SIEMENS

Ingenuity for life

Sending SIMATIC S7-1200/S7-1500 CPU Security Messages via Syslog to SINEC INS

SIMATIC, TIA Portal, SINEC INS

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: https://www.siemens.com/industrialsecurity.

© Siemens AG 2021 All rights reserved

Table of Contents

© Siemens AG 2021 All rights reserved

1 Introduction

1.1 Overview

Simple and efficient: the Syslog protocol

Syslog is a simple binary UDP protocol. It allows applications to send messages, warnings, or error states to a server. Syslog is typically used for computer system management and security monitoring and has established itself as the standard (RFC 5424) in 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

In order to be able to use the Syslog protocol in a SIMATIC S7 Controller, we offer you an applicative solution with the "LSyslog" library.

Note

> The "LSyslog" library is part of the "Libraries for Communication". You can download the library separately from Siemens Industry Online Support:
> https://support.industry.siemens.com/cs/ww/en/view/109780503

This application example uses this library and provides you with the "LSyslog_Send" function block for the SIMATIC S7-1500, which sends certain safety-relevant messages to the Syslog server as an example in order to document and track accesses to the S7 Controller.

The following messages are sent to the Syslog server:

- Security messages that occur (e.g., when logging into the controller).
- Occurring alarm messages (e.g., in case of failure of a module).
- Warning message when a program or safety program has been changed and loaded into the controller. The checksums of the old and new programs are integrated into the message.

Detailed information on the function and wiring of the "LSyslog_Send" function block contained in the "LSyslog" library can be found in the corresponding library description.

© Siemens AG 2021 All rights reserved

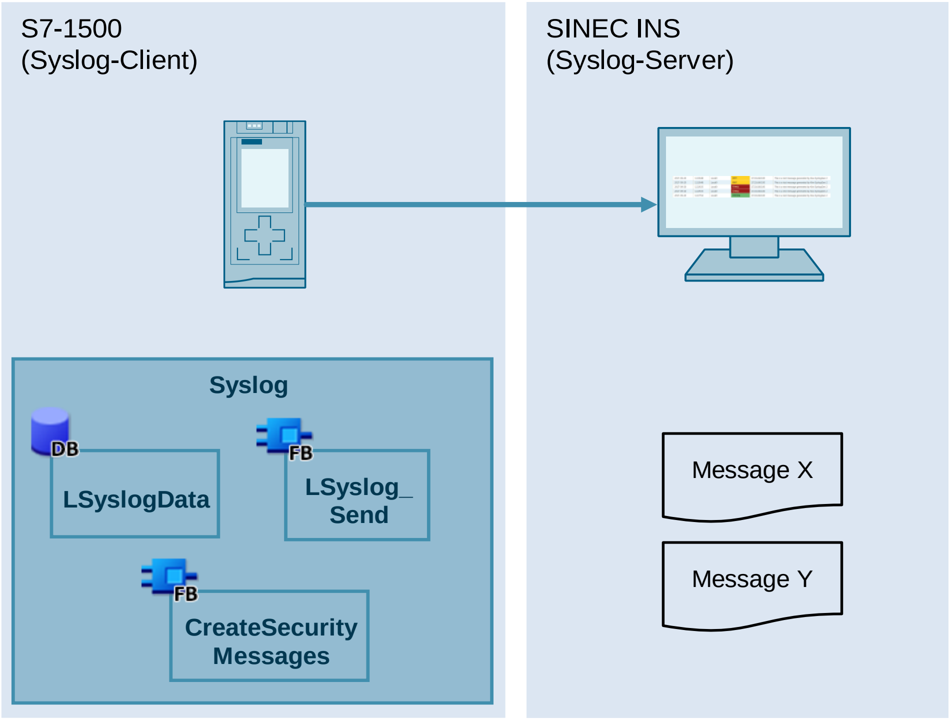
1.2 Operating Principle

In this example, we use the central Syslog server that is included in the SINEC INS product.

Schematic representation

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

Figure 1-1:



© Siemens AG 2021 All rights reserved

1.3 Components Used

This application example was created with the following hardware and software components:

Table 1-1

Components	Quantity	Item Number	Note
CPU 1516-3 PN/DP	1	6ES7516-3AN01-0AB0	Alternatively, you can also use the following components: • Another S7-1500 CPU with firmware V2.0 or higher • An S7-1200 CPU with firmware V4.4 or higher • One ET 200 CPU (ET 200SP, ET 200pro) with firmware V2.0 or higher • CP 1243-1 (6GK7243-1BX30-0XE0) with firmware V3.2 or higher • CP 1243-7 LTE (6GK7243-7KX30-0XE0 / 6GK7243-7SX30-0XE0) with firmware V3.2 or higher
SINEC INS Server	1	6GK8751-1..	V1.0 in any version. SINEC INS includes a demo license with 10 nodes by default. If you want to increase the number of nodes, you can purchase licenses for 50, 100, 250, 500, 1000, and 5000 nodes.

This application example consists of the following components:

Table 1-2

Components	File name	Note
Description	51929235_Syslog_DOC_de.pdf	This document
Project	51929235_Syslog_PROJ.zip	TIA Portal V17

© Siemens AG 2021 All rights reserved

© Siemens AG 2021 All rights reserved

2 Engineering

The provided sample project shows the finished configuration of the Syslog application including the security functions (see Section 2.3). In Section 2.1, you will learn all the necessary steps to integrate Syslog into a new project. You must then implement the security functions relevant for the application.

2.1 Using the Syslog Block

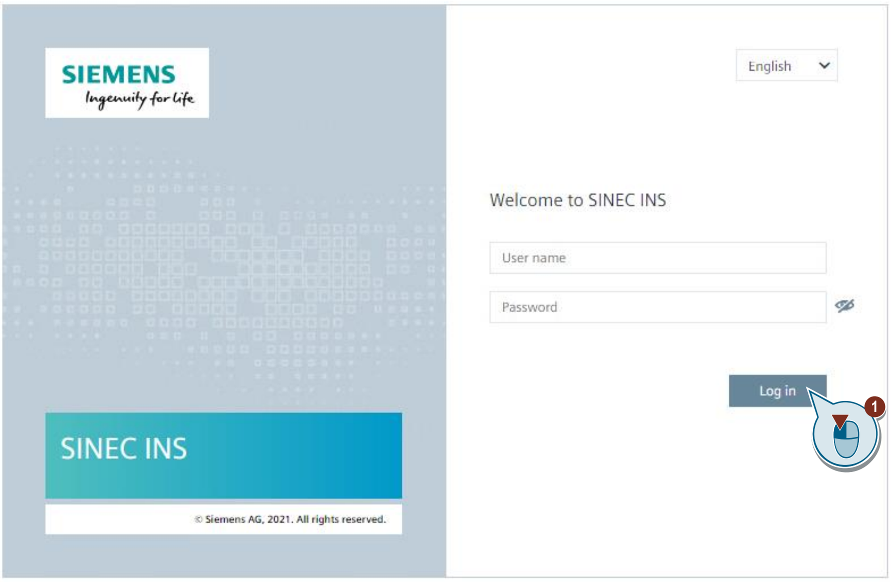
2.1.1 Parameterizing the SINEC INS Server

Requirements

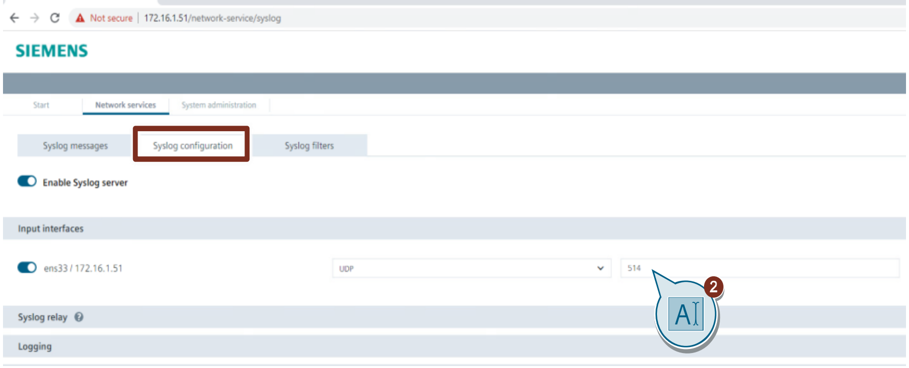
Install SINEC INS according to the installation instructions.

Parameterization

1. Log into the web interface of SINEC INS.



2. Select "Syslog services" from "Network services" and then "Syslog configuration". Set the connection type to "UDP" and the port to "514". The IP address of the Syslog server is the IP address of the computer on which SINEC INS is installed.



172.16.1.51/network-service/syslog

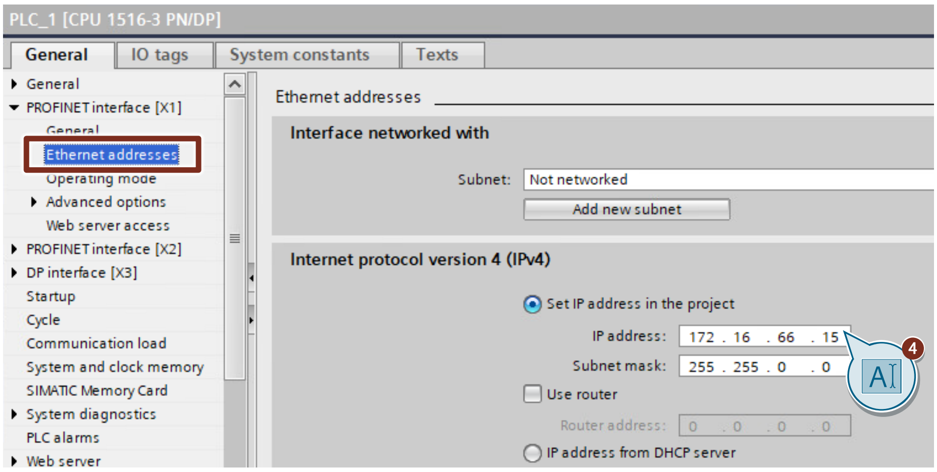
Enable Syslog server

ens33 / 172.16.1.51 | UDP | 514

2.1.2 Creating the TIA Portal project

1. In TIA Portal V17, create a new project with the S7 CPU that you wish to use for the application example.

   In TIA Portal V17, when you add a new PLC, a context menu opens where you can directly adjust security settings and passwords of the PLC.
2. In the hardware and network editor, open the "Device configuration" of the S7 CPU.
3. Select the S7 CPU. The properties of the S7 CPU are displayed in the Inspector window.
4. Now adjust the IP address of the PROFINET interface [X1] ("PROFINET interface [X1]"). Select a free IP address in your network and enter it and the subnet mask.



