

SIEMENS

SIMATIC

Industrial Software Safety Matrix

Programming and Operating Manual

<u>Security information</u>	1
<u>Preface</u>	2
<u>Product Overview</u>	3
<u>Installing</u>	4
<u>Software user interface</u>	5
<u>Configuring</u>	6
<u>Access protection</u>	7
<u>Transferring a Safety Matrix</u>	8
<u>Compiling and downloading</u>	9
<u>Operator control and monitoring</u>	10
<u>Documentation of a Safety Matrix</u>	11
<u>Acceptance test for a Safety Matrix</u>	12
<u>Explanation of parameter assignment options</u>	13
<u>Requirements for virtual environments and remote access</u>	A
<u>Resulting cause logic for Degraded Voting</u>	B

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Security information	7
2	Preface	9
2.1	Preface	9
2.2	Warnings index	16
3	Product Overview	17
3.1	What is the Safety Matrix?	17
3.2	Optional packages of the Safety Matrix	20
3.3	Example view of a Safety Matrix	21
3.4	Definition of terms	21
3.5	Guide to the procedure	25
4	Installing	27
4.1	Requirements for the installation	27
4.2	Installing	28
4.3	Uninstalling previous versions of the Safety Matrix	31
4.4	Upgrading to Safety Matrix V6.3	31
4.4.1	Overview of the upgrade	31
4.4.2	User scenario 1	33
4.4.3	User scenario 2	37
4.4.4	User scenario 3	38
5	Software user interface	41
5.1	Overview of the software user interface	41
5.2	Menu bar of the Safety Matrix	44
5.3	"SIF Filter" drop-down list	47
6	Configuring	49
6.1	Overview of Configuring	49
6.1.1	Basic procedure for creating a safety program	49
6.1.2	Inserting a new Safety Matrix	50
6.1.3	The Safety Matrix tags	52
6.1.4	Syntax rules for tag names in the Safety Matrix	54
6.1.5	Preprocessing	56
6.1.6	The "Degraded Voting" function	60
6.1.7	Group deactivation of maintenance operations	63
6.1.8	F-channel drivers	64
6.1.9	Configuration of the F-channel driver acknowledgment	66
6.1.10	Message configuration	67
6.1.10.1	Overview for configuring messages	67

6.1.10.2	Safety Matrix message block F_MA_AL.....	68
6.1.10.3	Cause message block F_SC_AL.....	69
6.1.10.4	Cause message block F_SC_AL2.....	75
6.1.10.5	Effect message block F_SE_AL.....	81
6.1.11	OS interface	86
6.1.12	Introducing the new Safety Matrix block icons into the PCS 7 OS.....	87
6.1.13	Safety Matrix function blocks	88
6.2	Editing the properties of the Safety Matrix	88
6.2.1	"Properties" dialog box of the Safety Matrix.....	88
6.2.2	"Customize" dialog boxes	94
6.2.3	"Track changes" menu command	97
6.3	Configuring the causes	97
6.3.1	Overview of configuring the Causes	97
6.3.2	Creating/changing the Cause and row for Cause	100
6.3.3	Overview of the "Cause details - Cause x" dialog	101
6.3.4	"Cause details" dialog - "Configure" tab.....	102
6.3.5	"Cause details" dialog - "Analog parameter" tab.....	104
6.3.6	"Cause details" dialog box - "Options" tab	105
6.3.7	"Cause details" dialog box - "Alarms" tab.....	108
6.4	Configuring the effects	109
6.4.1	Overview of configuring the effects	109
6.4.2	Creating/changing the effect and column for effect.....	109
6.4.3	Overview of the "Effect details - Effect x" dialog	110
6.4.4	"Effect details" dialog - "Configure" tab	111
6.4.5	"Effect details" dialog box - "Options" tab.....	113
6.4.6	"Effect details" dialog box - "Alarms" tab.....	116
6.5	Configuring the intersections.....	117
6.5.1	Editing or changing intersections	117
6.5.2	"Intersection details" dialog box	118
6.6	Importing/exporting a matrix.....	120
6.6.1	Bulk data engineering using a spreadsheet.....	120
6.6.2	Exporting Safety Matrix as spreadsheet	121
6.6.3	Importing the spreadsheet of a Safety Matrix	122
6.6.4	Importing a Safety Matrix file (*.cem) into a PCS 7 project.....	124
7	Access protection	127
8	Transferring a Safety Matrix	129
8.1	Transferring the Safety Matrix to the program	130
8.2	Result of the transfer and overview of the created charts.....	135
8.3	F-runtime groups and run sequence	139
8.4	Notes on working with CFC.....	139
8.5	"Selective transfer" dialog box	140
8.6	"Selective transfer - Progress" dialog box.....	141
8.7	"Selective transfer - Log" dialog box	142

9	Compiling and downloading	143
9.1	Compiling and downloading to the F-CPU	143
9.2	Compiling and downloading to the operator station (OS)	144
10	Operator control and monitoring	147
10.1	Overview of operator control and monitoring	147
10.2	Using the Safety Matrix Viewer via "Web Option for OS"	148
10.3	Starting online mode in the engineering tool	149
10.4	Opening the Safety Matrix faceplates (Safety Matrix Viewer)	150
10.5	Safety Matrix faceplate (Viewer)	155
10.5.1	Layout and views of a faceplate (Viewer)	155
10.5.2	Layout of the faceplate overview row (Viewer)	156
10.5.3	Safety Matrix faceplate, "Standard" view	160
10.5.4	Safety Matrix faceplate, "Messages" view	161
10.5.5	Safety Matrix faceplate, "User rights" view	162
10.6	Monitoring the Safety Matrix (Engineering Tool / Viewer)	163
10.6.1	Color codes for status display in the Safety Matrix display	163
10.6.2	Status displays for selected Cause/Effect	165
10.7	Operating	168
10.7.1	Initiator and confirmer permission (Viewer)	168
10.7.2	Secure Write	170
10.7.2.1	Transaction for Secure Write	170
10.7.2.2	Variants of Secure Write	173
10.7.3	Operations in the Safety Matrix	173
10.7.3.1	Operating over the control bar (Engineering Tool / Viewer)	173
10.7.3.2	Example: Reset effect with two operators (Viewer)	177
10.7.3.3	Example: Acknowledge Cause with two operators (Viewer)	179
10.7.3.4	Perform maintenance changes (Engineering Tool / Viewer)	181
10.8	Events and messages	184
10.8.1	Messages in the event protocol of the Safety Matrix	184
10.8.2	Operator messages of the Safety Matrix Viewer	184
10.8.3	PCS 7 alarm messages in the WinCC message system	185
10.8.4	Warning messages	186
10.8.5	Messages of the matrix message blocks	186
11	Documentation of a Safety Matrix	193
11.1	Print Safety Matrix	193
11.2	Comparing Safety Matrices	194
11.3	Comparing CFCs	195
11.4	Configuration report	198
11.5	Validation report	200
12	Acceptance test for a Safety Matrix	201
13	Explanation of parameter assignment options	203
13.1	Parameter assignment options for causes	203

13.1.1	Time response	203
13.1.2	Inhibit.....	204
13.1.3	Bypass	205
13.1.4	Auto acknowledge active cause.....	205
13.1.5	"Bad Quality" Voting.....	206
13.1.6	Alarm on input trip	206
13.2	Parameter assignment options for effects.....	207
13.2.1	Reset/override.....	207
13.2.2	Reset/override with output delay.....	209
13.2.3	Bypass	211
13.2.4	Bypass with output delay	214
13.2.5	Pass through process data and mask enable	218
A	Requirements for virtual environments and remote access	221
A.1	Overview	221
A.2	Configuration and operation.....	222
A.2.1	Virtual environments	222
A.2.2	Remote Access and Control	223
A.3	Examples of valid configurations in PCS 7	225
A.3.1	Example 1	225
A.3.2	Example 2	227
A.4	Abbreviations and explanations of terms	229
A.5	References.....	229
B	Resulting cause logic for Degraded Voting	231
B.1	Function type "OR" with 2 input tags (1oo2)	231
B.2	Function type "AND" with 2 input tags (2oo2)	232
B.3	Function type "OR" with 3 input tags (1oo3)	233
B.4	Function type "2oo3"	235
B.5	Function type "AND" with 3 input tags (3oo3)	237
	Glossary	239
	Index.....	247

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 under
<https://www.siemens.com/industrialsecurity>.

Preface

2.1 Preface

Purpose of this documentation

The information in this manual enables you to configure "S7 F/FH Systems" fail-safe systems using Safety Matrix V6.3.

In addition, you need the:

- The system manual "Safety Engineering in SIMATIC S7 (<https://support.industry.siemens.com/cs/ww/en/view/12490443>)"
- and the Programming and Operating Manual "S7 F/FH Systems Configuring and Programming (<https://support.industry.siemens.com/cs/ww/en/view/109742100>)".

Basic knowledge requirements

General basic knowledge of automation engineering is needed to understand this documentation. Basic knowledge of the following is also necessary:

- Fail-safe automation systems
- S7-400H automation systems
- S7 F/FH Systems
- Distributed I/O systems on PROFIBUS DP and PROFINET IO
- STEP 7/PCS 7 basic software, particularly:
 - Working with SIMATIC Manager
 - Hardware configuration with HW Config
 - CFC optional software
 - PCS 7 OS (for Safety Matrix Viewer)

Scope of this documentation

Optional package	Order number	Release number and higher	License type (location)
Safety Matrix Engineering Tool optional package including license key	<ul style="list-style-type: none"> • Full version: 6ES7833-1SM03-0YA5 	V6.3	Floating, Trial (14 days) (ES or ES/OS)
	<ul style="list-style-type: none"> • Upgrade version from V6.x -> V6.3: 6ES7833-1SM03-0YE5 		Floating (as upgrade), trial (14 days) (ES or ES/OS)

Optional package	Order number	Release number and higher	License type (location)
Safety Matrix Viewer optional package including license key	<ul style="list-style-type: none"> Full version: 6ES7833-1SM63-0YA5 	V6.3	Floating, Trial (14 days) (OS or ES/OS; also for "Web Option for OS")
	<ul style="list-style-type: none"> Upgrade version from V6.x -> V6.3: 6ES7833-1SM63-0YE5 		Floating (as upgrade), trial (14 days) (OS or ES/OS; also for "Web Option for OS")

The optional packages of the Safety Matrix are used for the safety life cycle engineering and management of S7 F/FH Systems fail-safe automation systems and provide support for all phases of the safety life cycle.

Changes and new features in version 6.3

Description of the main new features/changes:

- Safety Matrix:
 - Group deactivation of maintenance operations
 - Export/import of the matrix color settings
 - Export/import of the matrix data to a spreadsheet for bulk data engineering
 - New function "Selective transfer" to transfer multiple matrices
 - Improved visualization during the transfer
 - Configuration of the channel driver acknowledgment
- Causes:
 - Timed soft bypass for a Cause
 - Soft bypass for individual tags of a Cause
 - Degraded Voting for input tags
 - Group acknowledgment of active Causes
 - New function block for Cause alarms F_SC_AL2 (when using the new functions)
- Effects:
 - Dynamic color scheme
 - Group reset of saved effects with the intersection type S or R

- Safety Matrix Viewer:
 - Uniform operating philosophy of Safety Matrix and PCS 7 Advanced Process Library (APL)
 - Improved display of the operator transactions (Secure Write)
 - Support of "Web Option for OS" for operator control and monitoring of matrices via Intranet/Internet
- General improvements/expansions:
 - Revision of the user interface
 - Improvement of the status dialog for Causes/Effects
 - Improvement of the print function for matrices and matrix reports
 - Support of Asian characters (Unicode) in the engineering tool
 - Performance enhancements

Approvals

The Safety Matrix optional packages are certified for use in safety mode up to:

- Safety Integrity Level SIL3 in compliance with IEC 61508:2010
- Performance Level (PL) e and Category 4 according to ISO 13849-1:2015 or EN ISO 13849-1:2015

Position in the information landscape

You will need supplementary documentation for working with the Safety Matrix according to the application.

This documentation includes references to the supplementary documentation where appropriate.

For more information, refer to the FAQs at:FAQs Safety Matrix (<https://support.industry.siemens.com/cs/ww/en/ps/14364/faq>)

Documentation for	Brief Description of Relevant Contents
S7 F/FH Systems	<ul style="list-style-type: none"> • The "S7 F/FH Systems Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/109742100)" Programming and Operating Manual describes the configuring and programming of fail-safe systems with the aid of S7 F/FH systems. • The "Automation System S7-400 Hardware and Installation (http://support.automation.siemens.com/WW/view/en/1117849)" installation manual describes the installation and wiring of S7-400 systems. • The "S7-400H fault-tolerant systems (https://support.industry.siemens.com/cs/ww/en/view/82478488)" manual describes the CPU 41x-H central processing units and the tasks required to set up and commission an S7-400H fault-tolerant system.
Safety Engineering in SIMATIC-IC S7	<p>The "Safety Engineering in SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/12490443)" System Manual provides an informational overview of the use, installation, and mode of operation of the S7 Distributed Safety and S7 F/FH Systems fail-safe automation systems and describes basic properties and detailed technical information about these fail-safe systems.</p>
STEP 7 manuals	<ul style="list-style-type: none"> • The "Configuring hardware and communication connections with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/109751824)" manual describes how to use the corresponding standard tools of STEP 7. • The "System and Standard Functions for S7-300/400, Volume 1 and Volume 2 (https://support.industry.siemens.com/cs/ww/en/view/109751826)" reference manual describes access / diagnostics functions of the distributed I/O/CPU. • The "SIMATIC Process Control System PCS 7 CFC for SIMATIC S7 (https://support.industry.siemens.com/cs/ww/en/view/109759209)" manual / online help provides a description of programming with CFC. • The "Configuration in Run (CiR) (https://support.industry.siemens.com/cs/ww/en/view/45531308)" manual
STEP 7 Online Help	<ul style="list-style-type: none"> • Describes the operation of STEP 7 standard tools • Contains information on configuring and assigning parameters for I/Os with HW Config.
PCS 7	<p>The "PCS 7 manuals (www.siemens.com/pcs7-documentation)" describe operation of the PCS 7 process control system (necessary when the S7 F-System is integrated into a higher-level process control system).</p> <p>The following documents are also available by using the link above:</p> <ul style="list-style-type: none"> • Configuration manual <i>"Process Control System PCS 7; Engineering System"</i> • Function manual <i>"Process Control System PCS 7; Fault-tolerant Process Control Systems"</i> • Configuration Manual <i>"Process Control System PCS 7; Operator Station"</i> • Function Manual <i>"Process Control System PCS 7 Web Option for OS"</i> • Operating Manual <i>"Process Control System PCS 7; PCS 7-PC Configuration"</i> • Compendium <i>"Process Control System PCS 7 Compendium Part B - Process Safety"</i> • Compendium <i>"Process Control System PCS 7 Compendium Part F – Industrial Security"</i>

Guide

This documentation describes the use of the Safety Matrix Engineering Tool and Safety Matrix Viewer optional packages. It includes both instructional material and reference material (description of possible parameter assignments).

The following topics are addressed:

- Configuring the safety program (safety-related user program) for S7 F/FH Systems
- Transferring, compiling, and downloading the Safety Matrix
- Access protection for the Safety Matrix
- Operating and monitoring of the Safety Matrix in PCS 7
- Support for the system acceptance test

Conventions

In this documentation, the terms "safety engineering" and "fail-safe engineering" are used synonymously. The same applies to the terms "fail-safe" and "F-".

The term "configuring" used here corresponds to the term "programming" used in the referenced documentation.

"S7 F systems" refers to the optional package for the "S7 F/FH systems" fail-safe system.

The term "Safety program" refers to the fail-safe portion of the user program and is used instead of "fail-safe user program," "F-program," etc. For purposes of contrast, the non-safety-related user program is referred to as the "standard user program".

"F-CPU" denotes a CPU with fail-safe capability. An F-CPU with fail-safe capability is a central processing unit that is approved for use in S7 F/FH Systems.

Additional support

If you have further questions about the use of products presented in this manual, contact your local Siemens representative.

Your contact persons are listed in the Internet (https://www.automation.siemens.com/aspa_app/?ci=yes).

A guide to the technical documentation for the various SIMATIC products and systems is available in the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109742705>).

You will find the online catalog and online ordering system in the Internet (<https://mall.industry.siemens.com>).

Training center

We offer courses to help you get started with the SIMATIC S7 automation system. Contact your regional training center or the central training center in D 90327 Nuremberg, Federal Republic of Germany.

You will find more information in the Internet (<https://www.sitrain-learning.siemens.com/PLG/>).

Technical Support

To contact Technical Support for all Industry Automation products, use the Support Request Web form (<https://support.industry.siemens.com/My/ww/en/requests>).

Additional information on our Technical Support is available in the Internet (<https://support.industry.siemens.com/cs/start?lc=en-WW>).

Service & Support on the Internet

In addition to our documentation, our complete knowledge base is available online in the Internet (<https://support.industry.siemens.com/cs/start?lc=en-WW>).

There, you will find the following information:

- The notifications which provide the latest information about your products.
- A search engine in Service & Support for locating the documents you need.
- A forum where users and experts from all over the world exchange ideas.
- Your local contact person for Industry Automation products is listed in the Contacts database.
- Information about on-site service, repairs, spare parts, and much more is available under "Repairs, spare parts, and consulting".

Important notes for maintaining operational safety of your plant

Note

Operation of safety-related systems

Systems with safety-related characteristics are subject to special operational safety requirements on the part of the operator. The supplier is also obliged to comply with special product monitoring measures. For this reason, we provide you with information on product developments and features that are (or could be) relevant to operation of safety-related systems. In order to obtain the latest information on this topic and to enable you to undertake modifications to your system you must subscribe to the corresponding notifications. To subscribe, go to the Internet (<https://support.industry.siemens.com/My/ww/en/>).

Register on this website and under "Notifications" select the notifications for the following topics, for example:

- S7-300/S7-300F
- S7-400/S7-400H/S7-400F/FH
- Distributed I/O
- SIMATIC Industrial Software
- Safety Matrix
- S7 F/FH Systems

You can find more information on setting up notifications on the page "Helpful functions in Online Support (<https://support.industry.siemens.com/cs/ww/en/sc/2063>)".

Safety concepts and communication

The PCS 7 safety concepts described in the document "PCS 7 Compendium Part F - Industrial Security" must be observed for safe operation of the system.

Additional information on this document is available in the table above under "PCS 7".

In particular we recommend the following:

- The protection of the devices/systems, e.g. PCS 7 OS server and clients
 - Ensuring the integrity and confidentiality of the communication between the devices/systems, e.g.:
 - By means of encrypted and authenticated communication between the systems involved, such as PCS 7 OS system and/or also between engineering stations (ES)
 - When using Industrial Ethernet CPs through VPN tunnels between the OS systems and/or automation systems (AS).
-

2.2 Warnings index

Overview

The table below shows the title and the location of use for the warning notices.

Warning	Section
Warnings of the "S7 F/FH Systems Configuring and Programming" Programming and Operating manual	What is the Safety Matrix? (Page 17)
Safe state for digital F-I/O	Definition of terms (Page 21)
Additional safety measures for group deactivation of maintenance operations	Group deactivation of maintenance operations (Page 63)
Operation of Safety Matrix	Requirements for the installation (Page 27)
Check installed version of the Safety Matrix components	Installing (Page 28)
Unique names for Safety Matrix	Inserting a new Safety Matrix (Page 50)
Safety note - Do not change automatically inserted Safety Matrix function blocks	Safety Matrix function blocks (Page 88)
Assigning colors	"Customize" dialog boxes (Page 94)
Effect of the "Changes only" transfer option on download of changes	Transferring the Safety Matrix to the program (Page 130)
<ul style="list-style-type: none"> • Nested chart of the F-channel drivers • Nested chart of the matrix logic • Name of the Safety Matrix top chart 	Result of the transfer and overview of the created charts (Page 135)
Independent paths to the display	Overview of operator control and monitoring (Page 147)
Operator authorization for standard operator	Operating (Page 168)
<ul style="list-style-type: none"> • The "Secure Write" functionality allows changes to the safety program to be made during RUN mode • Operating a Safety Matrix • Secure Write: checking correct functioning of the operation • Checking a transaction • Checking the technological assignment • Cancellation of a transaction 	Transaction for Secure Write (Page 170)
Use of virtual environments in ES/OS	Virtual environments (Page 222)
Remote access from higher-level control room and Engineering Center	Remote Access and Control (Page 223)

Product Overview

3.1 What is the Safety Matrix?

Comprehensive tool for safety life cycle

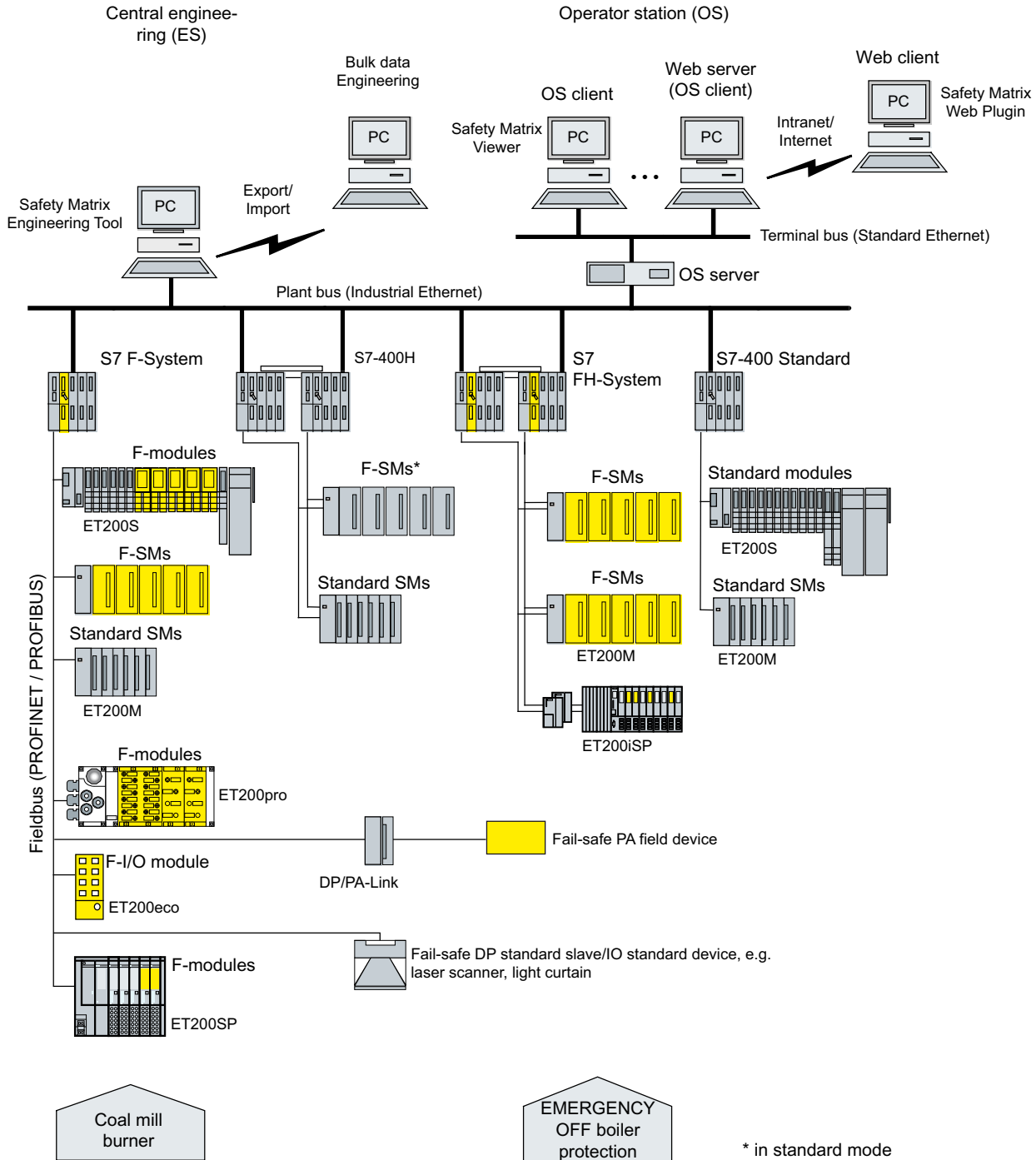
The SIMATIC Safety Matrix is the comprehensive tool for safety life cycle engineering and management of the S7 F/FH Systems fail-safe automation system and provides support for all phases of the safety life cycle:

- The Safety Matrix is a configuring tool for processes that require safety reactions to specified conditions.
- The Safety Matrix can be used to create a CFC safety program for S7 F/FH systems in accordance with the rules of a Cause/Effect matrix.
- The Safety Matrix is an integrated tool for all activities, maintenance, error handling, and change management during operation.


3.1 What is the Safety Matrix?

Use in process control

The figure below shows you the possible ways of integrating S7 F/FH Systems with the Safety Matrix into you process automation system with PCS 7.



Relationship to S7 F Systems

 WARNING
Warnings of the "S7 F/FH Systems Configuring and Programming" Programming and Operating manual
<p>The Safety Matrix is an optional package for S7 F/FH Systems. You must read, understand, and comply with all warning notices in the "S7 F/FH Systems Configuring and Programming" Programming and Operating Manual.</p>
<small>(SMW-001)</small>

The following table illustrates the relationship between the Safety Matrix and S7 F Systems.

S7 F Systems	Safety Matrix
Programming with CFC	Intuitive configuring based on the conventional Cause/Effect method
CFC as basis (charts, runtime groups, run sequence) CFC documentation	
S7 F systems safety concept	
Documentation through printouts of the safety program	Documentation through printouts of the Safety Matrix

Basic mode of operation

Analysis phase

When performing a risk assessment for the system, the user can assign events occurring during a process (Causes) to precisely defined reactions (Effects) and thus specify the system behavior.

Implementation phase

The user enters possible process events (one or more entries) in the Safety Matrix and then configures the events in terms of type, number, logic combinations, possible delays and interlocks, and any permitted deviations.

Next, the user defines the reactions (one or more outputs) to a particular event.

The Causes and Effects are linked by clicking the cell at their intersection.

When the Safety Matrix is transferred, a plausibility check of the configuration is performed.

The Safety Matrix documents the safety-instrumented function groups (SIF), and the Cause/Effect matrix itself is an important component of the safety program specification.

The safety program is specified by configuring the Cause/Effect parameters in the Safety Matrix. Using these specifications, the Safety Matrix automatically generates the S7 F systems program logic based on CFC using F-blocks from the Safety Matrix library and the "S7 F Systems Lib".

3.2 Optional packages of the Safety Matrix

In addition, the Safety Matrix provides revision and change tracking as well as functions for comparing matrices and for support during acceptance testing of the system.

Operational phase

The Engineering Tool of the Safety Matrix as well as the Safety Matrix Viewer available on the SIMATIC PCS 7 Operator Station enable operator control and monitoring of the system in safety mode. The signal status is represented online in the Cause/Effect matrix.

The operator can display and save initial alarm messages and specify that safety-relevant events be recorded. Parameter changes, for example, using bypass, reset, and override functions, are also supported.

Safety life cycle management functions for revision management as well as for the documentation of operator inputs and program changes supplement the configuring, operational, and service functions of the Safety Matrix.

Achievable Safety Requirements

The following safety requirements are met with the Safety Matrix:

- Safety Integrity Level SIL3 in compliance with IEC 61508:2010
- Performance Level (PL) e and Category 4 according to 13849-1:2015 or EN ISO 13849-1:2015

3.2 Optional packages of the Safety Matrix

Optional packages and range of functions

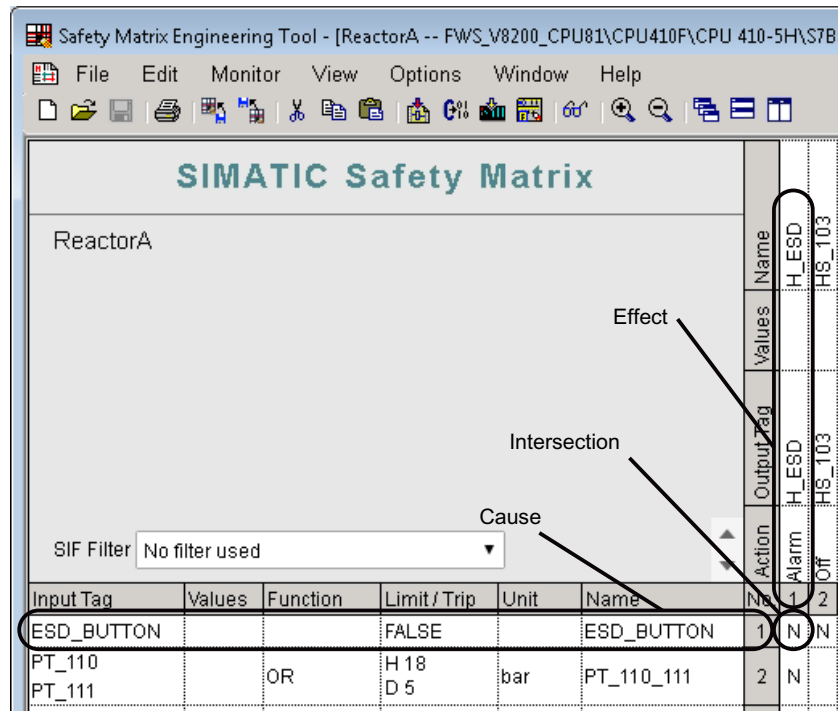
The Safety Matrix consists of multiple products which can also be ordered individually as optional packages.

