

**SIEMENS**

*Ingenuity for life*

*Industry Online Support*

Home

# Safety Function with PROFINET IO via IWLAN

Safety Integrated / S7-1500 F-CPU/ IWLAN

<https://support.industry.siemens.com/cs/ww/en/view/28609440>

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>.

# Table of contents

<b>Legal information</b> .....	<b>2</b>
<b>1 Introduction</b> .....	<b>4</b>
1.1 Overview.....	4
1.2 Principle of operation.....	5
1.3 Components used .....	7
<b>2 Engineering</b> .....	<b>8</b>
2.1 Evaluation of the safety function .....	8
2.2 Hardware setup .....	10
2.3 Configuration .....	10
2.4 Parameterization .....	11
2.4.1 Parameterization of the SCALANCE network components .....	11
2.4.2 Determination and parameterization of the update time .....	19
2.4.3 Determination and parameterization of the F-monitoring time.....	20
2.5 Programming.....	23
2.5.1 Standard user program .....	23
2.5.2 Safety program.....	24
2.6 Operation.....	27
2.7 Error handling.....	28
<b>3 Appendix</b> .....	<b>29</b>
3.1 Service and support .....	29
3.2 Industry Mall .....	30
3.3 Links and literature .....	30
3.4 Change documentation .....	30

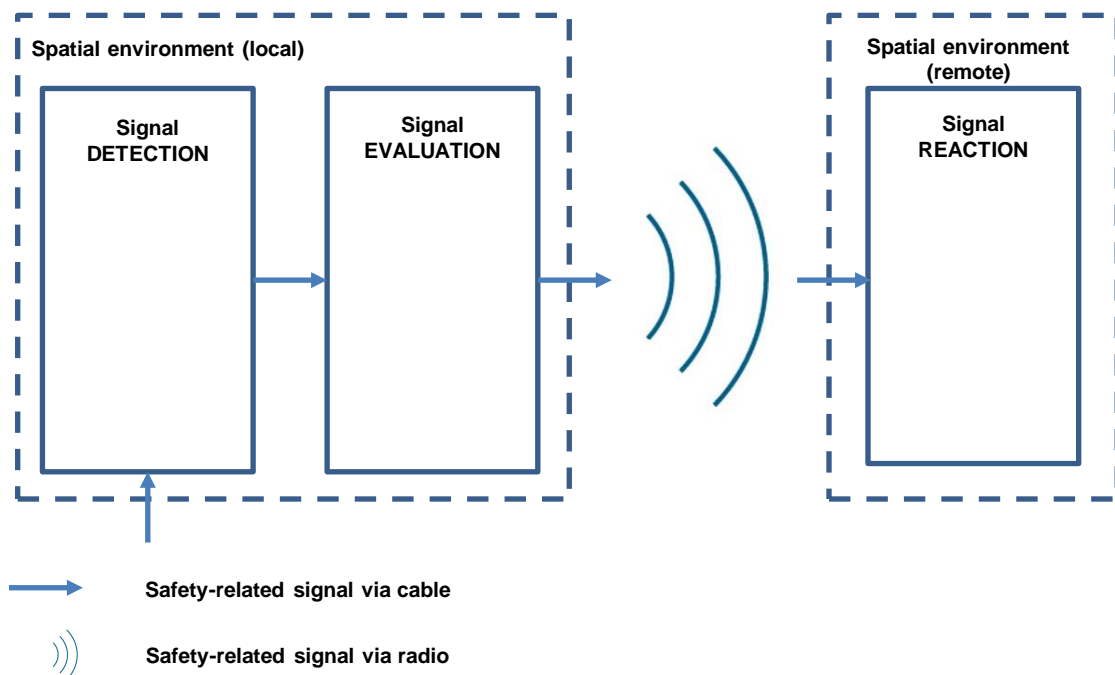
# 1 Introduction

## 1.1 Overview

### PROFIsafe transmission methods

Use of the PROFIsafe protocol in safety-related automation solutions is regarded as state of the art today. The safety mechanisms of PROFIsafe not only act independent of the bus system in use (e.g. PROFIBUS or PROFINET) but they also apply to wireless transmission technologies. This application example demonstrates the latter:

Figure 1-1 Safety-related signal via wireless transmission technology (radio)



### Focus of this application example

This application example implements a supplementary "Emergency Stop" safety function. The function achieves the highest Performance Level (PL e) or the highest Safety Integrity Level (SIL 3) in this example. The safety-related signal for switching off the actuator takes place over a wireless connection (see [Figure 1-1](#)).

Based on this scenario, the application example explains in particular the engineering required to implement the wireless connection. And all while taking the safety-related application into account.

The iFeature iPCF (industrial Point Coordination Function) is suitable for use in applications requiring reliable data exchange in a PROFINET network, also through the air, using Industrial Wireless LAN (IWLAN). In contrast to the IEEE 802.11 standard, the access point (AP) controls the communication of the IWLAN clients, which prevents collisions and enables deterministic data communication. In addition, iPCF also allows a very fast handover between radio cells of less than 50 ms.



## 1.2 Principle of operation

### Safety function

The implemented safety function (Emergency Stop) is based primarily on use of the following components:

- Software
  - Safety Advanced add-on software for the TIA Portal
  - PROFIsafe profile
- Hardware
  - PL/SIL-certified components

### Communication

Communication takes place using PROFINET IO with the PROFIsafe profile, over both a wired connection and an Industrial WLAN (IWLAN).

### Automation solution

[Figure 1-2](#) shows the automation solution.

The "Spatial environment" column refers to the location at which the tag is being read in or out (see [Figure 1-1](#)).

Table 1-1 Input tags in the S7 program

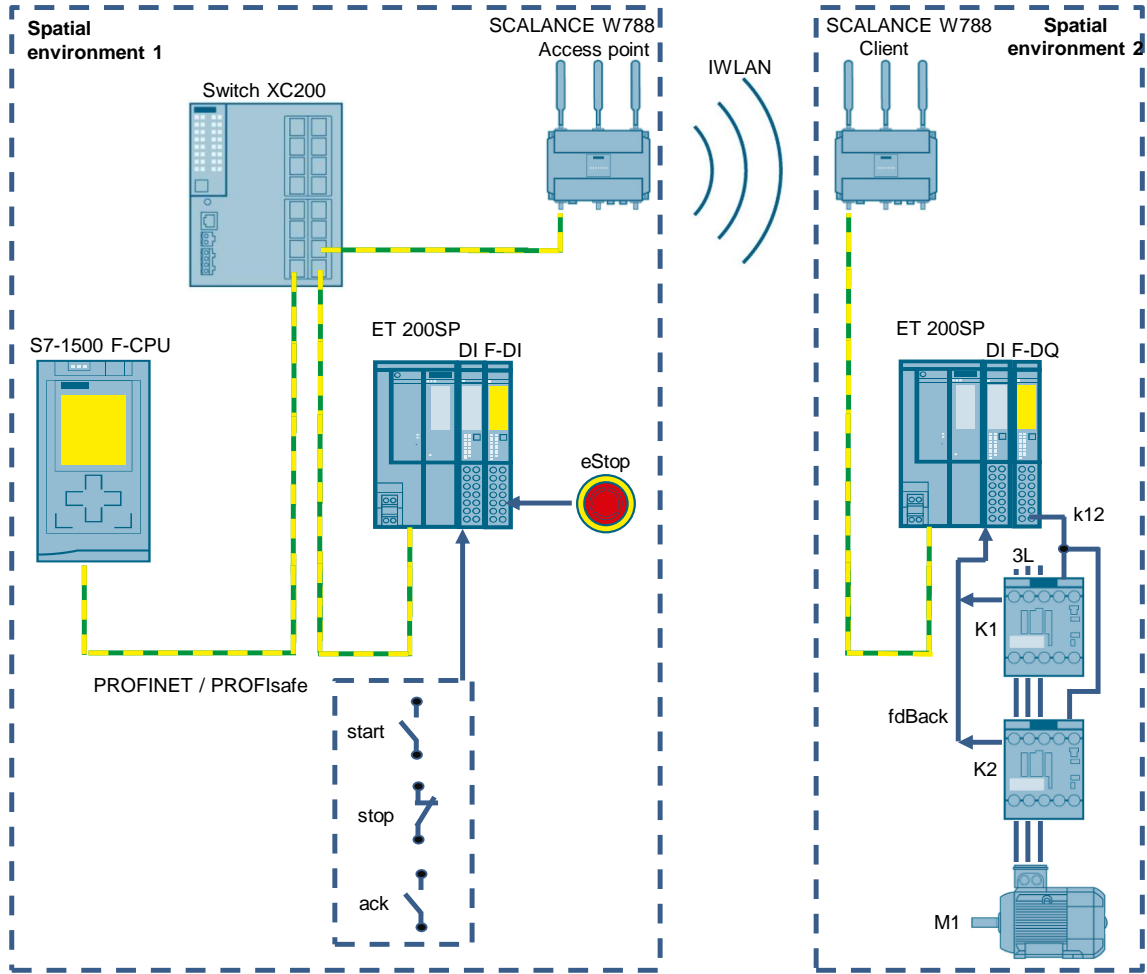
Tag	Data type	Standard or Safety tag	Note	Spatial environment
start	BOOL	Standard	Operational "Start"	Local
stop	BOOL	Standard	Operational "Stop"	Local
ack	BOOL	Standard	Acknowledgment	Local
fdBack	BOOL	Standard	Feedback signal of contactors K1 and K2	Remote
eStop	BOOL	Safety	Emergency Stop signal	Local

