

**SIEMENS**

*Ingenuity for life*

*Industry Online Support*

Home

# Sending security messages using the syslog protocol with an S7-1500 PLC

SIMATIC, TIA Portal, Logging

<https://support.industry.siemens.com/cs/ww/en/view/51929235>

Siemens  
Industry  
Online  
Support



## Legal information

### Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

### Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

### Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://support.industry.siemens.com>) shall also apply.

### Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: <http://www.siemens.com/industrialsecurity>.

# Table of contents

<b>Legal information</b> .....	<b>2</b>
<b>1 Introduction</b> .....	<b>4</b>
1.1 Overview.....	4
1.2 Mode of operation .....	5
1.3 Components used .....	7
<b>2 Engineering</b> .....	<b>8</b>
2.1 Parameter assignment of the hardware .....	8
2.2 Parameter assignment of the data block "LSyslog_Data" .....	9
2.3 Operation.....	10
<b>3 Useful information</b> .....	<b>12</b>
3.1 The syslog protocol .....	12
3.2 The "Get_Alarm" instruction .....	12
3.3 The "GetChecksum" instruction .....	12
<b>4 Appendix</b> .....	<b>13</b>
4.1 Service and Support.....	13
4.2 Links and Literature .....	14
4.3 Change documentation .....	14

# 1 Introduction

## 1.1 Overview

### Simple and efficient the syslog protocol

Syslog is a simple binary UDP/IP protocol. It allows applications to send alerts, warnings or error conditions to a syslog server. Syslog is used typically in computer system management and security monitoring and has now become established as a standard ([RFC 5424](https://www.rfc-editor.org/rfc/rfc5424)) in the field of logging.

### Features of syslog

The syslog protocol is distinguished by the following features:

- Simple protocol with low transport overhead
- Minimal need for network bandwidth through push mechanism
- Severity and origin as information in the header
- Message texts individually configurable

### Applicative implementation

The "LSyslog" library provides a solution for implementing the syslog protocol in a SIMATIC S7 controller. The library is available at the following address:

<https://support.industry.siemens.com/cs/ww/en/view/51929235>

You can find more information on the syslog protocol and the function of the block in the corresponding library description.

This application example uses this library and provides you with a function block for the SIMATIC S7-1500. The function block "LSyslog\_Send" integrates the syslog client function, inserts the message texts in the syslog protocol and sends these messages to the syslog server.

The following messages are sent to the syslog server:

- Information about the controller (order number, serial number, firmware version).
- Any security messages that come up, e.g. when logging on to the controller.
- Warning message when a program has been changed and loaded into the controller. The checksums of the old and new programs are integrated into the message.
- Warning message when a safety program has been changed and loaded into the controller. The checksums of the old and new programs are integrated into the message.

## 1.2 Mode of operation

In this application example, security messages are read out with the instructions "Get\_Alarm" and "GetChecksum" and sent to the syslog server. This allows you to track and document access to your controls.

### Schematic representation

The figure below schematically shows the relationship between the components involved.

Figure 1-1:

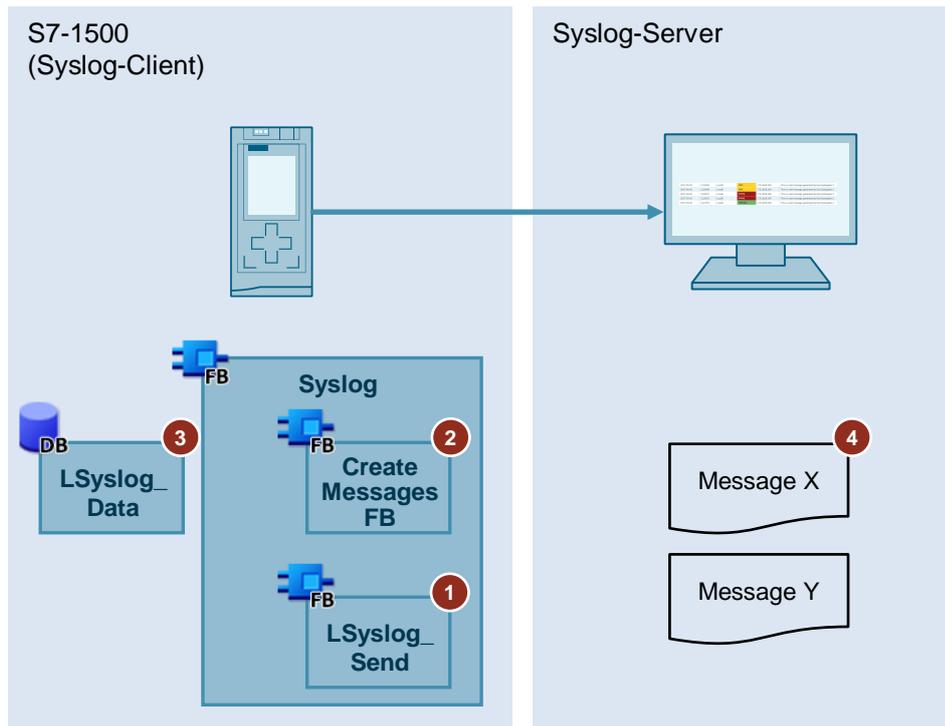


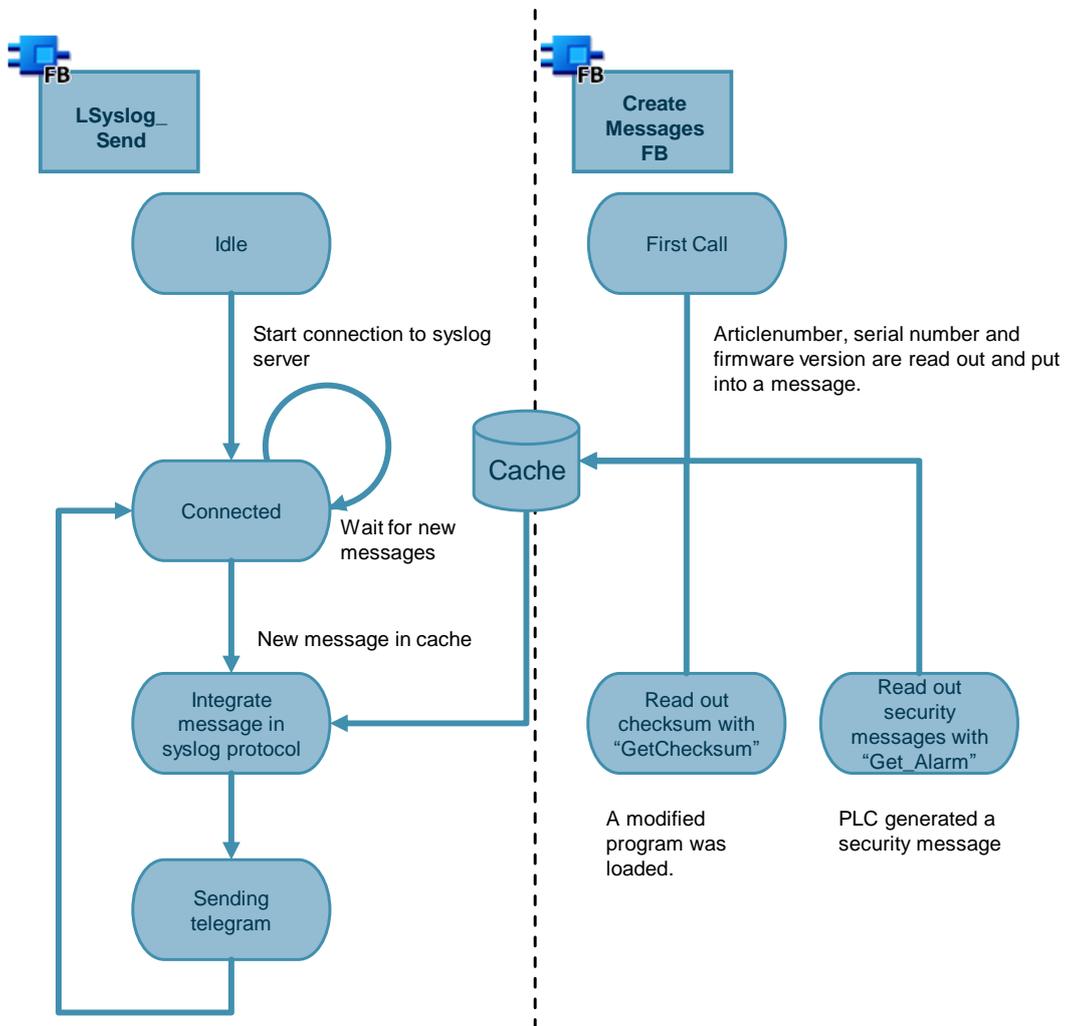
Table 1-1

Step	Description
1	The block "LSyslog_Send" establishes the UDP connection to the server. Messages from the cache are embedded in the syslog log and sent to the syslog server.
2	The "CreateMessagesFB" block reads security messages and the current checksums and creates messages from them that are sent to the syslog server.
3	The data block "LSyslog_Data" manages the parameters of the connection and stores occurring messages in a cache.
4	The syslog server receives the messages and displays them

**Program sequence**

The following figure shows the sequence and the interaction of the function blocks "LSyslog\_Send" and "CreateMessageFB". Both blocks are called up in the application example in the "Syslog" function block.

Figure 1-2



## 1.3 Components used

The application example was created with these hardware and software components:

Table 1-2

Component	Number	Article number	Note
SIMATIC S7-1500	1	6ES7 516-3FN01-0AB0	Firmware V2.1 At least Firmware V2.0 is required.
Kiwi Syslog server	1	<a href="https://www.kiwisyslog.com/free-tools/kiwi-free-syslog-server">https://www.kiwisyslog.com/free-tools/kiwi-free-syslog-server</a>	

This application example consists of the following components:

Table 1-3

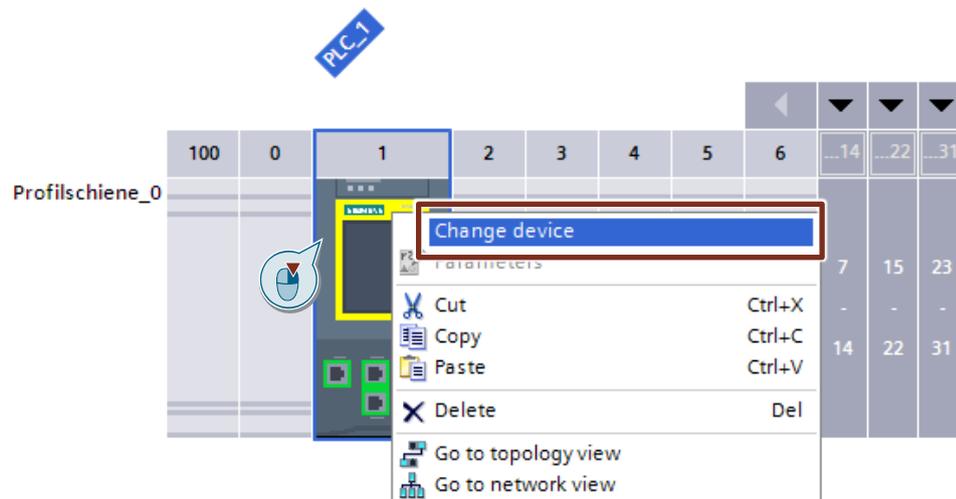
Component	Note
Description	This document
Project	STEP 7 (TIA Portal)