Optional package	Range of functions	Environment	Operating mode	Utilization phase
Safety Matrix Engineering Tool	Creation of a Safety Matrix in SIMATIC Manager or importing a "*.cem" matrix file, configuring a Safety Matrix, export and import of the matrix data to/from a spreadsheet for bulk data engineering, automatic generation and loading of CFC charts including driver blocks to a PCS 7 project, operator control and monitoring by means of STEP 7 SIMATIC Manager on a PCS 7 Engineering System (ES)	Engineering System (ES) PCS 7 or STEP 7 and CFC	Offline, online	Analysis, implementation, and operational phase (total safety life cycle)
Safety Matrix Viewer	Operator control and monitoring on a PCS 7 Operator Station (OS) by means of faceplates	PCS 7 Operator Station (OS)	Online	Operational phase (operator control and monitoring)

3.3 Example view of a Safety Matrix

Example view of a Safety Matrix

The following figure shows the example view of a Safety Matrix.



Example: If Cause 1 becomes active (triggered with FALSE, also with input tag = "0"), Effect 1 is triggered and not saved.

3.4 Definition of terms

Main terms of the Safety Matrix are explained below.

Cause

A Cause represents a process event.

Conditions configured in the Cause must be fulfilled in order for the Cause to become active and thus to trigger an Effect defined by an intersection.

Analog or discrete values can be selected in the Cause as the input type. The values of at least one but no more than three input tags together with the function type represent a Cause.

You can create a maximum of 128 Causes.

Causes are arranged in rows in the Safety Matrix.

Effect

An effect represents the reaction that the Safety Matrix exerts on the process.

Certain conditions must be fulfilled in order for the effect to be triggered and thus have an effect on the process by means of its output tags.

The values of at least one but no more than four discrete output tags define the action to be performed on the process.

The following applies for triggering an effect:

- The trigger depends on various factors (status of the linked Causes, type of intersection, specified options for the Effect).
- The trigger always relates to the entire effect, so that all the tags of the respective effect can be controlled according to the configuration. The type of effect tag (external, internal, not specified, user-specific, etc.) has no influence on this behavior.

You can create a maximum of 128 effects.

Effects are arranged in columns in the Safety Matrix.

Intersection

The Safety Matrix intersections from the link between the Causes and Effects and specify which Causes have an Effect on the respective Effects. The properties of the link are specified with the intersection type.

You can define up to 1024 intersections.

Active

A Cause or Effect can be active, which means that it has been tripped.

Whether or not a Cause is active and when it becomes active is determined by the input tags, the function type, and the options for the Cause.

The activation of an Effect depends on the relationship (defined by intersections) to the Causes and the options for the Effect. If an effect is active, the output tags are set to "0" or "1", depending on the "Energize-to-trip" option.

Inactive

A Cause or Effect can be inactive, which means that the conditions for activation are not fulfilled.

Whether or not the Cause is inactive is determined by the input tags, the function type, and the options for the Cause.

The deactivation of an Effect depends on the relationship (defined by intersections) to the Causes and the options for the Effect. If an effect is inactive, the output tags are set to "0" or "1", depending on the "Energize-to-trip" option.

Energize-to-trip (ETT)

Trip on TRUE: The Cause is active if input tag = "1" (high-active). The output tag is "1" if the effect is active.



WARNING

Safe state for digital F-I/O

In S7 F/FH Systems the safe state for digital F-I/O is the signal value "0". For Energize-to-trip applications you must plan and implement suitable measures in the application (e.g. redundancy).

(SMW-002)

Deenergize-to-trip (DTT)

Trip if FALSE: The Cause is active if input tag = "0" (low-active). The output tag is "0" if the effect is active. This negative logic is the default setting for the inputs and outputs of the Safety Matrix.

By default, the input tag causes an activation of the Cause according to the "Deenergize-to-trip" principle, which means that a Cause becomes active when the input tag is "0". The Cause becomes inactive when the input tag is "1". If a Cause has multiple input tags, the function type must also be taken into consideration for an activation of the Cause.

The same is true for the output tags. If the effect is active, the output tags are set to "0", if the effect is not active, to "1".

Function type

The function type combines with the input tags and their options to govern whether and when a Cause is active or inactive.

- Normal: One input tag
- 2oo3: Three input tags, 2 of 3 tripping criteria must be fulfilled
- AND: 2-3 input tags, all tripping criteria must be fulfilled
- OR: 2-3 input tags, at least one tripping criterion must be fulfilled
- Comment only

Bypass

Bypass function that is normally used for maintenance purposes (e.g., to check effect logic or to replace a sensor).

- Bypass for the entire Cause or Effect:
A bypass for the entire Cause/Effect can be set by means of a so-called "hard bypass" or "soft bypass":
 - "Hard bypass"
In case of a "hard bypass" the bypass is controlled by a configured bypass tag. A Boolean tag can be selected or entered as bypass tag. The bypass becomes active when the value of the bypass tag is TRUE.
 - "Soft Bypass"
In case of a "soft bypass" the operator can set the bypass manually for the Cause/Effect by means of an operator input using Secure Write.

If a bypass is active, a Cause or Effect cannot become active even if the tripping condition and options are fulfilled.

- Bypass for individual tags of a Cause:
A "soft bypass" can also be permitted for the individual tags of a Cause. The operator can manually set a bypass for individual tags of a Cause.
When the "soft bypass" is activated for an individual tag, Degraded Voting automatically becomes active for this Cause.

Degraded Voting

The "Degraded Voting" function allows you to take the individual input tags of a Cause "out of the evaluation" for the Cause in case of a bad signal status ("Bad Quality") or with an active soft bypass.

Degraded Voting results in a change of the Cause logic.

You can find additional information on this in section "The "Degraded Voting" function (Page 60)".

Safety instrumented function groups (SIF groups)

You can create your own safety instrumented function groups for your application, that is, by dividing your application into function groups that you can then monitor and change selectively in the Safety Matrix Engineering Tool and Safety Matrix Viewer (e.g., "level measurement and shut off").

In order to use this function, you must assign the individual Causes and Effects of the safety program to your safety instrumented functions groups. Then, you can display one or more (or all) safety-instrumented function groups.

Secure Write

The "Secure Write" functionality allows operator control functions to be performed to the Safety Matrix. This can be done in online mode of the Safety Matrix Engineering Tool or from the PCS 7 OS via the Safety Matrix Viewer.

Transaction for Secure Write

A transaction for operating a Safety Matrix via Secure Write can be executed in online mode of the Safety Matrix Engineering Tool or from the PCS 7 OS via the Safety Matrix Viewer. The transaction consists of a sequence of operations that can be performed by one or two operators.

The transaction must be completed within a time interval specified by the user (timeout). If the transaction is not finished before the timeout expires, the transaction is automatically canceled.

3.5 Guide to the procedure

This chapter provides a brief overview of the procedure when using the Safety Matrix components within the PCS 7 automation system.

Step	What to do	Safety Matrix component	See section
1	Insert a new Safety Matrix	Engineering Tool	Inserting a new Safety Matrix (Page 50)
2	Edit the properties of the Safety Matrix	Engineering Tool	Editing the properties of the Safety Matrix (Page 88)
3	Configure the functions of the Safety Matrix: <ul style="list-style-type: none"> • Causes • Effects • Intersections 	Engineering Tool External configuration via bulk data engineering	Overview of Configuring (Page 49) Configuring the causes (Page 97) Configuring the effects (Page 109) Configuring the intersections (Page 117) Bulk data engineering using a spreadsheet (Page 120)
4	Transferring the Safety Matrix	Engineering Tool	Transferring a Safety Matrix (Page 129)
5	Compiling and downloading	Engineering Tool	Compiling and downloading (Page 143)
6	Operator control and monitoring	Engineering Tool, Safety Matrix Viewer	Operator control and monitoring (Page 147)
7	Documentation of a Safety Matrix	Engineering Tool	Documentation of a Safety Matrix (Page 193)
8	Acceptance of a Safety Matrix	Engineering Tool	Acceptance test for a Safety Matrix (Page 201)

Installing


4.1 Requirements for the installation

Hardware components

For information on the hardware components of S7 F/FH Systems, refer to the *"S7 F/FH Systems Configuring and Programming"* programming and operating manual. Additional information on this document is available in the preface.

Software requirements

The following software is required to operate the complete range of functions of the Safety Matrix components.

 WARNING
Operation of Safety Matrix
You may only operate the Safety Matrix components in the released system environments. Operation in a virtual environment or remote access are permitted under the conditions listed in section "Requirements for virtual environments and remote access (Page 221)".
(SMW-003)

Safety Matrix Engineering Tool

To operate the Safety Matrix Engineering Tool V6.3, you must have installed the following software packages on the ES:

- Required optional packages
 - S7 F Systems
 - S7 F Systems Lib V1_3
 - For offline testing, e.g. S7-PLCSIM
 - Automation License Manager (ALM)
- For use with PCS 7:
 - PCS 7
 - Windows version corresponding to PCS 7 version

- For use with SIS compact:
 - SIS compact
 - Windows version corresponding to SIS compact version
- For use without PCS 7 or SIS compact:
 - STEP 7
 - CFC

The related version designations and minimum requirements can be found in the readme file.

Safety Matrix Viewer

To operate the Safety Matrix Viewer V6.3, you must have installed the following software packages on the OS:

- PCS 7 or SIS compact
- Automation License Manager (ALM)

The related version designations and minimum requirements can be found in the readme file.

With Safety Matrix Viewer V6.3, operator control and monitoring of safety matrices of versions V6.2 and V6.3 is possible.

4.2 Installing

Note

Installations of older versions of the Safety Matrix components must be uninstalled prior to installing Safety Matrix V6.3.

Note

For installing the Safety Matrix Engineering Tool/Viewer V6.3, the same requirements apply as described in the *"PCS 7 Process Control System; PCS 7 PC Configuration"* Manual. Additional information on this document is available in the preface.

 WARNING
--

Check installed version of the Safety Matrix components
--

After installation of the Safety Matrix components, verify the respective version via "Installed SIMATIC software".

(SMW-004)

Reading Readme files

Important current information regarding the delivered software is available in the Readme files "Safety Matrix Engineering Tool – Readme", "Safety Matrix Viewer – Readme" and "Safety Matrix AS-OS-Engineering – Readme". You can arrange for the Readme files to be displayed at the end of the corresponding setup program. At a later point, you can open the readme file by selecting **SIMATIC > Product Notes > English** in the Windows Start menu. You will find the Readme files in the installation directory of the respective Safety Matrix component.

Installation options

The following options are available in the setup:

Option	Description
Engineering AS and OS	The option is used for installation of all Safety Matrix components on the ES, which means the computer is used for the engineering of AS and OS. This option is used for the installation under SIMATIC PCS 7.
Engineering AS	The option is used for installation of the Safety Matrix components on the ES, which means the computer is used for the engineering of the AS. This option is used: <ul style="list-style-type: none"> • For the installation under SIMATIC STEP 7. • For updating the Safety Matrix Engineering Tool including Safety Matrix Library under PCS 7.
Engineering OS	The option is used for installation of OS components on the ES, which means the computer is used for the configuration of AS and OS and when only the OS is to be updated. This option is used for installation of the OS components Safety Matrix Viewer and Safety Matrix AS-OS-Engineering under SIMATIC PCS 7.
Runtime	The option is used for installing of the OS component Safety Matrix Viewer on the OS, which means the computer is only used as OS (for example, in OS single station system or on OS server).

Optional packages of the SIMATIC Safety Matrix can also be installed via the SIMATIC Management Console.

Installing Safety Matrix Engineering Tool

1. Start the Engineering station.
2. Backup your changes in the "SafetyMatrix Lib" before performing installation, e.g. charts for pre-processing.
You can find additional information on this in the paragraph below "Backup of pre-processing charts when upgrading the "SafetyMatrix Lib"".
3. Ensure that no STEP 7 applications are open.
4. Insert the "Safety Matrix" product CD.

5. Start the SETUP.EXE program on the CD.
6. Follow the setup program instructions.
Select a program package with the Safety Matrix Engineering Tool in the setup.
 - "Engineering AS and OS"
 - "Engineering AS"

Detailed information on the options/program packages is available in the "Installation options" table above.

Installing Safety Matrix Viewer

1. Start your ES/OS. Ensure that no SIMATIC applications are open.
2. Insert the "Safety Matrix" product CD.
3. Start the SETUP.EXE program on the CD.
4. Follow the setup program instructions.
Select a program package with the Safety Matrix Viewer in the setup.
 - "Engineering OS"
 - "Runtime"

Detailed information on the options/program packages is available in the "Installation options" table above.

License key (usage authorization)

A license key is required for each component of Safety Matrix. This license key is installed in the same way as for STEP 7 and the optional packages. For information on installing and working with license keys, refer to the Readme file and the STEP 7 basic help.

Backup of pre-processing charts when upgrading the "SafetyMatrix Lib"

Because the preprocessing charts are saved in the "Templates" folder of the "SafetyMatrix Lib", you must back up the preprocessing charts used prior to an upgrade of the "SafetyMatrix Lib", for example, in a different library. After the upgrade you can move the backed-up charts back to the "Templates" folder of the "SafetyMatrix Lib".

Documentation

When a component of Safety Matrix is installed, a shortcut for English and German with the name "Safety Matrix - Engineering Tool" and "Safety Matrix Viewer" is stored in the respective SIMATIC directory for manuals (Windows Start menu in the subdirectory **SIMATIC > Documentation**).

4.3 Uninstalling previous versions of the Safety Matrix

Uninstalling Safety Matrix components

Note

For uninstalling the Safety Matrix Engineering Tool/Viewer, the same requirements apply as those described in the *"PCS 7 Process Control System; PCS 7 PC Configuration"* manual. Additional information on this document is available in the preface.

Use the normal procedure in Windows for uninstalling software:

1. In the Windows Control Panel start the dialog for uninstalling or changing programs.
2. Select the "SIMATIC Safety Matrix Engineering Tool", "SIMATIC Safety Matrix AS-OS Engineering" and/or "SIMATIC Safety Matrix Viewer" entry in the list of installed software. Click the "Uninstall" button to uninstall the software.
3. If you uninstall the Safety Matrix of a version below V6.3, then you must also uninstall the Safety Matrix Editor.

4.4 Upgrading to Safety Matrix V6.3

4.4.1 Overview of the upgrade

Basic procedure for upgrading

When upgrading the Safety Matrix to V6.3, the following steps must be carried out in the order given:

1. Upgrade the Safety Matrix as described below.
2. If necessary, upgrade the "S7 F Systems Lib" F-library as described in the *"S7 F/FH Systems Configuring and Programming"* Programming and Operating Manual. Additional information on this document is available in the preface.
3. If necessary, upgrade PCS 7 as described in the PCS 7 documentation.

User scenarios for upgrading

Upgrading of version	Updating the Safety Matrix library	Upgrading to Safety Matrix V6.3
Safety Matrix V6.1 or 6.2 (including Service Packs) <ul style="list-style-type: none"> • With transfer of the Matrix 	Yes	User scenario 1 (Page 33)
Safety Matrix 6.2 (including Service Packs) <ul style="list-style-type: none"> • Without transfer of the Matrix • without changing the safety program and the collective signature of the safety program 	No	User scenario 2 (Page 37)
Safety Matrix 6.2 (including Service Packs); Update of the Safety Matrix Viewer only	No	User scenario 3 (Page 38)

General notes on upgrading

After the Safety Matrix Engineering Tool V6.3 is installed and changes are made to existing Safety Matrices, the Safety Matrix library must be upgraded.

After the upgrade you have to run the OS project editor in the WinCC projects. Then you must compile the OS with the option "Entire OS with memory reset".

Effects of the upgrade

Before you upgrade a project to Safety Matrix V6.3 keep in mind the following consequences:

Installation variant	Consequences	
	Advantages	Disadvantages
"Engineering OS" or "Runtime" options	<ul style="list-style-type: none"> • Safety program is unchanged, which means a CPU STOP is not necessary. • No transfer required • New representation and revised interface of the faceplates 	<ul style="list-style-type: none"> • No new functionality • OS compilation required • Only new representation of the faceplates
"Engineering AS" or "Engineering AS and OS" options; With update of the Safety Matrix library	<ul style="list-style-type: none"> • Expanded engineering • Expanded functionality for operator control and monitoring • Full scope of functions 	<ul style="list-style-type: none"> • Changed safety program • CPU STOP required • Transfer required • OS compilation required
"Engineering AS" or "Engineering AS and OS" options; without update of the Safety Matrix library	<ul style="list-style-type: none"> • Safety program is unchanged, which means a CPU STOP is not necessary. • No transfer required • New representation and revised interface of the faceplates 	<ul style="list-style-type: none"> • No new functionality • OS compilation required • Only new representation of the faceplates

The new functions of the Safety Matrix V6.3 can only be used after updating the Safety Matrix library.

4.4.2 User scenario 1

Objective

Update of the Safety Matrix Engineering Tool as well as the Safety Matrix library with transfer of the matrices to be migrated.

Introduction

This user scenario helps you when switching from Safety Matrix V6.1 or 6.2 (and Service Packs) to Safety Matrix V6.3 with an update of the Safety Matrix library.

Requirement

A project has been compiled and downloaded (acceptance tested, if necessary). This project must include the blocks of the F-library "Failsafe Blocks" (V1_3 or later). You can check this as follows:

- Open the block folder of the program in the detail view in SIMATIC Manager. The column "Version (Header)" must include the information "4.0" (or later) for the following F-channel drivers:
 - F_CH_DI
 - F_CH_DO
 - F_CH_AI

There must not be any offline changes that are not downloaded online.

Consequences

- Change of the collective signature of the safety program
- Change of the Safety Matrix signature
- Complete download with STOP of F-CPU required
- Compilation and download of the OS required

Procedure

1. Create a backup copy of the entire S7 project for comparison purposes before you install Safety Matrix V6.3.
2. If you have created your own templates in the Safety Matrix library (for preprocessing), save the current library under a new name. Changes to the existing library will otherwise be lost during the upgrade.
3. Start the Safety Matrix V6.3 installation program on the ES.

4. Select a program package in the setup.
 - "Engineering AS and OS" if you are using ES and OS on this computer.
 - "Engineering AS" if you are using only the ES on this computer.Detailed information on the options/program packages is available in the section "Installing (Page 28)" in the "Installation options" table.
5. If you are using an OS single station system or an OS server, start the installation program on the respective computer.
Select the program package in the setup:
 - "Runtime"
6. To update the library in the project, open the Safety Matrix library "SafetyMatrix Lib (V1_4)" on the ES in SIMATIC Manager.
In the library, open the "Blocks" folder.
7. Select the menu command "Options > Charts > Update block types...".
8. Select the S7 program you want to update, and in the next dialog select the blocks for updating. Follow the on-screen instructions.

Note

For "Update block types" all blocks of the Safety Matrix library must be selected and updated. Do not use mixed libraries.

The blocks are copied to the "Blocks" folder of S7 program, and the block instances in the respective charts are updated. The actions taken are documented in the report.
Note that the acknowledgment behavior of channel drivers may change when migrating matrices from older versions. Therefore, check the settings for the channel driver acknowledgment in the "Channel driver" dialog prior to the transfer. You can find additional information on this in section "Configuration of the F-channel driver acknowledgment (Page 66)".

9. To migrate the desired matrices, close all matrices in the engineering.
Transfer requirement:
 - The selected matrices must all be saved, and all critical and non-critical changes must be accepted.In SIMATIC Manager, select the "Safety matrices" folder and the menu command **Options > Safety Matrix > Selective transfer**.
All Safety matrices are displayed in the next dialog. Select the matrices you want to transfer. Transfer with the "Entire Safety Matrix" option is required for upgrading with update of the Safety Matrix library. To do this, click the "Transfer options" button. In the next dialog box, select the "Entire Safety Matrix" option and close the dialog box with "OK." You can find additional information on this in section ""Selective transfer" dialog box (Page 140)".
10. Confirm the start of the transfer of the selected matrices.
11. Compile the F-CPU program with the migrated matrices.

12. Compare the safety program with the backup copy from step 1 by using the **Options > Compare programs** menu command in the Engineering Tool.

The following change is listed for each Safety Matrix after successful upgrade:

```
Matrix modified; new version of matrix
```

13. Also compare the safety program with the backup copy. To do so, use the Compare... button in the "Edit Safety Program" dialog of SIMATIC Manager.

Result of comparison in step 13

The result of the comparison in a list with three sections: "Execution level", "Chart" and "Changes to system block". The "@FMatrices" chart is created automatically.

"Execution level" section

The following changes are listed in the "Execution level" section after successful upgrade:

Note

In the description below only the top level of the changes is shown for each block.

Lower-level changes exist but are not listed here to get a better overview.

Runtime group "@F_ShutDn"

Block "@F_ShutDn\F_SHUTDOWN(F_SHUTDOWN)"

In each runtime group with Safety Matrix F-blocks:

- One section per Safety Matrix for the Causes for the **F_StatDB F-FB**
Block "MatrixName\@MatrixName\C_Status(F_StatDB)": Signature changed
- One section per Safety Matrix for the effects for the **F_StatDB F-FB**
Block "MatrixName\@MatrixName\E_Status(F_StatDB)": Signature changed
- One section per Safety Matrix for each **F_Cause F-FB**
Block "MatrixName\@MatrixName\Cx(F_Cause)": Signature changed, interface changed (number of parameters)'y' <-- 'x'
- One section per Safety Matrix for the effects for the **F_Inters F-FB**
Block "MatrixName\@MatrixName\Inters(F_Inters)": Signature changed
- One section per Safety Matrix for the **F_Effect F-FB**
Block "MatrixName\@MatrixName\Ex(F_Effect)": Signature changed, interface changed (number of parameters)'y' <-- 'x'
- One section per Safety Matrix for each **F_Matctl F-FB**
Signature changed, interface changed (number of parameters)'y' <-- 'x'

"Chart" section

"Matrixname" chart, "@Matrixname" chart

"@Matrixname" chart

EN_GDM added

SET_GDM added

MA_AL added

Alarm deleted

Listed changes of the matrix in the "Chart" section are displayed in more detail during comparison with the menu command **Options > Compare programs**.

"Changes to system block" section

The following changes are listed in this section after successful upgrade:

Block "F_StatDB": Signature changed

Block "F_StatDB": Interface changed (number of parameters)'y' <-- 'x'

Block "F_Cause": Signature changed

Block "F_Cause": Interface changed (number of parameters)'y' <-- 'x'

Block "F_Inters": Signature changed

Block "F_Inters": Interface changed (number of parameters)'y' <-- 'x'

Block "F_Effect": Signature changed

Block "F_Effect": Interface changed (number of parameters)'y' <-- 'x'

Block "F_Matctl": Signature changed

Block "F_Matctl": Interface changed (number of parameters)'y' <-- 'x'

If you receive items in addition to the listed changes for the comparison results in steps 12 and 13, you must determine the plant-specific background of the change, evaluate it and possibly change it to meet your requirements.

Measures after upgrading

Implement the following measures after successful upgrade of the Safety Matrix.

1. For you to be able to operate the safety matrices after the upgrade, you must set the EN_SWC input parameters of all nested charts of the matrix logic ("@MatrixName") to TRUE. You can find additional information on this in section "Transaction for Secure Write (Page 170)".
2. Set the time interval for a transaction for a specific plant, especially if you want to use the "2-operator scenario" function on the PCS 7 OS. You can freely configure this time in the "Parameters" tab of the "Properties" dialog. Default setting is 60 s.
3. If required, an approval of the changes according to section "Acceptance test for a Safety Matrix (Page 201)" can take place. No additional function test is required for the changes listed under steps 12 and 13.
4. Upgrade the block icons in the OS pictures as described in section "Introducing the new Safety Matrix block icons into the PCS 7 OS (Page 87)".
5. Compile and download the OS.
6. Download the S7 program to the F-CPU.

4.4.3 User scenario 2

Objective

Updating the Safety Matrix Engineering Tool.

Introduction

This user scenario helps you when switching from Safety Matrix V6.2 to Safety Matrix V6.3 without an update of the Safety Matrix library.

Requirement

A project has been compiled and downloaded (acceptance tested, if necessary).

There must not be any offline changes that are not downloaded online.

Consequences

- No changes to safety program
- No change of the collective signature of the safety program
- No change of the Safety Matrix signature
- No transfer of matrices.

Note

When you select this scenario, the Safety Matrix continues to use the blocks of version V6.2 and no CPU STOP is required. The software user interface corresponds to version V6.3, but the range of functions is still that of version V6.2.

If you want to use the new blocks of the "SafetyMatrix Lib (V1_4)" and the functions of the Safety Matrix V6.3, you can upgrade the blocks in the project to the blocks of the "SafetyMatrix Lib (V1_4)" at a later time. Keep in mind that this change causes a **CPU STOP** (see section "User scenario 1 (Page 33)").

You cannot change back from "SafetyMatrix Lib (V1_4)" to "SafetyMatrix Lib (V1_3)".

Procedure

1. Create a backup copy of the entire S7 project for comparison purposes before you install Safety Matrix V6.3.
2. Start the Safety Matrix V6.3 installation program on the ES.

3. Select a program package in the setup.

- "Engineering AS and OS"
- "Engineering AS"

Detailed information on the options/program packages is available in the section "Installing (Page 28)" in the "Installation options" table.

4. If you are using an OS single station system or an OS server, start the installation program on the respective computer.

Select a program package in the setup.

- "Engineering OS"
- "Runtime"

5. Because no blocks are updated in this scenario and there is no transfer of matrices, no additional steps are required.
To confirm that the matrices and the safety program have not been changed, execute the following steps.

6. Compare the safety program with the backup copy from step 1 by using the **Options > Compare programs** menu command in the Safety Matrix Engineering Tool.

The following change is listed for each Safety Matrix:

No differences found

7. Also compare the safety program with the backup copy. To do so, use the Compare... button in the "Edit Safety Program" dialog of SIMATIC Manager.

Result of comparison in step 7

No changes to the safety program

Measures after upgrading

The following measures must be implemented after successful upgrade of the Safety Matrix.

1. Upgrade the block icons in the OS pictures as described in section "Introducing the new Safety Matrix block icons into the PCS 7 OS (Page 87)".
2. Compile and download the OS.

4.4.4 User scenario 3

Objective

Update of the Safety Matrix Viewer.

Introduction

This user scenario helps you when migrating from Safety Matrix Viewer V6.2 (incl. Service Packs) to Safety Matrix Viewer V6.3.

Requirement

A project has been compiled and downloaded (acceptance tested, if necessary).

There must not be any offline changes that are not downloaded online.

Consequences

- No changes to safety program
- No change of the collective signature of the safety program
- No change of the Safety Matrix signature
- Compilation and download of the OS required

Procedure

1. Create a backup copy of the entire S7 project for comparison purposes before you install Safety Matrix V6.3.
2. Start the Safety Matrix V6.3 installation program.
Select a program package with the Safety Matrix Viewer in the setup.
 - "Engineering OS" on the ES
 - "Runtime" on the OS

Detailed information on the options/program packages is available in the section "Installing (Page 28)" in the "Installation options" table.

The selected program package is installed on the computer.

Execute the following steps to use the new features of the Safety Matrix faceplate in an existing project.

1. Launch the **WinCC Explorer** for the OS assigned to the Safety Matrix project.
2. Open the **OS Project Editor** and click **OK**. The project is reconfigured and, as a result, the new block icon will be adopted.
3. Open the **Global Script C-Editor** and select the **Options > Regenerate headers** menu command.

In order to introduce the new block icon into existing plant pictures, you must compile and download the OS for the relevant project.

If necessary, configure the desired permissions for the block icons.

1. Start SIMATIC Manager.
2. Make sure that the "Derive block icons from the plant hierarchy" option is selected in the "Block icons" tab of the object properties for the relevant picture object. (This is the default setting with PCS 7.)
3. Highlight the OS object and select "Compile" in the context menu to compile the OS.
4. Click the "Compile" button in the last dialog of the "Compile OS" wizard.
5. Repeat these steps for all projects.
6. Download all operator stations.

Result

Once you have performed these steps, your project contains the new Safety Matrix block icon.