Table 1-2 Output tag in the S7 program

Tag	Data type	Standard or Safety tag	Note	Spatial environment
k12	BOOL	Safety	Control signal for contactors K1 and K2	Remote

# 1 Introduction

Figure 1-2 Automation solution



## 1.3 Components used

The following hardware and software components were used to create this application example:

Table 1-3 Hardware components

Component	Quantity	Article number	Note
CPU 1516F-3PN/DP	1	6ES7516-3FN00-0AB0	
ET 200SP BusAdapter	2	6ES7193-6AR00-0AA0	
ET 200SP, IM155-6PN HF	2	6ES7155-6AU00-0CN0	
ET 200SP, DI 8x24VDC ST	2	6ES7131-6BF00-0BA0	
ET 200SP, F-DI 8x24VDC HF	1	6ES7136-6BA00-0CA0	
ET 200SP, F-DQ 4xDC 24V/2A	1	6ES7136-6DB00-0CA0	
ET 200SP, server module	1	6ES7193-6PA00-0AA0	
BaseUnit Type A0, BU15-P16+A10+2D	2	6ES7193-6BP20-0DA0	
BaseUnit Type A0, BU15-P16+A0+2B	2	6ES7193-6BP00-0BA0	
Emergency stop	1	3SU1851-0NB00-2AA2	
Contactors	2	3RT2015-1BB42	3 kW/400 V 1 NC, 24 VDC 3-pin
SCALANCE W788-2 RJ45	1	6GK5788-2FC00-0AA0	Access point
SCALANCE W774-1 RJ45	1	6GK5774-1FX00-0AA0	Client
Key-Plug W740 iFeatures		6GK5907-4PA00	
Key-Plug W780 iFeatures		6GK5907-8PA00	

This application example consists of the following components:

Table 1-4 Software components

Component	File name	Note
STEP 7 Professional V16	6ES7822-1AA06-0YA5	
Safety Advanced V16	6ES7833-1FA16-0YA5	

## 2 Engineering

### 2.1 Evaluation of the safety function

#### Definition of the safety function

The (supplementary) "Emergency Stop" safety function examined in this application example is as follows:

*Pressing the Emergency Stop ("eStop") results in the switching off of the actuator ("k12").*

#### Implementation of the safety function

The safety function is implemented by certified hardware (F-CPU, F-I/O) and certified software (Safety Advanced).

#### Achievable Performance Level and Safety Integrity Level

In this application example, the safety function achieves:

- PL e in accordance with ISO 13849-1:2016
- SIL 3 in accordance with IEC 62061:2016

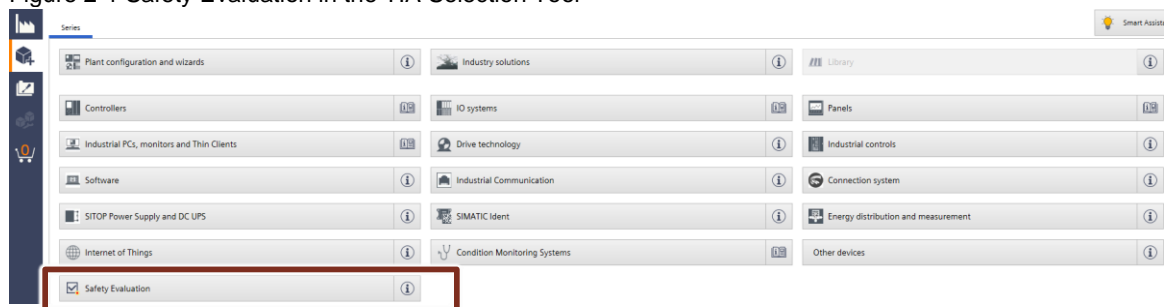
Achievement of PL e / SIL 3 is valid for the following basic conditions:

- Use of the hardware and software of this application example
- Assumptions made for the "Emergency Stop" safety function, e.g.:
  - Number of actuations of the Emergency Stop within a certain time.
  - CCF (common cause failure factor) > 65

#### Tool for verification of PL e / SIL 3

The PL e / SIL 3 rating is verified with Safety Evaluation from the TIA Selection Tool:

Figure 2-1 Safety Evaluation in the TIA Selection Tool



#### Link to TIA Selection Tool

<https://support.industry.siemens.com/cs/ww/en/view/109767888>

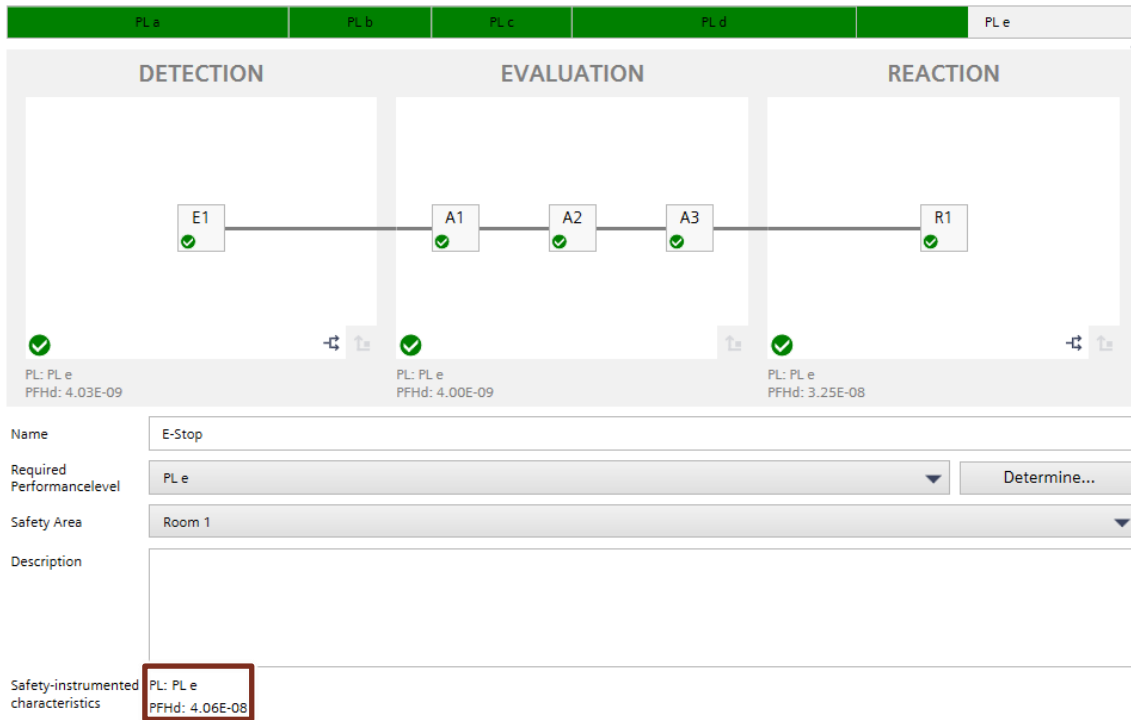
#### Result of Safety Evaluation

[Figure 2-2](#) and [Figure 2-3](#) show the achieved PL and SIL, respectively.



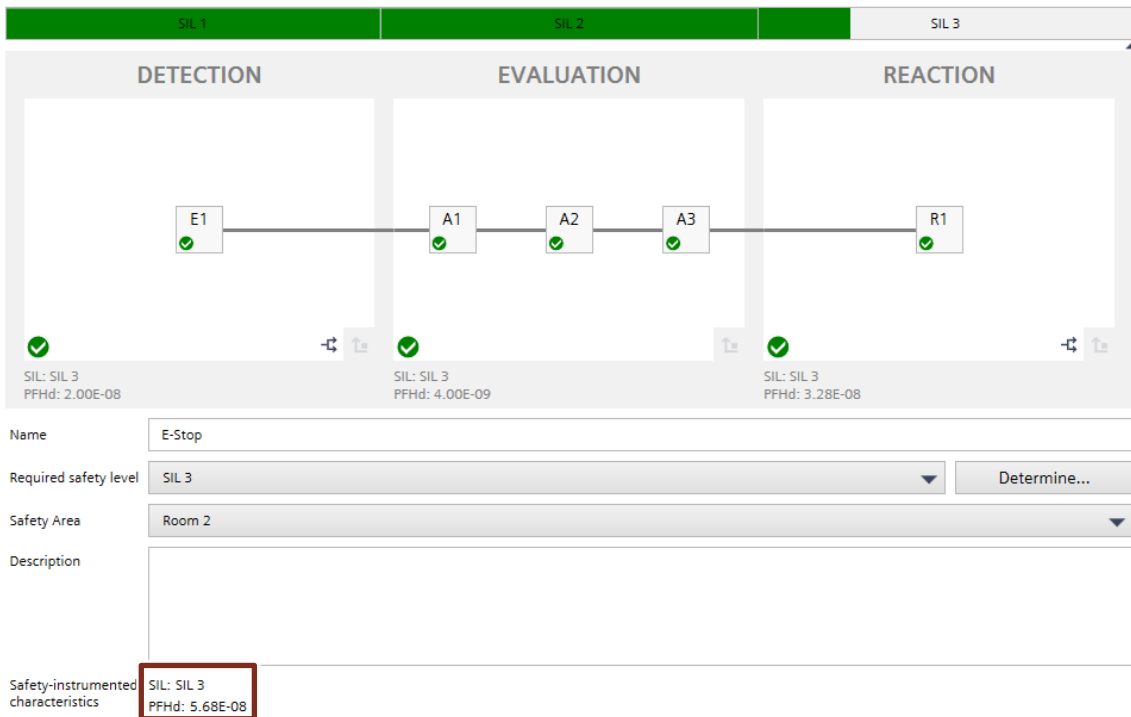
### PL e in accordance with ISO 13849-1:2016

Figure 2-2 Evaluation of the safety function in accordance with ISO 13849-1:2016



### SIL 3 in accordance with IEC 62061:2016

Figure 2-3 Evaluation of the safety function in accordance with IEC 62061:2016



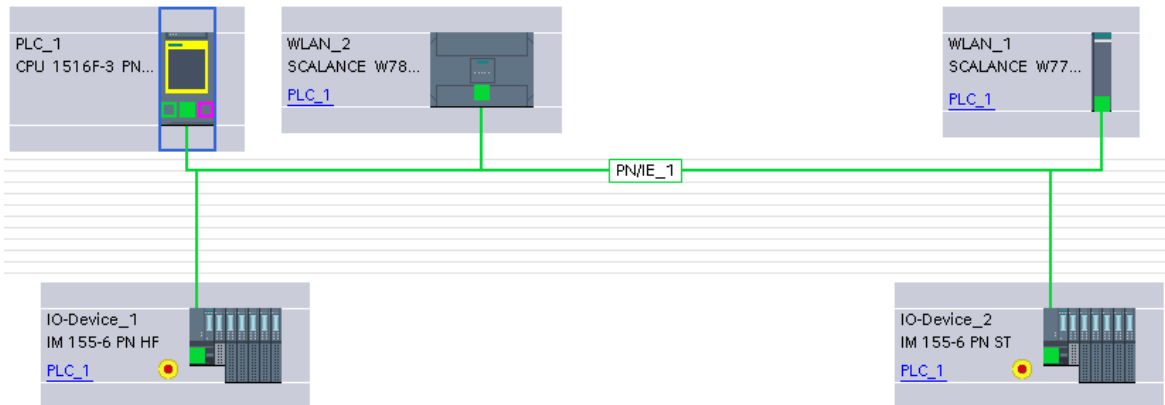
## 2.2 Hardware setup

For the hardware setup, refer to [Figure 1-2](#) or section [2.3](#).

## 2.3 Configuration

### Hardware configuration in STEP 7

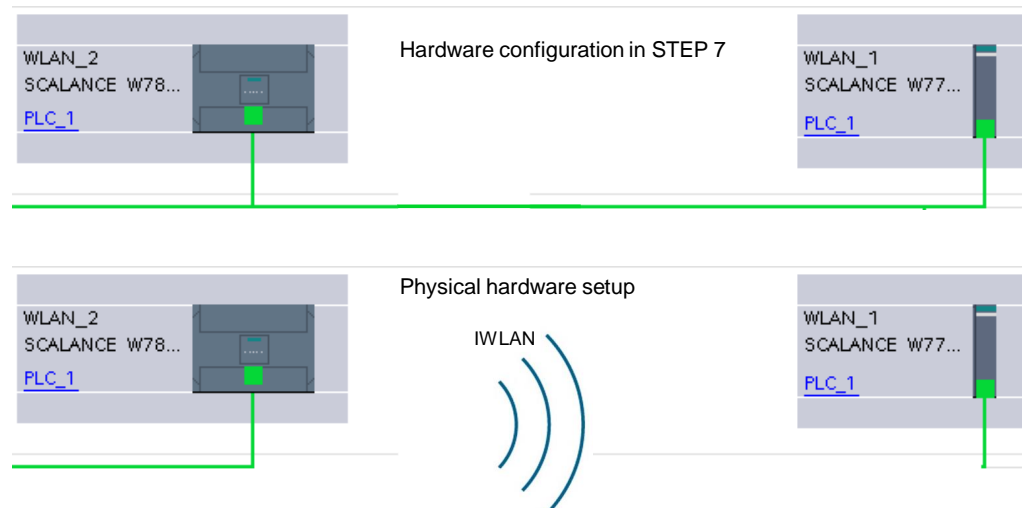
Figure 2-4 Hardware configuration in STEP 7



### Hardware configuration and physical setup

The hardware configuration presented above shows the configured network in a (PROFINET-)wired arrangement. The connection between the two SCALANCE network components in the physical setup is wireless, however (see next figure).