PLC_1 [CPU 1516-3 PN/DP]

General | IO tags | System constants | Texts

- General
- PROFINET interface [X1]
  - General
  - Ethernet addresses
  - Operating mode
  - Advanced options
  - Web server access
- PROFINET interface [X2]
- DP interface [X3]
- Startup
- Cycle
- Communication load
- System and clock memory
- SIMATIC Memory Card
- System diagnostics
- PLC alarms
- Web server

Ethernet addresses

Interface networked with

Subnet: Not networked

Add new subnet

Internet protocol version 4 (IPv4)

● Set IP address in the project

IP address: 172 . 16 . 66 . 15

Subnet mask: 255 . 255 . 0 . 0

□ Use router

Router address: 0 . 0 . 0 . 0

○ IP address from DHCP server

© Siemens AG 2021 All rights reserved

2.1.3 Integrating the Block into the User Program

The Syslog block, as well as the required data types, are available in the Communication Libraries.

Note The module description can be found in the documentation for the Communication Libraries. (https://support.industry.siemens.com/cs/ww/en/view/109780503)

2.1.3.1 Integrating the Global Library into the Project

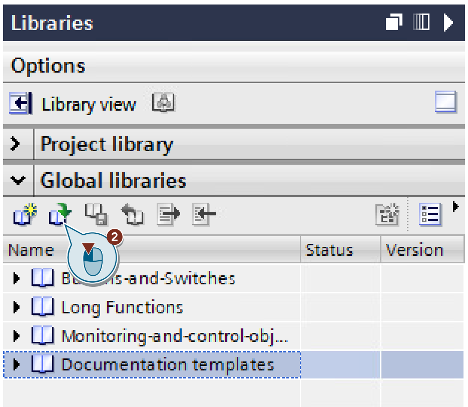
Requirements

Download the Communication Libraries for SIMATIC Controllers from the Siemens Industry Online Support at the following link:
https://support.industry.siemens.com/cs/ww/en/view/109780503

Then unzip the file in a directory of your choice.

Instructions

1. In the TIA Portal project, click the Libraries tab and open the Global libraries palette.
2. Click the "Open global library" button. The "Open global library" dialog is opened.



Libraries

Options

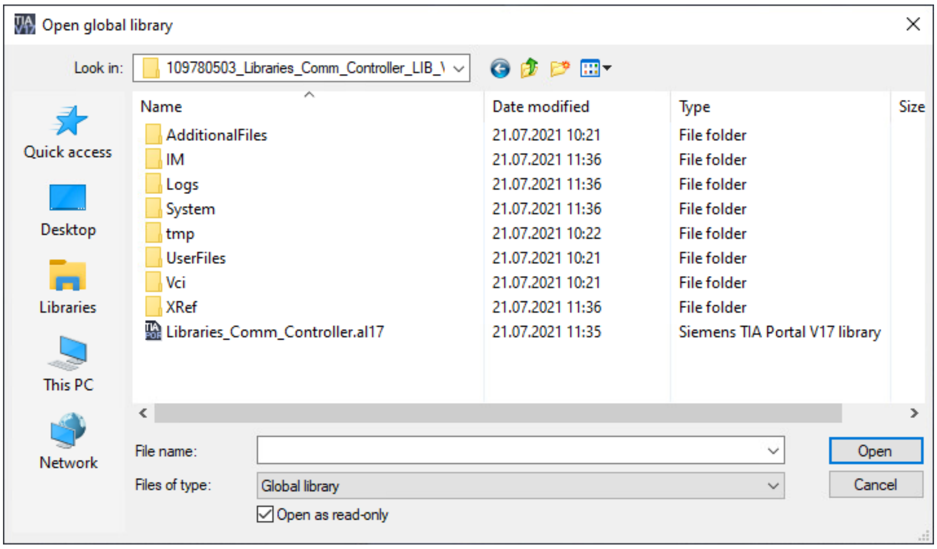
Library view

Project library

Global libraries

Name	Status	Version
Bu ns-and-Switches		
Long Functions		
Monitoring-and-control-obj...		
Documentation templates		

3. Select the global library "Libraries_Comm_Controller" and confirm the selection with the "Open" button.



Open global library

Look in: 109780503_Libraries_Comm_Controller_LIB_\

Name	Date modified	Type	Size
AdditionalFiles	21.07.2021 10:21	File folder	
IM	21.07.2021 11:36	File folder	
Logs	21.07.2021 11:36	File folder	
System	21.07.2021 11:36	File folder	
tmp	21.07.2021 10:22	File folder	
UserFiles	21.07.2021 10:21	File folder	
Vci	21.07.2021 10:21	File folder	
XRef	21.07.2021 11:36	File folder	
Libraries_Comm_Controller.al17	21.07.2021 11:35	Siemens TIA Portal V17 library	

File name:

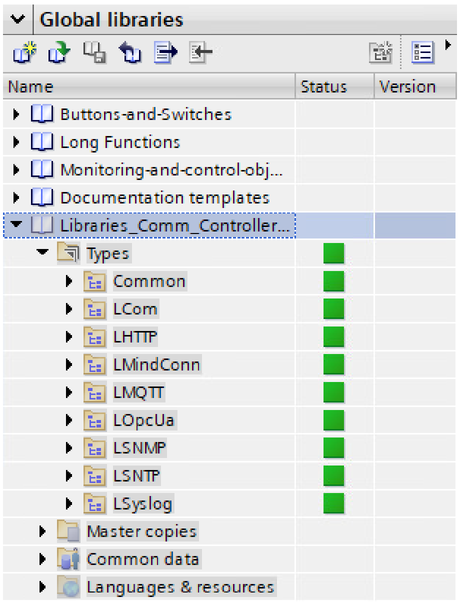
Files of type: Global library

☑ Open as read-only

© Siemens AG 2021 All rights reserved

Result

The Libraries_Comm_Controller library now appears in the Global libraries palette.

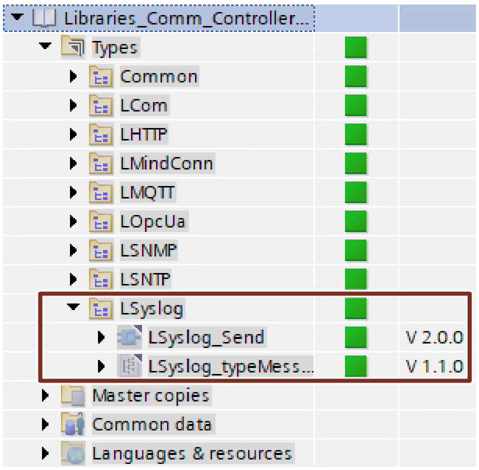


Name	Status	Version
Buttons-and-Switches		
Long Functions		
Monitoring-and-control-obj...		
Documentation templates		
Libraries_Comm_Controller...		
Types	🟩	
Common	🟩	
LCom	🟩	
LHTTP	🟩	
LMindConn	🟩	
LMQTT	🟩	
LOpcUa	🟩	
LSNMP	🟩	
LSNTP	🟩	
LSyslog	🟩	
Master copies		
Common data		
Languages & resources		

© Siemens AG 2021 All rights reserved

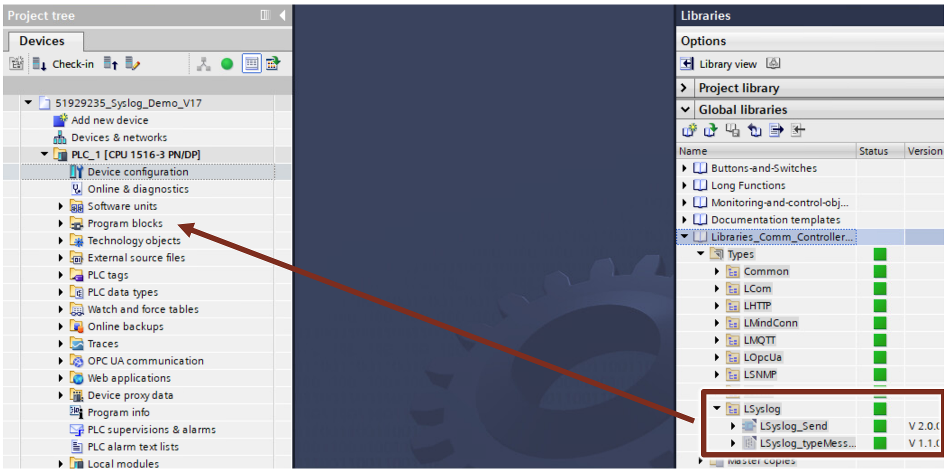
2.1.3.2 Copying the Syslog Block and Data Types into the User Program

In the "Libraries_Comm_Controller" library, you will find the FB and the data types used for the Syslog application under "Types > LSyslog".