See also

Introducing the new Safety Matrix block icons into the PCS 7 OS (Page 87)

Software user interface

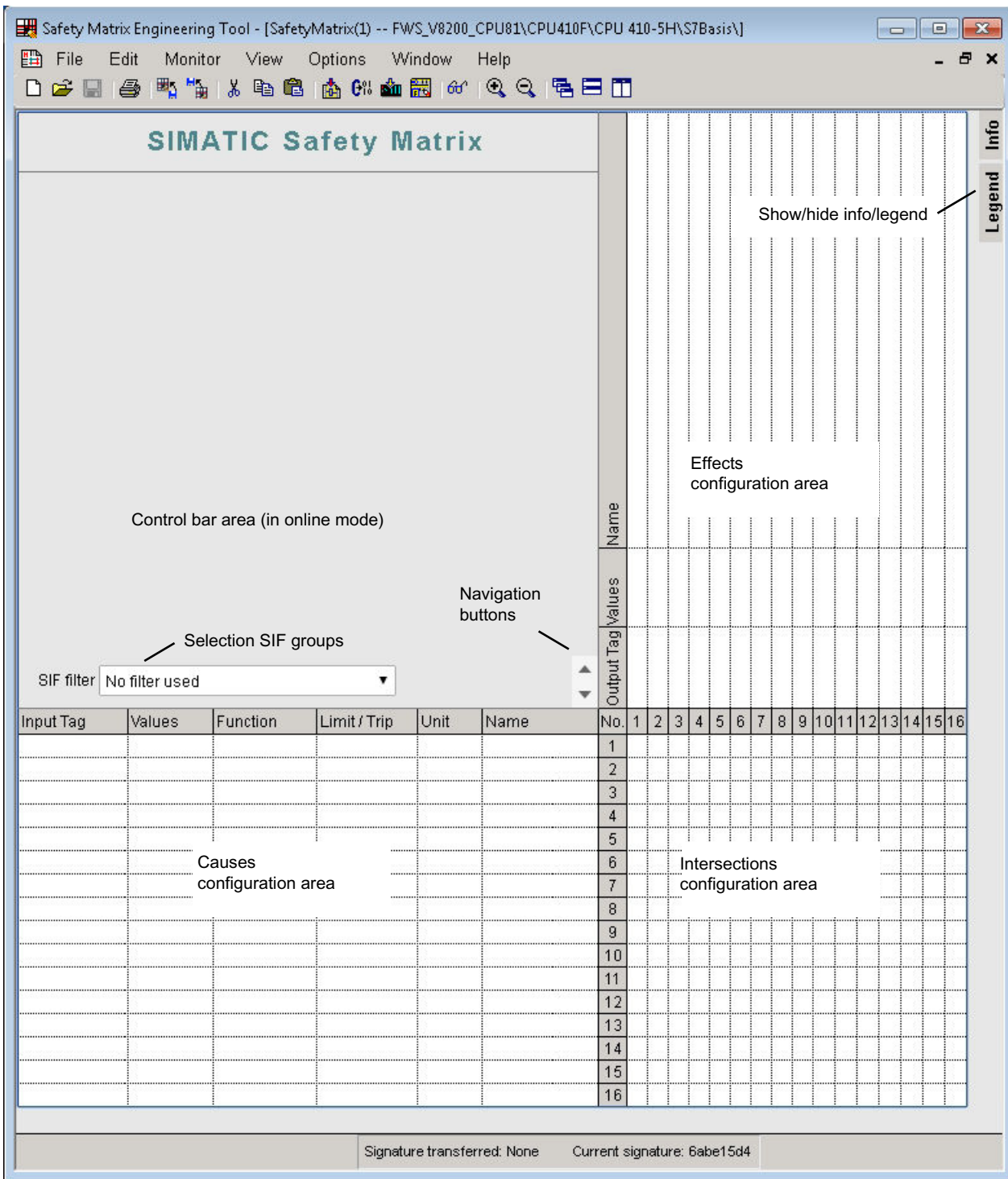
5.1 Overview of the software user interface

Overview

For configuration, the Safety Matrix is opened in the Safety Matrix Engineering Tool.

The following figure shows the user interface of a newly created Safety Matrix with highlighted configuration and information areas.

5.1 Overview of the software user interface



Additional columns can be displayed in the configuration areas of the Matrix view. You can find additional information on this in section ""Customize" dialog boxes (Page 94)".

Elements of the software user interface

In addition to the configuration areas listed in the figure above, the software user interface contains additional elements.

Menu bar

In the menu bar you can find the functions of the software user interface.

You can find additional information on this in section "Menu bar of the Safety Matrix (Page 44)".

Toolbar

Various functions are available via buttons in the toolbar; these functions can also be executed with menu commands.

Info/Legend

The "Info" and "Legend" tabs can be shown or hidden and display the following information:

- "Info" tab
 - Version information
 - Major revision
 - User notes
 - SIF groups
- "Legend" tab
 - Intersection types
 - Cause-Effect options

The options and user notes can also be displayed in a separate column in the Matrix view. You can find additional information on this in section ""Customize" dialog boxes (Page 94)".

Control bar

The control bar is available in the Safety Matrix Viewer or in online mode of the Safety Matrix Engineering Tool.

You can find additional information on this in section "Operating over the control bar (Engineering Tool / Viewer) (Page 173)".

"SIF Filter" drop-down list

Using the "SIF Filter" drop-down list, the display of the Causes and Effects can be filtered for single or multiple safety instrumented function groups (SIF groups).

You can find additional information on this in section ""SIF Filter" drop-down list (Page 47)".

Navigation buttons (Effects)

You can use the navigation buttons to influence the display of effects if they are not fully shown due to the row heights.

- The "Up" button displays a new row at the top of the effects table.
- The "Down" button displays a new row at the bottom of the table.

Status bar

The status bar of the Safety Matrix is different in online and offline modes:

- In offline mode, the status bar contains an area for status displays and an area for error displays.
The signatures of the current (offline) and the transferred matrix are displayed.
- In online mode, the status bar contains an area for status displays, an area for error displays, and additionally a date/time display "CPU time".
The signatures of the current (offline) and the matrix loaded to the CPU (online) are displayed.

Reports window

Another important component of the Safety Matrix user interface is the reports window.

The window can be opened with the menu items **View > Reports** or **Options > Create report**.

Different reports are displayed in the window in separate tabs.

- Events
- Maintenance operations
- Transfer
- Comparison
- Configuration
- Validation
- Import/export

The reports window is arranged below the Safety Matrix by default, but you can move and resize it as needed.

In the reports window, a reduced menu bar is available containing commands for saving and printing.

5.2 Menu bar of the Safety Matrix

Overview of menu bar

The menu bar of the Safety Matrix Engineering Tool contains the following menu commands:

- File
- Edit
- Monitor
- View
- Options
- Window
- Help

The respective subcommands of the menu commands are explained below.

"File" menu command

Command	Function
New	Opens a dialog for selecting the project in which you want to create the new matrix and for specifying the name of the new matrix. You can find additional information on naming in section "Inserting a new Safety Matrix (Page 50)". A new Safety Matrix can be created with this menu command.
Open	Opens a dialog for selecting the project and a Safety Matrix existing in it. With this menu command you open an existing Safety Matrix for editing.
Close	Closes the current Safety Matrix file. You will be prompted to save your changes to the Safety Matrix before closing the file.
Save	Saves the current Safety Matrix configuration. Changes (critical/non-critical) must be accepted. Password for the safety program is required.
Transfer	Transfers the Safety Matrix to the project. See section "Transferring a Safety Matrix (Page 129)".
Import...	Imports the Safety Matrix data from a file in "*.ods" format.
Export...	Exports the Safety Matrix data to a file in "*.ods" format.
Print...	Opens the "Print" dialog box. The "Print" dialog box allows you to specify the print settings and to start the printout of the current Safety Matrix. The Print command is only available in offline mode.
Recent files	The Recent files command provides you with a list of recently opened Safety Matrix files for selection.
Exit	Closes all dialog boxes and exits the program.

"Edit" menu command

Command	Function
Properties	The "Properties" dialog box provides you comprehensive information and possible entries for the general properties of the Safety Matrix. See section ""Properties" dialog box of the Safety Matrix (Page 88)".

"Monitor" menu command

Command	Function
Configure...	The "Configure" dialog box allows you to specify the duration, in seconds, of the monitoring cycle, i.e., the cycle time for updating the user interface. Value range: 1 to 60 s
Monitor On/Off	Switches online mode on and off.

"View" menu command

Command	Function
Customize	Opens the "Customize - Layout" and "Customize - Colors" dialog boxes. These dialog boxes offer numerous options for adjusting the appearance of the Safety Matrix as well as the information displayed. See section ""Customize" dialog boxes (Page 94)".
Reports	Opens the "Reports" window. The various reports, such as the configuration report, validation report and event log, are shown in tabs. This information is overwritten by the latest processes. The reports can be saved and printed with the "Save..." and "Print..." icons in the toolbar.
Update or <F5>	Refreshes the view of the Safety Matrix. This function allows you to apply changes that were made to the symbol table and the safety program while the Safety Matrix is open.

"Options" menu command

Command	Function
CFC	This compiles the program in which the opened Safety Matrix is located. See section "Compiling and downloading (Page 143)".
CPU	<ul style="list-style-type: none"> • "Download..." This loads the program in which the opened Safety Matrix is located into the F-CPU. See section "Compiling and downloading (Page 143)". • "Module information" Opens the "Operating mode" dialog box with status and diagnostic information of the CPU. • "Operating mode" Shows the current operating mode of the CPU. You can change the operating mode of the CPU with the buttons. The buttons that can be selected in the current operating mode are active.
Edit safety program...	Opens the "Safety program" dialog box.
Track changes	<ul style="list-style-type: none"> • "Apply changes" When you select this option you are prompted to check the changes in the reports window and specify which changes you want to accept (critical/non-critical). • "Accept Changes Automatically with Save" When you select this option the changes are automatically accepted while saving.
Compare Safety Matrix with	Use this command to compare the Safety Matrix with other Safety Matrices. See section "Comparing Safety Matrices (Page 194)".

Command	Function
Compare programs...	The "Compare Programs" dialog box enables you to compare all CFC charts of a chart folder, which have been created during transfer by the Safety Matrix Engineering Tool, and to display and print out differences. See section "Comparing CFCs (Page 195)".
Create report	<ul style="list-style-type: none"> "Configuration" generates a report with the complete Safety Matrix configuration in the "Reports" window. "Validation" starts a plausibility check of the Safety Matrix configuration and shows the results in the "Reports" window. <p>The reports can be saved and printed with the "Save..." and "Print..." icons in the toolbar.</p>

"Window" menu command

Here you will find the standard Windows commands for displaying multiple windows and for displaying the currently opened Safety Matrices.

"Help" menu command

Command	Function
Help topics...	Opens the content directory of the help system.
User Manual (PDF)	Opens the PDF file of the user manual.
Info...	Displays version info of the Safety Matrix software.

5.3 "SIF Filter" drop-down list

Introduction

With safety instrumented function groups "SIF" you can divide your application into function groups that you can then monitor and change selectively in the Safety Matrix Engineering Tool and Safety Matrix Viewer (e.g., "level measurement and shutdown").

By using the "SIF Filter" drop-down list in the Safety Matrix Engineering Tool and Safety Matrix Viewer, the display of the Causes and Effects can be filtered for single or multiple safety instrumented function groups (SIF groups).

Requirements

- The safety instrumented function groups are created in the "General" tab in the "Properties" dialog box of the Safety Matrix.
- SIF groups are assigned in the options of the Causes and Effects. Not all Causes and Effects must be assigned to an SIF group. A Cause or Effect can be assigned to up to four SIF groups.

Structure of the selection dialog

Options

The following options can be selected in the selection dialog.

Option	Description
"No filter used" (Status indicator only; not directly selectable)	No SIF filter is currently in use. To clear a filter, select the "Select all" option in the selection box and then disable it.
"(Select all)"	All groups are selected and the Causes and Effects of these groups are displayed.
Check box + number + name	A row is displayed for each SIF group that is created in the "Properties" dialog box, "General" tab of a Safety Matrix. <ul style="list-style-type: none"> • Check box: The associated SIF group is selected for display by selecting the check box. It is possible to select multiple check boxes. • Number + name: This information corresponds to the configuration of the SIF group in the "Properties" dialog box of the Safety Matrix.

Buttons

- "OK" button
The selected filter conditions are applied with this button, and only the Causes and Effects of the Safety Matrix that meet these filter criteria are displayed.
- "Cancel" button
This button closes the dialog box and the filter conditions are not changed.
Alternatively, the selection dialog can also be closed by clicking outside of the dialog in the user interface of the engineering tool without changing the filter conditions.

Configuring

6.1 Overview of Configuring

6.1.1 Basic procedure for creating a safety program

Introduction

Based on the well-established Cause/Effect method, the Safety Matrix allows simple configuration in which you assign precisely defined reactions (Effects) to event occurrences (Causes), thus specifying the system behavior. The Safety Matrix provides comprehensive support for configuring in the form of:

- Structured user interface
- Simple parameter assignment and linking of Causes and Effects
- Automatic checking of the configuration for validity
- Automatic placement of the F-channel drivers during transfer to a CFC chart
- Automatic generation of an S7 F-Systems program logic based on CFC using F-blocks from the Safety Matrix library.
- Revision and change tracking, functions for comparing matrices and for support during system acceptance testing

Requirements

- You must have created a project structure in SIMATIC Manager.
- You must have assigned your safety program to an F-capable CPU S7-400H, such as CPU 410-5H.
- The "CPU contains safety program" option must have been selected for the F-CPU, and a password must have been assigned for the F-CPU. This option is configured in the "Protection" tab in HW Config in the properties of the F-CPU.
- You must have configured the inputs and outputs in HW Config or in the symbol table in SIMATIC Manager. The Safety Matrix works with the symbolic names of the inputs (input tags) and outputs (output tags) of the F-modules.

Basic procedure

Proceed as follows to create a safety program:

1. After you have specified the program structure, insert a Safety Matrix into the S7 program.
2. Insert the following into the Safety Matrix
 - Input tags for Causes and
 - Output tags for effects
3. Assign parameters for the following
 - Causes
 - Effects
 - Intersections
4. Save and accept the changes.
5. Transfer the Safety Matrix to CFC charts.
6. Compile and download the S7 program.
7. Test and document the safety program.
8. Perform the acceptance test.

6.1.2 Inserting a new Safety Matrix


Safety Matrix object

In the S7 program folder of an F-CPU, the Cause/Effect logic is stored in a Safety Matrix object in which the logic is set up and transferred to a CFC chart in the form of function blocks. Each Safety Matrix object supports up to 128 Causes and 128 Effects with a maximum of 1024 intersections. Depending on its memory capacity, one F-CPU can support several matrices.

Adding a Safety Matrix object in a project

1. Open SIMATIC Manager and select the component view.
2. Open the project in SIMATIC Manager.
3. Navigate to the required S7 program folder in the project.
4. Right-click the S7 program folder, and select **Insert New Object > Safety Matrix folder**. A new Safety Matrix folder named "Safety Matrices" is created in the S7 program.
5. Right-click the "Safety Matrices" folder and select the **Object properties** of the matrix folder.
6. If required, change the default name for the matrix folder (maximum of 24 characters) or enter an author (maximum of 40 characters) and a comment (maximum of 254 characters) in the "Name:" field.
7. Right-click the matrix folder and select **Insert New Object > Safety Matrix**. A new object "SafetyMatrix(n)" is created in the "Safety Matrices" directory.

8. Right-click the new Safety Matrix object and select the **Object properties**.
If required, change the default name of the matrix in the "Name:" field in the "General" tab.
Up to 16 characters are possible for the name. This entry is not case-sensitive.
Note the following information when assigning a name:

 WARNING
Unique names for Safety Matrix
You must assign each Safety Matrix a name that is unique from all others in the system in order to provide adequate safety for online communication during a Secure Write transaction.
(SMW-005)

Note

The name of the Safety Matrix contains incorrect characters

The following characters are not permitted in Safety Matrix names:

Spaces & \ " ` ' * + , / : ; < = > ? [] \ \ | .

Note

Copying Safety Matrix

To copy an existing Safety Matrix, export it with the menu command **File > Export** in the Safety Matrix Engineering Tool and save it in an export file in ODS format. Afterwards you can import the exported data to a new Safety Matrix.

Export files in CEM format from previous Safety Matrix versions can also be imported.

For more information on export and import, refer to the section "Importing a Safety Matrix file (*.cem) into a PCS 7 project (Page 124)".

9. Double-click the Safety Matrix object in SIMATIC Manager.

Result

The newly created Safety Matrix is opened in the Safety Matrix Engineering Tool.

You can find additional information on the elements of the software user interface in section "Overview of the software user interface (Page 41)".

6.1.3 The Safety Matrix tags

Which tags are supported by Safety Matrix?

The following tags are supported by the Safety Matrix:

- Input and output tags
These form the interface of the Safety Matrix to the F-I/O. The input and output tags include the symbolic names of the inputs and outputs of the SIMATIC F-modules configured in the SIMATIC project and the assigned F-channel drivers.
- Any signals from the safety program by means of connections on the nested chart
- State of a Cause, Effect or Effect tag by means of internal references
- Customer-specific F-channel drivers

Note

F-channel drivers of a Safety Matrix

All F-channel drivers used in a Safety Matrix must be located in the F-shutdown group of that Safety Matrix.

In addition, all F-channel drivers of a module must also be contained in the same F-shutdown group.

Integration of the tags into the Safety Matrix

In the "Cause details" dialog box, "Configure" tab, you can use the "I/O" button of a tag to open the "Select I/O Tag" dialog box. This dialog offers the following options for integration of tags into the Safety Matrix (see section ""Cause details" dialog - "Configure" tab (Page 102)").

Option "External connection" (prefix "#")

If a Cause or Effect is to be interconnected with **any signal from the safety program**, you must select one of the following options when configuring the tag:

- For input tags (Causes or bypass tag, for example), a chart input is created at the nested chart of the matrix logic (as input from CFC).
- For output tags (effects), a chart output is created at the nested chart of the matrix logic (for processing the effect tag in the CFC).

Option "Internal reference" ("Cause[x]", "Effect[x]", or "Effect[x][y]")

The state of a Cause, Effect or Effect tag within the Safety Matrix can be further processed as an input tag. To do so, you must select the Cause "[x]" or the tag "[y]" at the Effect "[x]".

Option "Channel driver" (Safety Matrix input and output tags)

The Safety Matrix Engineering Tool automatically places F-channel drivers of SIMATIC F-modules for input and output tags. This occurs during the transfer to a CFC chart if there is no F-channel driver for the respective F-channels.

- **Channel driver - with "monitoring" (suffix "#")**

As with input and output tags, one F-channel driver is created in the nested chart of the F-channel drivers.

In addition, the following applies:

- Chart output is created at the nested chart of the F-channel drivers for input tags (for further processing of the read driver signal in the CFC, in addition to processing in the Safety Matrix)
- A chart output is created at the nested chart of the matrix logic for output tags (for further processing of the effect in the CFC, in addition to output to the F-channel driver).

If both the "#" prefix and suffix are specified, the suffix will be removed during the transfer. Externally used channel drivers cannot be configured as "Monitoring" in the Safety Matrix.

- Configuring in the "Channel driver" dialog box:
The monitoring for the tag is configured in the "Cause details"/"Effect details" dialog box, "Configure" tab, "..." button. To do so, the "Monitoring active" option in the "Monitoring" area is selected in the "Channel driver" dialog box, "Options" tab.

The name of Safety Matrix input/output tags for which the "Monitoring active" option should be activated can contain no more than 23 characters.

- **Channel driver with preprocessing (prefix "*")**

You can interconnect a preprocessing for discrete and analog input tags. Such an interconnection with preprocessing is marked with a prefix "*" in the configuration box of the tag by the Safety Matrix Engineering Tool after the transfer. You can find additional information on this in section "Preprocessing (Page 56)".

- Configuring in the "Channel driver" dialog box:
The preprocessing for the tag is configured in the "Cause details" dialog box, "Configure" tab, "..." button. To do so, a preprocessing chart is selected in the "Preprocessing" area in the "Channel driver" dialog box, "Options" tab.
- Display in the "Select I/O Tag" dialog box:
The configured preprocessing of a tag is displayed in the "*" table column of the respective tag in the "Select I/O Tag" dialog box. You can use the "I/O" button in the "Cause details" dialog box, "Configure" tab, to open the "Select I/O Tag" dialog box.

- **Channel driver - used externally (prefix "@")**
If the input/output tag was already configured by another Safety Matrix or user logic, the transferred Safety Matrix interconnects the tag to the existing F-channel driver. Such an interconnection with an existing F-channel driver is automatically marked with a prefix "@" in the configuration box of the tag by the Safety Matrix Engineering Tool.
 - Display in the "Select I/O Tag" dialog box:
The external interconnection of a tag is displayed in the "@" table column of the respective tag in the "Select I/O Tag" dialog box. You can use the "I/O" button in the "Cause details" dialog box, "Configure" tab, to open the "Select I/O Tag" dialog box.

Note

If the F-channel driver with the specified tag does not exist during the Safety Matrix transfer, the prefix is removed and the tag is treated as an input/output tag of the Safety Matrix. Likewise, the prefix is automatically added during transfer if the F-channel driver is already being used by another Safety Matrix or user logic.

- **Option "Channel driver - Customer-specific" (prefix "~")**
You can interconnect Causes and Effects with the signals of customer-specific F-channel drivers. Such an interconnection with a customer-specific F-channel driver is automatically marked with a prefix "~" in the configuration box of the tag by the Safety Matrix Engineering Tool.
See also section "Customer-specific F-channel driver (Page 64)".

6.1.4 Syntax rules for tag names in the Safety Matrix

Types of tag names

The following types of tag names are possible in the Safety Matrix:

- Input or output tag of the Safety Matrix
- Any signals from the safety program
- Internal references ("Cause[x]", "Effect[x]", "Effect[x][y]")
- Customer-specific F-channel drivers

Permissible characters

The permitted character set is the range of ASCII characters from 16#20 (blank space) to 16#7a (lower case "z").

Both upper case and lower case letters may be entered, but the symbols are not case-sensitive, i.e., symbols "TIC2344", "TiC2344" and "tic2344" are identical. Internal references are an exception (see below).

Input/output tag of the Safety Matrix

Maximum number of characters: 24

The name of Safety Matrix input/output tags for which the "Monitoring active" option should be activated can contain no more than 23 characters.

Safety Matrix input/output tags are tags that are interconnected completely by the Safety Matrix during transfer to a CFC chart (possibly also tags interconnected with the transfer option "Integrate external channel drivers", see section "Transferring a Safety Matrix (Page 129)").

Following characters may be used for a Safety Matrix tag:

- Special characters: !\$&()*+,- ;<=>? []^_`
- Numbers: 0123456789
- Upper case letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Lower case letters: abcdefghijklmnopqrstuvwxyz
- . (period) can be used for the channel driver, e.g. "E1.6"

The following special characters must **not** be used:

- " (quotation mark)
- % (percent sign)
- ~ (tilde)

The following special characters must not be used in certain positions:

- (blank character): Must not be located at the start or end of a symbol.
- # (number sign): Must not be located at the start or end of a symbol because here it serves to label the tag as a chart connection.
- ' (inverted comma): Must not be located at the end of a symbol.
- @ ('at' character): Must not be located at the start of a symbol because here it serves to label the tag as an external address.

Any signals from the safety program

Maximum number of characters: 24

Special syntax rules apply for chart inputs in the CFC which subsequently also apply to all tags with the prefix or suffix "#":

- With prefix "#": The name can only start with letters or an underscore.
- With suffix #: The name can only start with letters or numbers.
- Only letters, numbers, and underscores are allowed within the name.
- Underscores must not be used more than once in succession.
- An underscore must not be used at the start of the name (with suffix "#") or at the end of the name.

Examples of valid chart connection names

- #TIC4711
- #TIC_4711
- #_4_321

Examples of invalid chart connection names

- #4711 (number at start)
- #TIC__543 (repeated underscore)
- #TIC_4711_ (underscore at end)
- _TIC_4711# (underscore at start with suffix "#")

Internal references ("Cause[x]", "Effect[x]", "Effect[x][y]")

Selection of internal references is guided by menus.

6.1.5 Preprocessing

Preprocessing for input tags

You can interconnect a preprocessing for discrete and analog input tags.

With preprocessing an input signal supplied by the F-channel driver can be prepared for the Safety Matrix by means of an editing function, for example, to convert the input value for an analog value with a calculation function into a quantity that is more meaningful for the user.

The preprocessing is a CFC that you can create yourself. Two types of templates are available for this purpose in the "Templates" folder.

The preprocessing chart must be saved in the "SafetyMatrix Lib" in the "Templates" folder and must meet the requirements described below.

Templates for preprocessing charts

The "SafetyMatrix Lib" contains two templates in the "Templates" folder for preprocessing charts without internal functionality that you can copy and customize as needed.

- "F_SM_PP_B"
Template for preprocessing chart for binary input values (e.g. with the F-channel block F_CH_DI)
- "F_SM_PP_R"
Templates for preprocessing chart for analog input values (e.g. with the F-channel block F_CH_AI)

These templates for preprocessing charts meet the requirements described below.

Requirements for preprocessing charts

Analog preprocessing:

- Chart interface

REAL	
V_IN	Input process data
V_OUT	Output process data
SIM_V_IN	Input simulation value
SIM_V_OUT	Output simulation value

- A comment that starts with "SM_REAL_..." must be entered in the properties of the preprocessing chart.

Discrete preprocessing:

- Chart interface

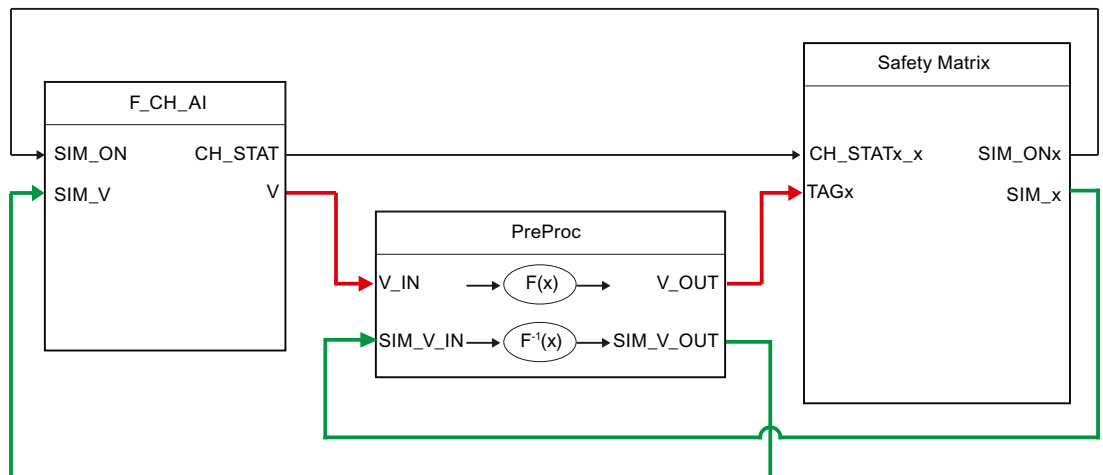
BOOL	
Q_IN	Input process data
Q_OUT	Output process data
SIM_I_IN	Input simulation value
SIM_I_OUT	Output simulation value

- A comment that starts with "SM_BOOL_..." must be entered in the properties of the preprocessing chart.

Principle of preprocessing

Preprocessing is possible for input tags with the option "Channel driver" or "Channel driver - Customer-specific".

The following diagram shows the preprocessing based on an analog input tag.



The signal processing with preprocessing:

- In preprocessing, the current process value of "V_IN" is processed with the function $F(x)$ and transferred to the Safety Matrix with "V_OUT".
- The following outputs of the Safety Matrix are used when activating the simulation:
 - The F-channel driver "F_CH_AI" is switched to simulation via the "SIM_ON" output.
 - The simulation value set in the matrix via the "SIM_x" output is transferred to the input "SIM_V_IN".
- In the preprocessing, the simulation value at the "SIM_V_IN" input is processed by the reversing function $F^{-1}(x)$ and transferred to the F-channel driver input "SIM_V" via the "SIM_V_OUT" output.

By preprocessing with the $F(x)$ function the preprocessed values are used in the Safety Matrix.

During simulation, a value from the value range of the preprocessed signal is therefore also specified in the Safety Matrix. The reversing function $F^{-1}(x)$ calculates this simulation value back into the same value range that applies for the "V" output of the F-channel driver.

Implementation of the preprocessing in nested CFC charts in the project

For purposes of the preprocessing, a separate nested chart "PP_Chart" is created in the nested chart of the matrix logic. In this "PP_Chart", a separate nested chart is created for each preprocessing. You can edit these nested charts, but they must not be moved.

Principle of configuration

The preprocessing of a Cause is generally configured in the following steps.