Figure 2-5 Hardware configuration and physical setup



The SCALANCE W components are integrated into the TIA Portal to be used as PROFINET devices. Configuration is done via Web based Management (WBM), see chapter [2.4.1](#).

Adding a SCALANCE as PROFINET device is also possible by downloading the current GSDML file from the WBM at "System > Load & Save > GSDML" and installing it in STEP 7.

## 2.4 Parameterization

### 2.4.1 Parameterization of the SCALANCE network components

This section describes the parameterization of the SCALANCE W hardware components.

#### Web Based Management

**NOTE** For compatibility reasons configuration is shown with the Web based management. The SCALANCE W configured in the TIA Portal network view are just used to integrate the SCALANCE W as PROFINET devices.

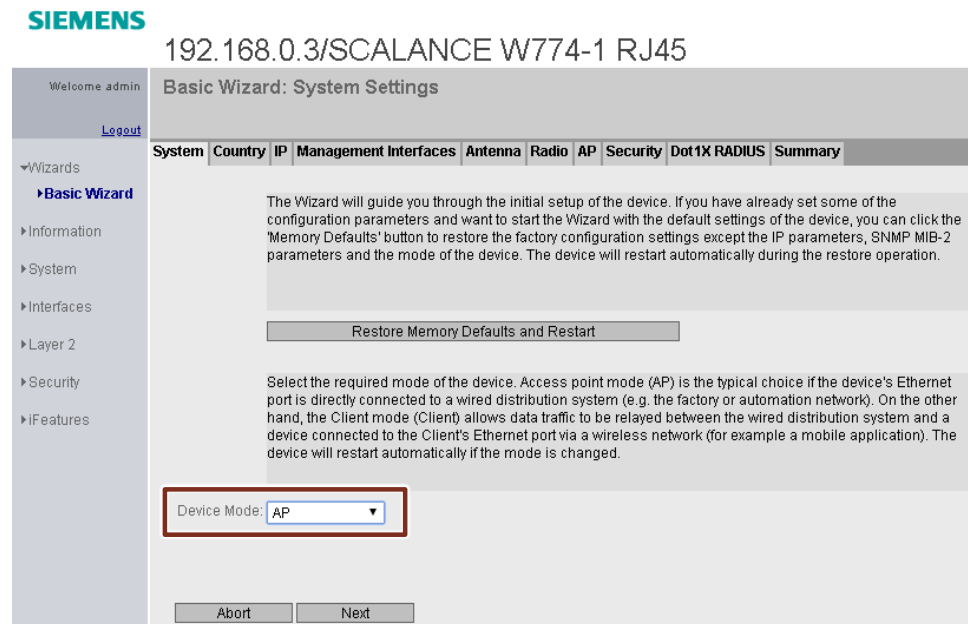
The parameterization of both components takes place in a web browser (e.g. Google Chrome). For this purpose, you specify the IP address of your component in the web browser:

- 192.168.0.3 for the access point
- 192.168.0.4 for the client

You can then assign the parameters of the selected component.

You select between access point (AP) and client under "Device Mode" (for devices that can be either an access point or a client):

Figure 2-6 Parameterization as access point (or as client)



### Settings on the access point and client

You can use the Basic Wizard to commission the access point and client. You will find the Basic Wizard in the navigation bar (see [Figure 2-6](#)). The wizard guides you through the tabs (System, Country, IP, etc.). The same can be done without wizard.

The primary settings for the access point are presented in the following. Unless described otherwise, these settings also apply analogously to the client.

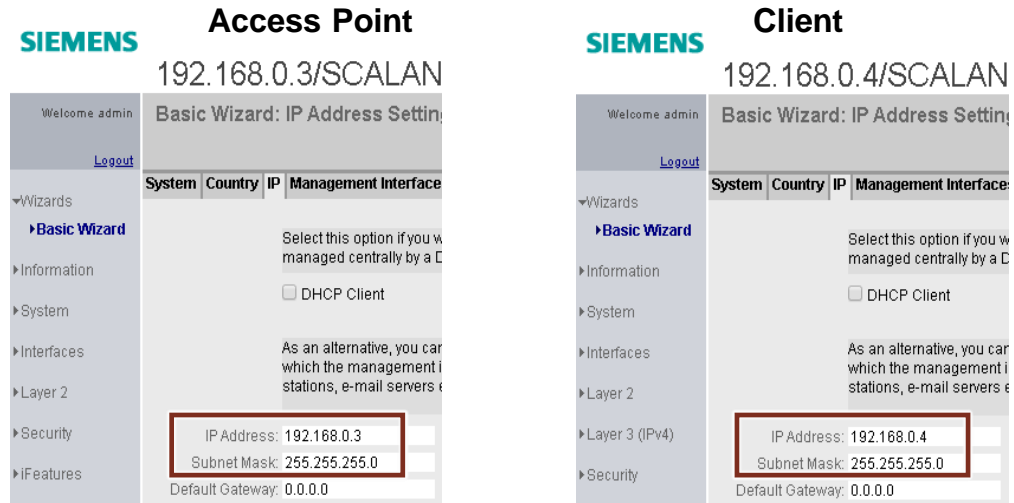
#### Tab "Country"

Select your country code here.

**Tab "IP"**

Specify the IP address and subnet mask here:

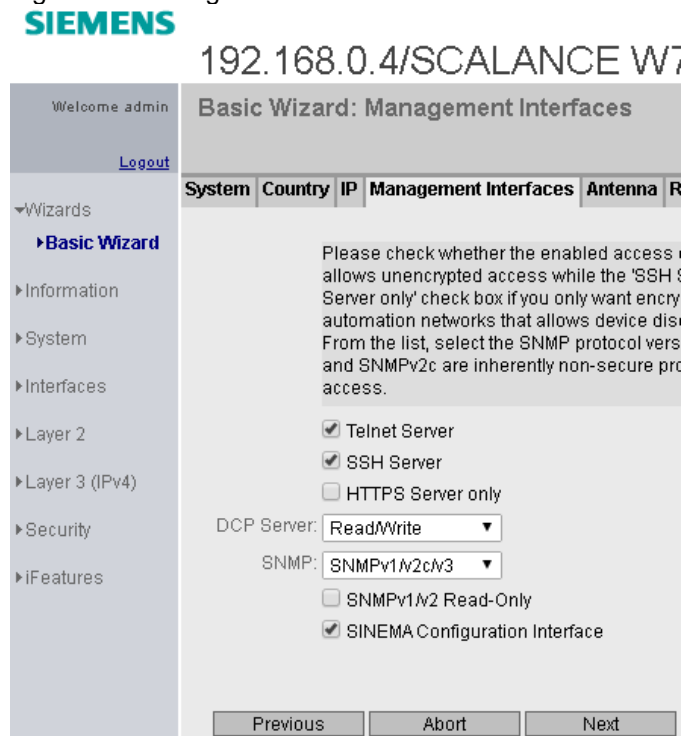
Figure 2-7 Setting the IP address



**Tab "Management Interfaces"**

Select the protocols to be used by the access point. Set these protocols for the client as well.

Figure 2-8 Management Interfaces



**Tab "Antenna"**

Specify the antennas that you want to use for the access point and the client. Unused antenna connections must be provided with a 50 Ω terminating resistor.