Name	Status	Version
Libraries_Comm_Controller...		
Types	🟩	
Common	🟩	
LCom	🟩	
LHTTP	🟩	
LMindConn	🟩	
LMQTT	🟩	
LOpcUa	🟩	
LSNMP	🟩	
LSNTP	🟩	
LSyslog	🟩	
LSyslog_Send	🟩	V 2.0.0
LSyslog_typeMess...	🟩	V 1.1.0
Master copies		
Common data		
Languages & resources		

1. Move the "LSyslog" folder into the "Program blocks" folder of your device (e.g., the S7-1500 CPU) using drag & drop.

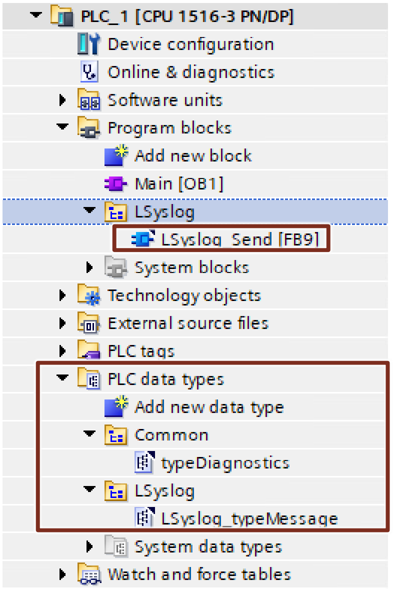


- 51929235_Syslog_Demo_V17
  - Add new device
  - Devices & networks
  - PLC_1 [CPU 1516-3 PN/DP]
    - Device configuration
    - Online & diagnostics
    - Software units
    - Program blocks
    - Technology objects
    - External source files
    - PLC tags
    - PLC data types
    - Watch and force tables
    - Online backups
    - Traces
    - OPC UA communication
    - Web applications
    - Device proxy data
    - Program info
    - PLC supervisions & alarms
    - PLC alarm text lists
    - Local modules

Name	Status	Version
Buttons-and-Switches		
Long Functions		
Monitoring-and-control-obj...		
Documentation templates		
Libraries_Comm_Controller...		
Types	🟩	
Common	🟩	
LCom	🟩	
LHTTP	🟩	
LMindConn	🟩	
LMQTT	🟩	
LOpcUa	🟩	
LSNMP	🟩	
LSyslog	🟩	
LSyslog_Send	🟩	V 2.0.(
LSyslog_typeMess...	🟩	V 1.1.(
Master copies		

© Siemens AG 2021 All rights reserved

The data types used by the FB are automatically inserted into the folder "PLC data types" on your device (e.g., an S7-1500 CPU).



- PLC_1 [CPU 1516-3 PN/DP]
  - Device configuration
  - Online & diagnostics
  - Software units
  - Program blocks
    - Add new block
    - Main [OB1]
    - LSyslog
      - LSyslog_Send [FB9]
    - System blocks
  - Technology objects
  - External source files
  - PLC tags
  - PLC data types
    - Add new data type
    - Common
      - typeDiagnostics
    - LSyslog
      - LSyslog_typeMessage
    - System data types
  - Watch and force tables

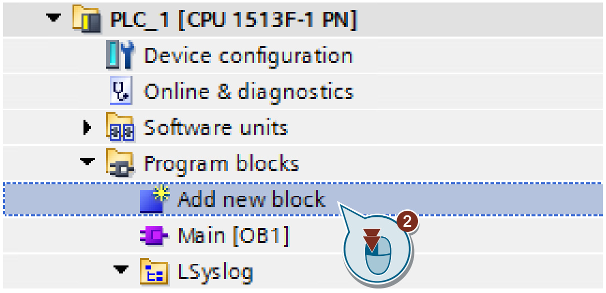
2.1.3.3 Creating a Global Data Block for the Syslog Application

In this Section, you will create a global data block that has the following tasks:

- Definition of connection parameters
- Control and monitor communication to the Syslog server
- Saving the Syslog message

Connection parameters

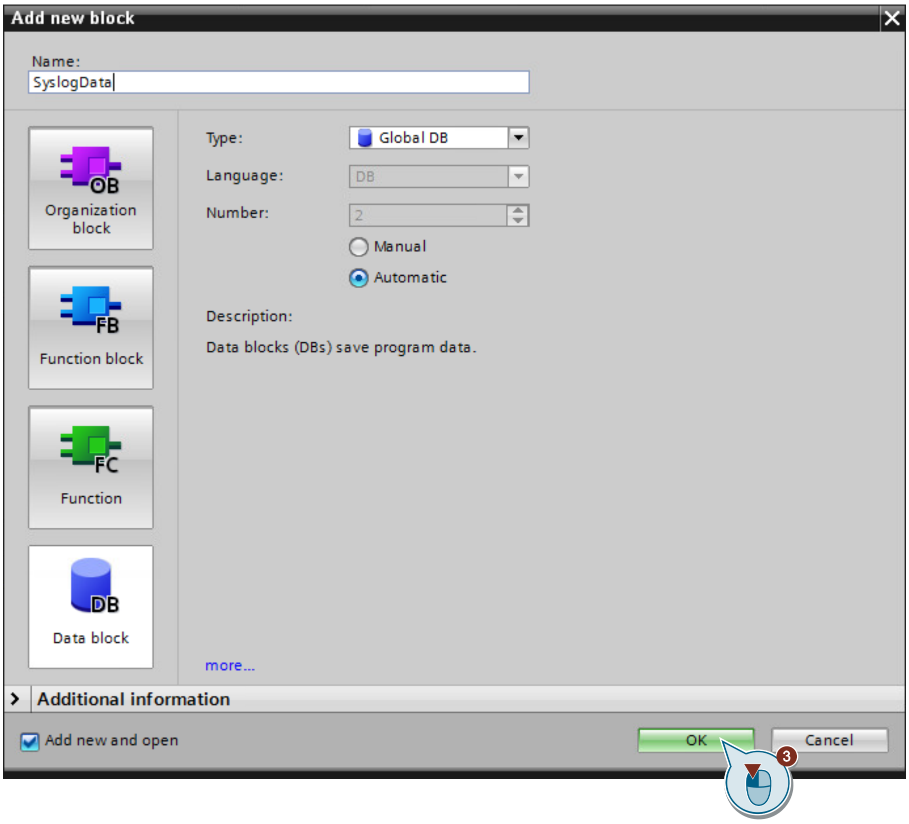
1. In the project navigation, go to the device folder of the S7 CPU.
2. Open the "Program blocks" folder and double-click the "Add new block" command.
   The dialog "Add new block" opens.



- PLC_1 [CPU 1513F-1 PN]
  - Device configuration
  - Online & diagnostics
  - Software units
  - Program blocks
    - Add new block
    - Main [OB1]
    - LSyslog

© Siemens AG 2021 All rights reserved

3. Create a new global DB for the Syslog data with the parameters shown in the graphic and confirm the dialog with "OK".



Add new block

Name: SyslogData

Type: Global DB

Language: DB

Number: 2

○ Manual

● Automatic

Description:

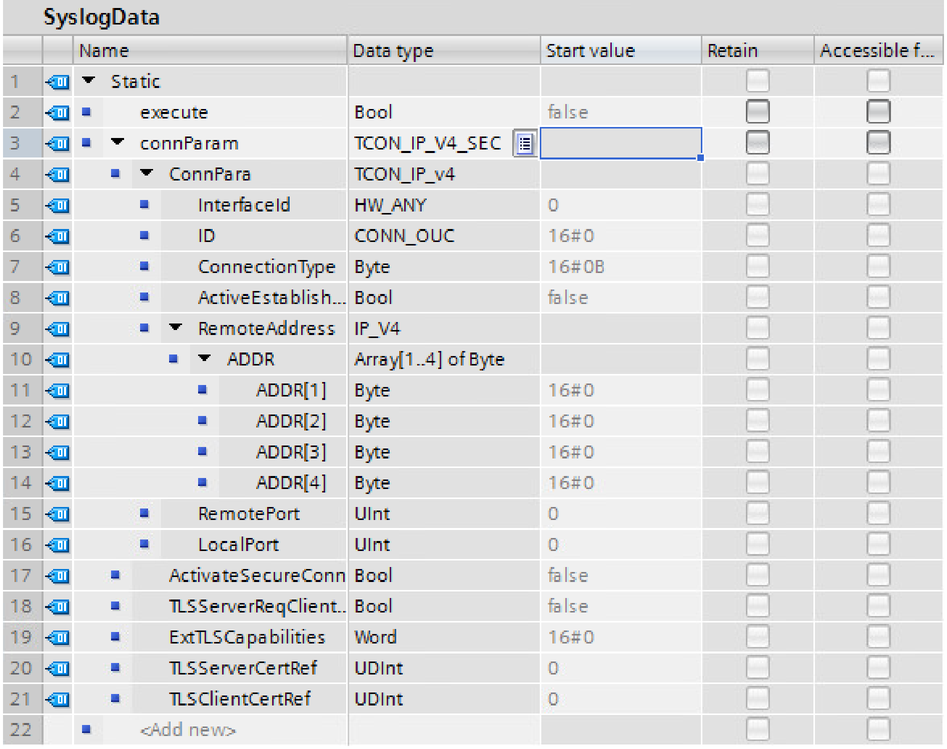
Data blocks (DBs) save program data.

more...