## 2 Engineering

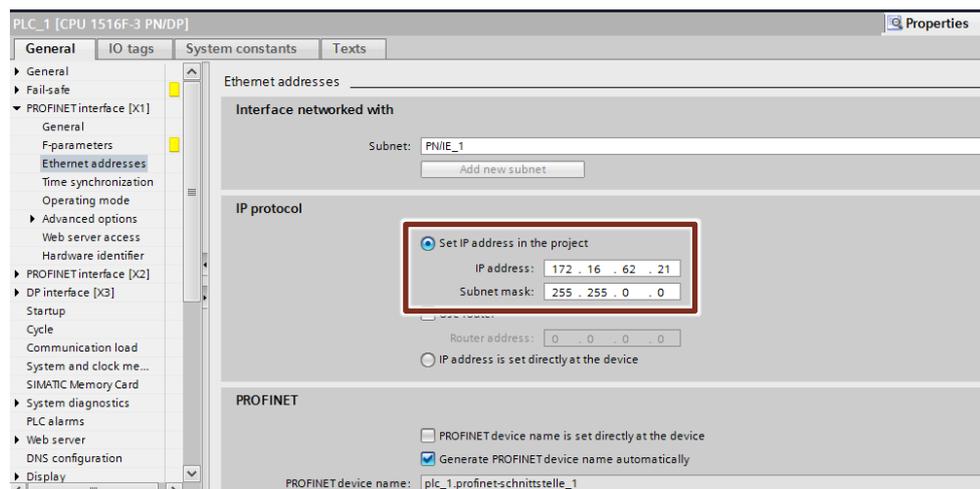
To use the application example, the following steps are necessary:

### 2.1 Parameter assignment of the hardware

1. Open the TIA portal project from the article page of this application example: <https://support.industry.siemens.com/cs/ww/en/view/51929235>
2. Open the hardware configuration of the controller.
3. If you do not have the controller used in the application example, replace the controller using the "Change device..." dialog.



4. Select the PLC and switch to the "Properties" tab in the Inspector window. Now adapt the IP address of the PROFINET interface [X1]. Select a free IP address in your network and enter it with the subnet mask.



5. Access passwords are configured for the controller. These are required after loading the hardware configuration to log in to the controller; the following passwords are needed:

Table 2-1: Passwords of the configured PLC

Access level	Password
Full access incl. fail-safe (no protection)	Level3
Full access (no protection)	Level2
Read access	Level1

## 2.2 Parameter assignment of the data block "LSyslog\_Data"

1. Now open the data block "LSyslog\_Data".
2. Adjust the following variables:

Variable	Value
plcName	PLC name
hostAddress	IP address of PLC
ConnectionDescription.RemoteAddress.ADDR	IP address of the syslog server

**Note** If you do not want to use the internal PN interface of the PLC, also adapt the "Interfaceld" parameter.

Name	Datentyp	Startwert
Static		
plcName	String	'PLC_1'
hostAddress	String	'172.16.62.21'
ConnectionDescription	TCON_IP_v4	
Interfaceld	HW_ANY	64
ID	CONN_OUC	5
ConnectionType	Byte	16#13
ActiveEstablished	Bool	false
RemoteAddress	IP_V4	
ADDR	Array[1..4] of Byte	
ADDR[1]	Byte	172
ADDR[2]	Byte	16
ADDR[3]	Byte	1
ADDR[4]	Byte	50
RemotePort	UInt	514
LocalPort	UInt	2000
error	Bool	false

3. Compile the project. If errors occur, rectify them.
4. Load the project into your controller.

## 2.3 Operation

To send messages from the controller to the syslog server, you must perform the following steps:

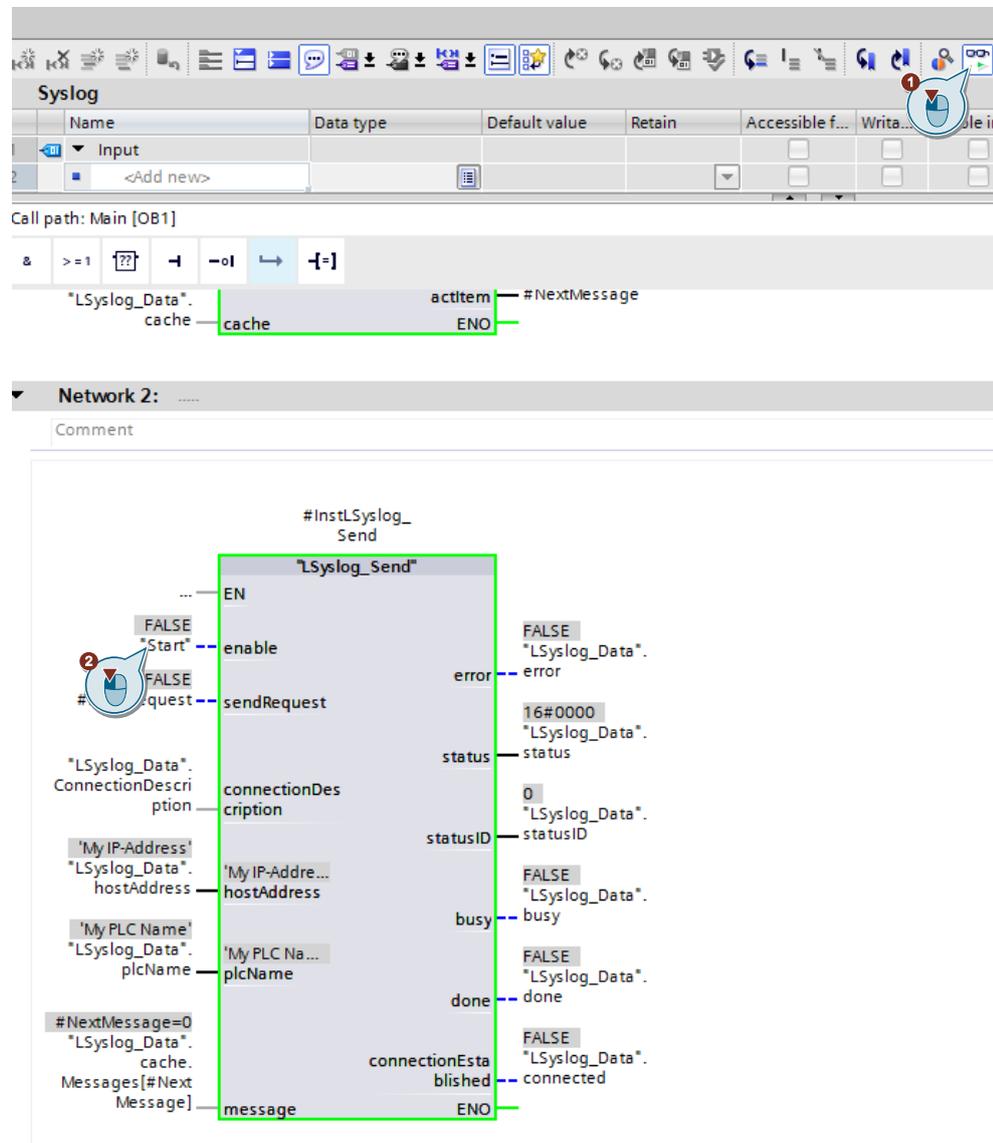
### Establish the connection to the server

1. Open the "Syslog" block and click on the "Monitoring on/off" button.
2. Set the variable "Start" at the input "enable" to "true". Click on the variable "Start" and then press the key combination "Ctrl + F2".

### Result

The block establishes the connection to the syslog server. As soon as the block returns the value "true" at the "connectionEstablished" output, message frames can be sent.

Figure 2-1



### Generate warning messages

You can generate a warning message with the following procedure:

1. Exit the observation mode by clicking on the "Monitoring on/off" button.
2. Open the data block "LSyslog\_Data".
3. Change the value for "plcName".
4. Compile the program and download the changes to your controller.

### Result

A message has been generated which indicates that a new program has been uploaded. The message was automatically sent to the syslog server.

The following figure shows how the message is structured.



Message Text  
1 2017-11-16T12:39:25.638 My IP-Address My PLC Name - Actual (previous) program signature: EFC12CEF5D90A06B (B700D9E57730431B)

### Generate security messages

You can generate a security message with the following procedure:

1. To be able to log on to the controller, close the open project.
2. Open the project again.
3. Go online by pressing the "Go online" button on the toolbar.
4. Enter the password for the specified access level "Read access" (see [Table 2-1](#)).

### Result

A message has been generated that indicates that someone has logged into the controller. The message was automatically sent to the syslog server.

The following figure shows how the message is structured.



Message Text  
1 2017-11-24T07:50:20.140 My IP-Address My PLC Name - Security information: Session authentication successful SessionID 0-0 PLC

## 3 Useful information

### 3.1 The syslog protocol

Syslog is a logging system for the transmission of messages in an IP network and has since become a standard (RFC 5424) in the field of logging.