It is recommended to set the second antenna at "Interfaces > WLAN > Antenna" to Antenna mode "RX" only.

Figure 2-9 Antennas used

SIEMENS 192.168.0.4/SCALANCE W774-1 RJ45

Connector	Antenna Type	Antenna Gain 2.4 GHz [dBi]	Antenna Gain 5 GHz [dBi]	Cable Length [m]	Additional Attenuation [dB]
R1 A1	Omni-Direct-Mount ANT795-4MC	3	5	0	0
R1 A2	Omni-Direct-Mount ANT795-4MC	-	-	-	-

**Tab "Radio"**

Here, set the frequency and the standard to be used by the access point. Use the 5 GHz frequency band. Although its range is less than the 2.4 GHz frequency band, it is less prone to interference.

IEEE 802.11a is selected to maintain the most robust connection possible, as many industrial environments have shown the advantages of a pure antenna diversity, without the IEEE 802.11n MIMO mechanisms.

The DFS option allows the upper channels of the 5 GHz band to also be used. This is not recommended when using iPCF because interference from radar signals may occur and interrupt the communication.

Figure 2-10 Frequency band and WLAN standard

SIEMENS 192.168.0.4/SCALANCE W774-1 RJ45

Radio	Enabled	Radio Mode	Frequency Band	WLAN Mode 2.4 GHz	WLAN Mode 5 GHz	DFS (802.11h)	Outdoor Mode	max. Tx Power	Tx Power Check
WLAN 1	<input checked="" type="checkbox"/>	Client	5 GHz	802.11 n	802.11a	<input type="checkbox"/>	<input type="checkbox"/>	18 dBm	Allowed



**Tab "AP" (only present for access point)**

Specify the channel used and the SSID (name of the network).

For iPCF only one radio should be used. With iPCF-MC a dual radio AP is mandatory.

Figure 2-11 Channel and SSID

**SIEMENS** 192.168.0.3/SCALANCE W788-2 RJ45

Welcome admin [Logout](#)

**Basic Wizard: Access Point Settings**

System	Country	IP	Management Interfaces	Antenna	Radio	AP	Security	Dot1X RADIUS	Summary
--------	---------	----	-----------------------	---------	-------	----	----------	--------------	---------

On this page, you specify the configuration for the access point. Specify the main channel, or allow the AP itself to find a free channel by selecting 'Auto'. If you enabled the 'DFS' function previously to support the IEEE 802.11h standard and obtain more channels due to radar detection, specify the alternative channel as well. With the IEEE 802.11n transmission standard, you may extend the channel bandwidth by using either the neighboring channel '40 up' above or below '40 down'.

Radio	Channel	Alternative DFS Channel	HT Channel Width [MHz]
WLAN 1	36 (5180)	-	20
WLAN 2	Auto	-	20

Enter the name of the wireless network (SSID). A client that will connect to the wireless network must be configured to use the same name. The length of the character string for an SSID is 1 to 32 characters. Use only ASCII codes in the range 'A..Z', 'a..z', '0..9' and special characters !\$#%&()\*+,-./:;=?@[\^\_`{|}~ and the space. This means the hexadecimal character codes 0x20 to 0x7e.

Port	SSID
VAP 1.1	Siemens WLAN
VAP 2.1	Siemens Wireless Network 2

Warning: The approval process may not be finished in current country for channels denoted by a "\*" character.

Please check the following website for more detailed information:  
<http://www.siemens.com/wireless-approvals>

**Tab "Client" (only present for client)**

Select "Layer 2 Tunnel" for MAC Mode. The client then uses the MAC address of the Ethernet interface for the WLAN interface. The network is informed of the up to 8 MAC addresses connected to the Ethernet interface of the client.

Specify the SSID (name of the network) as you did before for the access point.

Figure 2-12 MAC Mode and SSID

**SIEMENS**  
192.168.0.4/SCALANCE W774-1 RJ45

Welcome admin [Logout](#)

**Basic Wizard: Client Settings**

System	Country	IP	Management Interfaces	Antenna	Radio	Client	Channels	Security	D
--------	---------	----	-----------------------	---------	-------	--------	----------	----------	---

On this page, you specify the configuration for a client. If you only want to enable IP-based (OSI layer 3) communication with devices attached to the Ethernet port, use 'Own' to make the client use the MAC address of the Ethernet interface for the WLAN interface as well. Similarly, selecting 'Manual' allows you to enter any MAC address in the 'MAC Address' column. If MAC-based (OSI layer 2) communication is intended with a single device, use 'Automatic' to make the client automatically adopt the source MAC address of the first frame that it receives over the Ethernet interface. For multiple devices, 'Layer 2 Tunnel' makes the client use the MAC address of the Ethernet interface for the WLAN interface. But the network will also be informed of up to eight MAC addresses connected to the Ethernet interface of the client. If the 'Any SSID' check box is selected, the device attempts to connect to the network with the best transmission quality and that has suitable security settings.

Radio	MAC Mode	MAC Address	Any SSID
WLAN 1	Layer 2 Tunnel	00-00-00-00-00-00	<input type="checkbox"/>

If the 'Any SSID' check box is not selected, you will need to enter the SSID of the access point with which the client will connect to have better control over the behavior of the device. The length of the character string for an SSID is 1 to 32 characters. Use only ASCII codes in the range of 'A'..'Z', 'a'..'z', '0'..'9' and special characters !\$#%&'()\*+,-./:;=?@[\^\_`{|}~ and the space. This means the hexadecimal character codes 0x20 to 0x7e.

Radio	SSID	Security Context
WLAN 1	Siemens WLAN	1

**Tab "Channels" (only present for client)**

You should deselect unused channels.

Figure 2-13



192.168.0.4/SCALANCE W774-1 RJ45

Welcome admin [Logout](#)

Basic Wizard: Client Allowed Channel Settings

System Country IP Management Interfaces Antenna Radio Client Channels Security Dot1X Supplicant Summary

Wizards

- Basic Wizard
- Information
- System
- Interfaces
- Layer 2
- Layer 3 (IPv4)
- Security
- IFeatures

On this page, you specify which channels may be used for communication with an AP, for example to reduce the amount of time required to scan for a new AP while roaming. If you enable the option 'Allowed Channels', you restrict the selection of channels via which a device is allowed to establish the connection, and the channels on which the client searches for an AP. To specify the valid channels for the required frequency band, select the appropriate check box for the channel number.

Radio Use Allowed Channels only  
WLAN 1

Frequency Band: 2.4 GHz

Select / Deselect all

Radio	Radio Mode	1	2	3	4	5	6	7	8	9	10	11	12	13
WLAN 1	Client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Frequency Band: 5 GHz

Select / Deselect all

Radio	Radio Mode	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161	165
WLAN 1	Client	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Previous Abort Next

**Tab "Security"**

Use "iPCF Authentication" for the authentication.

Figure 2-14



192.168.0.4/SCALANCE W774-1 RJ45

Welcome admin [Logout](#)

Basic Wizard: Security Settings

System Country IP Management Interfaces Antenna Radio Client Channels Security Dot1X Supplicant Summary

Wizards

- Basic Wizard
- Information
- System
- Interfaces
- Layer 2
- Layer 3 (IPv4)
- Security

To make the network secure, authentication and encryption are used to verify a communication partner's identity and to protect the transferred data from eavesdropping. Selecting an entry with 'PSK' from the list requires you to enter a password and to confirm the password to catch mistyped characters. Other settings require additional configuration steps to be performed later on. It is not advisable to select 'Open system', as this represents no security at all. With WPA-PSK you can achieve a low level of security, but also compatibility with certain legacy systems. With WPA2-PSK you can achieve a moderate level of security, while WPA2-RADIUS will give you the highest level of security but requires extra network infrastructure. If you are unsure about the proper security settings, simply accept the default values and enter the passwords to achieve a reasonable level of security. Make sure that you note down the passwords, as you will need to configure the other devices in the same way.