Additional information

☑ Add new and open

4. In the newly created data block, double-click "<Add new>" to create the variables with the respective data types as follows:



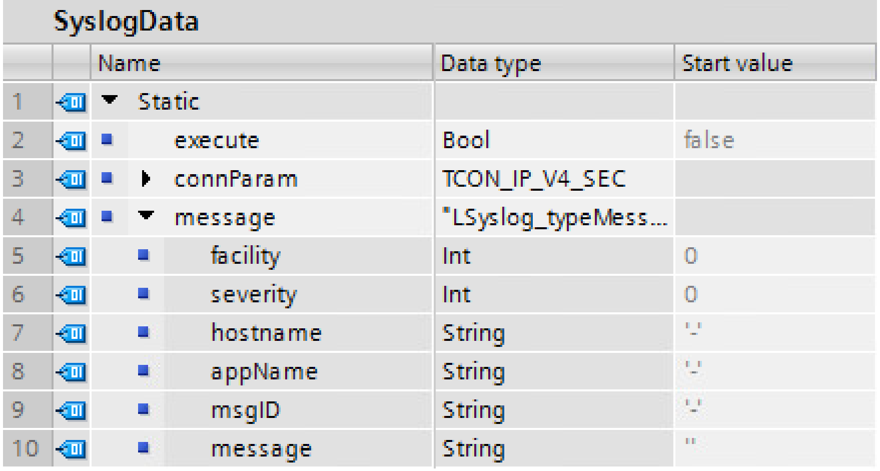
SyslogData

	Name	Data type	Start value	Retain	Accessible f...
1	Static			□	□
2	execute	Bool	false	□	□
3	connParam	TCON_IP_V4_SEC		□	□
4	ConnPara	TCON_IP_v4		□	□
5	InterfaceId	HW_ANY	0	□	□
6	ID	CONN_OUC	16#0	□	□
7	ConnectionType	Byte	16#0B	□	□
8	ActiveEstablish...	Bool	false	□	□
9	RemoteAddress	IP_V4		□	□
10	ADDR	Array[1..4] of Byte		□	□
11	ADDR[1]	Byte	16#0	□	□
12	ADDR[2]	Byte	16#0	□	□
13	ADDR[3]	Byte	16#0	□	□
14	ADDR[4]	Byte	16#0	□	□
15	RemotePort	UInt	0	□	□
16	LocalPort	UInt	0	□	□
17	ActivateSecureConn	Bool	false	□	□
18	TLSServerReqClient..	Bool	false	□	□
19	ExtTLSCapabilities	Word	16#0	□	□
20	TLSServerCertRef	UDInt	0	□	□
21	TLSClientCertRef	UDInt	0	□	□
22	<Add new>			□	□

© Siemens AG 2021 All rights reserved

Syslog message

In the new DB, double-click "<Add new>" to insert the variable "Message" with the data type "LSyslog_typeMessage" accordingly:

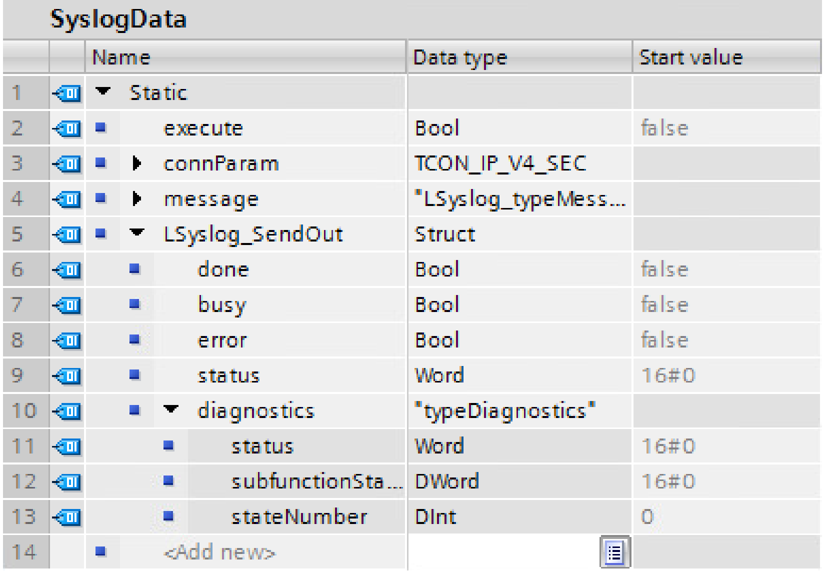


SyslogData

	Name	Data type	Start value
1	▼ Static		
2	■ execute	Bool	false
3	■ ▶ connParam	TCON_IP_V4_SEC	
4	■ ▼ message	"LSyslog_typeMess...	
5	■ facility	Int	0
6	■ severity	Int	0
7	■ hostname	String	'-'
8	■ appName	String	'-'
9	■ msgID	String	'-'
10	■ message	String	''

LSyslog_Send FB diagnostics

In the new DB, double-click "<Add new>", and create a structure "LSyslog_SendOut" with the following elements:



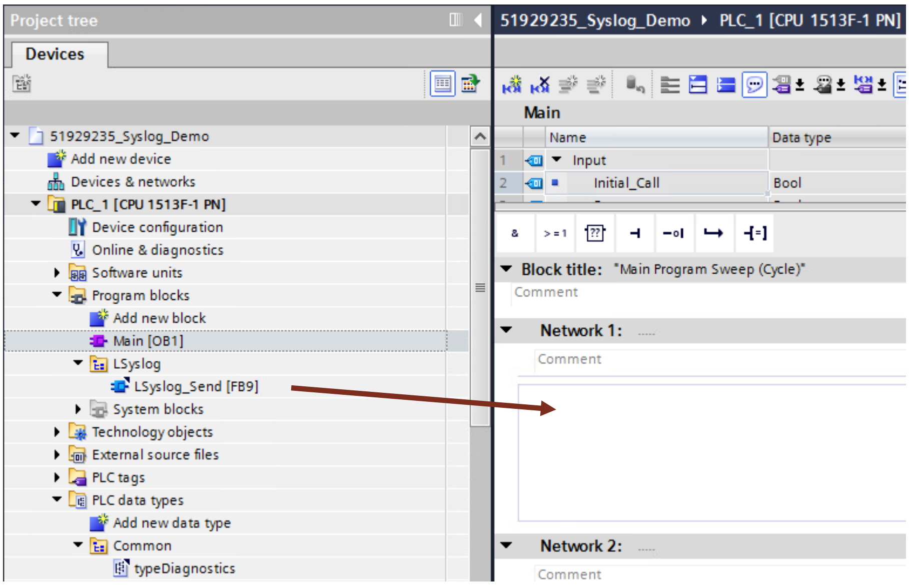
SyslogData

	Name	Data type	Start value
1	▼ Static		
2	■ execute	Bool	false
3	■ ▶ connParam	TCON_IP_V4_SEC	
4	■ ▶ message	"LSyslog_typeMess...	
5	■ ▼ LSyslog_SendOut	Struct	
6	■ done	Bool	false
7	■ busy	Bool	false
8	■ error	Bool	false
9	■ status	Word	16#0
10	■ ▼ diagnostics	"typeDiagnostics"	
11	■ status	Word	16#0
12	■ subfunctionSta...	DWord	16#0
13	■ stateNumber	DInt	0
14	■ <Add new>		

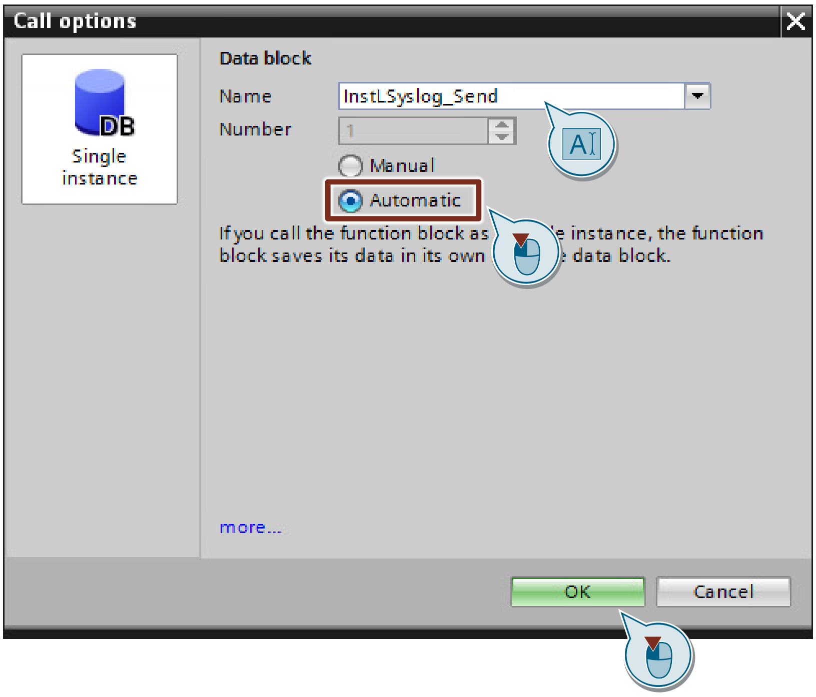
© Siemens AG 2021 All rights reserved

2.1.3.4 Call "LSyslog_Send" in the user program

1. In the project navigation, open the folder "Program blocks" of your CPU.
2. Double-click the block "Main [OB1]" to open the corresponding program editor.
3. Move the FB "LSyslog_Send" from the project navigation into any network within OB1 using drag & drop.



4. Create the corresponding instance DB.



Call options

DB Single instance

Data block

Name: InstLSyslog_Send

Number: 1

○ Manual

● Automatic

If you call the function block as ... instance, the function block saves its data in its own ... data block.

more...

OK Cancel

© Siemens AG 2021 All rights reserved

2.1.3.5 Assigning Variables to Inputs and Outputs of the "LSyslog_Send" FB

Assign the inputs and outputs of the "LSyslog_Send" FB with the variables that you created in the "SyslogData" data block (see Section 2.1.3.3).