1. Configuring the function $F(x)$

Open the corresponding template for preprocessing charts in the "Templates" folder:

- "F_SM_PP_B"
Template for preprocessing chart for binary input values
- "F_SM_PP_R"
Template for preprocessing chart for analog input values
- For your specific preprocessing, create a copy of this master chart in the "Templates" folder of the "SafetyMatrix Lib" and assign the desired name. For preprocessing according to the figure above, you need a copy of the master chart "F_SM_PP_R" for analog values.
- Configure the function $F(x)$ in this copy of the master chart with the desired F-blocks, e.g. "F_MUL_R".
- Interconnect the inputs/output of the blocks with the chart connections of the preprocessing chart, for example, "V_IN" and "V_OUT" for preprocessing of an analog value.
The template charts in the "SafetyMatrix Lib" can be copied and used to create different versions of the preprocessing charts. All preprocessing charts must meet the requirements described above.

Note

Backup of preprocessing charts when upgrading the "SafetyMatrix Lib"

Because the preprocessing charts and the copies created are saved in the "Templates" folder of the "SafetyMatrix Lib", you must back up the preprocessing charts used prior to an upgrade of the "SafetyMatrix Lib", for example, in a separate library. You can find additional information on this in section "Installing (Page 28)".

2. Configuring the reversing function $F^{-1}(x)$

If a bypass or simulation value is set at a Cause of the Safety Matrix, the simulation value is to occur not only within the matrix but also be entered into the signal processing of the associated input value by means of the F-channel block.

To do so, the reversing function $F^{-1}(x)$ must convert the simulation value at the "SIM_x" output of the matrix into the value range of the "V" output of the F-channel driver.

- Configure the function $F^{-1}(x)$ in the preprocessing chart with the required F-blocks, e.g. "F_DIV_R".
- Interconnect the inputs/output of the blocks with the chart connections of the preprocessing chart, for example, "SIM_V_IN" and "SIM_V_OUT" for preprocessing of an analog value.

3. Assignment of a preprocessing to the tag of a Cause
 - Open the required matrix in the Safety Matrix Engineering Tool and select the desired Cause or create a new Cause.
 - Double-click on the desired Cause to open the " Cause - Details" dialog box.
 - In the "Configure" tab you use the "..." button of the tag, e.g. "IW234", to open the associated "Channel driver" dialog box.
 - In the "Options" tab, select the desired preprocessing chart in the "Preprocessing" area.
4. Transferring the Safety Matrix to CFC charts and updating the preprocessing charts

After configuration, preprocessing and assignment to a Cause, the Safety Matrix must still be implemented in the CFC charts in the program folder with the "Transfer" function. The preprocessing charts from the "Templates" folder of the "SafetyMatrix Lib" are copied to the project with this transfer.

 - During transfer of the Safety Matrix, select the "Update preprocessing" option in the "Transfer options" area of the "Transfer to Project" dialog box.

Note

Transfer after template changes in the "SafetyMatrix Lib"

Manual changes to existing preprocessing charts in the program are overwritten by a transfer with the "Update preprocessing" option.

If you do not want to overwrite the existing preprocessing charts in the project, you must not activate the "Update preprocessing" option, or you must save the preprocessing charts before the transfer, as described in the note above.

You can find additional information on this in section "Transferring the Safety Matrix to the program (Page 130)".

- A new CFC "PP_Chart" is available in the Safety Matrix top chart after the transfer. The "PP_Chart" chart is a nested chart. It contains all preprocessing charts of a matrix. The preprocessing charts start with the prefix "PP_", e.g. "PP_IW234".
5. Compiling and downloading

Finally you have still have to compile and download the program.

6.1.6 The "Degraded Voting" function

Overview

The "Degraded Voting" function allows you to take the individual input tags of a Cause "out of the evaluation" for the Cause in case of a bad signal status ("Bad Quality") or with an active soft bypass for a tag.

Activation of Degraded Voting

- When the "soft bypass" is activated for at least one input tag of a Cause, Degraded Voting is automatically activated for this Cause.
- When the "Degraded Voting" option is activated in the properties of the Cause in case of "Bad Quality", Degraded Voting is activated in case of a bad signal status ("Bad Quality"). You can find additional information on this in section ""Cause details" dialog box - "Options" tab (Page 105)".

Degraded Voting results in a change of the Cause logic. If an input tag is taken out of the evaluation in case of a 2oo3 logic, for example, it will result in a 1oo2 logic. If an additional tag is excluded from the evaluation, it will result in a 1oo1 logic.

You can find additional information on this in section "Resulting cause logic for Degraded Voting (Page 231)".

Representation in the Safety Matrix

If Degraded Voting is active in a Cause, this fact is displayed in the "Function" column of the associated Cause.

- The configured function type is shown in the table cell at the top as being crossed out.
- The current function type with Degraded Voting, i.e. the resulting Cause logic, is shown below.

Sample display of active Degraded Voting through soft bypass

The figure below shows a Cause with three discrete input tags and active Degraded Voting through a soft bypass of the input tag "TSD_100_a".

Groups	Input Tag	Values	Function	Limit / Trip	Unit	Name	Description	SIL	No.
FO 1	TS_100_a	TRUE		FALSE		Tank_100	Tank 100 High Temperature Switch	3	11
	TS_100_b	TRUE	2oo3	FALSE					
	TS_100_c	TRUE	1oo2	FALSE					

Meaning:

- A soft bypass is set at the input tag "TSD_100_a", indicated by the background highlighted in color. This soft bypass automatically activates Degraded Voting for this Cause.
- The active Degraded Voting is shown in the "Function" column. Configured function type is "2oo3" (can be identified by the crossed out characters); currently active function type is "1oo2".
- The color in the column "No." for the Cause 11 shows the status "Attention Required" because Degraded Voting is active through the soft bypass set at the "TSD_100_a" tag.

Sample display of active Degraded Voting through Bad Quality

The figure below shows a Cause with three discrete input tags and active Degraded Voting through "Bad Quality" of the input tag "TSD_100_a".

Groups	Input Tag	Values	Function	Limit / Trip	Unit	Name	Description	SIL	No.
FO 1	TS_100_a	FALSE	2oo3	FALSE		Tank_100	Tank 100 High Temperature Switch	3	11
	TS_100_b	TRUE	1oo2	FALSE					
	TS_100_c	TRUE		FALSE					

Meaning:

- The input tag "TSD_100_a" has a poor signal status ("Bad Quality"), indicated by the background highlighted in color. This signal status automatically activates Degraded Voting for this Cause.
- The active Degraded Voting is shown in the "Function" column. Configured function type is "2oo3" (can be identified by the crossed out characters); currently active function type is "1oo2".
- The color in the column "No." for the Cause 11 shows the status "Attention Required" because Degraded Voting is active for this Cause.

Degraded Voting using the function type "2oo3" as an example

The table below shows the resulting Cause logic for a Cause with three input tags and the function type "2oo3".

The following option is configured at the Cause in the ""Bad Quality" Voting" area:

- Degraded Voting at "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	2oo3	Inactive
2	Not tripped	Not tripped	Tripped	2oo3	Inactive
3	Not tripped	Not tripped	Bad Quality	1oo2	Inactive
4	Not tripped	Not tripped	Bypass	1oo2	Inactive
5	Not tripped	Tripped	Tripped	2oo3	Active
6	Not tripped	Tripped	Bad Quality	1oo2	Active
7	Not tripped	Tripped	Bypass	1oo2	Active
8	Not tripped	Bad Quality	Bad Quality	1oo1	Inactive
9	Not tripped	Bad Quality	Bypass	1oo1	Inactive
10	Not tripped	Bypass	Bypass	1oo1	Inactive
11	Tripped	Tripped	Tripped	2oo3	Active
12	Tripped	Tripped	Bad Quality	1oo2	Active
13	Tripped	Tripped	Bypass	1oo2	Active
14	Tripped	Bad Quality	Bad Quality	1oo1	Active
15	Tripped	Bad Quality	Bypass	1oo1	Active
16	Tripped	Bypass	Bypass	1oo1	Active
17	Bad Quality	Bad Quality	Bad Quality	(1oo1)	Active

Cause	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
18	Bad Quality	Bad Quality	Bypass	(1001)	Active
19	Bad Quality	Bypass	Bypass	(1001)	Active
20	Bypass	Bypass	Bypass	Bypass	Inactive

6.1.7 Group deactivation of maintenance operations

Introduction

All active maintenance operations for Causes/Effects of a Safety Matrix, such as simulations, soft bypasses and override functions, can be deactivated with one external signal, for example, if visualization is not available (anymore).


To achieve this the following inputs are available in the interface of the nested matrix logic chart:

- SET_GDM
- EN_GDM

The group deactivation takes place over a key-operated switch.

Overview

- Hardware and configuration:
If the enable group deactivation is to take place over a keyswitch, for example, this keyswitch is connected to an input of an F-DI module and the associated output signal of the F-channel driver is connected to the EN_GDM input of the matrix logic nested chart "@MatrixName".
- Function of the inputs:
 - EN_GDM
F_BOOL data type
Enable for the group deactivation function
The EN_GDM input must be TRUE for the group deactivation to take place over the SET_GDM input.
The active status of the input is displayed by a message in the engineering tool and the Safety Matrix Viewer.
 - SET_GDM
F_BOOL data type
In case of a rising edge at this input, all active simulations, soft bypasses and override functions are deactivated for Causes/Effects of a Safety Matrix.

 WARNING
<p>Additional safety measures for group deactivation of maintenance operations</p> <p>The group deactivation of maintenance operations requires additional safety measures:</p> <ul style="list-style-type: none"> • Ensure that the deactivation can only take place when the safety of the plant is not compromised. • You must use the provided EN_GDM input for enabling the group deactivation by controlling it, for example, with a key-operated switch or with the safety program, depending on the process. • Make sure that the enabling of group deactivation is valid only for the desired period. • Make sure that the following steps for group deactivation cannot be executed in a single operation. <ol style="list-style-type: none"> 1. Enabling the group deactivation (EN_GDM=1), 2. Execution of the group deactivation (SET_GDM=1) 3. Reset of enabling the group deactivation (EN_GDM=0) • Please ensure that only authorized personnel can execute the group deactivation. <p>(SMW-022)</p>

6.1.8 F-channel drivers

Integrating F-channel drivers into the Safety Matrix

The Safety Matrix offers various options for integrating F-channel drivers into the Safety Matrix. The following table presents an overview of the methods you can use to achieve this.

Channel driver type	Integration
F_CH_AI F_CH_DI F_CH_DO	<p>The F-channel drivers are:</p> <ul style="list-style-type: none"> • Positioned and interconnected in the nested chart of the F-channel drivers upon transfer • placed in advance (external) and interconnected during transfer
F_CH_BI F_CH_BO	<p>The F-channel drivers are:</p> <ul style="list-style-type: none"> • placed in advance (external) and interconnected during transfer
F_CH...* F_PA... F-typicals	<p>The F-channel drivers are:</p> <ul style="list-style-type: none"> • Positioned in advance and integrated using the "customer-specific" option.

*) but not the explicitly named F_CH_AI, F_CH_DI/DO, F_CH_BI/BO

Customer-specific F-channel drivers

An F-block is identified as a customer-specific F-channel driver when it has been introduced into the safety program and one of the following criteria is met:

- This is an F-block of S7 F Systems of the type
 - F_CH... (but not F_CH_AI, F_CH_DI/DO, F_CH_BI/BO)
 - F_PA...
- It is an F-block type or F-block with the following properties:
 - It has an interface as follows:
 - Input parameter for turning on the simulation: SIM_ON
 - Input parameter for specifying the simulation value:
SIM_I for discrete tags / SIM_V for analog tags
 - Output parameter channel status CH_STAT:
generate by means of F_FBO_SM, see below
 - Parameter for signal output or input:
Q for discrete tags / V or I for analog tags
 - Optional: Parameter ACK_REQ and ACK_REI for acknowledgment
 - The F-block type contains the F-block F_FBO_SM.

Note

If the parameter SIM_V of your customer-specific F-channel driver does not have the data type REAL, it will be marked as "Used externally" (prefix "@") after the transfer. If you still want to simulate this F-channel driver, you can create an F-block type that contains the corresponding data conversion, and integrate it into the Safety Matrix.

F-block F_FBO_SM

You can use the F-Block F_FBO_SM to create the output parameter Channel Status CH_STAT for the Safety Matrix. This output is required to integrate an F-block type as a customer-specific F-channel driver.

When creating the block typical, pay attention to the position of the F_FBO_SM in the run sequence. This block must not be at the top position.

The following information can be provided to the Safety Matrix by means of the channel status:

- QBAD of the F-channel driver
- QSIM of the F-channel driver
- PASS_OUT of the F-channel driver
- PROFIsafe failure of the F-module driver

Connections of the F-block F_FBO_SM

	Name	Data type	Description	Default
Inputs:	QBAD	F_BOOL	1 = Process data invalid	FALSE
	QSIM	F_BOOL	1 = Simulation active	FALSE
	PASS_OUT	F_BOOL	1 = Passivation because of error	FALSE
	PS_ERR	F_BOOL	1 = PROFIsafe communication error	FALSE
Outputs:	CH_STAT	F_WORD	Channel status of Safety Matrix	W#16#0

6.1.9 Configuration of the F-channel driver acknowledgment

Overview

For the tags of Causes and Effects, you can use the "Driver acknowledgment" option of the "Channel driver" dialog box to configure whether an acknowledgment is required for reintegrating the channel.

The "Channel driver" dialog box can be opened in the details of the Cause/Effect with the "..." button in the "Configuration" tab if an F-channel driver is configured through the "I/O" button.

Settings:

- The "Acknowledgment required" option is set by default and the input at the channel driver is ACK_NEC = 1 after the transfer.
- The parameter assignment of the input ACK_NEC = 0 is only permitted when an automatic reintegration is acceptable for the process from a safety point of view after an F-channel fault.

Note

See the warnings and notes on the topic "Reintegration after error elimination" in the *"S7 F/FH Systems, Configuring and Programming"* Programming and Operating Manual.

Comments:

- F-channel driver settings for bulk data engineering:
F-channel driver settings can be configured for bulk data engineering in the respective columns for Causes and Effects.
If a symbol is used multiple times but different settings are configured, the last setting is adopted for all points of use.
- Migration:
If a CEM file is opened with a matrix of an older version, the "Acknowledgement required" option is set, which means ACK_NEC is set to "1" during the next transfer.

- Please note that the acknowledgment behavior of the F-channel drivers can change when migrating matrices from older versions.
- Comparison and reports:
The F-channel driver configuration is not displayed in the Safety Matrix comparison and is not included in the configuration report.

6.1.10 Message configuration

6.1.10.1 Overview for configuring messages

Message configuration for Safety Matrix and for individual Causes and Effects

You can configure messages for the entire Safety Matrix as well as messages for individual Causes and Effects. Depending on the configuration, the following message blocks are positioned during the transfer:

- A message block F_MA_AL for the Safety Matrix.
- One message block F_SC_AL or F_SC_AL2 for each Cause.
- One message block F_SE_AL for each effect.

There are different alarm profiles for:

- Messages of individual Causes.
There are three pre-defined alarm profiles for Causes: "Standard", "Sequential", "Energized".
- Messages of individual effects.
There are two pre-defined alarm profiles for effects: "Standard", "Sequential".
- Messages of the Safety Matrix
- Group messages (linking of statuses of all message blocks of Causes and Effects)

You can configure these alarm profiles as follows:

- Lock individual messages
- Change message classes
- Change priorities of message classes
- Specify the acknowledgment request

Connections of message blocks

Additional information for further processing is available at the message blocks in the CFC. You can also configure functions such as "Locking alarms during startup" in the CFC. See the following sections for more on this:

- Safety Matrix message block F_MA_AL (Page 68)
- Cause message block F_SC_AL (Page 69)
- Cause message block F_SC_AL2 (Page 75)
- Effect message block F_SE_AL (Page 81)

Syntax rules for message configuration

If messages are configured for Causes and Effects, the respective Cause/Effect name is integrated in the message text. Which is why you should observe the syntax rules.

You can find additional information about syntax rules for the Cause/Effect name in the following sections:

- "Cause details" dialog - "Configure" tab (Page 102)
- "Effect details" dialog - "Configure" tab (Page 111)

If the rules are not observed, the errors are listed in the report window in the "Transfer" tab and the message configuration is not implemented.

See also

Messages of the matrix message blocks (Page 186)

6.1.10.2 Safety Matrix message block F_MA_AL

Additional information for further processing

Additional information for further processing is available at the Safety Matrix message block F_MA_AL in the CFC. You can also configure functions such as "Locking alarms during startup" in the CFC.

Connections of Safety Matrix message block F_MA_AL

	Name	Data type	Description
Inputs	M_Name	String[16]	Safety Matrix name
	MSG_LOCK	BOOL	1= Disable all alarms

	Name	Data type	Description
Outputs	ACK_REQ	BOOL	Request for acknowledging F-channel drivers
	SM_CHG	BOOL	Change in the matrix signature or version (information available for one cycle only)
	MatrixSIG	DWORD	Matrix signature
	MtxVersion	STRING [20]	Permanently set version of the Safety Matrix library
	MajorRev	INT	Major revision of configured matrix
	MinorRev	INT	Minor revision of configured matrix
	Any_CA	BOOL	1= A Cause in the matrix is active 0= No Cause is active
	Any_EA	BOOL	1= An Effect in the matrix is active 0= No Effect is active
	Any_CB	BOOL	1= A Cause of the Matrix is bypassed (bypass) 0 = No Cause is bypassed
	Any_EB	BOOL	1= An effect of the Matrix is bypassed (bypass) 0 = No effect is bypassed
	Any_CW	BOOL	1= A Cause prewarning is active 0 = No Cause prewarning is active
	Any_EW	BOOL	1= An effect prewarning is active 0= No effect prewarning is active
	CAct_Num	INT	Number of active Causes
	EAct_Num	INT	Number of active effects
	CByP_Num	INT	Number of Causes bypassed
	EByP_Num	INT	Number of effects bypassed
	Msec	DINT	Current matrix runtime; includes the runtime of all matrix blocks and F-channel drivers
	MaxMsec	DINT	Previous maximum matrix runtime; includes the highest runtime of all matrix blocks and F-channel drivers
	Any_MAINT	BOOL	1= A maintenance function for a Cause/Effect is active 0= No maintenance function for a Cause/Effect is active
	CWrn_Num	INT	Number of Causes with a prewarning
	EWrn_Num	INT	Number of effects with a prewarning
ANY_SIM	BOOL	Simulation active 1= At least one tag is simulated	
ANY_QBAD	BOOL	Bad Quality active 1= At least one tag has a bad signal state "Bad Quality"	

6.1.10.3 Cause message block F_SC_AL

Additional information for further processing

Additional information for further processing is available at the Cause message blocks F_SC_AL in the CFC. You can also configure functions such as "Locking alarms during startup" in the CFC.

Connections of Cause message block F_SC_AL

	Name	Data type	Description
Inputs	M_Name	String[16]	Safety Matrix name This string is used for the name of the associated faceplate in the Viewer.
	Number	INT	Cause number
	MSG_LOCK	BOOL	1=Disable all alarms

	Name	Data type	Description
Outputs	CONFIG_V	DWORD	Cause configuration; see below: Table "CONFIG_V"
	STATE_V	DWORD	Cause status; see below: Table "STATE_V"
	DIAG_V	DWORD	Cause error; see below: Table "DIAG_V"
	P_LIM_V	REAL	Configured prewarning limit for analog values; a prewarning is issued when this value is exceeded
	LIMIT_V	REAL	Configured limit for analog values; the analog tag trips when this value is exceeded
	HYST_V	REAL	Configured hysteresis for tripping the analog tag or canceling the tripping
	DELTA_V	REAL	Configured discrepancy permitted between the values of the analog tags
	DELAY_V	DINT	Value configured for the time delay for tripping of Causes, in ms
	TAG1_R	REAL	Analog value tag 1 that is processed in the Safety Matrix
	TAG2_R	REAL	Analog value tag 2 that is processed in the Safety Matrix
	TAG3_R	REAL	Analog value tag 3 that is processed in the Safety Matrix
	VMOD1_R	REAL	Analog value read in over the module for tag 1
	VMOD2_R	REAL	Analog value read in over the module for tag 2
	VMOD3_R	REAL	Analog value read in over the module for tag 3
	TAG1_B	BOOL	Discrete value tag 1 that is processed in the Safety Matrix
	TAG2_B	BOOL	Discrete value tag 2 that is processed in the Safety Matrix
	TAG3_B	BOOL	Discrete value tag 3 that is processed in the Safety Matrix
	VMOD1_B	BOOL	Value read in over the module for tag 1
	VMOD2_B	BOOL	Value read in over the module for tag 2
	VMOD3_B	BOOL	Value read in over the module for tag 3
	TAG_TYPE	BOOL	Configuration tag: 1= analog tag 0= discrete tag
	ACK_REQ	BOOL	1= Acknowledgment request
	FIRSTOUT	BOOL	First Out alarm; 1= If the Cause is the first Cause in its FO group to be tripped
	ACTIVE	BOOL	1= Cause has tripped 0= Cause has not tripped
	ANY_BYP	BOOL	Bypass active; 1= If one of the following bypasses is active: (Hard) bypass, Soft bypass, Tag inhibit
	PRE_AL	BOOL	Prewarning active; 1= If an analog tag of the Cause has exceeded the configured prewarning limit (P_LIM_V) or 1 = If a prewarning is active for a timed soft bypass
	ANY_DIAG	BOOL	1= If diagnostic messages exist (DIAG_V not 0)
	CH_STAT1	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 1); see below: Table "CH_STATx"
	CH_STAT2	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 2); see below: Table "CH_STATx"
	CH_STAT3	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 3); see below: Table "CH_STATx"
ELAP_TM	DINT	Time elapsed for time delay (DELAY_V), in ms	

6.1 Overview of Configuring

	Name	Data type	Description
	ANY_SIM	BOOL	Simulation active 1= At least one tag is simulated
	ANY_QBAD	BOOL	Bad Quality active 1= At least one tag has a bad signal state "Bad Quality"

CONFIG_V

The information in output parameter CONFIG_V of Cause message block F_SC_AL is stored as follows:

Bit No.	Assignment
Bit 0	Trip on "Bad Quality"
Bit 1	-
Bit 2	Soft bypass allowed
Bit 3	Auto acknowledge active Cause
Bits 4 to 6	Function type: 1: Normal 2: 2oo3 3: AND 4: OR 6: Comment only
Bit 7	Alarm on input trip
Bit 8	0= Tripping with tag 1 = FALSE 1= Tripping with tag 1 = TRUE
Bit 9	0= Tripping with tag 2 = FALSE 1= Tripping with tag 2 = TRUE
Bit 10	0= Tripping with tag 3 = FALSE 1= Tripping with tag 3 = TRUE
Bit 11	-
Bit 12	Limit type: 0= low 1= high
Bit 13	-
Bit 14	Mutually locked maintenance operations
Bit 15	Cause used
Bits 16 -17	Input type: 1= discrete 2= analog
Bits 18 - 20	Number of inputs: 1= 1 input 2= 2 inputs 3= 3 inputs
Bits 21 - 22	Time: 0= No time manipulation 1= ON delay 2= OFF delay 3= Timed Cause

Bit No.	Assignment
Bit 23	-
Bits 24 - 27	First Out Alarm Group
Bit 28	Tag 1: External input
Bit 29	Tag 2: External input
Bit 30	Tag 3: External input
Bit 31	-

STATE_V

The information in output parameter STATE_V of Cause message block F_SC_AL is stored as follows:

Bit No.	Assignment
Bit 0	Bypass active (bypass tag or soft bypass)
Bit 1	Soft bypass active
Bit 2	Acknowledged
Bit 3	Result of logic operation of tag = 1
Bit 4	Tripping tag 1
Bit 5	Tripping tag 2
Bit 6	Tripping tag 3
Bit 7	-
Bit 8	Cause active
Bit 9	Time manipulation active
Bit 10	Inhibit tag active
Bit 11	Hysteresis active
Bit 12	Tag 1: Simulation
Bit 13	Tag 2: Simulation
Bit 14	Tag 3: Simulation
Bit 15	-
Bit 16	-
Bit 17	-
Bit 18	-
Bit 19	-
Bit 20	Positive edge on bit 8
Bit 21	-
Bit 22	-
Bit 23	Cause used
Bit 24	-
Bit 25	-
Bit 26	-
Bit 27	-
Bit 28	Value tag 1 that is processed in the Safety Matrix
Bit 29	Value tag 2 that is processed in the Safety Matrix

Bit No.	Assignment
Bit 30	Value tag 3 that is processed in the Safety Matrix
Bit 31	-

DIAG_V

The information in output parameter DIAG_V of Cause message block F_SC_AL is stored as follows:

Bit No.	Assignment
Bit 0	-
Bit 1	-
Bit 2	-
Bit 3	-
Bit 4	-
Bit 5	-
Bit 6	-
Bit 7	-
Bit 8	PROFIsafe error module tag 1
Bit 9	PROFIsafe error module tag 2
Bit 10	PROFIsafe error module tag 3
Bit 11	-
Bit 12	Prewarning tag 1
Bit 13	Prewarning tag 2
Bit 14	Prewarning tag 3
Bit 15	-
Bit 16	Incorrect configuration
Bit 17	SDF error (error in safety data format)
Bit 18	Configuration changed
Bit 19	-
Bit 20	Channel fault tag 1
Bit 21	Channel fault tag 2
Bit 22	Channel fault tag 3
Bit 23	-
Bit 24	Bad Quality tag 1
Bit 25	Bad Quality tag 2
Bit 26	Bad Quality tag 3
Bit 27	-
Bit 28	Delta Alarm tag 1 and 2
Bit 29	Delta Alarm tag 2 and 3
Bit 30	Delta Alarm tag 3 and 1
Bit 31	Tripping of a tag

CH_STATx

The information in output parameters CH_STAT1 to 3 of Cause message block F_SC_AL is stored as follows:

Bit No.	Assignment
Bit 0	QBAD
Bit 1	QSIM (inactive)
Bit 2	PASS_OUT (error)
Bit 3	ACK_REQ
Bit 4	PASS_ON
Bit 5	Redundant module present
Bit 6	PROFIsafe error
Bit 7	PROFIsafe module failure on redundant module
Bit 8	QCHF_LL (only analog tag)
Bit 9	QCHF_HL (only analog tag)
Bit 10	QSUBS
Bit 11	-
Bit 12	-
Bit 13	-
Bit 14	-
Bit 15	-

Additional information can be found in the description of the corresponding F-channel driver.

6.1.10.4 Cause message block F_SC_AL2

Additional information for further processing

Additional information for further processing is available at the Cause message blocks F_SC_AL2 in the CFC. You can also configure functions such as "Locking alarms during startup" in the CFC.

The Cause message block F_SC_AL2 is used by the engineering tool when the following functions are used:

- Degraded Voting
- Soft bypass for a tag
- Timed soft bypass for a Cause

If these functions are used, an F_SC_AL2 is placed in the CFC charts during the transfer instead of the existing F_SC_AL block.

If the new functionality, e.g. timed soft bypass, is no longer used for a Cause, the placed F_SC_AL2 block is retained and not replaced with a F_SC_AL block.