Security Context	Authentication Type	Cipher	WPA(2) Pass Phrase	WPA(2) Pass Phrase Confirmation
1	iPCF Authentication	AES		

### Additional settings: iPCF

Enable iPCF for the utilized IWLAN "WLAN 1".

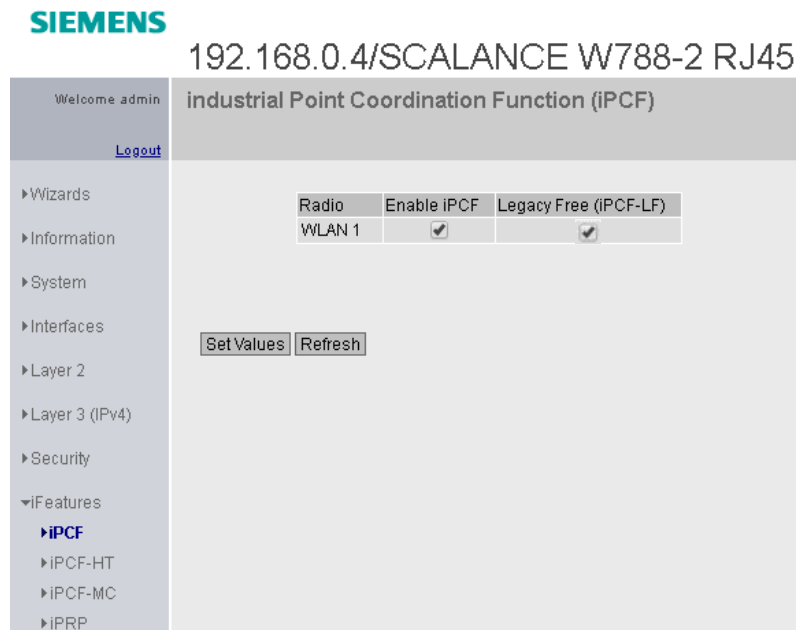
Figure 2-15 shows the settings for the Client.

On the AP side iPCF and iPCF-LF also need to get activated.

Additionally the iPCF cycle time should be

1. higher than the Number of clients \* 2 (for 7 clients this means 16 ms cycle time)
2. half of the PROFINET update time to have one conservative "retry cycle", here 16ms; with a higher number of clients (see 1.) PROFINET update time should be equal to iPCF cycle time.

Figure 2-15 Enable the iPCF iFeature



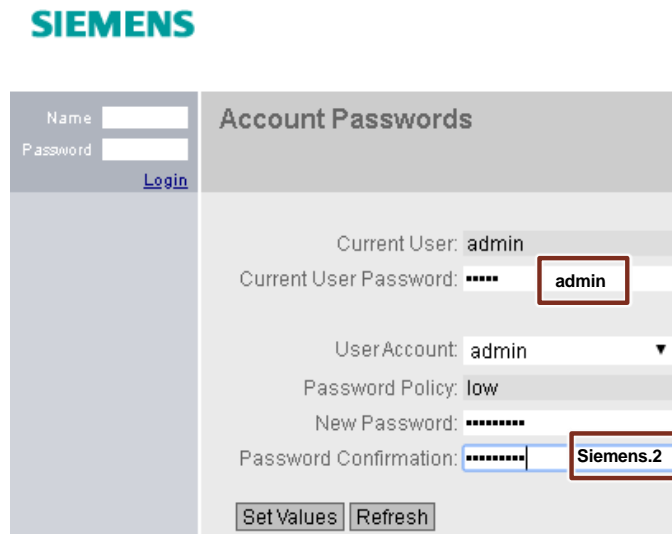
**Additional settings: Password**

The following passwords are stored:

Table 2-1 Passwords

	Access point	Client
User account	admin	admin
Password	Siemens.2	Siemens.1

Figure 2-16 Password



© Siemens AG 2022. All rights reserved.

**2.4.2 Determination and parameterization of the update time**

**What is the update time?**

The update time determines the interval at which output data is sent from the IO controller to the IO device and input data is sent from the IO device to the IO controller. The shorter the update time, the sooner the current data of the CPU reaches the IO device or the response frame of the IO device reaches the CPU. For this reason, when using PROFINET via LAN, the update time is preset to a few milliseconds. The update time can be specified separately for each IO device.

**Empirical values**

When using PROFINET via IWLAN, longer watchdog times must be parameterized for stability reasons. A common watchdog time is 192 ms, here achieved by the combination of 32 ms update time and 6 accepted update cycles without IO data.

Bitte beachten Sie <https://support.industry.siemens.com/cs/ww/en/view/22681042>

For the Emergency Stop signal, this setting means that the process image output (PIQ) reaches the assigned F-channel after 64 ms at the earliest.

**Note**

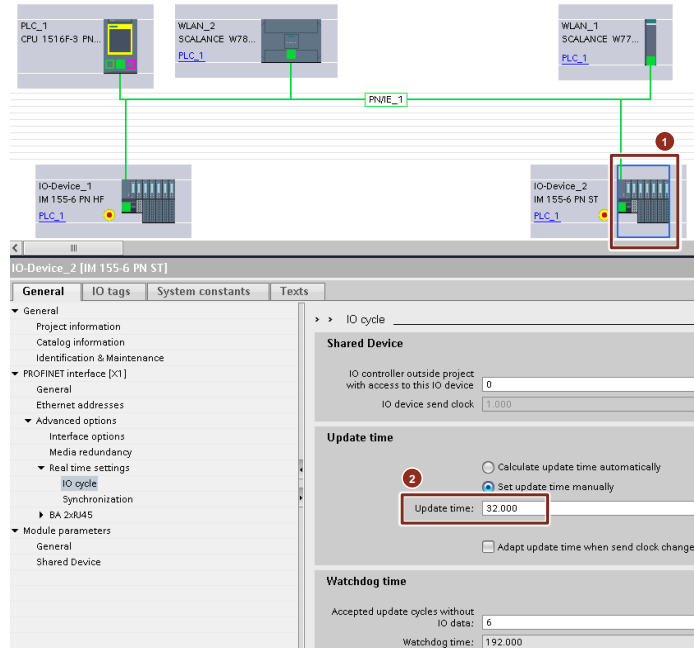
The minimum cycle time when using iPCF is calculated as follows: Number of clients x 2 ms

## Parameterization

This section describes the parameterization of the update time. Follow these steps:

1. Open the hardware configuration of STEP 7 and select the remote IO device.
2. Set the update time.

Figure 2-17 Setting the update time of the remote IO device



### 2.4.3 Determination and parameterization of the F-monitoring time

#### What is the F-monitoring time?

The F-monitoring time is the time within which an F-component (e.g. F-DQ) must receive the PROFIsafe telegram. If this time is exceeded, a communication error is output and the F-component involved goes into passivated state. The default value of the F-monitoring time is 150 ms but can be adapted by the user.

#### Empirical values


For safety applications via IWLAN, the recommendation is to set the F-monitoring time to at least twice the watchdog time.

With the watchdog time of 192 ms used in this application example (chapter 2.4.2), this means an F-monitoring time of 384 ms. This setting means that in the event of a communication error, the F channel goes into the safe state after 384 ms at the latest.

To calculate a value taking more parameters in account please refer to the following table: <https://support.industry.siemens.com/cs/ww/en/view/58856512>

For this project the F-monitoring time is set to 384 ms, assuming a well planned WLAN infrastructure and frequency planning.