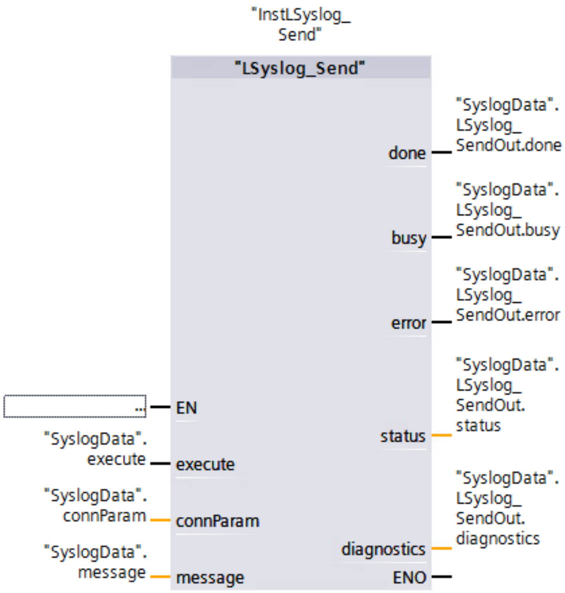
Table 2-1

Name	Data type	Connecting the FB
execute	"BOOL"	Input parameter FB "execute"
connParam	"TCON_IP_V4_SEC"	Throughput parameter FB "connParam"
message	"LSyslog_typeMessage"	Input parameter FB "message"
LSyslog_SendOut.done	"BOOL"	Output parameter FB "done"
LSyslog_SendOut.busy	"BOOL"	Output parameter FB "busy"
LSyslog_SendOut.error	"BOOL"	Output parameter FB "error"
LSyslog_SendOut.status	"WORD"	Output parameter FB "status"
LSyslog_SendOut.diagnostics	"typeDiagnostics"	Output parameter FB "diagnostics"

© Siemens AG 2021 All rights reserved

Connecting FB "LSyslog_Send"

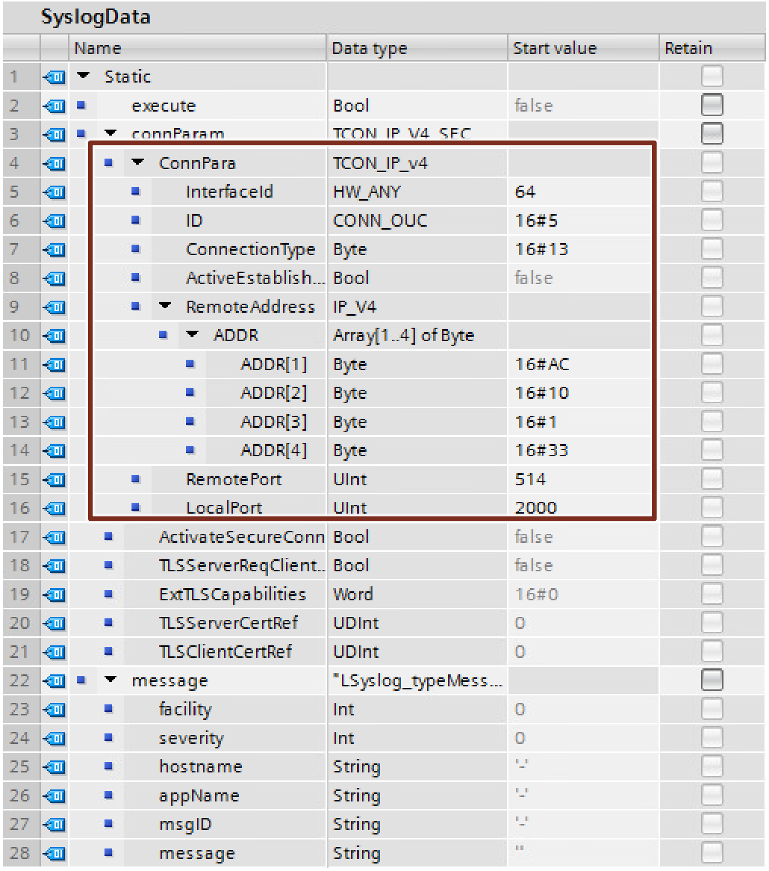
Figure 2-1


"InstLSyslog_Send"
"LSyslog_Send"
EN
"SyslogData".execute
execute
"SyslogData".connParam
connParam
"SyslogData".message
message
done
"SyslogData".LSyslog_SendOut.done
busy
"SyslogData".LSyslog_SendOut.busy
error
"SyslogData".LSyslog_SendOut.error
status
"SyslogData".LSyslog_SendOut.status
diagnostics
"SyslogData".LSyslog_SendOut.diagnostics
ENO

2.1.4 Parameterizing the "SyslogData" Data Block

1. Open the added global data block for the Syslog data.
2. Adjust the following variables:

Variable	Value
connParam.InterfaceId	Must be set to the ID of the communication interface. These can be found in the "Properties" of the PLC under "System constants". Set it to "0" for automatic selection.
connParam.ID	Unique connection ID (Can be freely assigned, but may only be used once)
connParam.ConnectionType	Connection type of the Syslog server (UDP = 13 or 19) (TCP/IP = 11 or 17)
connParam.RemoteAddress.ADDR	IP address of the Syslog server (in HEX)
connParam.RemotePort	Port of the Syslog server
connParam.LocalPort	Port of the PLC (default setting: 2000)



SyslogData

	Name	Data type	Start value	Retain
1	Static			□
2	execute	Bool	false	□
3	connParam	TCON_IP_V4_SEC		□
4	ConnPara	TCON_IP_v4		□
5	InterfaceId	HW_ANY	64	□
6	ID	CONN_OUC	16#5	□
7	ConnectionType	Byte	16#13	□
8	ActiveEstablish...	Bool	false	□
9	RemoteAddress	IP_V4		□
10	ADDR	Array[1..4] of Byte		□
11	ADDR[1]	Byte	16#AC	□
12	ADDR[2]	Byte	16#10	□
13	ADDR[3]	Byte	16#1	□
14	ADDR[4]	Byte	16#33	□
15	RemotePort	UInt	514	□
16	LocalPort	UInt	2000	□
17	ActivateSecureConn	Bool	false	□
18	TLSServerReqClient...	Bool	false	□
19	ExtTLSCapabilities	Word	16#0	□
20	TLSServerCertRef	UDInt	0	□
21	TLSClientCertRef	UDInt	0	□
22	message	"LSyslog_typeMess...		□
23	facility	Int	0	□
24	severity	Int	0	□
25	hostname	String	'-'	□
26	appName	String	'-'	□
27	msgID	String	'-'	□
28	message	String	''	□

3. Compile the project.
4. Download the project to your controller.

© Siemens AG 2021 All rights reserved

2.1.5 Operation

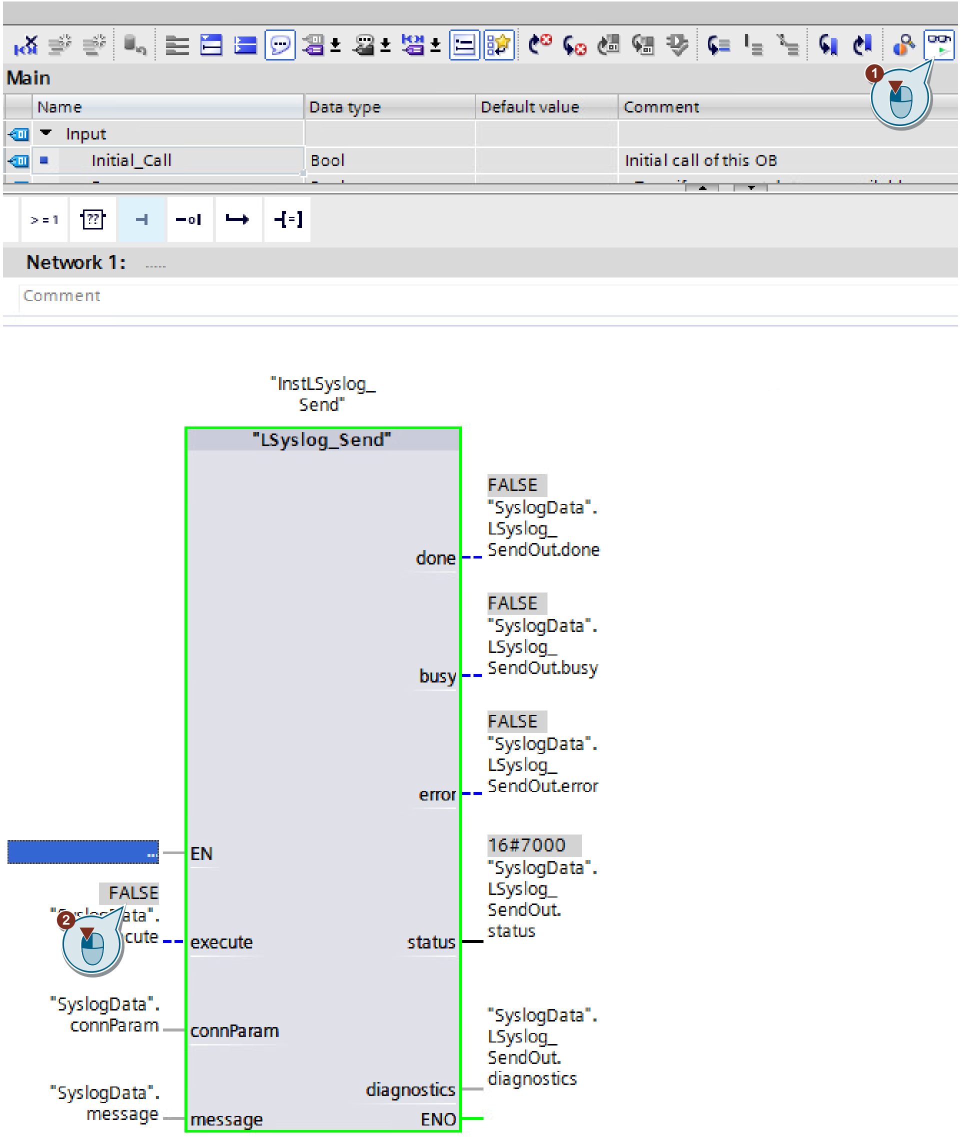
To send messages from the controller to the Syslog server, you must perform the following steps:

Establishing the connection to the server

1. Open the block in which you have inserted the FB "LSyslog_Send" and click the "Monitoring on/off" button.
2. Assign the variable "SyslogData.execute" at the "execute" input to "true". To do this, click the variable "execute" 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 output "done", a telegram has been sent.