Connections of the Cause message block F_SC_AL2

	Name	Data type	Description
Inputs	M_Name	String[16]	Safety Matrix name This string is used for the name of the associated faceplate in the Viewer.
	Number	INT	Cause number
	MSG_LOCK	BOOL	1=Disable all alarms

	Name	Data type	Description
Outputs	CONFIG_V	DWORD	Cause configuration; see below: Table "CONFIG_V"
	STATE_V	DWORD	Cause status; see below: Table "STATE_V"
	DIAG_V	DWORD	Cause error; see below: Table "DIAG_V"
	P_LIM_V	REAL	Configured prewarning limit for analog values; a prewarning is issued when this value is exceeded
	LIMIT_V	REAL	Configured limit for analog values; the analog tag trips when this value is exceeded
	HYST_V	REAL	Configured hysteresis for tripping the analog tag or canceling the tripping
	DELTA_V	REAL	Configured discrepancy permitted between the values of the analog tags
	DELAY_V	DINT	Value configured for the time delay for tripping of Causes, in ms
	TAG1_R	REAL	Analog value TAG1 to be processed in the Safety Matrix
	TAG2_R	REAL	Analog value TAG2 to be processed in the Safety Matrix
	TAG3_R	REAL	Analog value TAG3 to be processed in the Safety Matrix
	VMOD1_R	REAL	Analog value read in over the module for tag 1
	VMOD2_R	REAL	Analog value read in over the module for tag 2
	VMOD3_R	REAL	Analog value read in over the module for tag 3
	TAG1_B	BOOL	Discrete value TAG1 to be processed in the Safety Matrix
	TAG2_B	BOOL	Discrete value TAG2 to be processed in the Safety Matrix
	TAG3_B	BOOL	Discrete value TAG3 to be processed in the Safety Matrix
	VMOD1_B	BOOL	Value read in over the module for tag 1
	VMOD2_B	BOOL	Value read in over the module for tag 2
	VMOD3_B	BOOL	Value read in over the module for tag 3
	TAG_TYPE	BOOL	Configuration tag: 1= analog tag 0= discrete tag
	ACK_REQ	BOOL	1= Acknowledgment request
	FIRSTOUT	BOOL	First Out alarm; 1= If the Cause is the first triggered Cause of its FO group
	ACTIVE	BOOL	1= Cause has tripped 0= Cause has not tripped
	ANY_BYP	BOOL	Bypass active; 1= If one of the following bypasses is active: (Hard) bypass, Soft bypass, Tag inhibit
	PRE_AL	BOOL	Prewarning active; 1= If an analog tag of the Cause has exceeded the configured prewarning limit (P_LIM_V) or 1 = If a prewarning is active for a timed soft bypass
	ANY_DIAG	BOOL	1= If diagnostic messages exist (DIAG_V not 0)
	CH_STAT1	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 1); see below: Table "CH_STATx"
	CH_STAT2	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 2); see below: Table "CH_STATx"
	CH_STAT3	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 3); see below: Table "CH_STATx"

6.1 Overview of Configuring

Name	Data type	Description
ELAP_TM	DINT	Time elapsed for time delay (DELAY_V), in ms
BYP_ELAP_TM	DINT	Elapsed time of the timed bypass in ms
BYPTM_W	DINT	Prewarning bypass time in ms
BYPTM_V	DINT	Bypass time in ms
ANY_SIM	BOOL	Simulation active 1= At least one tag is simulated
ANY_QBAD	BOOL	Bad Quality active 1= At least one tag has a bad signal state "Bad Quality"

CONFIG_V

The information in the CONFIG_V output parameter of the Cause message block F_SC_AL2 is stored as follows:

Bit No.	Assignment
Bit 0	Trip on "Bad Quality"
Bit 1	Timed soft bypass is allowed
Bit 2	Soft bypass allowed
Bit 3	Auto acknowledge active Cause
Bits 4 to 6	Function type: 1: Normal 2: 2oo3 3: AND 4: OR 6: Comment only
Bit 7	Alarm on input trip
Bit 8	0= Tripping with tag 1 = FALSE (DTT) 1= Tripping with tag 1 = TRUE (ETT)
Bit 9	0= Tripping with tag 2 = FALSE (DTT) 1= Tripping with tag 2 = TRUE (ETT)
Bit 10	0= Tripping with tag 3 = FALSE (DTT) 1= Tripping with tag 3 = TRUE (ETT)
Bit 11	Tag 2 soft bypass allowed
Bit 12	Limit type: 0= Low 1= High
Bit 13	Tag 3 soft bypass allowed
Bit 14	Mutually locked maintenance operations
Bit 15	Cause used
Bits 16 -17	Input type: 1= Discrete 2= Analog
Bits 18 - 20	Number of inputs: 1= 1 input 2= 2 inputs 3= 3 inputs

Bit No.	Assignment
Bits 21 - 22	Time: 0= No time manipulation 1= ON delay 2= OFF delay 3= Timed Cause
Bit 23	Degraded Voting active
Bits 24 - 27	First Out Alarm Group
Bit 28	Tag 1: External input
Bit 29	Tag 2: External input
Bit 30	Tag 3: External input
Bit 31	Tag 1: Soft bypass allowed

STATE_V

The information in the STATE_V output parameter of the Cause message block F_SC_AL2 is stored as follows:

Bit No.	Assignment
Bit 0	Bypass active (bypass tag or soft bypass)
Bit 1	Soft bypass active
Bit 2	Acknowledged
Bit 3	Result of logic operation of tag = 1
Bit 4	Tripping tag 1
Bit 5	Tripping tag 2
Bit 6	Tripping tag 3
Bit 7	Timed soft bypass active
Bit 8	Cause active
Bit 9	Time manipulation active
Bit 10	Inhibit tag active
Bit 11	Hysteresis active
Bit 12	Tag 1: Simulation
Bit 13	Tag 2: Simulation
Bit 14	Tag 3: Simulation
Bit 15	-
Bit 16	-
Bit 17	-
Bit 18	-
Bit 19	-
Bit 20	Positive edge on bit 8
Bit 21	-
Bit 22	Degraded Voting active
Bit 23	Cause used
Bit 24	Tag 1: Soft bypass active
Bit 25	Tag 2: Soft bypass active

6.1 Overview of Configuring

Bit No.	Assignment
Bit 26	Tag 3: Soft bypass active
Bit 27	-
Bit 28	Value tag 1 that is processed in the Safety Matrix
Bit 29	Value tag 2 that is processed in the Safety Matrix
Bit 30	Value tag 3 that is processed in the Safety Matrix
Bit 31	-

DIAG_V

The information in the DIAG_V output parameter of the Cause message block F_SC_AL2 is stored as follows:

Bit No.	Assignment
Bit 0	-
Bit 1	-
Bit 2	-
Bit 3	-
Bit 4	-
Bit 5	-
Bit 6	-
Bit 7	-
Bit 8	PROFIsafe error module tag 1
Bit 9	PROFIsafe error module tag 2
Bit 10	PROFIsafe error module tag 3
Bit 11	-
Bit 12	Prewarning tag 1
Bit 13	Prewarning tag 2
Bit 14	Prewarning tag 3
Bit 15	-
Bit 16	Incorrect configuration
Bit 17	SDF error (error in safety data format)
Bit 18	Configuration changed
Bit 19	Timed soft bypass stopped via timeout
Bit 20	Channel fault tag 1
Bit 21	Channel fault tag 2
Bit 22	Channel fault tag 3
Bit 23	-
Bit 24	"Bad Quality" tag 1
Bit 25	"Bad Quality" tag 2
Bit 26	"Bad Quality" tag 3
Bit 27	-
Bit 28	Delta Alarm tag 1 and 2
Bit 29	Delta Alarm tag 2 and 3

Bit No.	Assignment
Bit 30	Delta Alarm tag 3 and 1
Bit 31	Tripping of a tag

CH_STATx

The information in the CH_STAT1 to 3 output parameters of the Cause message block F_SC_AL2 is stored as follows:

Bit No.	Assignment
Bit 0	QBAD
Bit 1	QSIM (inactive)
Bit 2	PASS_OUT (error)
Bit 3	ACK_REQ
Bit 4	PASS_ON
Bit 5	Redundant module present
Bit 6	PROFIsafe error
Bit 7	PROFIsafe module failure on redundant module
Bit 8	QCHF_LL (only analog tag)
Bit 9	QCHF_HL (only analog tag)
Bit 10	QSUBS
Bit 11	-
Bit 12	-
Bit 13	-
Bit 14	-
Bit 15	-

Additional information can be found in the description of the corresponding F-channel driver.

6.1.10.5 Effect message block F_SE_AL

Additional information for further processing

Additional information for further processing is available at the effect message blocks F_SE_AL in the CFC. You can also configure functions such as "Locking alarms during startup" in the CFC.

Connections of effect message block F_SE_AL

	Name	Data type	Description
Inputs	M_Name	String[16]	Safety Matrix name This string is used for the name of the associated faceplate in the Viewer.
	Number	INT	Effect number
	MSG_LOCK	BOOL	1= Disable all alarms

	Name	Data type	Description
Outputs	CONFIG_V	DWORD	Effect configuration; see below: Table "CONFIG_V"
	STATE_V	DWORD	Effect status; see below: Table "STATE_V"
	DIAG_V	DWORD	Effect error; see below: Table "DIAG_V"
	OVERTM_W	DINT	Configured warning time for override timeout prewarning, in ms; a warning is output when this value is exceeded
	OVERTM_V	DINT	Configured value for the maximum override time, in ms
	DELAY_V	DINT	Configured value for the time manipulation for effect activation, in ms
	TAG1_B	BOOL	Value tag 1 that is formed in the Safety Matrix
	TAG2_B	BOOL	Value tag 2 that is formed in the Safety Matrix
	TAG3_B	BOOL	Value tag 3 that is formed in the Safety Matrix
	TAG4_B	BOOL	Value tag 4 that is formed in the Safety Matrix
	ACK_REQ	BOOL	1= Acknowledgment request for override error
	ACTIVE	BOOL	1= Effect is activated 0= Effect is not activated
	ANY_BYP	BOOL	1= If one of the following bypasses is active: (hard) bypass, soft bypass of a tag
	OK_RESET	BOOL	1= Acknowledgment request for "Reset effect"
	OVER_AL	BOOL	1= If the configured warning time for override timeout (OVERTM_W) is exceeded
	ANY_DIAG	BOOL	1= If diagnostic messages exist (DIAG_V not 0)
	CH_STAT1	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 1); see below: Table "CH_STATx"
	CH_STAT2	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 2); see below: Table "CH_STATx"
	CH_STAT3	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 3); see below: Table "CH_STATx"
	CH_STAT4	WORD	If the tag is connected to an F-channel driver, the channel status is displayed here (tag 4); see below: Table "CH_STATx"
ELAP_TM	DINT	Elapsed time of DELAY_V or OVERTM_V, in ms (dependent on the active function: Bit 9 from output parameter STATE_V = TRUE → DELAY_V; Bit 11 from STATE_V = TRUE → OVERTM_V; see below: Table "STATE_V")	
ANY_SIM	BOOL	Simulation active 1= At least one tag is simulated	
ANY_QBAD	BOOL	Bad Quality active 1= At least one tag has a bad signal state "Bad Quality"	

CONFIG_V

The information in output parameter CONFIG_V of effect message block F_SE_AL is stored as follows:

Bit No.	Assignment
Bit 0	-
Bit 1	Enables "process data pass through"
Bit 2	Soft bypass allowed
Bit 3	-

Bit No.	Assignment
Bits 4 to 6	Function type: 1: Normal 3: Comment only
Bit 7	-
Bit 8	0= With effect active tag 1 = FALSE (DTT) 1= With effect active tag 1 = TRUE (ETT)
Bit 9	0= With effect active tag 2 = FALSE (DTT) 1= With effect active tag 2 = TRUE (ETT)
Bit 10	0= With effect active tag 3 = FALSE (DTT) 1= With effect active tag 3 = TRUE (ETT)
Bit 11	0= With effect active tag 4 = FALSE (DTT) 1= With effect active tag 4 = TRUE (ETT)
Bit 12	-
Bit 13	Output delay
Bit 14	-
Bit 15	0= Deactivate prewarning of override timeout 1= Activate prewarning of override timeout
Bit 16	-
Bit 17	-
Bit 18	-
Bit 19	-
Bit 20	-
Bit 21	-
Bit 22	Mutually locked maintenance operations
Bit 23	Effect used
Bit 24	-
Bit 25	-
Bit 26	-
Bit 27	-
Bit 28	Tag 1: External output
Bit 29	Tag 2: External output
Bit 30	Tag 3: External output
Bit 31	Tag 4: External output

STATE_V

The information in output parameter STATE_V of effect message block F_SE_AL is stored as follows:

Bit No.	Assignment
Bit 0	Bypass active (bypass tag or soft bypass)
Bit 1	Soft bypass active
Bit 2	"Process data pass through" active
Bit 3	-

Bit No.	Assignment
Bit 4	Old value reset/override tag
Bit 5	Override permitted
Bit 6	Acknowledgment request for reset
Bit 7	Effect interlocked
Bit 8	Effect active
Bit 9	Time manipulation active
Bit 10	Mask enable tag active
Bit 11	Override active
Bit 12	Tag 1: Simulation
Bit 13	Tag 2: Simulation
Bit 14	Tag 3: Simulation
Bit 15	Tag 4: Simulation
Bit 16	-
Bit 17	-
Bit 18	-
Bit 19	-
Bit 20	-
Bit 21	-
Bit 22	-
Bit 23	Effect used
Bit 24	Effect not stored is requested
Bit 25	Effect stored is requested
Bit 26	Effect overridable is requested
Bit 27	Effect resettable and overridable is requested
Bit 28	Value tag 1 that was formed by the Safety Matrix
Bit 29	Value tag 2 that was formed by the Safety Matrix
Bit 30	Value tag 3 that was formed by the Safety Matrix
Bit 31	Value tag 4 that was formed by the Safety Matrix

DIAG_V

The information in output parameter DIAG_V of effect message block F_SE_AL is stored as follows:

Bit No.	Assignment
Bit 0	-
Bit 1	-
Bit 2	-
Bit 3	-
Bit 4	-
Bit 5	-
Bit 6	-
Bit 7	-

Bit No.	Assignment
Bit 8	PROFIsafe error module tag 1
Bit 9	PROFIsafe error module tag 2
Bit 10	PROFIsafe error module tag 3
Bit 11	PROFIsafe error module tag 4
Bit 12	Override timeout prewarning
Bit 13	-
Bit 14	-
Bit 15	-
Bit 16	-
Bit 17	SDF error (error in safety data format)
Bit 18	-
Bit 19	-
Bit 20	Channel fault tag 1
Bit 21	Channel fault tag 2
Bit 22	Channel fault tag 3
Bit 23	Channel fault tag 4
Bit 24	"Bad Quality" tag 1
Bit 25	"Bad Quality" tag 2
Bit 26	"Bad Quality" tag 3
Bit 27	"Bad Quality" tag 4
Bit 28	Override cancellation due to new tripping
Bit 29	Override cancellation due to timeout
Bit 30	-
Bit 31	-

CH_STATx

The information in output parameters CH_STAT1 to 3 of effect message block F_SE_AL is stored as follows:

Bit No.	Assignment
Bit 0	QBAD
Bit 1	QSIM (inactive)
Bit 2	PASS_OUT (error)
Bit 3	ACK_REQ
Bit 4	PASS_ON
Bit 5	Redundant module present
Bit 6	PROFIsafe error
Bit 7	PROFIsafe module failure on redundant module
Bit 8	QCHF_LL (only analog tag)
Bit 9	QCHF_HL (only analog tag)
Bit 10	QSUBS
Bit 11	-

Bit No.	Assignment
Bit 12	-
Bit 13	-
Bit 14	-
Bit 15	-

Additional information can be found in the description of the corresponding F-channel driver.

6.1.11 OS interface

Requirements for generating block icons

Requirement for generating the block icons for the Safety Matrix is the corresponding configuration of the message blocks and the transfer of the Safety Matrix with the enabled options "Positioning of Cause and Effects" and "Positioning of Safety Matrix":

- On the "Alarms" tab of the "Properties" dialog box for the Safety Matrix (see Chapter ""Properties" dialog box of the Safety Matrix (Page 88)")
- On the "Alarms" tab of the "Cause details" dialog (see Chapter ""Cause details" dialog box - "Alarms" tab (Page 108)")
- On the "Alarms" tab of the "Effect details" dialog (see Chapter ""Effect details" dialog box - "Alarms" tab (Page 116)")
- On the "Options" tab of the "Transfer to project" dialog box (see Chapter "Transferring the Safety Matrix to the project (Page 130)")

User permissions

The user permissions, such as for alarm acknowledgment in the PCS 7 OS, are configured on the "OS permissions" tab of the "Properties" dialog box for the Safety Matrix (see Chapter ""Properties" dialog box for the Safety Matrix (Page 88)").

See also

Opening the Safety Matrix faceplates (Safety Matrix Viewer) (Page 150)

6.1.12 Introducing the new Safety Matrix block icons into the PCS 7 OS

Introducing pictures into an existing Safety Matrix project

To use the new Safety Matrix faceplates in an existing project, you must update the project.

1. To do so, launch **WinCC Explorer** for the OS contained in the Safety Matrix project.
2. Open the **OS Project Editor** and click **OK**. The project is reconfigured and the new block icons are applied.
3. Open the **Global Script C-Editor** and select the **Options > Regenerate headers** menu command.

OS compiling in the respective project

1. To do so, start SIMATIC Manager and navigate to the required OS object.
2. Make sure that the "Derive block icons from the plant hierarchy" option is selected in the "Block icons" tab of the object properties for the relevant picture object. (This is the default setting with PCS 7.)

Note

If user settings for the block icon of a Safety Matrix are to be retained during a subsequent OS compilation of an existing picture, you must clear the "Derive block icons from the plant hierarchy" option for this WinCC picture.

3. Highlight the OS object and select "Compile" in the context menu to compile the OS.
4. Click the "Compile" button in the last dialog of the "Compile OS" wizard.


Result

Once you have performed these steps, your project contains the new Safety Matrix block icons. Repeat these steps for all projects.

6.1.13 Safety Matrix function blocks

Function

The Safety Matrix function blocks are automatically added and interconnected during transfer of the Safety Matrix to the project, which means during generation of an S7 F-Systems program logic based on CFC.

 WARNING
Safety note - Do not change automatically inserted Safety Matrix function blocks
After the transfer, the SIMATIC Safety Matrix function blocks, (F-)system charts and (F-)runtime groups are visible with the identification "@F". You must not delete them or change them (except for expressly described changes).
(SMW-006)

Connections

Undocumented connections are automatically supplied or interconnected during compilation of the S7 program and must not be changed. Online changes to undocumented connections can result in an F-STOP. Remedy manipulations at such connections by compiling the S7 program again.

6.2 Editing the properties of the Safety Matrix

6.2.1 "Properties" dialog box of the Safety Matrix

"Properties" dialog box of the Safety Matrix

Select the **Edit > Properties...** menu command. The "Properties - (Matrix name)" dialog box is opened with the "General" tab displayed.

"General" tab

Title

Enter a title to serve as the Safety Matrix designation.

This title is displayed in the view of the open matrix in the engineering tool / Viewer below the line "SIMATIC Safety Matrix". A maximum of 60 characters is possible.

Project

Enter the name of the project to which the Safety Matrix belongs. A maximum of 60 characters is possible.

Description

Enter a process-related description of the Safety Matrix. This is displayed in the Safety Matrix faceplate. A maximum of 248 characters is possible.

General Notes

Enter general comments for this specific Safety Matrix. A maximum of 248 characters is possible.

User Notes

You can enter up to 32 notes, whereby each note can be up to 64 characters long. These notes can be linked to specific Causes and/or Effects. Each Cause and Effect can be assigned a maximum of four comments in the associated "Options" dialog box.

These comments are displayed under "User notes" in the "Info" tab of Safety Matrix.

Safety Instrumented Function Groups

You can use the safety instrumented function groups (SIF) to divide your application into function groups that you can then monitor and change selectively in the Engineering Tool and Viewer (e.g. "level measurement and shutdown").

To use this function, you must assign the individual Causes and Effects of the safety program to safety instrumented function groups. See section ""Cause details" dialog box - "Options" tab (Page 105)" or ""Effect details" dialog box - "Options" tab (Page 113)".

Up to 64 safety instrumented function groups can be configured. A maximum of 32 characters is possible for the name of a SIF group. The safety instrumented function groups are displayed in the "Info" tab of Safety Matrix.

The following options are available for creating an SIF group:

- "Properties" dialog, "General" tab
- In the properties of a Cause or Effect in the "Options" tab.

Once you have created the safety instrumented function groups and have assigned them in the options to Causes and Effects, you can display individual, multiple or all safety instrumented function groups in the Engineering Tool and Viewer.

The following options are available for this purpose:

- Click the "SIF Filter" drop-down list and select one or multiple safety instrumented function groups you want to display. The Causes and Effects of all other safety instrumented functions groups are hidden. As well as the Causes and Effects that are not assigned to a safety instrumented function group.
- Select the menu command **View > Customize > Layout** and select the "Show groups (Cause/Effect)" check box in the "General" tab. Click "OK" to confirm. The "Groups" column is then shown in the "Causes" and "Effects" tables; it shows the First Out (FO) alarm group and the safety instrumented function groups to which the individual Causes and Effects are assigned.

Safety Matrix cycle time (ms)

Can be used to specify the execution time of the Safety Matrix in the CPU. The desired time (in ms) can be selected from the available settings in the drop-down menu. These cycle times are associated with the configured execution times of OB 30 to OB 38.

"Version" tab

Major Revision

Displays the number of the major revision. The "Next revision" button allows you to create the next major revision. You will be prompted to provide a description for it. A time stamp is automatically added to each major revision.

Minor Revision

Displays the number of the minor revision. The "Next revision" button allows you to create the next minor revision. A time stamp is automatically added to each minor revision. The number of the minor revision is reset to zero when the number of the major revision is incremented. Each time when you apply critical changes (see section ""Track changes" menu command (Page 97) "), the minor version is incremented by one.

File Revision

Displays the revision number and the time stamp of the most recently saved Safety Matrix file.

Safety Matrix Signature

Displays the current signature of the Safety Matrix.

The signature is displayed in the Safety Matrix status bar and is printed out when the Safety Matrix is printed.

"Storage" tab

Safety Matrix File Directory

Specifies the file path under which the Safety Matrix file (*.cem) is saved.

Path to Simatic Project

Indicates the path to the SIMATIC project to which the Safety Matrix belongs.

Logical Path to S7 Program

Indicates the path to the S7 program to which the Safety Matrix belongs in the component view.

Safety Matrix in Plant Hierarchy

Indicates the path to the Safety Matrix in the plant hierarchy. The field only displays content if the Safety Matrix top chart is assigned in the plant hierarchy. Otherwise, this field is empty.

"Statistics" tab

Contains information regarding the usage statistics: Number of Causes, Effects and the intersections.

"Parameter" tab

Secure Write

"#EN_SWC" is shown read-only in the "Enable tag" field. Use this Boolean input of the nested chart of the Safety Matrix to enable and, if necessary, disable the "Secure Write" function for the purpose of making operator inputs either in online mode of the engineering tool, or via the

Safety Matrix Viewer. This takes place by means of a signal that is connected in the CFC prior to compiling (= TRUE).

In the "Time interval" field, specify the time in seconds that the Secure Write transaction uses as the timeout. The maximum value for the time is 32767 seconds.

Note

Secure Write is required for controlling the Safety Matrix with the Safety Matrix Viewer. If Secure Write is not enabled, then it can only be monitored.

Additional information is available in the sections "Secure Write (Page 170)" and "Transferring the Safety Matrix to the program (Page 130)".

"Alarms" tab**"Refresh time" field ("Alarm blocks" area):**

Here you can enter the time in minutes for the cyclic refresh of the following messages: "Bypass", "Inhibit", "Override", "Mask" und "Process data pass-through".

If the message is still pending after this time, it will be reported in a cycle as outgoing first and then as incoming. The default setting for this time is 8 hours. If you assign the time as "0", there is no cyclic refresh.

"Positioning of Cause and Effect" check box:

You must select this check box if you want to enable messages for individual Causes and Effects (message blocks F_SC_AL, F_SC_AL2 and F_SE_AL). This activation is the requirement for the "Alarms" tab to appear in the "Cause details" or "Effect details" dialog boxes by positioning the message block for the respective Cause or Effect and configuring the messages (see section ""Cause details" dialog box - "Alarms" tab (Page 108)" or ""Effect details" dialog box - "Alarms" tab (Page 116)").

"Extend event by symbolic Tag name" check box

By selecting the "Extend event by symbolic Tag name" check box, the message text can be extended by the process tag name.

If the check box is selected here, this setting generally applies to all Causes and Effects but it can be disabled in the properties of individual Causes and Effects.

"Positioning of Safety Matrix" check box:

You must select this check box if you want to enable messages for the Safety Matrix (message block F_MA_AL). Proceed as follows:

- If necessary, assign the message block for the Safety Matrix to a CFC chart in the "Chart assignment" field. Click the associated "..." button to open a browser for this purpose. No new CFC charts can be created and no charts can be renamed in the dialog box.
- Select the "Enable Safety Matrix messages" check box to enable these messages. Click the associated "..." button to open the dialog box for configuring the predefined alarm profile for the Safety Matrix.

The following actions are available in the dialog:

- Lock individual messages
- Change message classes
- Change priorities of message classes
- Specify the acknowledgment request
- Select the "Enable group messages" check box to link states of all message blocks of Causes and Effects. Click the associated "..." button to open the dialog box for configuring the predefined alarm profile for the group messages.

The following actions are possible in the dialog:

- Change priorities of message classes.
- Specify the acknowledgment request.

"Permissions OS" tab

In this tab you configure the user permissions, which means the assignment of the Safety Matrix functions to a permission level in the PCS 7 OS.

The Safety Matrix Viewer makes a distinction between:

- **Monitoring functions** without access protection
Which means without assignment of a permission level
- **Operator control functions** with access protection
Which means a separate permission level can be specified for each operator control function.
- **User roles** with access protection
There are two roles available for this purpose:
 - Initiator permission: the operator may **start** an operation.
 - Confirmer permission: the operator may **confirm** an operation.

See also section "Initiator and confirmer permission (Viewer) (Page 168)".

The following applies to all functions: Permission level 0 means 'no access protection', which means every operator has this permission.

You create the users and their individual permission levels for initiator and confirmer in the PCS 7 OS with the "User Administrator" editor.

Note

After changes in the "OS Permissions" tab you must compile and load the OS. No transfer of the Safety Matrix is required.

The following table provides an overview of the monitoring and operator control functions and their default permission levels in the Safety Matrix.

Function	Description	Permission level
Monitoring functions		
(only listed for overview here; are not displayed in dialog box.)		
View Event log		-
View Cause tags		-
View Effect tags		-
View Cause status		-
View Effect status		-
Operator roles		
Initiator	Permission level for initiator	0*
Confirmer	Permission level for confirmer	0*
Operator control functions		
Cause Acknowledge	Permission level for acknowledging a Cause	5
Cause Bypass	Permission level for Cause bypass	5
Cause Tag bypass	Permission level for Cause tag bypass	5
Cause Tag simulation on/off	Permission level for Cause tag simulation	5
Cause Tag simulation value	Permission level for specifying Cause tag simulation value	5
Cause First-Out Alarm Clear	Permission level for acknowledging Cause First Out	5
Cause Group Acknowledge	Permission level for acknowledgment of one or multiple Causes (includes the permission level "Cause Acknowledge")	6
Alarm Clear	Clear permission level for override Effect alarms and timed bypass Cause alarms	5
Effect Override	Permission level for override effect	5
Effect Reset	Permission level for reset effect	5
Effect bypass	Permission level for effect bypass	6
Effect Tag simulation on/off	Permission level for effect tag simulation	6
Effect Tag simulation value	Permission level for specifying effect tag simulation value	6
Effect Group reset	Permission level for resetting one or multiple tripped effects (includes the permission level "Effect Reset")	6
Events Clear	Permission level for clearing events	5
Acknowledge channel driver	Permission level for acknowledging/reintegrating a channel driver	5

*) For the Initiator and Confirmer permission, the permission level 0 is set by default. The 2-operator scenario is activated if different permission levels are entered for initiator and confirmer.

6.2.2 "Customize" dialog boxes

Introduction

The following dialogs are described below:

- "Customize - Layout" dialog box
- "Customize - Colors" dialog box

"Customize - Layout" dialog box

"General" tab

Select the **View > Customize > Layout** menu command. Open the "General" tab.

If you activate the checkboxes available in this tab, the settings made for Causes or Effects are displayed:

- For Causes, in additional columns.
- For effects, in additional rows.

Options in the "Safety Matrix view" area

1. "Highlight Bars and Intersection ToolTip"
When you click an intersection, the corresponding row and column is highlighted in color and a tooltip shows which Cause and Effect are connected to it.
2. "Show action"
Displays the text for an effect that is configured in the "Action" field of the effect configuration.
The text describes which action is triggered when the effect is active (for example, OPEN).
3. "Show description (Cause/Effect)"
Displays the description of the Cause/Effect.

4. "Show options (Cause/Effect)"
Displays the options set for Causes and Effects. The following list explains the abbreviations that may appear in the additionally displayed columns. This list is also displayed under "Cause/Effect options" in the "Legend" tab of Safety Matrix.

Abbreviation	Description
D	Delay configured
I	Inhibit configured
M	Mask configured
B	Soft bypass allowed
Bt	Timed soft bypass configured
Bx	Bypass for tag "x"
H	Hard bypass configured
N	Non-physical I/O tag configured (tag with prefix "#")
P	Process Data Pass Through used
A	Automatic acknowledgment of active Cause configured
T	Timed Cause configured
V	Degraded Voting at "Bad Quality"

5. "Show Notes (Cause/Effect)"
Shows the number(s) of the user notes that are assigned to this Cause or Effect. The comments corresponding to the numbers are displayed in the legend under "User notes".
6. "Show SIL (Cause/Effect)"
Shows the SIL number (Safety Integrity Level) that is assigned to this Cause or Effect.
7. "Show groups (Cause/Effect)"
Displays the First Out groups and/or Safety Instrumented Functional Groups (SIFs) to which this Cause or Effect is assigned. The First Out group is abbreviated as "FO". For example, FO2 indicates that the Cause belongs to First Out group (FO) 2. The numbers of the safety groups appear after the First Out group number. Example: FO3, 5, 17, 44 indicates that this Cause belongs to the First Out group (FO) 3 and the safety instrumented groups 5, 17 and 44.
8. "Show Reset/Override Tag (Effect)"
Shows the reset/override tag that is assigned to the effect.
9. "Show time remaining (Cause/Effect)"
Shows the remaining time of a configured delay in a separate column in the matrix for the Causes/Effects.
10. "Mark live values (Cause/Effect)"
Highlights the dynamic process values from the F-CPU. These are represented in blue font on the user interface to contrast them with the assigned values. The colors can be changed in the "Customize - Colors" dialog box.