WARNING

The values for F-monitoring times for an IWLAN application are significantly higher than for a wired application and depend heavily on the respective environment (IWLAN quality, roaming, EMC, etc.). This can also mean longer reaction times in case of errors. Take this into consideration and assess whether the respective safety function ensures the safe state of your application when these higher F-monitoring times are used.

### Example of a communication error

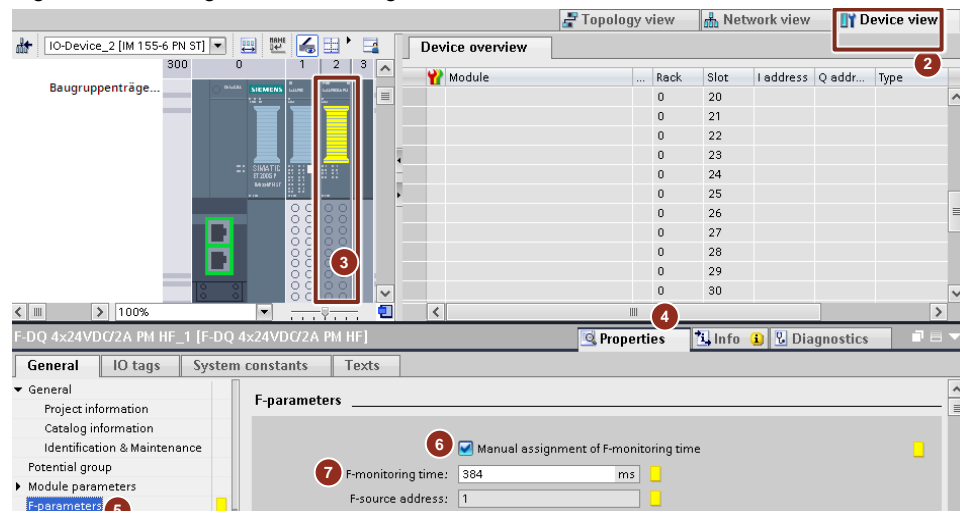
If the update time is set too low, the connection between the SCALANCE access point and the SCALANCE client is terminated. The PROFINET telegram then does not reach the interface module of the remote ET 200SP. The PROFIsafe telegram therefore also does not reach the F-DQ for switching off the actuator. The F-monitoring time expires without the F-DQ having received the PROFIsafe telegram within this time. Consequently, the F-module goes to safe state (passivated).

### Parameterization

This section describes the parameterization of the F-monitoring time (see [Figure 2-18](#)).

1. Select the remote IO device as shown in [Figure 2-17](#).
2. Select the "Device view" tab.
3. Select the F-DQ.
4. Select the "Properties" tab followed by the "General" tab.
5. Select "F-parameters".
6. Select the "Manual assignment of F-monitoring time" check box.
7. Enter the F-monitoring time.

Figure 2-18 Setting the F-monitoring time



8. Follow the same procedure for the F-CPU and the local F-DI. Set the following F-monitoring times:

For the F-CPU: The same as for the remote F-DQ

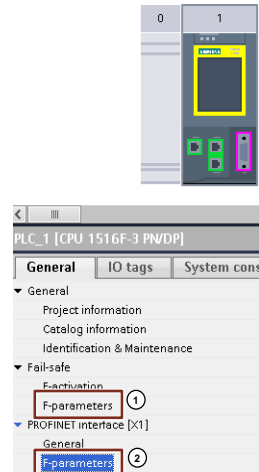
For the local F-DI: The default value of 150 ms

Note that there are two places (local and distributed) in the hardware configuration where the F-monitoring time can be defined:

Default F-monitoring time for

- Central F-I/O (1)
- F-I/O of the utilized interface (2)

Figure 2-19 F-monitoring time for central I/O and F-I/O of the utilized interfaces



Only the F-monitoring time under (2) is relevant in this application example, because no central F-I/Os are in use.

## 2.5 Programming

This section describes the standard user program and the safety program (F-program) of the provided STEP 7 project.

### 2.5.1 Standard user program

The standard user program consists of the following blocks:

- OB1
- DB "DataToSafety" (data from the standard user program for the safety program)
- DB "DataFromSafety" (data from the safety program for the standard user program)
- DB "ErrorHandling"

#### OB1

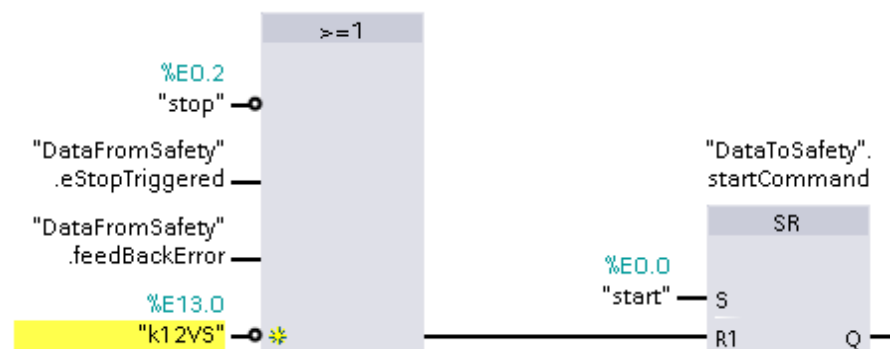
OB1 implements the operational start ("start") and stop ("stop") of the actuator in Network 1 using an SR flip-flop. The actuator is switched off by the following actions (reset of SR flip-flop):

- Stop button (NC) actuated ("stop" = false)
- Safety function (Emergency Stop) triggered ("eStopTriggered" = true)
- Feedback error at FDBACK in the safety program ("feedBackError" = true)
- Channel of the actuator has been passivated ("k12VS" = false)

#### Note

"k12VS" designates the value state of the F-DQ channel to which the actuator ("k12") is connected. The following convention applies to the value state:  
False: Channel is passivated; True: Channel supplies process values.

Figure 2-20 Operational start and stop



Network 2 connects only the bits of the diagnostics DB "ErrorHandling".

**DB "DataFromSafety"**

Table 2-2 DB "DataFromSafety"

Parameter	Data type	Description
feedBackError	BOOL	1: Feedback error
ackReqESTOP1	BOOL	1: Emergency STOP can be acknowledged.
ackReqFDBACK	BOOL	1: Feedback error can be acknowledged.
eStopTriggered	BOOL	1: Safety function (Emergency Stop) triggered.

**DB "DataToSafety"**

Table 2-3 DB "DataToSafety"

Parameter	Data type	Description
startCommand	BOOL	1: Operational start

**DB "ErrorHandling"**

For a description, refer to section [2.7](#) "Error handling".

**2.5.2 Safety program****Blocks used**

FB "Main\_Safety\_RTG1" calls FB "EmergencyStop". This calls FB "ESTOP1" and FB "FDBACK":

**FB "Main\_Safety\_RTG1"**

The system creates this block automatically. The user can create the safety program in this block.

**FB "EmergencyStop" (developed by user)**

Implements the "Emergency Stop" safety function using the two blocks FB "ESTOP1" and FB "FDBACK".

**FB "ESTOP1" (safety function of Safety Advanced)**

Certified (know-how-protected) block that implements an Emergency Stop.

**FB "FDBACK" (safety function of Safety Advanced)**

Certified (know-how-protected) block that switches an actuator (contactors) and monitors the feedback circuit.

**Note**

The feedback signal can be connected via a standard DI.