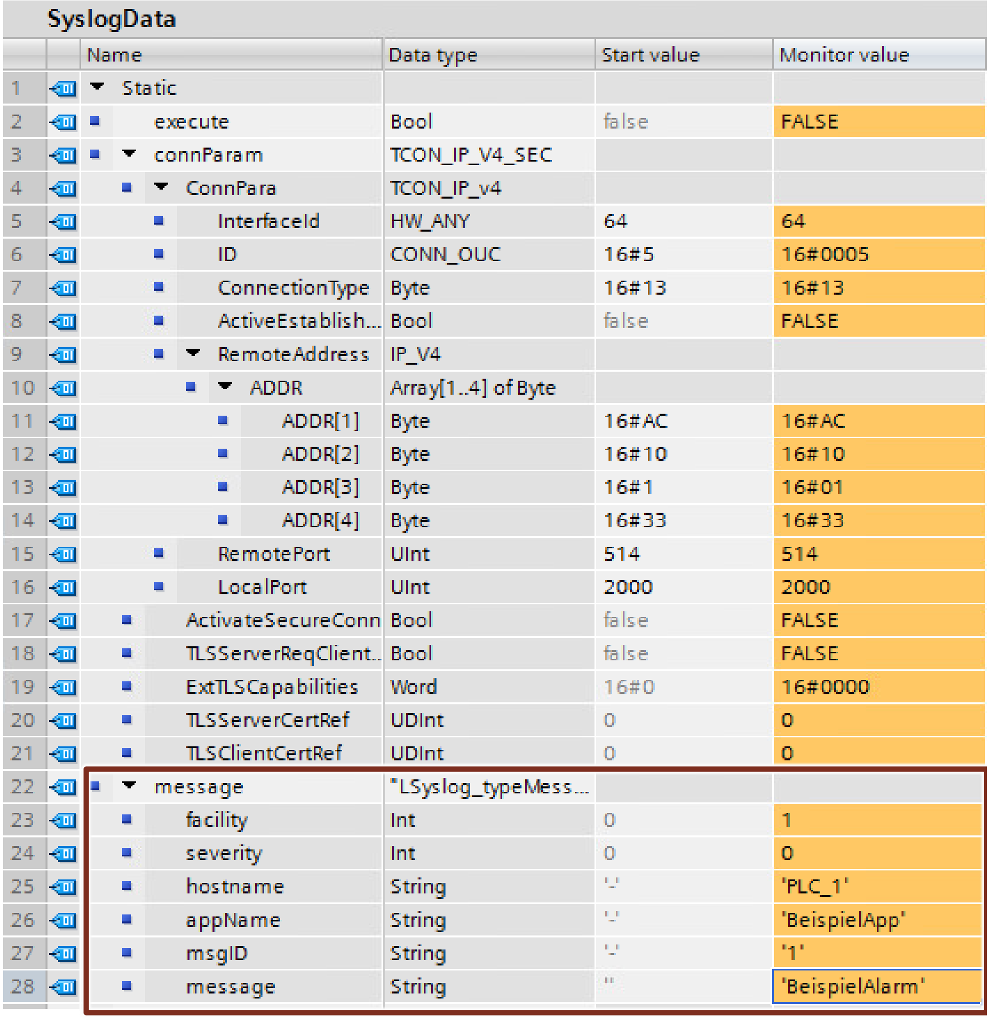
© Siemens AG 2021 All rights reserved

Generate Syslog message

To generate a warning message:

1. Open the "LSyslogData" data block. Click the "Monitoring on/off" button.
2. Enter values for "message.facility", "message.severity", "message.hostname", "message.appName", "message.msgID", and "message.message".

Note A description of the individual variables of the data type "LSyslog_typeMessage" can be found in 3.2.



SyslogData

	Name	Data type	Start value	Monitor value
1	Static			
2	execute	Bool	false	FALSE
3	connParam	TCON_IP_V4_SEC		
4	ConnPara	TCON_IP_v4		
5	InterfaceId	HW_ANY	64	64
6	ID	CONN_OUC	16#5	16#0005
7	ConnectionType	Byte	16#13	16#13
8	ActiveEstablish...	Bool	false	FALSE
9	RemoteAddress	IP_V4		
10	ADDR	Array[1..4] of Byte		
11	ADDR[1]	Byte	16#AC	16#AC
12	ADDR[2]	Byte	16#10	16#10
13	ADDR[3]	Byte	16#1	16#01
14	ADDR[4]	Byte	16#33	16#33
15	RemotePort	UInt	514	514
16	LocalPort	UInt	2000	2000
17	ActivateSecureConn	Bool	false	FALSE
18	TLSServerReqClient...	Bool	false	FALSE
19	ExtTLSCapabilities	Word	16#0	16#0000
20	TLSServerCertRef	UDInt	0	0
21	TLSClientCertRef	UDInt	0	0
22	message	"LSyslog_typeMess...		
23	facility	Int	0	1
24	severity	Int	0	0
25	hostname	String	'-'	'PLC_1'
26	appName	String	'-'	'BeispielApp'
27	msgID	String	'-'	'1'
28	message	String	''	'BeispielAlarm'

3. Set "execute" to "FALSE" and then back to "TRUE".

Result

A message was generated and sent to the Syslog server.

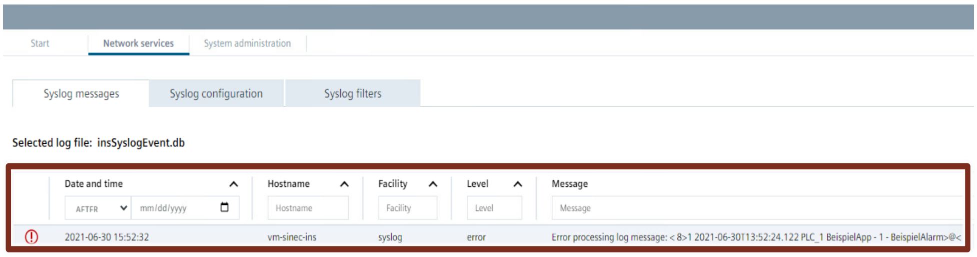
© Siemens AG 2021 All rights reserved

2.2 Reading out the Syslog Message in the Syslog Server SINEC INS

Switch to the web interface of the SINEC INS and then to the "Syslog service" ("Syslogservices").

Result

In the tab "Syslog messages" all received messages are displayed.



Selected log file: insSyslogEvent.db

	Date and time	Hostname	Facility	Level	Message
	AFTER mm/dd/yyyy	Hostname	Facility	Level	Message
ⓘ	2021-06-30 15:52:32	vm-sinec-ins	syslog	error	Error processing log message: < 8>1 2021-06-30T13:52:24.122 PLC_1 BeispielApp - 1 - BeispielAlarm>@<

© Siemens AG 2021 All rights reserved

2.3 Sending Security Messages using the Sample Project

A basic application of the Syslog protocol is sending security messages to the Syslog server. In the sample project, the functions "Get_Alarm" (see 3.4) and "GetChecksum" (see 3.5) are used to generate messages in the FB "CreateSecurityMessages".

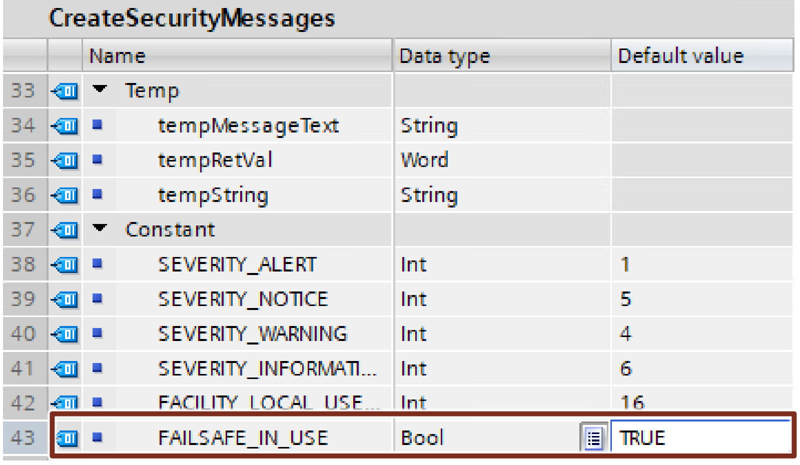
Requirements

You have downloaded the sample project from Industry Online Support and configured your syslog server (see chapter 2.1.1).
https://support.industry.siemens.com/cs/de/en/view/51929235

2.3.1 Adjusting the Sample Project

To start the sample project, you still need to adjust the following parameters in the example project:

- If necessary, replace the projected CPU with your CPU model
- IP address of the PLC (see 2.1.2)
- "ConnParam" of the "SyslogData" DB (see 2.1.4)
- If you use F blocks, you must set the default value of the "FAILSAFE_IN_USE" constant of the "CreateSecurityMessages" FB to TRUE



CreateSecurityMessages

	Name	Data type	Default value
33	▼ Temp		
34	tempMessageText	String	
35	tempRetVal	Word	
36	tempString	String	
37	▼ Constant		
38	SEVERITY_ALERT	Int	1
39	SEVERITY_NOTICE	Int	5
40	SEVERITY_WARNING	Int	4
41	SEVERITY_INFORMATI...	Int	6
42	FACILITY_LOCAL_USE...	Int	16
43	FAILSAFE_IN_USE	Bool	TRUE

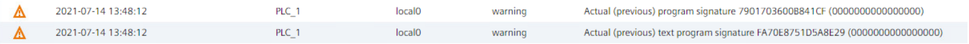
© Siemens AG 2021 All rights reserved

2.3.2 Generating a Security Message

After you have changed the parameters of the sample project, compile the program and load it into the controller. Security messages are sent automatically with the function block "CreateSecurityMessages". To send a self-created message, follow the instructions in Chapter 2.1.5.

Syslog message with the current and previous checksum

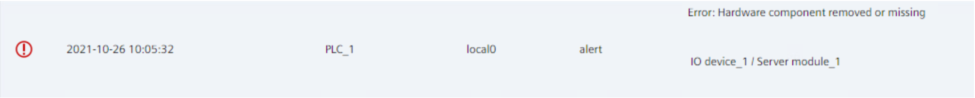
By changing the project, a new checksum of the program is created during the compile process. This is converted to a Syslog message by the "CreateSecurityMessages" block and sent to the Syslog server.
Example:



```
⚠  2021-07-14 13:48:12    PLC_1    local0    warning    Actual (previous) program signature 7901703600B841CF (0000000000000000)
⚠  2021-07-14 13:48:12    PLC_1    local0    warning    Actual (previous) text program signature FA70E8751D5A8E29 (0000000000000000)
```

Syslog message of an alarm

You can trigger an alarm from the controller by pulling out a module, for example. This alarm is converted to a Syslog message by the "CreateSecurityMessages" block and sent to the Syslog server.
Example:



```
                                                             Error: Hardware component removed or missing
ⓘ  2021-10-26 10:05:32    PLC_1    local0    alert
                                                             IO device_1 / Server module_1
```

© Siemens AG 2021 All rights reserved

3 Useful Information

3.1 The Syslog protocol

3.1.1 Description

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.