You can find more information on the syslog protocol and the block library "LSyslog" in the corresponding library description.

<https://support.industry.siemens.com/cs/ww/en/view/51929235>

### 3.2 The "Get\_Alarm" instruction

You can use the "Get\_Alarm" instruction to read messages in the user program via the alarm interface of the S7-1500 PLC. The "Get\_Alarm" instruction, like a SIMATIC HMI, logs on to the alarm system interface of the S7-1500 PLC to read out an incoming or outgoing alarm.

Alarms allow you to detect errors in process control in the automation system quickly, to localize them precisely, and to eliminate them.

You can find additional information on the "Get\_Alarm" instruction here.

<https://support.industry.siemens.com/cs/ww/en/view/109748168>

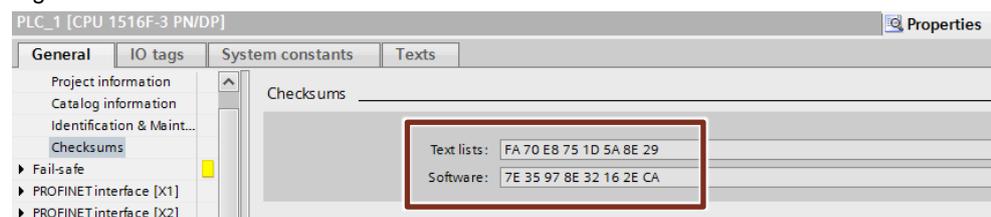
### 3.3 The "GetChecksum" instruction

#### Checksum

PLC programs are automatically marked with unique checksums during compilation. You can use the checksum to identify your program and determine whether two PLC programs are identical.

Since the checksum is loaded into the PLC together with the PLC program, it can also serve as important information during servicing. For example, you can easily tell if the program currently running on the PLC is the same program that you downloaded a long time ago, or if it has been changed in the meantime.

Figure 3-1: Checksum



#### Generate checksum

If it is determined during the next compilation that the PLC program has been changed, the program receives a new checksum. If the PLC program has not changed and is still being translated, the checksum remains the same.

#### Read out checksum

You can use the "GetChecksum" instruction to read the checksum of a group of objects.

For more information about GetChecksum, see the TIA Portal Help or the manual.

## 4 Appendix

### 4.1 Service and Support

#### Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, and application examples – all the information you need is accessible with just a few mouse clicks at:

<https://support.industry.siemens.com/>

#### Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

You can send queries to Technical Support via the web form:

<https://support.industry.siemens.com/My/ww/en/requests>

#### SITRAIN – Training for Industry

With our globally available training courses for our products and solutions, we help you with innovative learning methods.

You can find out more about the training and courses offered as well as their locations and dates at:

<https://www.sitrain-learning.siemens.com/DE/en/index.do>

#### Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information about our range of services in the service catalog:

<https://support.industry.siemens.com/cs/sc>

#### Industry Online Support App

You can also receive optimum support wherever you are on the go using the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:

<https://support.industry.siemens.com/cs/ww/en/sc/2067>

## 4.2 Links and Literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support <a href="https://support.industry.siemens.com/">https://support.industry.siemens.com/</a>
\2\	Link to the entry page of the library description "LSyslog" <a href="https://support.industry.siemens.com/cs/ww/en/view/51929235">https://support.industry.siemens.com/cs/ww/en/view/51929235</a>
\3\	Link to RFC 5424 <a href="http://tools.ietf.org/html/rfc5424">http://tools.ietf.org/html/rfc5424</a>
\4\	Link to the entry page of the application sample "Get_Alarm" <a href="https://support.industry.siemens.com/cs/ww/en/view/109748168">https://support.industry.siemens.com/cs/ww/en/view/109748168</a>
\5\	Link to the TIA Portal Manual V15.1 <a href="https://support.industry.siemens.com/cs/ww/en/view/109755202">https://support.industry.siemens.com/cs/ww/en/view/109755202</a>

## 4.3 Change documentation

Table 4-2

Version	Date	Modification
V1.0	01/2018	First version
V3.0	07/2019	Update for STEP 7 (TIA Portal) V15.1