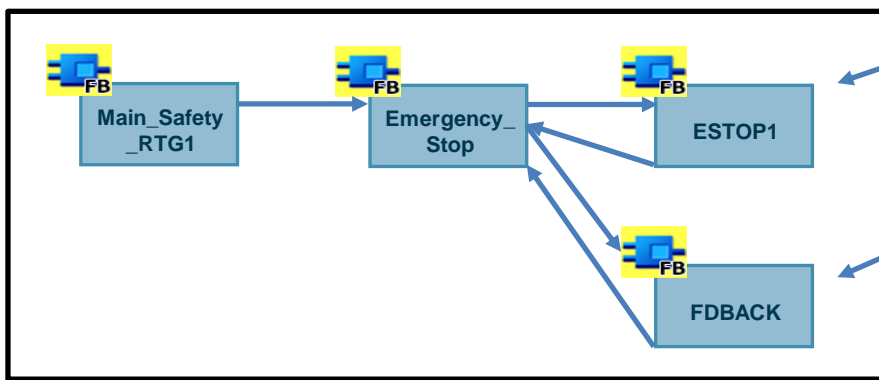
**Overview**

Figure 2-21 User-developed F-FB and safety functions of Safety Advanced

**Safety functions of Safety Advanced**

Basic instructions	
Name	
General	
Bit logic operations	
Safety functions	
ESTOP1	
TWO_H_EN	
MUT_P	
EV1 oo2DI	
FDBACK	
SFDOOR	
ACK_GL	
Timer operations	
Counter operations	

**Safety program**



**FB "EmergencyStop"**

Figure 2-22

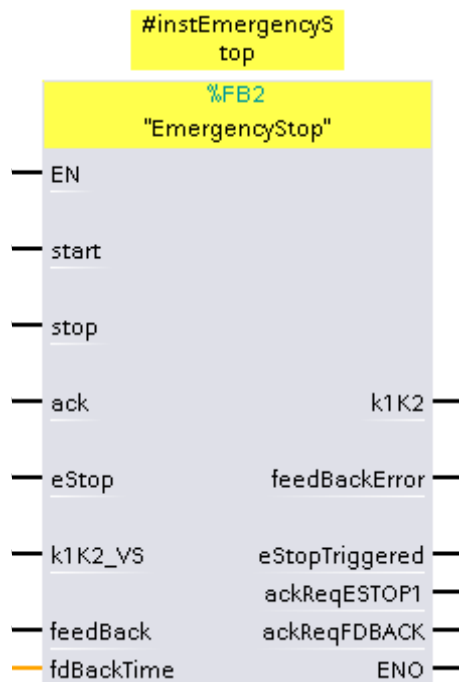


Table 2-4 Input parameters of FB "EmergencyStop"

Parameter	Data type	Description
start	BOOL	1: Switching on of the actuator.
stop	BOOL	0: Switching off of the actuator.
ack	BOOL	1: Acknowledgment signal
eStop	BOOL	1: Emergency Stop released and FB "ESTOP1" enabled (output "Q" on FB "ESTOP1" = 1)
k1K2_VS	BOOL	Value state of the channel to which the actuator is connected: 0: Channel is passivated. 1: Channel supplies process values.
feedBack	BOOL	Feedback signal of the actuator (auxiliary contactor contacts (NC)): 0: If actuator controlled (output parameter k1K2 = 1) 1: If actuator not controlled (output parameter k1K2 = 0)
fdBackTime	Time	Feedback time

Table 2-5 Output parameters of FB "EmergencyStop"

Parameter	Data type	Description
k1K2	BOOL	1: Actuator (contactors) controlled.
feedBackError	BOOL	1: Feedback error "k1K2" does not correlate with input parameter "feedBack" (see description of input signal "feedBack").
eStopTriggered	BOOL	1: Safety function (Emergency Stop) was triggered.
ackReqESTOP1	BOOL	1: Emergency Stop has been released and FB "ESTOP1" can be acknowledged.
ackReqFDBACK	BOOL	1: Feedback error has been eliminated and FB "FDBACK" can be acknowledged.

**FB "ESTOP1"**

You can find a description of the functionality and parameters in the online help of Safety Advanced (select block in the safety program and press <F1>).

**FB "FDBACK"**

You can find a description of the functionality and parameters in the online help of Safety Advanced (select block in the safety program and press <F1>).



## 2.6 Operation

### Requirements

The following requirements must be met for operation of the application example:

- Access point and client have been parameterized.
- The STEP 7 project is located in the F-CPU.
- The Emergency Stop has been released.

#### NOTE

Use for the following points also the "Watchtable1" from the TIA Portal project.

### Switching the actuator on and off

1. Press the acknowledgment button (ack).
2. Press the start button (start).  
Result: Contactors K1 and K2 close.
3. Press the stop button (stop).  
Result: Contactors K1 and K2 release.

To switch on again, begin at "2."

### Triggering the safety function

1. Press the acknowledgment button (ack).
2. Press the start button (start).  
Result: Contactors K1 and K2 close.
3. Press the Emergency Stop (eStop).  
Result: The safety function has been triggered. Contactors K1 and K2 release.
4. Before you switch on the actuator again, the Emergency Stop must be released. Then start over at "1".

## 2.7 Error handling

DB "errorHandling" provides you with (standard) diagnostic information in the event of an error. The behavior described in the following table is present if the corresponding bit is set.

Table 2-6 Structure of DB "errorHandling"

Bit	Response	(Possible) cause	Remedy
0	The channel to which the Emergency Stop is connected was passivated.	The Emergency Stop was pressed in such a way that a discrepancy error occurred.	
1	The channel to which the contactors are connected was passivated.	Communication error because the F-monitoring time was exceeded.	Check the F-monitoring time on the F-DQ.
2	The channel to which the Emergency Stop is connected can be reintegrated again.	Channel is ready again to handle process data.	
3	The channel to which the contactors are connected can be reintegrated again.	Channel is ready again to handle process data.	
4	A feedback error was detected. The actuator cannot be switched on.	Feedback error at FB "FDBACK".	Check the feedback time at parameter "feedBack" on FB "EmergencyStop".
5	Safety function (Emergency Stop) was triggered.	Emergency STOP was pressed.	See section <a href="#">2.5</a> "Triggering the safety function" No. 4.

## 3 Appendix

### 3.1 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](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.

Please send queries to Technical Support via Web form:

[support.industry.siemens.com/cs/my/src](https://support.industry.siemens.com/cs/my/src)

#### 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](https://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](https://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](https://support.industry.siemens.com/cs/ww/en/sc/2067)

## 3.2 Industry Mall



The Siemens Industry Mall is the platform on which the entire Siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:

[mall.industry.siemens.com](https://mall.industry.siemens.com)

## 3.3 Links and literature

Table 3-1

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 this application example <a href="https://support.industry.siemens.com/cs/ww/en/view/28609440">https://support.industry.siemens.com/cs/ww/en/view/28609440</a>
\3\	TIA Selection Tool <a href="https://support.industry.siemens.com/cs/ww/en/view/109767888">https://support.industry.siemens.com/cs/ww/en/view/109767888</a>
\4\	FAQ "How do you link a PNIO device to a PNIO controller via WLAN and iPCF?" <a href="https://support.industry.siemens.com/cs/ww/en/view/92649989">https://support.industry.siemens.com/cs/ww/en/view/92649989</a>
\5\	FAQ regarding update time and F-monitoring time <a href="https://support.industry.siemens.com/cs/ww/en/view/109475919">https://support.industry.siemens.com/cs/ww/en/view/109475919</a>

## 3.4 Change documentation

Table 3-2

Version	Date	Modifications
V1.0	10/2008	First edition
V2.0	12/2021	Complete revision
V2.1	02/2022	Adjustments of statements and parameters