMATIC of the S5 and S7 series. PLC Simatic must be equipped with the serial communication point-to-point modules - for more details see the description of [Siemens SIMATIC 3964\(R\)](#) protocol.

### Communication line configuration

- Communication line category: [Serial](#), [SerialOverUDP Device Redundant](#).
- Serial line parameters must be configured according to the setting of the SIMATIC communication module.

### Line protocol parameters

A dialog window of [communication line configuration](#) - **Protocol parameters** tab. They influence some optional protocol parameters.

The following line protocol parameters are defined:

| Parameter         | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Unit / size                           | Default value |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|---------------|
| Mode              | A mode of communication: <ul style="list-style-type: none"><li>Active - active communication (sending requests and receiving replies).</li><li>Passive - eavesdropping of Control Web communication with the PLC. This mode requires that only PLC responses are intercepted.</li><li>Passive (duplex) - eavesdropping of Control Web communication with the PLC. This mode requires that both Control Web requests and PLC responses are intercepted.</li></ul> <p>Note: Active communication is used when Control Web is replaced by D2000. The eavesdropping is used during D2000 deployment and allows parallel operation with the Control Web system.</p> | Active<br>Passive<br>Passive (duplex) | Active        |
| Max Data Size     | Maximum size (in bytes) of data read by a single request. Add to this size a 7-byte Control Web header to obtain full length of response (without duplicated DLE bytes) according to the SIMATIC 3964(R) standard.                                                                                                                                                                                                                                                                                                                                                                                                                                             | 4 až 249 B                            | 128 B         |
| Retry Count (hex) | Maximum number of request retries in case of communication error.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | -                                     | 2             |
| Retry Timeout     | A delay before resending a request in case of communication error.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | ms                                    | 100 ms        |

|              |                                                                                                                                                                                   |        |    |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----|
| Debug Values | Activates a debug info about the loaded values of I/O tags. Use this parameter only when communication must be debug because it highly uses CPU and slows down the communication. | YES/NO | NO |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----|

## Communication station configuration

- Communication protocol: **Siemens SIMATIC 3964(R) CW**.
- No address is specified, only a single Simatic PLC can be attached to one communication line.

## Station protocol parameters

The [Communication station dialog box](#) - tab **Protocol parameters**.

Parameters defined in the input field have effect on some optional protocol parameters. The following station protocol parameters can be defined (the same as parameters of protocol [Siemens SIMATIC 3964\(R\)](#)):

**Table 1**

| Parameter          | Meaning                                                                                                                                                | Unit    | Default value |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------------|
| Wait Timeout       | Delay between response readings till its finalization.                                                                                                 | ms      | 50 ms         |
| Max Wait Retry     | Repetition count of response readings till its finalization.                                                                                           | -       | 600           |
| 3964 (without BCC) | Enable the 3964 protocol, i.e. version with no transmission security using the checksum. By default, the 3964R protocol with the BCC checksum is used. | YES /NO | NO            |

## I/O tag configuration

Possible I/O tag types: **Ai, Ci, Di**.

The I/O tag address is compatible with the I/O tag addressing in the [Siemens SIMATIC S7 ISO on TCP](#) protocol with the following limitations:

- only "DB" addresses can be used, i. e. only variables in data blocks are available.
- the protocol implements a 1-byte address of the data block, i. e. it supports addressing of data blocks 0-255
- all value types except STRING are available:

| Identifier <type> | Description                                                         |
|-------------------|---------------------------------------------------------------------|
| X                 | Bit (boolean). Specify a bit number 0 to 7 - e.g. DB9,X8.3          |
| B                 | Byte (8 bits unsigned).                                             |
| W                 | Word (16 bits unsigned).                                            |
| D                 | Double word (32 bits unsigned).                                     |
| CHAR              | Character (8 bits signed).                                          |
| INT               | Integer (16 bits signed).                                           |
| DINT              | Double integer (32 bits signed).                                    |
| BCD               | BCD-coded 2-byte number (0-9 999)                                   |
| LBCD              | BCD-kódované 4-byte number (0-99 999 999)                           |
| REAL              | Floating point number (32 bits according to IEEE754 standard).      |
| LREAL             | Long floating point number (64 bits according to IEEE754 standard). |
| DT                | Date and Time, 8 bytes in BCD format.                               |
| TIME              | Time (32 bits signed) in ms.                                        |
| TOD               | Time of day (32 bits unsigned) in ms.                               |

- address examples:  
DB3,REAL0  
DB3,W4  
DB3,B6

## Literature

---

-

## Changes and modifications

---

-

## Document revisions

---

- Ver. 1.0 - January 16th, 2020 - document creation.
- Ver. 1.1 - July 10, 2020 - Support for BCD and LBCD.



### Related pages:

[Communication protocols](#)