There are now many applications that are able to generate Syslog entries. A big advantage of Syslog is its clear structure and its use in distributed systems. In principle, Syslog entries from different computers can be sent via the network to a central computer and collected there.
Generating a Syslog entry is quite simple:
A UDP packet is sent to port 514 on a machine running a Syslog server. The content of the UDP packet may not exceed 1024 characters, must be defined in the US7 - ASCII character set and should be formatted accordingly. If necessary, the following information can be transferred to the server via formatting:

- Priority and type of package
- Time of generation
- Name of the source computer
- Different identification numbers

If packages are formatted incorrectly, they will also be accepted. However, the complete content is interpreted as message text. For unrecognized parameters (such as the time of generation), corresponding default values are used.

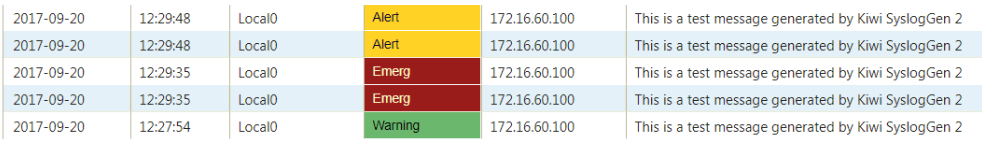
The Syslog protocol has a simple structure and can be divided into two main blocks: the header and the actual message.

Figure 3-1

Header
Message

The following graphic shows Syslog messages received by the Syslog server:

Figure 3-2



2017-09-20	12:29:48	Local0	Alert	172.16.60.100	This is a test message generated by Kiwi SyslogGen 2
2017-09-20	12:29:48	Local0	Alert	172.16.60.100	This is a test message generated by Kiwi SyslogGen 2
2017-09-20	12:29:35	Local0	Emerg	172.16.60.100	This is a test message generated by Kiwi SyslogGen 2
2017-09-20	12:29:35	Local0	Emerg	172.16.60.100	This is a test message generated by Kiwi SyslogGen 2
2017-09-20	12:27:54	Local0	Warning	172.16.60.100	This is a test message generated by Kiwi SyslogGen 2

© Siemens AG 2021 All rights reserved

3.2 The message header

Description

The header manages the following information:

- Message type
- Time
- VersionID
- Hostname

Note

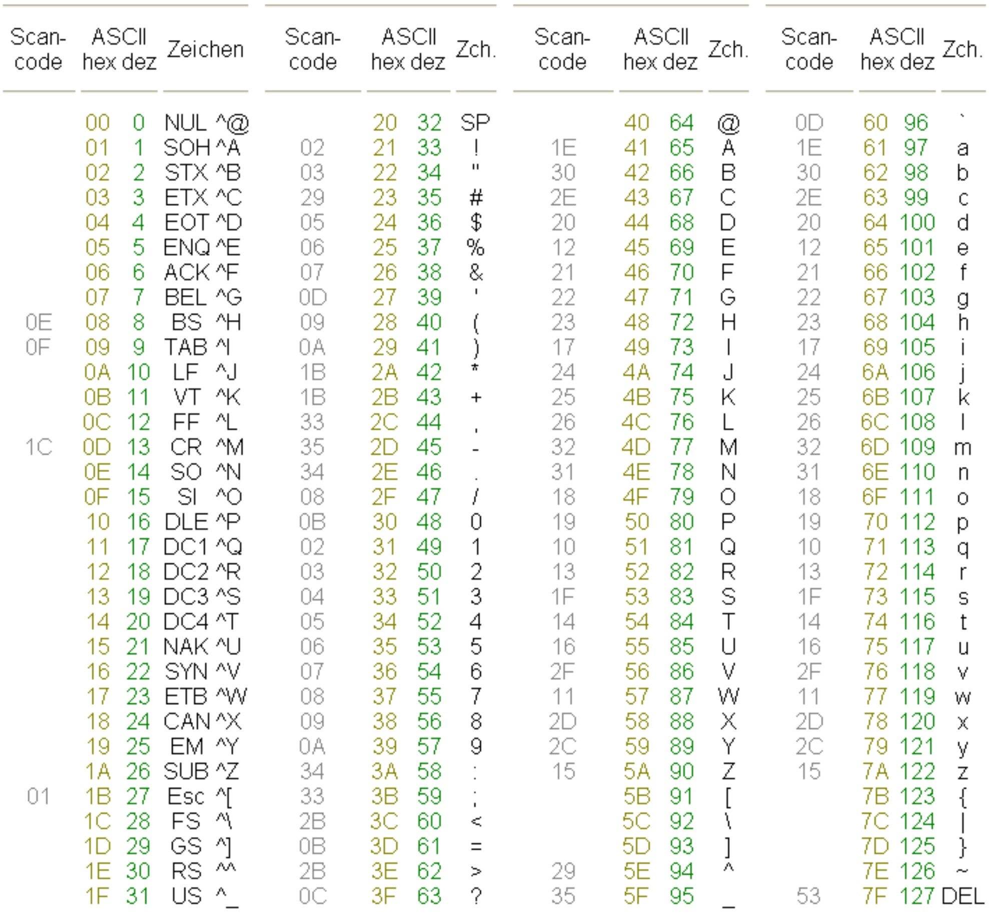
> Except for the "type of message", the Syslog client cannot make any further modifications to the header.
>
> The remaining parameters are all filled with values by the Syslog server.

Formatting

The characters used must be in ASCII (7-bit) format in an 8-bit field.

The following section shows the ASCII character table.

Figure 3-3: ASCII character table



Scan-code	ASCII hex	ASCII dez	Zeichen	Scan-code	ASCII hex	ASCII dez	Zch.	Scan-code	ASCII hex	ASCII dez	Zch.	Scan-code	ASCII hex	ASCII dez	Zch.
	00	0	NUL ^@		20	32	SP		40	64	@	0D	60	96	`
	01	1	SOH ^A	02	21	33	!	1E	41	65	A	1E	61	97	a
	02	2	STX ^B	03	22	34	"	30	42	66	B	30	62	98	b
	03	3	ETX ^C	29	23	35	#	2E	43	67	C	2E	63	99	c
	04	4	EOT ^D	05	24	36	$	20	44	68	D	20	64	100	d
	05	5	ENQ ^E	06	25	37	%	12	45	69	E	12	65	101	e
	06	6	ACK ^F	07	26	38	&	21	46	70	F	21	66	102	f
	07	7	BEL ^G	0D	27	39	'	22	47	71	G	22	67	103	g
0E	08	8	BS ^H	09	28	40	(	23	48	72	H	23	68	104	h
0F	09	9	TAB ^I	0A	29	41	)	17	49	73	I	17	69	105	i
	0A	10	LF ^J	1B	2A	42	*	24	4A	74	J	24	6A	106	j
	0B	11	VT ^K	1B	2B	43	+	25	4B	75	K	25	6B	107	k
	0C	12	FF ^L	33	2C	44	,	26	4C	76	L	26	6C	108	l
1C	0D	13	CR ^M	35	2D	45	-	32	4D	77	M	32	6D	109	m
	0E	14	SO ^N	34	2E	46	.	31	4E	78	N	31	6E	110	n
	0F	15	SI ^O	08	2F	47	/	18	4F	79	O	18	6F	111	o
	10	16	DLE ^P	0B	30	48	0	19	50	80	P	19	70	112	p
	11	17	DC1 ^Q	02	31	49	1	10	51	81	Q	10	71	113	q
	12	18	DC2 ^R	03	32	50	2	13	52	82	R	13	72	114	r
	13	19	DC3 ^S	04	33	51	3	1F	53	83	S	1F	73	115	s
	14	20	DC4 ^T	05	34	52	4	14	54	84	T	14	74	116	t
	15	21	NAK ^U	06	35	53	5	16	55	85	U	16	75	117	u
	16	22	SYN ^V	07	36	54	6	2F	56	86	V	2F	76	118	v
	17	23	ETB ^W	08	37	55	7	11	57	87	W	11	77	119	w
	18	24	CAN ^X	09	38	56	8	2D	58	88	X	2D	78	120	x
	19	25	EM ^Y	0A	39	57	9	2C	59	89	Y	2C	79	121	y
	1A	26	SUB ^Z	34	3A	58	:	15	5A	90	Z	15	7A	122	z
01	1B	27	Esc ^[	33	3B	59	;		5B	91	[		7B	123	{
	1C	28	FS ^\	2B	3C	60	<		5C	92	\		7C	124	|
	1D	29	GS ^]	0B	3D	61	=		5D	93	]		7D	125	}
	1E	30	RS ^^	2B	3E	62	>	29	5E	94	^		7E	126	~
	1F	31	US ^_	0C	3F	63	?	35	5F	95	_	53	7F	127	DEL

© Siemens AG 2021 All rights reserved

Structuring

The Syslog protocol prescribes a specified order and structure of the parameters for the header. If these rules are disregarded, the information from the Syslog server cannot be interpreted as such.

In detail, the structure is as follows:

PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID

A Syslog message does not necessarily have to contain all elements. Unrecognized parameters are allocated default values.

Note All elements and parameters must be entered in ASCII format (7 bits) in the header.