Options in the "Dialogs view" area

1. "Show I/O Physical Address (View Tags)"
Shows the physical I/O address together with the icon in the "View tags - Cause x" and "View tags - Effect x" dialog boxes in online mode.

"Size" tab

Select the **View > Customize > Layout** menu command. Open the "Size" tab.

If the Safety Matrix no longer contains any empty rows (for Causes) or columns (for Effects), you can increase the number of rows/columns in this dialog box.

Number of Causes/number of Effects

By default, 16 Causes/Effects are entered here. This number can be increased to max. 128.

Note

When the size of the Safety Matrix is changed in this tab, the Engineering Tool automatically activates the transfer option "Entire Safety Matrix" when the Safety Matrix is transferred. You can find additional information on this in section "Transferring the Safety Matrix to the program (Page 130)".

"Customize - Colors" dialog box

Select the menu command **View > Customize > Colors**.

The status of the Causes, Effects, and intersections whose assignment is indicated in this dialog box are shown with various colored backgrounds in online mode of the Safety Matrix.

You can change the color assigned to a status or alarm profile and the color of the text.

Changes made or differences in offline mode are indicated by red text by default. Dynamic values are displayed in blue text if the checkbox "Mark dynamic values" in the "Customize - Layout" dialog box, "General" tab is activated. You can also change the assigned text colors.

Buttons:

- With the "Export" button, you can save the current color settings in a file. A dialog is opened with the button to select the directory and the file name.
- With the "Import" button, you can import previously saved color settings. A dialog is opened with the button to select the directory and the export file you want to import. You can also import color settings that were saved in other matrices.
- With the "PCS 7" button you can adapt the colors of the Safety Matrix to the PCS 7 color conventions.
- The "Reset" button enables you to restore the default setting of the Safety Matrix.

 WARNING
Assigning colors
The assignment of colors must comply with all relevant application-specific standards and be appropriate for your application.
(SMW-007)

6.2.3 "Track changes" menu command

Handling changes

You can specify how the Safety Matrix handles changes.

Select the **Options > Track changes > Apply changes** menu command. The "Tracked changes - (Matrix name)" dialog box is opened.

Specify which type of changes you want to accept:

- Critical changes - these are process-relevant changes and changes in the safety logic; for example, in the number of rows or columns of the Safety Matrix
- Non-critical changes - these are formal changes, e.g., to user notes or display functions

For support, you can check the changes with the help of the protocol. To do this, click the "Show details" button.

Saving changes

You can specify how changes are being handled in the Safety Matrix during saving.

To do this, select the menu command **Options > Track changes > Accept Changes Automatically with Save**.

6.3 Configuring the causes

6.3.1 Overview of configuring the Causes

Introduction

Analog and discrete values are available as input type. A minimum of one value and a maximum of three values together with the function type represent a Cause.

Discrete input tags

For each discrete input tag of a Cause, you can select:

- Energize-to-trip (ETT = trip on TRUE)
- Deenergize-to-trip (DTT = tripping if FALSE)

In the table below we assume that the setting is always DTT. Thus, the input tag is active if it is FALSE.

You can also check the input tags for signal quality by activating the "Trip on Bad Quality" option at the Cause. As a result, in case of bad signal quality ("Bad Quality"), the Cause will be tripped.

Analog input tags

In the case of analog values, the input tag is activated in accordance with a limit. If this limit is exceeded or fallen below, the Cause becomes active. If multiple analog input tags are used for a Cause, a permitted discrepancy (delta) specified by the user is evaluated. If the values deviate by more than this permitted discrepancy, a discrepancy alarm is tripped.

You can also check the input tags for signal quality by activating the "Trip on Bad Quality" option at the Cause. As a result, in case of bad signal quality ("Bad Quality"), the Cause will be tripped.

Mutual dependencies of the Cause parameters

Input type	Number of inputs	Function type	Limit type High / Low	Cause is tripped, if ...
Discrete*	1	Standard	-	Input tag = FALSE
		Comment only	-	Never
	2	AND	-	both input tags = FALSE
		OR	-	one of the two input tags = FALSE
		Comment only	-	Never
	3	2oo3	-	at least two of three input tags = FALSE
		AND		all three input tags = FALSE
		OR	-	one of three input tags = FALSE
		Comment only	-	Never

Input type	Number of inputs	Function type	Limit type High / Low	Cause is tripped, if ...
Analog	1	Standard	High	...the input tag has exceeded the limit. The Cause will not become inactive again until the input tag has undershot the limit minus hysteresis.
			Low	...the input tag has undershot the limit. The Cause will not become inactive again until the input tag has exceeded the limit plus hysteresis.
		Comment only	-	Never
	2	AND	High	...both input tags have exceeded the limit. The Cause will not become inactive again until the two input tag have undershot the limit minus hysteresis.
			Low	...both input tags have undershot the limit. The Cause will not become inactive again until one of the two input tags has exceeded the limit plus hysteresis.
		OR	High	... one of the two input tags has exceeded the limit. The Cause will not become inactive again until both input tags have undershot the limit minus hysteresis.
			Low	... one of the two input tags has undershot the limit. The Cause will not become inactive again until both input tags have exceeded the limit plus hysteresis.
		Comment only	-	Never
		3	2oo3	High
	Low			...at least two of the three input tags have undershot the limit. The Cause will not become inactive again until at least two input tags have exceeded the limit plus hysteresis.
	AND		High	...all three input tags have exceeded the limit. The Cause will not become inactive again until one of the three input tag has undershot the limit minus hysteresis.
			Low	...all three input tags have undershot the limit. The Cause will not become inactive again until one of the three input tag has exceeded the limit plus hysteresis.
	OR		High	... one of the three input tags has exceeded the limit. The Cause will not become inactive again until all three input tags have undershot the limit minus hysteresis.
			Low	... one of the three input tags has undershot the limit. The Cause will not become inactive again until all three input tags have exceeded the limit plus hysteresis.
	Comment only		-	Never

* when DTT is configured for all tags of the Cause

Data format REAL for input fields

In the Safety Matrix, the data type REAL according to IEEE standard (to Short-Real, 32 bits) is mapped in the text boxes, e.g. "Hysteresis", whereby in self-restraint only the normalized coding of the numbers is used (see table).

This REAL format corresponds to the format used in CFC.

Abbr.	Keyword, type	Value range (normalized) from... to	Examples of entries	Representation in the field
R	REAL; floating-point number	-3.402823e+38... -1.175495e-38... 0.0... 1.175495e-38... 3.402823e+38	22.78; 223.4E7; -3.456e-3; 2.573e19	22.78; 2.234E+09; -0.003456; 2.573E+19

6.3.2 Creating/changing the Cause and row for Cause

Procedure for creating/changing a Cause

Double-click an (empty or configured) row in the Causes configuration area of the Safety Matrix or click the row and select "Edit" in the shortcut menu.

The "Cause details - Cause x" dialog box opens and you can create or change the Cause.

The shortcut menu in the Causes configuration area of the Safety Matrix

When you click on a row in the Causes configuration area of the Safety Matrix, the shortcut menu offers a variety of functions.

The availability of the functions depends on whether the row is empty or filled.

- Copy (copy Cause)
- Cut (cut Cause)
- Paste (insert Cause into the selected row; if the row is filled, you will be queried as to whether you want to overwrite content)
- Edit (the "Cause details - Cause x" dialog box opens)
- Clear content (the Cause, which means the content of the row is deleted but the row is retained as an empty row)
- Insert (an empty row is inserted and all subsequent Causes are moved one row down)
- Delete (an empty row is deleted and all subsequent Causes are moved one row up)
- SIF filter active (sets the SIF filter for the SIF groups of this Cause)

Note

Effects on the comparison

"Insert" or "Delete" of a row causes all subsequent rows to be marked as changed in a subsequent matrix comparison and they must therefore be checked during an acceptance. You can avoid this situation with the following measures:

- Always add additional Causes at the end.
 - Do not cut, paste, copy or delete entire rows but merely their contents.
 - Avoid changing the size of the Safety Matrix.
-

Note**Effects on the transfer**

When the size of the Safety Matrix is changed by "adding" or "deleting" a row, the Engineering Tool automatically activates the transfer option "Entire Safety Matrix" when the Safety Matrix is transferred. You can find additional information on this in section "Transferring the Safety Matrix to the program (Page 130)".

6.3.3 Overview of the "Cause details - Cause x" dialog

Procedure for configuring a Cause

Double-click an (empty or configured) row in the Causes configuration area of the Safety Matrix or click the row and select "Edit" in the shortcut menu.
The "Cause details - Cause x" dialog box opens.

Cause "x"

Each Cause is assigned a unique number within the Safety Matrix. This assignment occurs automatically on the basis of the selected row. The Cause number cannot be changed.

Dialog box for configuring a Cause

The dialog box for configuring a Cause contains the following tabs:

- "Configure"
- "Options"
- "Alarms"
This tab is only displayed when the option "Positioning of Causes and Effects" is activated in the Matrix properties for the alarm blocks.

If you select "Analog" as the input type in the "Configure" tab, then another tab is displayed:

- "Analog parameter"

6.3.4 "Cause details" dialog - "Configure" tab

"Configure" tab

Field	Description
"Name"	<p>Name of the Cause.</p> <p>A maximum of 32 alphanumeric characters and the "_" (underscore) character are possible. The entry is mandatory.</p> <p>If messages are configured for the Cause, the respective Cause name is integrated in the message text. You can find additional information on this in section "Overview for configuring messages (Page 67)".</p>
"Description"	<p>Description of the Cause.</p> <p>A maximum of 80 Unicode characters is possible.</p> <p>Entry of the description is optional.</p>
"SIL"	<p>This field is used for documentation purposes. Here, you can enter the SIL (= Safety Integrity Level) for this Cause, as determined during your risk analysis (e.g., according to IEC 61508).</p> <p>An entry in this field is not required. No SIL value is entered by default.</p>
"Tag x"	<p>Specify at least one tag for each Cause. Please note the section "Syntax rules for tag names in the Safety Matrix (Page 54)".</p> <p>The number of tag fields displayed in the dialog box depends on the number in the field "Number of inputs".</p>
<ul style="list-style-type: none"> "I/O" button 	<p>To open the "Select I/O Tag" dialog box, click the "I/O" button. Please note the section "The Safety Matrix tags (Page 52)".</p>
<ul style="list-style-type: none"> "..." button 	<p>The "..." button is activated if the "Channel driver" option was selected in the "Select I/O Tag" dialog box. Click the "..." button to open the "Channel driver" dialog.</p> <ul style="list-style-type: none"> In the "Parameter" tab, you can configure the following options for F-channel drivers that are selected via symbols: <ul style="list-style-type: none"> "Set initial value" for the simulation "Acknowledgement required" for the F-channel driver after an outgoing channel fault You can find additional information on this in section "Configuration of the F-channel driver acknowledgment (Page 66)". Range limits for the encoders for analog input tags. The upper and lower range limits are displayed and can be entered in the REAL format. You can find additional information on the REAL format in section "Overview of configuring the Causes (Page 97)". In the "Options" tab, you can configure the following options: <ul style="list-style-type: none"> In the "Preprocessing" field select preprocessing for this input tag by selecting a corresponding preprocessing chart or deselect preprocessing. "Monitoring active" activates the monitoring for this tag. Additional information is available in the sections "Syntax rules for tag names in the Safety Matrix (Page 54)" and "The Safety Matrix tags (Page 52)". <p>These parameters can also be edited directly at the F-channel drivers in the CFC charts (including interconnection). If you use this option, you must be aware that inconsistencies may occur. The data saved to the CFC take precedence.</p>

Field	Description
<ul style="list-style-type: none"> "Energize-to-trip" 	<p>This is an option for discrete input types and specifies which Boolean condition a trip represents. In deenergize-to-trip applications, the input tag represents a trip if it switches to FALSE. In energize-to-trip applications, the input tag represents a trip if it switches to TRUE. By default, this check box is not selected, which means the default setting is deenergize-to-trip because the value "0" is regarded as the safe state for digital F-I/O. You can find additional information in the following table.</p>
<ul style="list-style-type: none"> "Soft Bypass allowed" 	<p>If the "Soft Bypass allowed" check box is selected for a tag of a Cause, the operator can activate a soft bypass manually only for this tag of the Cause in the Viewer or in the online mode of the engineering tool.</p> <p>A soft bypass removes this tag from the evaluation for the Cause. You can find additional information on this in section "The "Degraded Voting" function (Page 60)".</p> <p>This check box is selected by default.</p> <p>This function can be used for a function type with multiple tags, e.g. "2oo3", to set a bypass at only one tag and not for the entire Cause.</p>
"Input type"	An input type must be selected for each Cause.
<ul style="list-style-type: none"> "Discrete" 	The discrete type is a Boolean value (TRUE/FALSE). It is used, for example, for limit switches or motor feedback messages. The default setting for the input type is discrete type.
<ul style="list-style-type: none"> "Analog" 	An analog input represents a real value, e.g., the value of a temperature sensor or a flow quantity. If "analog" is selected as the input type, additional parameters must be assigned. The parameters are assigned in the "Analog parameters" tab of the "Cause details" dialog box.
"Alarm profile"	An alarm profile is assigned to each Cause. You can configure the alarm profiles for the Causes and Effects (see section ""Cause details" dialog box - "Alarms" tab (Page 108)"). The alarm profile selection determines the color representation in online mode and, if applicable, the Cause messages issued.
<ul style="list-style-type: none"> "Standard" 	"Standard" alarm profile is set (default).
<ul style="list-style-type: none"> "Sequential" 	"Sequential" alarm profile is set.
<ul style="list-style-type: none"> "Energized" 	"Energized" alarm profile is set.
"Number of inputs"	Specify how many tags are assigned to a particular Cause. For example, if three sensors are used to monitor a single process point, the value "3" should be selected. The selection in this field has an effect on the number of displayed tag fields "Tag x".
"Function type"	<p>The "Function type" defines the conditions under which a Cause becomes active. An entry in this field is mandatory.</p> <p>Note</p> <p>The tripping behavior can be influenced by further settings in the "Options" tab of the "Cause details" dialog box.</p>

Configuration	Input tag	Cause*
DTT	0	Active
	1	Inactive
ETT	1	Active
	0	Inactive

* Dependent on the configured function type and the bypass, inhibit, and time options

Refer also to section "Overview of configuring the Causes (Page 97)".

6.3.5 "Cause details" dialog - "Analog parameter" tab

"Analog parameter" tab

Field	Description
"Limit Value" area	
<ul style="list-style-type: none"> "Type" 	<p>This setting specifies whether the limit is an upper or lower limit. If it is a upper limit, the Cause tag satisfies the tripping condition if its value is greater than or equal to the entry value in the "Value" field. If it is a lower limit, the Cause tag satisfies the tripping condition if its value is less than or equal to the entry value in the "Limit" field.</p>
<ul style="list-style-type: none"> "Value" 	<p>The value entered in this field means that the Cause tag fulfills the tripping condition when the tag value is less than/equal to or greater than/equal to the input value, depending on the selected limit type.</p> <p>Data type is REAL. *1)</p>
<ul style="list-style-type: none"> "Prewarning" 	<p>A Cause tag is stored in the color configured for "Prewarning" as soon as the tag value is less than/equal to or greater than/equal to this input value, depending on the selected limit type.</p> <p>To disable this option, set the value greater than / equal to the limit value.</p> <p>Data type is REAL.*1)</p>
"Tolerances" area	
<ul style="list-style-type: none"> "Hysteresis" 	<p>The hysteresis specifies a deadband in the range of the limit value that applies if a Cause tag no longer satisfies the tripping condition. It prevents an input from constantly oscillating between active and inactive. The default setting is no hysteresis, i.e., the value "0".</p> <p>Examples:</p> <p>If a high limit of "90.0" and a hysteresis of "5.0" are set, the Cause remains active until the value falls below "85.0".</p> <p>If a low limit of "10.0" and a hysteresis of "2.0" are set, the Cause remains active until the value rises above "12.0".</p> <p>Data type is REAL. *1)</p>
<ul style="list-style-type: none"> "Delta" 	<p>This field is only enabled for analog inputs with more than one input tag.</p> <p>A diagnostic alarm is triggered when the input tags deviate by at least the specified delta value. To clear a diagnostic alarm, these values must lie within the delta range minus the hysteresis.</p> <p>If the value "0" is entered for "delta", delta is not taken into account.</p> <p>Example: If a delta value of "5.0" and a hysteresis of "2.0" is set, a diagnostic alarm is displayed when the values deviate by "5.0" or more. The difference of the values must be smaller than "3.0", so that the diagnostic interrupt is cleared.</p> <p>Data type is REAL. *1)</p>
"Display options" area	
<ul style="list-style-type: none"> "Unit" 	<p>Specifies the unit of measurement of the analog value. This specification can be up to 16 characters long and is used solely for documentation purposes.</p>

*1) You can find additional information on the analog parameters and the input in REAL format in section "Overview of configuring the Causes (Page 97)".

6.3.6 "Cause details" dialog box - "Options" tab

"Options" tab

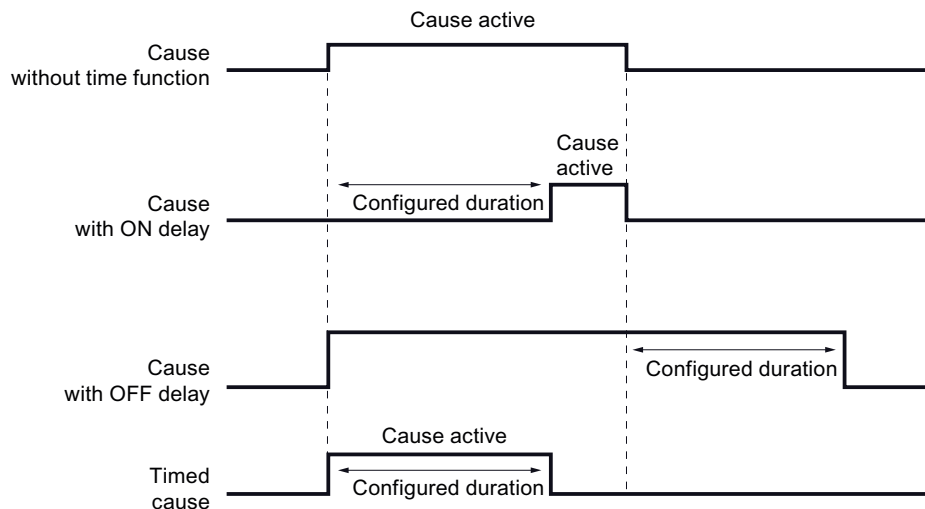
Field	Description
"Time" area	The Causes can be configured in such a way that the time functions described below are taken into consideration. You can find more detailed information on this in the description below "Time flow diagram for Cause time functions".
<ul style="list-style-type: none"> "Mode" selection field 	<ul style="list-style-type: none"> "None" This option deletes all time options for this Cause. "None" is the default setting. "ON delay" This specifies an ON delay. The tripping condition for the Cause must be fulfilled for at least the specified time period before the Cause becomes active. "OFF delay" This specifies an OFF delay. The tripping condition for the Cause must not be fulfilled for the time period specified by the OFF delay before the Cause becomes inactive. "Timed Cause" If this option is selected for a Cause, the Cause remains active after tripping for the time entered in the "Duration" field, regardless as to whether the tripping condition of the Cause is TRUE throughout the entire time or not. <p>Note A Cause requiring acknowledgment (not "Auto acknowledge active Cause") also becomes inactive in the case of "switch-off delay" and "timed Cause" without acknowledgment.</p>
<ul style="list-style-type: none"> "Duration" input field 	Here you enter the desired duration for the settings "ON delay", "OFF delay" or "timed Cause".
"Cause Bypass" area	Causes can be configured in such a way that the following bypass functions are available:
<ul style="list-style-type: none"> "Soft Bypass" <ul style="list-style-type: none"> "Soft Bypass allowed" "Time" and "Pre-alarm timeout" fields 	<ul style="list-style-type: none"> If the "Soft Bypass allowed" check box is selected, the operator can activate a bypass manually for the Cause for maintenance purposes in the Viewer or in the online mode of the engineering tool. This check box is selected by default. If the soft bypass is to be timed, the corresponding times can be entered in seconds in the "Time" and "Pre-alarm timeout" fields. With a value of "0" the timed function is disabled. The bypass is removed automatically when the configured time has elapsed.
<ul style="list-style-type: none"> "Hard bypass" "Tag" input field 	<p>The so-called "hard bypass" is configured via this field; here the bypass is controlled with a bypass tag.</p> <p>To open the "Select I/O Tag" dialog box, click the "I/O" button. Here you can select a Boolean tag as bypass tag. See section "The Safety Matrix tags (Page 52)".</p> <p>A bypass becomes active for the Cause when the value of the bypass tag = TRUE. A bypass is normally created for maintenance purposes. When a bypass is active, the Cause does not become active even though it should be active based on its tripping condition and options.</p> <p>A hard bypass overrides any set timed soft bypasses.</p>

6.3 Configuring the causes

Field	Description
"Inhibit Cause" area <ul style="list-style-type: none"> "Tag" input field 	To open the "Select I/O Tag" dialog box, click the "I/O" button. Here you can select a Boolean tag as inhibit tag. See section "The Safety Matrix tags (Page 52)". The "Inhibit" function is typically used to automatically inhibit a Cause during automatic start-up of a system. The Cause is inhibited when the inhibit tag is TRUE. When inhibit is active, the Cause does not become active even though it should be active based on its tripping condition and options.
"First Out Alarm" area <ul style="list-style-type: none"> "Group" input field 	In online operation, the First Out Alarm feature indicates which Cause of the First Out Alarm Group became active first (i.e., has Caused the tripping). The Cause that tripped first in each group is highlighted in color. For this, the option "Display groups (Cause/ Effect)" must be activated in the layout of the matrix. A Cause can be assigned to one of the 15 different First Out Alarm Groups. The first out alarm function is disabled by default. To add a Cause to a First Out Alarm Group, enter the desired group number in this text box.
"User Notes" area	Up to 32 comments can be configured in the properties of a safety matrix. Up to four comments can be assigned to each Cause in the "Comments" fields.
"SIF Grouping" area	Up to four Safety Instrumented Function (SIF) groups can be assigned to each Cause. An SIF group contains associated Causes and Effects that are typically assigned to a single safety circuit, made up of sensors, the F-CPU, and control elements, that executes a particular safety function. Assignment to an SIF allows filter functions to be used for displaying Causes and Effects in online mode. In this field, you can also select an SIF group which is not yet defined, i.e. does not contain a name. After selecting the SIF group number, you enter the corresponding name beside the number. The newly defined SIF group is then also displayed in the "Properties" dialog of the Safety Matrix, "General" tab. You can find additional information on this in section ""Properties" dialog box of the Safety Matrix (Page 88)".
"Features" area	
<ul style="list-style-type: none"> "Auto acknowledge active Cause" 	If the "Auto acknowledge active Cause" check box is selected, the Cause will be cleared automatically as soon as the tripping condition is no longer satisfied. If this check box is not selected, the operator must manually clear an active Cause. This check box is selected by default. Note: The acknowledgment has no effect on a Cause with configured OFF delay or a timed Cause.
<ul style="list-style-type: none"> Alarm on input trip 	If a Cause is configured with multiple input tags, the user can choose whether an alarm is indicated as soon as one of the inputs satisfies the tripping criteria. This option is activated by default.
<ul style="list-style-type: none"> "Mutually locked maintenance functions" 	When this option is activated, the maintenance operations, simulation and soft bypass at the tags of the Cause are mutually locked. This means that a simulation or a soft bypass can always only be activated for one tag of the Cause.
"Bad Quality" Voting' area	

Field	Description
<ul style="list-style-type: none"> 'Ignore "Bad Quality"' 	<p>When you activate this option, the bad signal status ("Bad Quality") of the input tags is not evaluated.</p> <p>Note</p> <p>For Safety Matrix input tags the F-channel drivers are created with the default SUBS_ON = 1 and SUBS_V = 0.0.</p> <p>This means that if there is a channel fault, the substitute value "0.0" is provided to the F-channel driver instead of the pending process value at the fail-safe input.</p> <p>This can result in a trigger being activated depending on the limit value type that is set, even if the option 'Ignore "Bad Quality"' is selected.</p> <p>If this is not the desired behavior, you have to modify the substitute value behavior at the F-channel driver in the nested chart for the F-channel driver.</p>
<ul style="list-style-type: none"> 'Trip on "Bad Quality"' 	<p>If this checkbox is activated, the poor signal status ("Bad Quality") of the input tag causes the input tag to trigger.</p>
<ul style="list-style-type: none"> 'Degraded voting at "Bad Quality"' 	<p>If this option is activated, then the input tag with a bad signal status ("Bad Quality") is taken out of the evaluation for the Cause.</p>

Time lapse diagram for Cause time functions



Refer also to section "Overview of configuring the Causes (Page 97)".

For detailed representations of the parameter assignment and the behavior of the Causes, see section "Parameter assignment options for causes (Page 203)".

See also

The "Degraded Voting" function (Page 60)

6.3.7 "Cause details" dialog box - "Alarms" tab

Requirement

To display the "Alarms" tab, the "Positioning of Cause and Effect" check box must be selected on the "Alarms" tab of the "Properties" dialog box for the Safety Matrix (**Edit > Properties** menu command).

See section ""Properties" dialog box of the Safety Matrix (Page 88)".

"Alarms" tab

Field	Description
"Alarm block" area	
<ul style="list-style-type: none"> "Positioning" 	When the "Positioning" check box is selected, an F_SC_AL or F_SC_AL2 message block is positioned for this Cause.
<ul style="list-style-type: none"> "Chart assignment" 	The chart assignment of the message block is specified in the field. Default setting is the Safety Matrix basic chart. A dialog is opened with the "..." button to select a different chart.
<ul style="list-style-type: none"> "Enable messages" 	Select the "Enable messages" check box. Click the associated "..." button to open the dialog box for configuring the alarm profile. This alarm profile is set in the "Configure" tab. The following actions are possible in this dialog: <ul style="list-style-type: none"> Lock individual messages Change message classes Change priorities of message classes Specify the acknowledgment request By selecting the "Extend event by symbolic Tag name" check box, the message text can be extended by the process tag name. If the check box of the same name is selected in the properties of the Safety Matrix, this setting generally applies to all Causes with this alarm profile, but it can be disabled here in the properties of the individual Cause.

For information on assigning a color to an alarm profile for the status display, see section ""Customize" dialog boxes (Page 94)".

6.4 Configuring the effects

6.4.1 Overview of configuring the effects

Overview

The values of at least one but no more than four discrete output tags define the action to be performed on the process. The activation of an effect depends on various factors:

- Type of intersection
- Set options of the effect

6.4.2 Creating/changing the effect and column for effect

Procedure for creating/changing an effect

Double-click on an empty or configured column in the Effects configuration area of Safety Matrix or click on the column and select "Edit" in the shortcut menu.

The "Effect Details - Effect x" dialog opens and you can create or change the effect.

Shortcut menu in the Effects configuration area of the Safety Matrix

When you click on a row in the Effects configuration area of the Safety Matrix, the shortcut menu offers a variety of functions.

The availability of the functions depends on whether the column is empty or has already been configured.

- Copy (copy effect)
- Cut (cut effect)
- Paste (paste effect into selected column; if column is filled, you will be queried as to whether you want to overwrite content)
- Edit (the "Effect details - Effect x" dialog box opens)
- Clear content (the effect, which means the content of the column is deleted but the column is retained as an empty column)
- Insert (an empty column is inserted and all subsequent effects are moved one column to the right)
- Delete (an empty column is deleted and all subsequent effects are moved one column to the left)
- SIF filter active (sets the SIF filter for the SIF group of this effect)

Note

Effects on the comparison

"Insert" or "Remove" of a column causes all subsequent columns to be marked as changed in a subsequent matrix comparison and they must therefore be checked during an acceptance. You can avoid this situation with the following measures:

- Always adding additional effects at the end.
 - Do not cut, insert, copy or delete entire columns but merely their contents.
 - Avoid changing the size of the Safety Matrix.
-

Note

Effects on the transfer

When the size of the Safety Matrix is changed by "adding" or "removing" a column, the Engineering Tool automatically activates the transfer option "Entire Safety Matrix" when the Safety Matrix is transferred. You can find additional information on this in section "Transferring the Safety Matrix to the program (Page 130)".

6.4.3 Overview of the "Effect details - Effect x" dialog

Procedure for configuring an effect

Double-click an (empty or configured) column in the Effects configuration area of the Safety Matrix or click the column and select "Edit" in the shortcut menu.