The parameters have the following meanings:

Table 3-1: Parameters of a Syslog message

Parameters	Meaning
PRI	The PRI range must be delimited by the characters "< (%d60)" and "> (%d62)" and has a size of 3 to 5 characters. Within the PRI, the priority of the Syslog message is encoded; this is divided into a severity and facility field.
VERSION	The VersionID has a size of up to 2 bytes and may only contain the characters from 1 to 9 (%d49-57). This field can be used to specify the version number of the Syslog specification.
TIMESTAMP	This area includes the timestamp and has its own structure.
HOSTNAME	HOSTNAME references the source computer with its name and IP address. The length can be from 1 to 255 characters and may contain all characters from %d33 to126. If no information about the source computer is known, the character "-" is output.
APP-NAME	APP-NAME contains the application name. The length can be from 1 to 48 characters. All characters from %d33 to 126 are allowed. If no application name is known, "-" is output.
PROCID	PROCID carries the ProcessID as information. The length can be from 1 to 128 characters. All characters from %d33 to 126 are allowed. If no ID is known, "-" is output.
MSGID	This parameter is used to identify the message and provides a length of 1 to 32 characters. All characters from %d33 to 126 are allowed. If no ID is known, "-" is displayed.
SP	Corresponds to the ASCII Code %d32.

Note Additional information on the meaning of the parameters can be found in RFC 5424.

https://tools.ietf.org/html/rfc5424

The coding for the PRI area

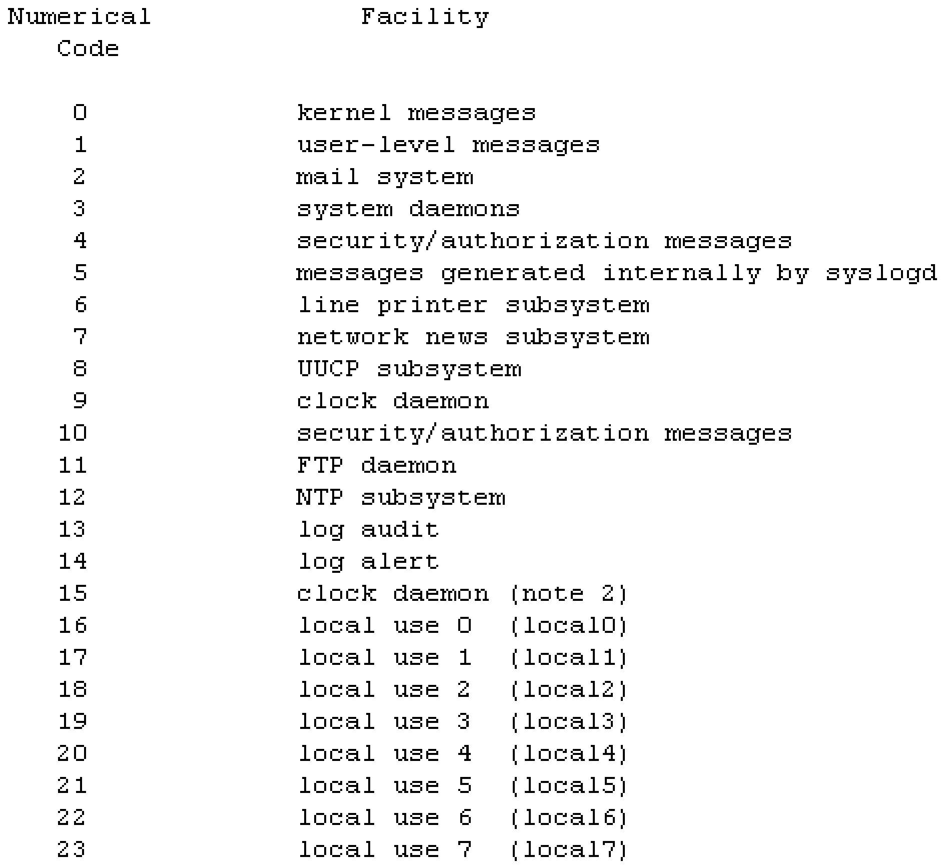
PRI stands for priority and defines the origin (facility field) and the severity (severity field) of the message. This parameter is the only one that can be modified via the Syslog client.

© Siemens AG 2021 All rights reserved

For the facility field there are 5 bits available which, depending on the numerical value, indicate the service or component which generated the Syslog message.

An excerpt from RFC 5424 shows the possible value ranges:

Figure 3-4: Excerpt from the RFC 5424 facility

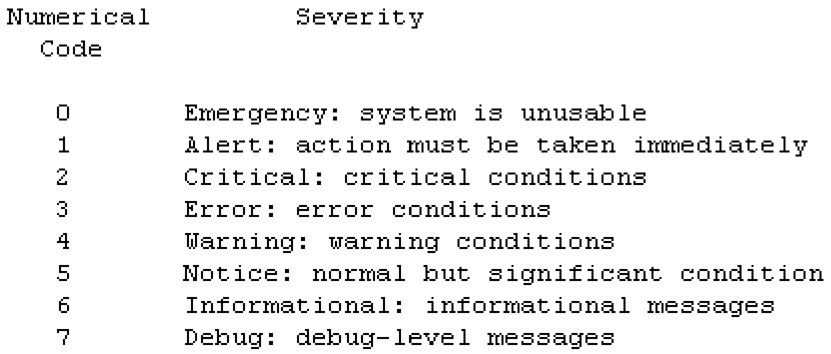


Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

For the severity field, there are 3 bits that define the severity of the Syslog message, depending on the numerical value.

An excerpt from RFC 5424 shows the possible value ranges:

Figure 3-5: Excerpt from the RFC 5424 severity



Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

The value to be entered between the characters "<[Value of Priority]>" (coded as ASCII characters) is calculated as follows:

Priority value = facility value * 8 + severity

© Siemens AG 2021 All rights reserved

Example:

A "local use 4" message (Facility = 20) with a "Notice" severity level (Severity = 5) has a Priority value of 20*8 + 5 = 165.
This result must be placed between the brackets as ASCII characters. In this case, the parameter PRI in the header is a total of 5 bytes long and contains as value "<165>" or in decimal terms "%d60 %d49 %d54 %d53 %d62".

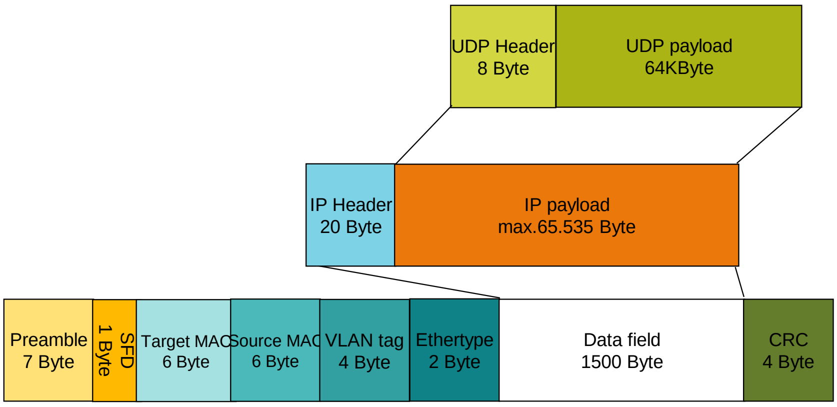
3.3 The transmission mechanism

Syslog uses UDP/IP and Ethernet as transmission protocol.
UDP is a connectionless and therefore unreliable transport protocol. A successful transmission cannot be 100% guaranteed.

For the transmission of the Syslog messages, these are packed into the payload area of the UDP frame. Theoretically, the Syslog message could take up the full capacity of the UDP payload (64kbyte). However, since the UDP frame is itself packed into the payload area of the IP frame, which in turn is in the address of the Ethernet, the size of a Syslog message is limited to the maximum size of the Ethernet payload area.

The data field for Ethernet measures 1500 bytes. With the overhead of the headers (IP (20 bytes), UDP (8 bytes) and the Syslog message), the Syslog message text must not exceed 1024 bytes in size.

Figure 3-6: Telegram frame structure



3.4 The "Get_Alarm" command

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

Messages 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" command here:
https://support.industry.siemens.com/cs/ww/en/view/109748168

© Siemens AG 2021 All rights reserved

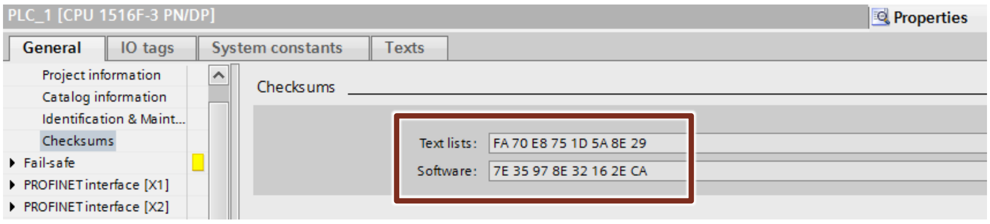
3.5 The "GetChecksum" command

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 CPU 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 CPU is the same program that you downloaded a long time ago, or if it has been changed in the meantime.

Figure 3-7: Checksum



Checksums

Text lists: FA 70 E8 75 1D 5A 8E 29

Software: 7E 35 97 8E 32 16 2E CA

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 compiled, the checksum remains the same.

Read out checksum

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

For more information about GetChecksum, see the TIA Portal Help or the manual. You can find the manual at the following link:

https://support.industry.siemens.com/cs/ww/en/view/109747136

© Siemens AG 2021 All rights reserved

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, application examples and videos – all information is accessible with just a few mouse clicks:

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.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

© Siemens AG 2021 All rights reserved

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

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 on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of this "LSyslog" application example https://support.industry.siemens.com/cs/ww/en/view/51929235
\3\	Link to the entry page of the Communication Libraries documentation https://support.industry.siemens.com/cs/ww/en/view/109780503
\4\	Link to RFC 5424 http://tools.ietf.org/html/rfc5424
\5\	Link to the entry page of the application example "Get_Alarm" https://support.industry.siemens.com/cs/ww/en/view/109748168
\6\	Link to the TIA Portal Manual V17 https://support.industry.siemens.com/cs/de/en/view/109798671

4.3 Change documentation

Table 4-2

Version	Date	Modifications
V1.0	01/2018	First version
V2.0	11/2021	Adaptation for new library block

© Siemens AG 2021 All rights reserved