The "Effect details - Effect x" dialog box opens.

Effect "x"

Each effect is assigned a unique number within the Safety Matrix. This assignment occurs automatically on the basis of the selected column. The effect number cannot be changed.

Dialog box for configuring an effect

The dialog box for configuring an effect contains the following tabs:

- "Configure"
- "Options"
- "Alarms"

This tab is only displayed when the option "Positioning of Causes and Effects" is activated in the Matrix properties for the alarm blocks.

6.4.4 "Effect details" dialog - "Configure" tab

"Configure" tab

Field	Description
"Name"	<p>Name of the effect.</p> <p>A maximum of 32 alphanumerical characters and the "_" (underscore) character are possible.</p> <p>The entry is mandatory.</p> <p>If messages are configured for the effect, the respective effect name is integrated in the message text. You can find additional information on this in section "Overview for configuring messages (Page 67)".</p>
"Description"	<p>Description of the effect.</p> <p>A maximum of 80 Unicode characters is possible.</p> <p>Entry of the description is optional.</p>
"SIL"	<p>This field is used for documentation purposes. Here, you can enter the SIL (= Safety Integrity Level) for this effect, as determined during your risk analysis (e.g., according to IEC 61508).</p> <p>An entry in this field is not required. No SIL value is entered by default.</p>
"Tag x"	<p>Specify at least one tag for each effect. Please note the section "Syntax rules for tag names in the Safety Matrix (Page 54)".</p> <p>The number of tag fields displayed in the dialog box depends on the number in the field "Number of outputs".</p>
<ul style="list-style-type: none"> "I/O" button 	<p>To open the "Select I/O Tag" dialog box, click the "I/O" button. See section "The Safety Matrix tags (Page 52)".</p>
<ul style="list-style-type: none"> "..." button 	<p>The "..." button is activated when the "Channel driver" option was selected in the "Select I/O Tag" dialog box. Click the "..." button to open the "Channel driver" dialog.</p> <ul style="list-style-type: none"> In the "Parameter" tab, you can select the following options for F-channel drivers that are selected via symbols: <ul style="list-style-type: none"> "Set initial value" for the simulation "Simulation has priority" over errors (parameter SIM_MOD in F-channel driver F_CH_DO) "Acknowledgement required" for the F-channel driver after an outgoing channel fault You can find additional information on this in section "Configuration of the F-channel driver acknowledgment (Page 66)". The following option can be selected in the "Options" tab: <ul style="list-style-type: none"> "Monitoring activate" activates the monitoring for this tag. You can find additional information on this in section "The Safety Matrix tags (Page 52)". <p>These parameters can also be edited directly at the F-channel drivers in the CFC charts (including interconnection). If you use this option, you must be aware that inconsistencies may occur. The data saved to the CFC take precedence.</p>
<ul style="list-style-type: none"> "Action" 	<p>In this field you can enter a text containing up to 8 characters that describes which action will be initiated when the effect is active (for example: open). This value is used only for display/documentation purposes.</p>

6.4 Configuring the effects

Field	Description
<ul style="list-style-type: none"> "Energize-to-trip" 	<p>This option for the output tags specifies when the output tag is set to "0" or "1".</p> <p>In deenergize-to-trip applications, the output tag is set to "0" when the effect is active.</p> <p>In energize-to-trip applications, the output tag is set to "1" when the effect is active.</p> <p>By default, this check box is not selected, which means the default setting is deenergize-to-trip because the value "0" is regarded as the safe state for digital F-I/O. You can find additional information in the following table.</p> <p>Output tags for which energize-to-trip is activated are identified by a "*" character at the end of the output tag in the Safety Matrix.</p>
"Alarm profile"	<p>An alarm profile is assigned to each effect. You can configure the alarm profiles for the Causes and Effects (see section ""Effect details" dialog box - "Options" tab (Page 113)").</p> <p>The alarm profile selection determines the color representation in online mode and, if applicable, the effect messages issued.</p> <p>Note</p> <p>When the "Dynamic color scheme" option is activated in the "Options" tab, this "Alarm profile" setting is no longer effective for the color display of the effect.</p>
<ul style="list-style-type: none"> "Standard" 	"Standard" alarm profile is set (default).
<ul style="list-style-type: none"> "Sequential" 	"Sequential" alarm profile is set.
"Number of outputs"	<p>Specify how many tags are assigned to the effect.</p> <p>The selection in this field has an effect on the number of displayed tag fields "Tag x".</p>
"Function type"	The "Function type" defines the conditions under which an effect becomes active. An entry in this field is mandatory.
<ul style="list-style-type: none"> "Normal" 	<p>When the effect is active, the associated output tags are set to "0" (DTT) or "1" (ETT).</p> <p>The tripping behavior can be influenced by further settings in the "Options" tab of the "Effect details" dialog box.</p>
<ul style="list-style-type: none"> "Comment only" 	<p>The effect will not be processed.</p> <p>It is used for visualization of additional signal states in the OS that are not directly a part of the Safety Matrix logic (e.g. feedback of an actuator).</p>

Effect	Configuration	Output tag
Active	DTT	0
	ETT	1
Inactive	DTT	1
	ETT	0

Refer also to section "Overview of configuring the effects (Page 109)".

For detailed representations of the parameter assignment and information on how effects work, especially taking into consideration the configured intersection types, see section "Parameter assignment options for effects (Page 207)".

See also

"Effect details" dialog box - "Alarms" tab (Page 116)

6.4.5 "Effect details" dialog box - "Options" tab

"Options" tab

Field	Description
"Time response" area	
<ul style="list-style-type: none"> "Mode" selection field 	<p>If the "Output delay" option is selected in the "Mode" selection field, the outputs are tripped after the set time delay has expired.</p> <p>You specify the duration of the time delay in the "Duration" entry field. To delete a configured output delay, you must set the mode to "None".</p> <p>Notes</p> <ul style="list-style-type: none"> The output delay only has an effect on the output tags of the effect but not on tripping the effect itself. The output delay has no effect during visualization and for internal references of the effect. The time delay for an effect does not become active in case of a CPU restart. The Effect is tripped immediately in case of a restart, if (at least) one associated Cause is tripped.
<ul style="list-style-type: none"> "Duration" input field 	Here you enter the desired duration for the setting "Output delay".
"Effect Bypass" area	
<ul style="list-style-type: none"> "Soft Bypass allowed" 	<p>If the "Soft Bypass allowed" check box is selected, the operator can activate a bypass manually for the effect for maintenance purposes in the Viewer or in the online mode of the engineering tool.</p> <p>This check box is cleared by default.</p>
<ul style="list-style-type: none"> "Tag" field 	<p>The so-called "hard bypass" is configured via this field; here the bypass is controlled with a bypass tag.</p> <p>To open the "Select I/O Tag" dialog box, click the "I/O" button. Here you can select a Boolean tag as "bypass tag". See section "The Safety Matrix tags (Page 52)".</p> <p>A bypass becomes active for the effect when the value of the bypass tag is TRUE. A bypass is normally created for maintenance purposes, e.g., for replacement of a sensor. In normal process mode, you should use the "Override" function.</p> <p>If bypass is active, an Effect is deactivated although it should be active based on the other conditions (Cause, intersection).</p>
"Reset/Override Effect" area	
<ul style="list-style-type: none"> "Tag" field 	<p>To open the "Select I/O Tag" dialog box, click the "I/O" button. Here you can select a Boolean tag as "reset/override tag". See section "The Safety Matrix tags (Page 52)".</p> <p>When you specify this tag, the reset/override of the effect is no longer possible over the PCS7 OS.</p> <p>The effect can be overridden when the intersection types V or R are used, or it can be reset when the intersection types S or R are used. The effect is reset when the reset/override tag executes a FALSE-TRUE transition. In the case of an override, the override status is switched on a FALSE-TRUE transition. See section ""Intersection details" dialog box (Page 118)" with more details.</p>

6.4 Configuring the effects

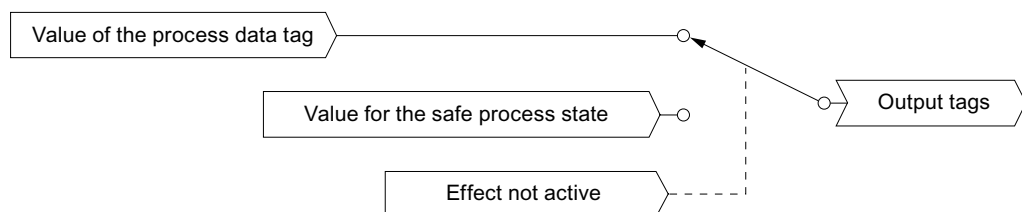
Field	Description
<ul style="list-style-type: none"> Override "Time" field 	<p>In this input field, the time for which the effect can remain in the override state must be entered in seconds for the intersection types R and V.</p> <p>If the conditions that tripped the effect are still present after expiration of the maximum override time, the effect becomes active again and an alarm "Override Failed: Timeout" appears. If a new Cause assigned to this Effect becomes active, the override function ends immediately, the Effect becomes active once again and an alarm "Override Failed: Cause" appears.</p> <p>The time configured in this field should not exceed the duration of any process state that the process or the plant tolerates.</p>
<ul style="list-style-type: none"> Override "Pre-alarm timeout" field 	<p>In this input field you can enter the maximum time in seconds after which a prewarning timeout is sent for reaching the override time entered in the "Time" field. The respective effect tag will be given a background in the color configured for "Prewarning" when this time has expired.</p>
"Pass through masking or process data" area	
<ul style="list-style-type: none"> "Enable process data pass through" 	<p>If you select this check box, the effect is configured to pass on the process data. A requirement is that a "process data tag" is specified. See description of "Process data pass through" following this table.</p>
<ul style="list-style-type: none"> "Process data" "Tag" field 	<p>Identifies an external process tag that is passed through to the output of the effect when "Process data pass through" is activated and when the effect is not active. This means an output can be controlled by a process value until a tripping condition activates the effect.</p> <p>If a mask enable tag is configured whose value is TRUE, the value of the process data tag is always passed through to the output tags.</p> <p>For Energize-to-trip (ETT) output tags, the value is inverted by the process data tag before it is written to the output tags.</p> <p>To open the "Select I/O Tag" dialog box, click the "I/O" button.</p>
<ul style="list-style-type: none"> "Mask enable" "Tag" field 	<p>The value of the mask enable-tag specifies whether the effect logic or an externally controlled process tag (see "Process data tag" above) is interconnected to the output tags of the effect. See description of "Mask" following this table.</p> <p>To open the "Select I/O Tag" dialog box, click the "I/O" button.</p>
"User Notes" area	<p>Up to 32 comments can be configured in the properties of a safety matrix.</p> <p>Up to four comments can be assigned to each effect in the "Comments" fields.</p>
"SIF Grouping" area	<p>Up to four Safety Instrumented Function (SIF) groups can be assigned to an effect. An SIF group contains associated Causes and Effects that are typically assigned to a single safety circuit, made up of sensors, the F-CPU, and control elements, that executes a particular safety function. Assignment to an SIF allows filter functions to be used for displaying Causes and Effects in online mode.</p> <p>In this field, you can also select an SIF group which is not yet defined, i.e. does not contain a name. After selecting the SIF group number, you enter the corresponding name beside the number. The newly defined SIF group is then also displayed in the "Properties" dialog of the Safety Matrix, "General" tab. You can find additional information on this in the section ""Properties" dialog box of the Safety Matrix (Page 88)".</p>
"Features" area	

Field	Description
<ul style="list-style-type: none"> "Mutually locked maintenance functions" 	When you activate this option, the maintenance operations of the tags of the effects are mutually locked. This means that only one tag of an effect can be simulated at a time.
<ul style="list-style-type: none"> "Dynamic color scheme" 	<p>When you activate this option, the colors for a tripped Effect are the colors of the alarm profile of the Cause initiating the tripping.</p> <p>When this "Dynamic color scheme" option is activated, the "Alarm profile" setting in the "Configure" tab is no longer effective for the color display of the effect.</p> <p>Note</p> <p>The alarm profile of the active Cause with the highest priority takes precedence when it comes to the color display of the Effect.</p> <p>Priority:</p> <ul style="list-style-type: none"> High = Sequential Medium = Energized Low = Standard

Process data pass through

This is a concept that allows an externally-controlled process tag (by a control system) to be interconnected with the output logic of the effect. The Safety Matrix will disregard the pass through of the process data if the effect becomes active. Process data pass through is configured by selecting the "Enable process data pass through" check box and input of a process data tag for the process tag.

The pass through is controlled by the state of the effect; see the following figure. The value of the process data tag is interconnected to the output tags when the effect logic is not active. If the effect logic is active, the interconnection of the process data tag value to the output tags of the effect is disconnected and the output is controlled by the values for the fail-safe process state. The value for the fail-safe process state is FALSE for a deenergize-to-trip (DTT) output and TRUE for an energize-to-trip (ETT) output.

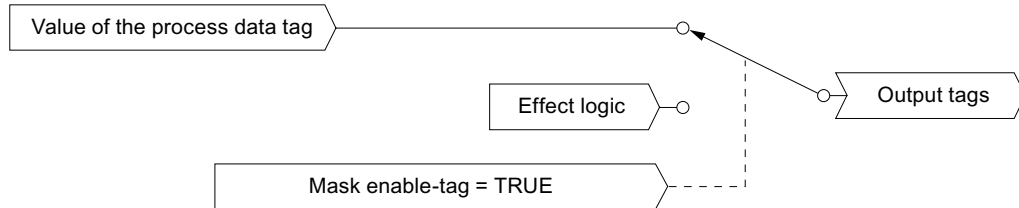


Note

There are no messages for tags that are tripped by process data pass through.

Mask

By masking the effect, you can override the effect logic using the process data value, as shown in the figure below. The override function is controlled by the value of the mask enable tag.



The configuration of an effect for masking requires that values are entered for the mask enable-tag and the process data tag and the "Enable process data pass through" check box is selected.

The value of the mask enable-tag specifies whether the effect logic or an externally controlled process tag (see "Process data tag" above) is interconnected to the output tags of the effect.

Refer also to section "Overview of configuring the effects (Page 109)".

For detailed representations of the parameter assignment and information on how effects work, especially taking into consideration the configured intersection types, see section "Parameter assignment options for effects (Page 207)".

6.4.6 "Effect details" dialog box - "Alarms" tab

Requirement

To display the "Alarms" tab, the "Positioning of Cause and Effect" check box must be selected on the "Alarms" tab of the "Properties" dialog box for the Safety Matrix (**Edit > Properties** menu command).

See section ""Properties" dialog box of the Safety Matrix (Page 88)".

"Alarms" tab

Field	Description
"Alarm block" area	
<ul style="list-style-type: none"> "Positioning" 	With selected "Positioning" check box, the message block F_SE_AL is positioned for this effect.

Field	Description
<ul style="list-style-type: none"> "Chart assignment" 	<p>The chart assignment of the message block is specified in the field. Default setting is the Safety Matrix basic chart.</p> <p>A dialog is opened with the "..." button to select a different chart.</p>
<ul style="list-style-type: none"> "Enable messages" 	<p>Select the "Enable messages" check box.</p> <p>Click the associated "..." button to open the dialog box for configuring the alarm profile. This alarm profile is set in the "Configure" tab.</p> <p>The following actions are possible in this dialog:</p> <ul style="list-style-type: none"> Lock individual messages Change message classes Change priorities of message classes Specify the acknowledgment request By selecting the "Extend event by symbolic Tag name" check box, the message text can be extended by the process tag name. <p>If the check box of the same name is selected in the properties of the matrix, this setting generally applies to all effects with this alarm profile, but it can be disabled here in the properties of the individual effect.</p>

For information on assigning a color to an alarm profile for the status display, see section ""Customize" dialog boxes (Page 94)".

6.5 Configuring the intersections

6.5.1 Editing or changing intersections

Editing or changing an intersection

Select a valid intersection cell in the intersection of a configured Cause and a configured Effect. Each Safety Matrix supports up to 1024 intersections.

Procedure for editing/changing an intersection

Double-click an (empty or configured) intersection in the intersection configuration area of the Safety Matrix or click the intersection and select "Edit" in the shortcut menu. The "Intersection details - Cause x, Effect x" dialog box opens and you can create or change the intersection.

Context menu in the intersection configuration area of the Safety Matrix

When you click on an intersection in the intersection configuration area of the Safety Matrix, the shortcut menu offers a variety of functions.

The availability of the functions depends on whether the row of the intersection is empty or has already been configured.

Menu command	Function
Copy	Copy intersection
Cut	Cut intersection
Paste	Insert intersection
Edit	Change intersection
Clear contents	Delete contents of the intersection cell
N - Not stored	Configure/change intersection type
S - Stored	
V - Overridable	
R - Resettable and overridable	
X - Not specified	
* - For note only	
None	
XooN (Specify X)	

6.5.2 "Intersection details" dialog box

Procedure for editing/changing an intersection

You can configure or change an intersection in the "Intersection details - Cause x, Effect x" dialog box.

Overview

Intersection type / field	Description
N - Not stored	Simple pass through function. If the Cause is active, the Effect is tripped.
S - Stored	If the Cause is active, the Effect is tripped and stored. If the effect is no longer tripped, the operator must manually clear it in the Viewer or in online mode of the Engineering Tool, or by setting the configured reset/override tag to TRUE.
V - Overridable	<p>If the Cause is active, the Effect is tripped. You can override the tripping of the effect by:</p> <ul style="list-style-type: none"> • Manual intervention, or • By setting the configured reset/override tag to TRUE as long as the effect is still tripped. <p>Condition:</p> <p>With this intersection type you must enter the maximum time that the effect can remain in the override state in the properties of the effect, "Options" tab, "Reset/Override Effect" area, "Time" field.</p>

Intersection type / field	Description
R - Resettable and overridable	<p>This intersection type is a combination of the S and V types described above. The Effects interconnected with this intersection type remain active if the associated Cause becomes inactive.</p> <p>However, the effects can be overridden with the override function as long as the Cause is active, and must be reset when the Cause is no longer active.</p> <p>Condition:</p> <p>With this intersection type you must enter the maximum time that the effect can remain in the override state in the properties of the effect, "Options" tab, "Reset/Override Effect" area, "Time" field.</p>
X - Not specified	<p>A connection between the Cause and Effect is required but the desired intersection type has not yet been specified.</p> <p>A Safety Matrix with intersection type X cannot be transferred.</p>
* - For note only	<p>A connection between this Cause and this Effect will not be processed.</p> <p>It is used for visualization of additional signal states in the OS that are not directly a part of the Safety Matrix logic (e.g. feedback of an actuator).</p>
None	<p>There is no connection between this Cause and this Effect (no entry in the intersection).</p>
XooN value (2-15)	<p>This enables you to assign Causes according to the majority method. X is entered by the user, and N is determined based on the number of intersections having X as a coefficient.</p> <p>Only one XooN assignment is allowed for each effect. Only intersections of the same type (for example, all S or all N) can be taken into consideration for assignment according to the majority principle.</p> <p>The figure below shows examples of this type of intersection.</p>

Examples of intersection assignment according to the majority principle

Name	Description	Action	Output Tag	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
FP_P	Feed Pump High Pressure Switch	1	2V	V			5N		N										
Tank_100_LH	Tank 100 Level Switch High	2	N	3S	2N	5N		R											
Hopper_200_LL	Hopper 200 Level Switch Low	3	2V	3S		5N		2S											
Hopper_200_P	Hopper 200 High Pressure	4		3S	S	5N		V											
Tank_100_L	Tank 100 Level	5	2V			5N													
FP	Feed Pressure	6		3S	2N	5N		2S	S										

Note

The Safety Matrix offers a convenient method for collectively processing the safety logic. If required, all effects can be activated simultaneously. This is possible by configuring a single Cause and configuring an intersection type with the desired Effects in all intersections of the Cause. If this Cause becomes active, it trips every Effect logic (including configured time delays).

For detailed representations of the parameter assignment and information on how effects work, especially taking into consideration the configured intersection types, see section "Parameter assignment options for effects (Page 207)".

6.6 Importing/exporting a matrix

6.6.1 Bulk data engineering using a spreadsheet

Overview

For bulk data engineering, the data of a Safety Matrix can be exported to a spreadsheet, edited with a spreadsheet program outside the engineering tool and imported into an existing or a new/empty Safety Matrix.

The spreadsheet is created in "*.ods" format.

6.6.2 Exporting Safety Matrix as spreadsheet

Introduction

For bulk data engineering, the data of a Safety Matrix can be exported to a spreadsheet.

During the export, the configuration data of a matrix is saved in multiple tables in the spreadsheet.

- Matrix properties
- Alarm profiles
- Causes configuration
- Intersections overview
- Effects configuration
- Legend

Note

Safety during data exchange of the spreadsheet

- Make sure that access to the transfer medium or the transfer directory is restricted to authorized personnel during data exchange via spreadsheet.
 - The spreadsheet does not contain any scripts. It is therefore not necessary to allow scripts when editing the spreadsheet.
-

Notes on exported data

Display and properties of exported data in the external editor:

- Table cells with "gray" as background color are for information only.
 - Specification of options for a tag:
The options for a tag are specified with an additional character, e.g. for "E6.3#" the "#" character at the tag name activates the option "with monitoring".
Possible additional characters at tag names:
 - "#" as prefix in front of tag name = "External connection"
 - [x] or [x][y] after the tag name = "Internal reference";
"x" = Number of the Cause/Effect; "y" = number of the tag of an Effect, e.g. tag name "Cause[1]" or "Effect[7][2]"
- F-channel drivers:
- "#" as suffix after the tag name = "with monitoring"
 - "@" as prefix in front of tag name = "used externally"
 - "~" as prefix in front of tag name = "customized"
 - "*" as prefix in front of tag name = "with preprocessing"

Procedure

To export the Safety Matrix to an "*.ods" spreadsheet, follow these steps:

1. Open the matrix whose data you want to export to a spreadsheet in the Safety Matrix Engineering Tool.
2. Select the **File > Export...** menu command.
3. In the next selection window select the desired directory and the file name of the spreadsheet.
4. Click on the "Save" button.
The export of the Safety Matrix data to the spreadsheet is started. After the process is completed, a message is displayed.

6.6.3 Importing the spreadsheet of a Safety Matrix

Introduction

If the data of a Safety Matrix was exported to a spreadsheet and edited outside the Safety Matrix Engineering Tool for bulk data engineering, the modified data can then be reimported into a Safety Matrix.

The import can only take place into an existing Safety Matrix.

Note**Safety during data exchange of the spreadsheet**

- For data exchange via a spreadsheet, note that the transfer medium or the transfer directory is only accessible to authorized persons.
 - The spreadsheet does not contain any scripts. It is therefore not necessary to allow scripts when editing the spreadsheet.
-

The size of the Safety Matrix is determined when importing

The size of the imported Safety Matrix is determined during import by the configured Causes and Effects in the spreadsheet.

During the import, the spreadsheets for Causes/Effects import those table rows for which a number is entered in the table cell for the Cause/Effect number. The import starts with the table row with the lowest Cause/Effect number.

The import for the respective spreadsheet ends at an empty table cell for the Cause/Effect number.

That means, if data for Causes/Effects is contained in other table rows following a table line without Cause/Effect number, then this data will not be imported.

A maximum of 128 Causes or Effects can be imported, even if more table rows for Causes or Effects include configuration data.

Procedure

To import an "*.ods" spreadsheet into a Safety Matrix, follow these steps:

1. Open the desired Safety Matrix into which you want to import the data of the spreadsheet in the Safety Matrix Engineering Tool.
2. Select the **File > Import...** menu command.
3. In the next selection window select the directory and the spreadsheet to be imported.
4. Click the "Open" button.

The import of data from the spreadsheet to the Safety Matrix is started.

When the process is finished, the safety matrix is displayed and the Reports window opens with the import log in the "Import/Export tab".

After importing a "*.ods" spreadsheet, the following values are entered in the "Matrix comparison" section of the import log:

- "Source" = Spreadsheet "*.ods"
- "Reference" = Safety Matrix before the import

Measures after an import

- The changes are highlighted in color in the Matrix view. Check the changes.
- Accept the changes and save the Safety Matrix.
- Transfer the Safety Matrix.
- Compile and download the program.
- Compile and download the OS.

Note

Possible effects of the bulk data engineering on existing and tested functions

Any existing and tested functions must not be reused after bulk data engineering without being checked first. They are subject to the acceptance process as are the functions that were newly created or changed during bulk data engineering. For detailed information on the acceptance process, refer to the section "Acceptance test for a Safety Matrix (Page 201)".

6.6.4 Importing a Safety Matrix file (*.cem) into a PCS 7 project

Introduction

Safety Matrices that were exported to a CEM file for external processing in versions prior to V6.3 can be imported into a SIMATIC project this way.

The CEM file contains all configuration data for one Safety Matrix.

Note

A new Safety Matrix is created by importing a CEM file.

A CEM file cannot be imported if a CFC with the same name already exists. In this case you must rename the CFC chart prior to importing the Safety Matrix file (in the S7 program, "Charts" folder) and then rename it again.

Note

If you delete the existing CFC, any interconnections made to the CFC of the Safety Matrix will be lost as well.

Procedure

To import the "*.cem" Safety Matrix file into a SIMATIC project, follow these steps:

1. Start SIMATIC Manager.
2. Open the project in which the Safety Matrix is to be imported.

3. In the S7 program, select the "Safety Matrices" folder.
4. In the shortcut menu select the menu command **Safety Matrix > Import...** .
5. In the next selection window select the CEM file to be imported.

Note

Safety during data exchange of the Safety Matrix file

Make sure that access to the transfer medium or the transfer directory is restricted to authorized personnel during data exchange of the "*.cem" Safety Matrix file.

Result

The imported Safety Matrix file appears in the "Safety Matrices" folder as a new Safety Matrix and can be edited, transferred, compiled and downloaded just like any other Safety Matrices.

Access protection

Purpose and mode of operation

Access protection protects S7 F/FH Systems from unauthorized access, such as undesirable downloads to the F-CPU from the Engineering System (ES). In addition to the password for the F-CPU, you need an additional password for the safety program for S7 F/FH Systems.

The table below provides information about the password for the F-CPU and the password for the safety program.

Password for F-CPU	
Assignment of the password	In HW Config during configuration of the F-CPU in the "Protection" tab of the "Properties" dialog box
Query of the password	<ul style="list-style-type: none"> • During download of the entire S7 program from the Safety Matrix Engineering Tool • During download of changes only in the safety program from the Safety Matrix Engineering Tool • For every online change in the Safety Matrix Engineering Tool
Validity of the password	<p>Access permission is valid until it is explicitly canceled using the corresponding function of SIMATIC Manager (with the Target system > Access Permission > Revoke menu command) or until you close the last STEP 7 application.</p> <p>Access permission can become invalid if the hardware configuration of the F-CPU is changed and downloaded.</p>

Password for safety program	
Assignment of the password	In SIMATIC Manager, Options > Edit Safety Program menu command
Query of the password	<ul style="list-style-type: none"> • When saving changes to a Safety Matrix • When transferring a Safety Matrix to the safety program • When compiling changes to the safety program • When downloading changes only to the safety program • When starting the operation via Secure Write in online mode of the Safety Matrix Engineering Tool • When saving the safety program as a reference
Validity of the password	The access permission lasts for one hour after correct password entry, during which time it is reset to another hour after each action requiring a password, or until access permission is explicitly revoked in SIMATIC Manager (Options > Edit Safety Program menu command, then click the "Password" button followed by the "Revoke" button).

This access protection is described in detail in the *"S7 F/FH Systems Configuring and Programming"* Programming and Operating Manual. Additional information on this document is available in the preface.

Transferring a Safety Matrix

Introduction

The transfer of a Safety Matrix to the project includes:

- Saving the Safety Matrix with plausibility check of the configuration.
- Generation of an S7 F-Systems program logic based on CFC using blocks from the Safety Matrix block library.
- Creating multiple F-runtime groups.



Transfer execution options

The following options are available for execution of the transfer:

- Transfer of the Safety Matrix currently open in the engineering tool.
To do so, select the **File > Transfer...** menu command in the engineering tool.
You can find additional information in section "Transferring the Safety Matrix to the program (Page 130)".
- Transfer of one Safety Matrix or multiple Safety Matrices in SIMATIC Manager.
In SIMATIC Manager, select the "Safety matrices" folder and the menu command **Options > Safety Matrix > Selective transfer...** .
With multiple selection, all Safety Matrices to be migrated can, for example, be migrated in one step.
Further information can be found in the following sections:
 - ""Selective transfer" dialog box (Page 140)"
 - "User scenario 1 (Page 33)"

Transfer status of a Safety Matrix

In SIMATIC Manager the transfer status is indicated by each Safety Matrix icon.

Icon	State
	"Transferred" This status is displayed after a transfer.
	"Not transferred" This status is displayed after saving changes to the Safety Matrix.

Nested charts after the transfer

A Safety Matrix top chart with the following nested charts exists for each Safety Matrix after the transfer:

- Nested chart of the matrix logic ("@MatrixName") This chart is protected, which means it cannot be opened in the CFC editor.

Optionally, these charts can also be present:

- Nested chart of the F-channel drivers ("MatrixName")
- Nested chart of the message blocks ("AL_Chart")
- Nested chart of the preprocessing ("PP_Chart")

You can find additional information on nested charts and the conditions for creating them in section "Result of the transfer and overview of the created charts (Page 135)".

8.1 Transferring the Safety Matrix to the program

After complete configuration of a Safety Matrix, it must be saved and transferred to the project before it can be compiled and downloaded to the F-CPU for execution.

The following description shows how the Safety Matrix currently open in the engineering tool is transferred.

Alternatively, you can also transfer one or more Safety Matrices in SIMATIC Manager with the menu command **Options > Safety Matrix > Selective transfer**. You can find additional information on this in section "Transferring a Safety Matrix (Page 129)".

Transferring a Safety Matrix to a project

1. Select the menu command **File > Transfer...** in the engineering tool.
2. In the next dialog box, select the "Entire Safety Matrix" or "Changes only" transfer options. The "Show Details ..." button opens the Reports window with the "Transfer" tab, which contains information about the pending transfer, for example for validation.
3. Optional: If necessary, select the desired transfer options "Integrate external channel drivers", "Clean nested chart connections" and/or "Update Preprocessing".
4. Start the transfer process by clicking the "OK" button.
5. Only for the initial transfer of a matrix:
Assign the generated Safety Matrix top chart to a hierarchy folder in the plant hierarchy by moving from the component view to the plant view (using cut & paste).
(See "*PCS 7 Process Control System; Engineering System*" configuration manual, section "How to assign objects to the PH". Additional information on this document is available in the preface.)

Perform steps 1 to 5 for each Safety Matrix to be transferred.

Transfer options

The "Transfer to Project" dialog box offers the options described below.

The "Entire Safety Matrix" option

The "Entire Safety Matrix" option clears the complete nested chart of the matrix logic ("@MatrixName") with the associated user-configured connections and creates a new one.

The following selection options are available for this option:

- Preselected by the engineering tool
- Selection by the user

Preselected by the engineering tool:

Under the following conditions, the option is specified by the Engineering Tool and cannot be deselected:

- The Safety Matrix is transferred for the first time or the associated CFC was deleted.
- The cycle time of the Safety Matrix was changed (cyclic interrupt OB).
- The size of the Safety Matrix was changed.
- A Cause row or an Effect column was added or deleted.

You also have the option of selecting the "Entire Safety Matrix" option for the transfer.

Note

In the report window for the transfer, you can see from the entry "Transfer parameter settings" whether the transfer was carried out with the option "Entire Safety Matrix". Check this entry based on the parameter assignment.

Selection by the user:

If you use the "Entire Safety Matrix" option to transfer, you must take the following into consideration:

- After the transfer, restore your user-configured connections to the nested chart in the matrix logic ("@MatrixName"), for example, by closing text references.
Afterwards, you must compile and download the assigned OS. Similarly, any active process control is not possible on this OS for the nested chart of the matrix logic ("@MatrixName") while the changes are being downloaded.
- If you then download changes to this Safety Matrix to the F-CPU, the Safety Matrix restarts with initial data:
 - All saved information (e.g., active timers, messages) are lost.
 - After the initial run, the output tags of the newly downloaded Safety Matrix F-blocks output the value determined from the Safety Matrix logic.
 - If Causes/Effects are coupled back, the value of the corresponding tags is FALSE during the initial run, if you:
 - Reference an Effect in a Cause
 - Reference another Cause with a higher number in a Cause
 - Output tags of the Safety Matrix prior to the initial run are FALSE. This is only important if these tags are evaluated in the run sequence **before** the Safety Matrix.

8.1 Transferring the Safety Matrix to the program

- While changes are being downloaded to the F-CPU, processing of the Safety Matrix is interrupted. Therefore, do not plan any active process control by the Safety Matrix during this time (all effects are in "not activated" state).
- Note the selection of additional options for positioning the alarm blocks when using this transfer option. You should select the settings "Update all" or "Update new".

Note

Transfer with the "Entire Safety Matrix" option

A transfer with the "Entire Safety Matrix" option always results in a new generation of the associated CFC charts and a changed collective signature of the safety program even if the Safety Matrix configuration was not changed.

"Changes only" option

You can download changes to the F-CPU with a Safety Matrix running if you have selected the "Entire Safety Matrix" option or the "Changes only" option for the transfer. This has no Effect on the processing of the Causes, Effects, and intersections that were not changed.

Take the following into consideration for the Causes and Effects that were changed:

- Saved information (e.g., active timers, messages) are retained when downloading changes to the F-CPU. This may result in inconsistencies between the old and new configurations. Example: If the old effect was active as a stored effect and was reconfigured as "not stored", this effect can no longer be reset due to the missing reset tag.
- If this behavior is not desired, you must download the changes in two steps:
 - First, delete the configurations of the Causes/Effects involved and then download.
 - Afterwards, configure and download the new configuration.

 **WARNING**

Effect of the "Changes only" transfer option on download of changes

- If you activate the "Changes only" transfer option, you must make sure that no inconsistencies occur when Causes/Effects are changed. These inconsistencies between the previous and the new configuration may arise because information stored in the F-CPU during the download of changes (e.g. active times, messages) is retained.
In case of doubt, activate the "Entire Safety Matrix" transfer option.
- Only select the "Changes only" transfer option if the changes you made can be verified.

(SMW-008)

"Integrate external channel drivers" option

External F-channel drivers are F-channel drivers that were not placed by the Safety Matrix. For the Safety Matrix to also interconnect external F-channel drivers as 'internal F-channel drivers', you must select the "Integrate external channel drivers" option for the transfer of the Safety Matrix to the project. This is necessary for the "Simulate tag" function to also act on these external F-channel drivers. Likewise, reintegration of F-channel drivers after errors that require acknowledgment from the Safety Matrix Viewer or in online mode of the Safety Matrix Engineering Tool via the "Acknowledge driver" button also incorporates these external F-channel drivers.

If an input/output tag was already configured by another Safety Matrix or user logic, the transferred Safety Matrix interconnects the tag to the existing F-channel driver.

By selecting this option, the following functions are integrated into the Safety Matrix in addition to the process value:

- "Simulating a tag" function:
Automatic interconnection of the simulation inputs (SIM_I, SIM_ON) of the F-channel driver block to the Safety Matrix.
This means the process value can be simulated at the F-channel driver block via the Safety Matrix.
- "Reintegration" function:
Automatic interconnection of the reintegration input (ACK_REI) of the F-channel driver block to the Safety Matrix.
This means the F-channels can be acknowledged with the Safety Matrix after an outgoing error. ("Acknowledge driver" button in the control bar)

Using the inputs of an F-channel driver:

To use this option none of these inputs must already be interconnected. If the inputs of an F-channel driver you want to use are already interconnected otherwise, these two matrix functions "Simulating a tag"/"Reintegration" are ineffective for this channel. Only the process value can then be used in the matrix.

Effects on interconnections of external F-channel drivers:

- When two Safety Matrices are using one F_CH_DI block and both are transferred with the "Integrate external channel drivers" option selected, the matrix transferred first prevails. After transfer of the first matrix, SIM_I, SIM_ON, ACK_REI, and ACK_REQ are interconnected and are no longer changed.
- If external F_CH_DI blocks already have interconnections to ACK_REI and SIM_x, the interconnections are retained.

"Clean nested chart connections" option

During a transfer with the "Clean nested chart connections" option selected, connections to the nested chart of the Safety Matrix that are no longer used internally are deleted. Note that the links that you have created to these connections of the nested chart of the Safety Matrix will be lost in this process.

"Update preprocessing" option

If this option is activated, all preprocessing charts will be updated with the templates in the "Templates" folder of the "SafetyMatrix Lib" during transfer.

- The option can be used to specify when the preprocessing charts should be updated.
- Manual changes to existing preprocessing charts in the project are overwritten by a transfer with the "Update preprocessing" option.
If the existing preprocessing charts should not be overwritten, then save them before updating.
- Preprocessing charts can also be updated during transfer with the option "Changes only"; therefore, transfer with the "Entire Safety Matrix" option is not required.
- The option is deactivated by default.
- The option is available for transfer with the Safety Matrix Engineering Tool and for selective transfer in the SIMATIC Manager.

You can find additional information on preprocessing charts in section "Preprocessing (Page 56)".

"Alarm blocks" area

"Positioning" option

When a transfer is performed with the "Positioning" option selected, the configured message blocks are positioned in a CFC.

Note

If the "Positioning" check box of the alarm blocks is **not** selected, the existing message blocks are deleted during the transfer and new message blocks are not positioned. Messages are not issued and block icons are not created for the OS. This also applies if the F_MA_AL (Safety Matrix, 1-time), F_SC_AL/F_SC_AL2 (Causes, x-times), and F_SE_AL (Effects, x-times) message blocks were correctly configured within the Safety Matrix.

To generate the block icons for the Safety Matrix, the message blocks must be configured appropriately (see section "Overview for configuring messages (Page 67)") and the Safety Matrix must be transferred with the "Positioning" option selected.

Additional options

In addition, you can choose one of three options:

- **Update all (recommended):**
The current message block configuration in the Safety Matrix is transferred to the CFC program. Message blocks are (re)positioned; those that are no longer used are deleted.
- **Update new**
Only the newly created message blocks are transferred to the CFC program. Message blocks that are no longer used are deleted.
- **Leave unchanged**
The current configuration of message blocks in the Safety Matrix is ignored. Message blocks are neither positioned nor deleted.

8.2 Result of the transfer and overview of the created charts

Transfer of Safety Matrix

When the Safety Matrix is transferred, it is checked for configuration errors, such as Causes without intersections. The results of this check are displayed in the Reports window. Use the "Show details" button to open the Reports window of the transfer operation.

If the results of the check are OK, the Safety Matrix Engineering Tool performs a comparison between the current Safety Matrix and the Safety Matrix stored in the project. Any discrepancies are displayed in the Reports window.

Check the logged changes in the reports and save and accept the changes.

Result of the transfer

During the transfer, a CFC chart with the name of the Safety Matrix is created in the chart folder of the F-CPU, the so-called Safety Matrix top chart.

The chart contains:

- A protected nested chart ("@MatrixName"), which contains the complete Safety Matrix configuration.

Optionally, these nested charts can also be present:

- A nested chart ("MatrixName") with the automatically created F-channel drivers. The F-channel drivers that were interconnected by means of the "Integrate external channel drivers" transfer option are not moved here.
- Nested chart of the message blocks (global) ("AL_Chart")
- Nested chart of the preprocessing ("PP_Chart")

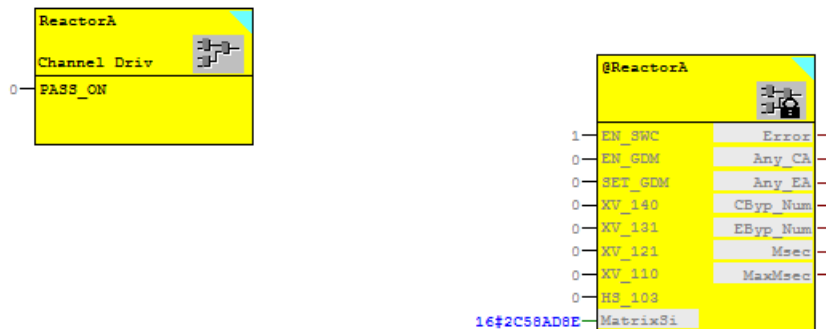
The conditions for creating these optional charts are listed in the associated chart description.

The created nested charts are described below.

Example for the generated Safety Matrix top chart

The following figure shows the Safety Matrix top chart created during the transfer of a Safety Matrix with the nested charts for the F-channel drivers "ReactorA" and the matrix logic "@ReactorA".

No nested charts were created in this example for message blocks (global) ("AL_Chart") and preprocessing ("PP_Chart").



Nested chart of the F-channel drivers ("MatrixName")

If only external connections are used in a Safety Matrix, then a nested chart for F-channel drivers is not created.


The Safety Matrix Engineering Tool automatically places the following F-channel drivers from S7 F Systems into a CFC chart during the transfer:

- F_CH_DI for discrete Cause tags: F-channel drivers for digital inputs of F-I/O (except fail-safe DP standard slaves and PA field devices *1))
F_CH_DI are also created for the configured functions "Inhibit", "Reset", "Bypass", "Masking" and "Process data pass through".
- F_CH_AI for analog Cause tags: F-channel drivers for analog inputs of F-I/O (except fail-safe DP standard slaves and PA field devices *1))
- F_CH_DO for effect tags: F-channel drivers for digital outputs of F-I/O (except fail-safe DP standard slaves and PA field devices *1))
 - *1) If you are using fail-safe DP standard slaves or fail-safe PA field devices in a Safety Matrix, place the F-channel drivers for them manually and interconnect the F-channel drivers with the Safety Matrix using chart connections to the nested chart of the matrix logic.

The nested chart of F-channel drivers has a visible input:

- Input PASS_ON is interconnected with input PASS_ON of all internal F-channel drivers. By interconnecting this input, you can passivate all F-channel drivers of the Safety Matrix, e.g., if you want to enable passivation as a function of particular states in your safety program.

The invisible chart connections (inputs and outputs) must not be changed.

 WARNING
<p>Nested chart of the F-channel drivers</p> <p>You must not rename, copy, or move the nested chart of the F-channel drivers ("MatrixName"). In addition, you must not delete any interconnections in this chart.</p> <p>(SMW-009)</p>

Note**Blocks in the nested chart of the F-channel drivers**

You must not change, rename, add, or delete any blocks in the nested chart of F-channel drivers.

Nested chart of the matrix logic ("@MatrixName")

The nested chart of the matrix logic always has at least the following **inputs**:

- MatrixSig: Contains the Safety Matrix signature
- EN_SWC: This input (F_BOOL) can be used to enable and, if necessary, to disable the Secure Write function for the purpose of making operator inputs either in online mode of the engineering tool or from the PCS 7 OS. This takes place by means of a signal that is wired in the CFC prior to compiling (enable, if signal = TRUE). See section "Secure Write (Page 170)".
- EN_GDM and SET_GDM:
With these two inputs of the F_BOOL type all active maintenance operations for Causes/ Effects, such as simulations, soft bypasses and override functions, can be deactivated with one external signal, e.g. over a keyswitch.
Deactivation can take place even if this is no longer possible online because visualization is no longer available. You can find additional information on this in section "Group deactivation of maintenance operations (Page 63)".


The nested chart of the matrix logic always has at least the following **outputs**:


- Error – Boolean flag indicating that an error was detected in the safety data format
- Any_CA – Indicates that at least one of the Causes in the Safety Matrix is active
- Any_EA – Indicates that at least one of the effects in the Safety Matrix is active
- CByP_Num – Integer value indicating how many Causes are currently bypassed
- EByP_Num – Integer value indicating how many effects are currently bypassed
- Msec – Current processing time of the Safety Matrix including F-channel drivers in the nested chart of F-channel drivers ("MatrixName")
- MaxMsec – Maximum processing time of the Safety Matrix including F-channel drivers in the nested chart of F-channel drivers ("MatrixName") This output is reset again to 0 on each startup of the Safety Matrix.

The invisible chart connections (inputs and outputs) must not be changed.

Note

After the Safety Matrix has been transferred to the project, the **Tools > Compare Matrix with > Program** function can be used to check whether the project configuration matches the Safety Matrix.

 WARNING
Nested chart of the matrix logic
You must not rename, delete, copy, or move the nested chart of the matrix logic (" @MatrixName ").
You may only change visible parameters, but not the " MatrixSig " parameter.
(SMW-010)

 WARNING
Name of the Safety Matrix top chart
You must not change the name of the Safety Matrix basic chart (visible in SIMATIC Manager).
(SMW-011)

Nested chart of the message blocks ("**AL_Chart**")

This nested chart is optionally created in the Safety Matrix top chart.

Only when a transfer is performed with the "Positioning alarm blocks" option selected are the configured message blocks positioned in this chart.

Alternatively, the message blocks can also be positioned in other charts. You make the corresponding settings in the matrix properties or the individual Cause/Effects in the "Chart assignment" field in the "Alarms" tab.

More information can be found in the following sections:

- "Transferring the Safety Matrix to the program (Page 130)"
- ""Properties" dialog box of the Safety Matrix (Page 88)"
- ""Cause details" dialog box - "Alarms" tab (Page 108)"
- ""Effect details" dialog box - "Alarms" tab (Page 116)"

Nested chart of the preprocessing ("**PP_Chart**")

This nested chart is optionally created in the Safety Matrix top chart.

Only if preprocessing is interconnected for discrete and/or analog input tags is this chart positioned in the Safety Matrix top chart.

You can find additional information on this in section "Preprocessing (Page 56)".

8.3 F-runtime groups and run sequence

Runtime groups following a transfer

When the Safety Matrix is transferred to the project, two or three runtime groups are created:

- The F-blocks of all matrices are positioned in the common "SafetyMatrixXX" F-runtime group, in which "XX" stands for the number of the OB specified beforehand. This F-runtime group contains the transferred code. You must not make any changes here.

Note

The F-runtime group is not changed by the CFC function "Optimize runtime sequence".

- A standard runtime group "m_SafetyMatrixXX" of the respective OB is created for all Safety Matrices and the standard blocks are placed there.
- For each Safety Matrix that has its own F-channel driver a standard run-time group "@MatrixName" is created.

Executable sequence

Each time the Safety Matrix is transferred, an executable sequence within the F-runtime group is ensured automatically. The run sequence is oriented to the data flow. If the run sequence was corrupted (e.g. through a faulty operator intervention), it is automatically corrected during the next transfer and an executable sequence is established once again.

This sequence has the following systematic structure:

Run sequence (with preprocessing)

1. Input channel driver
2. Preprocessing
3. F-blocks of the Safety Matrix
4. Output channel driver

Ensure that the run sequence for the preprocessing blocks is correct.

Note

You must not change the sequence of the Safety Matrix runtime groups.

You must not change the sequence of the blocks in the Safety Matrix runtime groups.

Failure to observe this note will result in F-STOP or prolonged reaction time of the safety program due to additional program cycles.

8.4 Notes on working with CFC

F-blocks are identified by color in the CFC chart. They are highlighted in yellow to indicate that a safety program is involved.

CFC charts and F-runtime groups with F-blocks are yellow and marked with an "F" to distinguish them from the charts and runtime groups of the standard user program.

Optimizing the length of the code area

If you get the following error message when compiling in CFC:

```
F: Maximum code area length (max. 64 KB) has been reached.
```

you must reduce the size of the F-runtime group of the Safety Matrix. You have two different configuration options:

- Move each Safety Matrix to its own F-runtime group.
Proceed as follows: In the runtime sequence of the CFC, move all blocks of a Safety Matrix top chart into a newly created F-runtime group. You can use the name of the Safety Matrix as the name of the new F-runtime group.
- If this is not sufficient, divide up your large Safety Matrix into several smaller Safety Matrices (if possible).

We always recommend that you move large Safety Matrices to their own F-runtime groups. Their F-channel drivers should be created prior to the transfer (e.g. with support of the IEA) and integrated by means of the "Integrate external channel drivers" transfer option.

You can change the position of the preprocessing if it is not part of the Safety Matrix runtime group (e.g. for external and customer-specific F-channel drivers).

Automatically generated charts

The Safety Matrix top chart ("MatrixName") is an automatically created CFC chart.

You must not rename, move or delete this chart and the nested charts it contains in the following table (and the nested charts contained in this table).

Description	Name in the program
Nested chart of the matrix	@MatrixName
Optional: Nested chart of the F-channel drivers	MatrixName
Optional: Nested chart of the message blocks	AL_Chart
Optional: Nested chart of the preprocessing	PP_Chart

8.5 "Selective transfer" dialog box

Overview

You can select one Safety Matrix or multiple Safety Matrices for transfer in this dialog box.

With multiple selection, all Safety Matrices can, for example, be migrated in one step.

The dialog box shows the:

- "Safety Matrix" area
All Safety Matrices of the project listed under "program name" are shown in the table. You can select one Safety Matrix or multiple Safety Matrices for transfer by selecting the associated check box.
The symbol on each Safety Matrix indicates the transfer status. You can find additional information on this in section "Transferring a Safety Matrix (Page 129)".
- "Transfer options" area
You can select one of the following options in this area:
 - "Last transfer settings used for each matrix"
In this case, the selected matrices are transferred with the option "Changes" and the last used transfer options for each matrix.
 - "User-defined options"
You can select additional options with the "Transfer options" button.
Detailed information on the user-defined transfer options is available in the section "Transferring the Safety Matrix to the program (Page 130)".

The transfer options are entered for each selected Safety Matrix in the transfer protocol.

Buttons

- "OK" button
This button starts the transfer process for the Safety Matrices selected in the table. The button is activated if at least one matrix has been selected in the table of the dialog.
- "Cancel" button
The dialog box can be closed with this button without starting a transfer.

8.6 "Selective transfer - Progress" dialog box

Overview

This dialog box shows the progress during the transfer of one Safety Matrix or multiple Safety Matrices.

The dialog box shows the:

- "Safety Matrix" area
An icon for the transfer status and the name of each Safety Matrix selected for the transfer.
- "Currently transferred Safety Matrix" area
The transfer progress of the Safety Matrix currently being transferred.

8.7 "Selective transfer - Log" dialog box

Buttons

- "Cancel transfer" button
You can use this button to cancel the transfer process.
The transfer of the Safety Matrix currently in progress will be completed and the process is canceled afterwards.
The button is activated as long as at least one of the selected matrices must still be transferred.
- "OK" button
The button is deactivated as long as the transfer process is in progress.

8.7 "Selective transfer - Log" dialog box

Overview

This dialog box shows the protocol for the transfer of one Safety Matrix or multiple Safety Matrices.

The log contains:

- Details on the transfer of individual Safety Matrices, for example, the transfer options used for each matrix.
- A summary of the completed transfer.

Toolbar

The floppy disk icon in the toolbar opens a dialog for saving the log.

Buttons

- "OK" button
This button closes the dialog box.

Compiling and downloading

9.1 Compiling and downloading to the F-CPU

Requirements

- All safety matrices of the program to be compiled have been successfully transferred.
- A Safety Matrix of the program to be compiled is opened in the Engineering Tool.
- If operation via Secure Write is to be possible in a Safety Matrix, then the following condition must be met:
In the associated Safety Matrix top chart "MatrixName", the EN_SWC input on the nested chart of the matrix logic ("@MatrixName") must be set to TRUE or interconnected.

Procedure

Compilation of the program

1. Select the **Options > CFC > Compile** menu command.
2. When compiling the Safety Matrix, activate the option "Generate module drivers" in the "Compile program" dialog box.
3. Check the compiler log. Correct the configuration according to the errors displayed in the log.
4. Once the program has been successfully compiled, it can be downloaded to the F-CPU.

Downloading the program to the F-CPU

1. Select the **Options > CPU > Download** menu command.
The "Download to target system" dialog opens.
2. Start the download with the "OK" button.

The logic of the Safety Matrix can now be checked for proper functioning.

9.2 Compiling and downloading to the operator station (OS)

Requirement

- One of the program packages "Engineering AS and OS" or "Engineering OS" must be installed for compiling and downloading to the Operator Station.
- For each Safety Matrix of the project, the Safety Matrix top chart generated during the transfer must be assigned to the desired hierarchy folder in the plant hierarchy (PH). (See *"PCS 7 Process Control System; Engineering System"* configuration manual, section "How to assign objects to the PH". Additional information on this document is available in the preface.)
- All S7 programs assigned to the OS have been compiled.

This ensures a unambiguous mapping of the WinCC faceplates to the Safety Matrices from the ES. See section "Installing (Page 28)".

Configuration and data storage

Configuring is performed exclusively in the ES in PCS 7 and then downloaded to the OS server. All configuration data is managed centrally and stored in the PCS 7 project. Project data, such as pictures, tags, and archives, are stored on the OS server and made available for the OS clients.

The OS server is connected to the plant bus and processes the process data. Operator input during process mode is carried out on the OS clients.

Compiling and downloading to the OS

A project is downloaded using the central "Compile and download objects" function in SIMATIC Manager. Objects represented in this dialog box correspond to the component view in SIMATIC Manager, which means all SIMATIC PC stations that you created in SIMATIC Manager are displayed in this dialog box. In this central location, you make all necessary settings for compiling and downloading. In addition, you specify whether you want to compile and download the entire project or individual operator stations in this dialog box.

Note

Compiling an OS with activated WinCC runtime followed by downloading is not supported on an ES/OS single-user system.

Transferring changes in a Safety Matrix

Changes in a Safety Matrix are not automatically transferred to the operator station. You must transfer the changes by compiling and downloading to the operator station.

Deviations between operator station (Viewer) and F-CPU are signaled in red text above the control bar in online mode:

- "Revision mismatch"
 - The matrix can still be operated.
 - Cause: Different main/minor revision of operator station (Viewer) and F-CPU.
 - Solution: Transfer changes, compile and download the program.
- "Matrix Mismatch"
 - The matrix cannot be operated.
 - Cause: Unambiguous mapping of the matrix in operator station (Viewer) to the one in the F-CPU is not possible.
 - Solution: Transfer changes, compile and download the program.

Special circumstances when downloading single-user systems

If the OS and ES are operated on one computer, you do not need to perform any download operations because all necessary data is already present on the computer.

Additional information

Detailed information regarding "Compiling/downloading to an OS" can be found in the *"Process Control System PCS 7; Operator Station"* configuration manual. Additional information on this document is available in the preface.

Operator control and monitoring

10.1 Overview of operator control and monitoring

Introduction

The "Operator control and monitoring" functionality of the Safety Matrix allows you to monitor and control the behavior of a Safety Matrix during operation. This can take place with the Engineering Tool in online mode as well as with the viewer from a PCS 7 OS.

Requirements for operator control and monitoring

You perform operator control and monitoring on the Engineering Station in online mode of the Safety Matrix Engineering Tool.


You perform operator control and monitoring on the Operator Station via the Safety Matrix Viewer faceplate.

The following requirements apply to operator control and monitoring of a Safety Matrix.

- On the ES (Safety Matrix Engineering Tool)
 - A Safety Matrix is created and transferred to the project.
 - The S7 program containing the Safety Matrix program is compiled and downloaded to the F-CPU.
 - For operator control: The EN_SWC input of the nested chart of the matrix logic ("@MatrixName") for enabling Secure Write is set to TRUE.
 - To execute operation actions, the F-password must be known.
- On the OS (Safety Matrix Viewer)
 - The S7 program containing the Safety Matrix program is compiled and downloaded to the F-CPU.
 - The user(s) with the relevant authorizations are set up. They have the authorization for the required operator controls.
 - The configuration of the Safety Matrix faceplates is downloaded to the OS.
 - For operator control: The EN_SWC input of the nested chart of the matrix logic ("@MatrixName") for enabling Secure Write is set to TRUE.
 - When using OS clients, make sure that no default server is set for tags (in WinCC Explorer select "Server Data," in the shortcut menu select "Default Server" and in the "Configure Default Server" dialog for the "Tags" component select "No Default Server").

Differences between operator control and monitoring on the ES and OS

ES (Safety Matrix Engineering Tool)	OS (Safety Matrix Viewer)
Control bar	Control bar <ul style="list-style-type: none"> Without the "Bypass report" control bar function
Operator control of Safety Matrix using Secure Write transaction in online mode	Operator control of Safety Matrix using Secure Write transaction via faceplate
F-password	User permissions and 2-operator scenario are supported.
Operator inputs that alter the signature of the program (values for delta, limit, and hysteresis)	-
Parameter assignment of upper and lower range limits of F-channel drivers for analog tags	-
Context menus are available	-
Events and messages <ul style="list-style-type: none"> Event log 	Events and messages <ul style="list-style-type: none"> Event log PCS 7 alarm and operation messages in the alarm log

<p> WARNING</p> <p>Independent paths to the display</p> <p>To introduce safety-critical actions, e.g., operations, you must use displays on paths that are independent of each other. The Safety Matrix offers the status displays and the event log for this purpose. The different status display types are not sufficient for this purpose, nor are the displays in online mode of the Safety Matrix Engineering Tool and the displays in the Safety Matrix Viewer.</p> <p>(SMW-012)</p>
--

10.2 Using the Safety Matrix Viewer via "Web Option for OS"

Overview

As of Safety Matrix V6.3, you can operate and monitor the matrices of the Safety Matrix over the intranet/Internet on a PCS 7 Web client with the help of the "PCS 7 Web Option for OS".

The display and operation corresponds to the Safety Matrix Viewer.

You can find a detailed description of the "Web Option for OS" in the Function Manual *"Process Control System PCS 7 Web Option for OS"*. Additional information on this document is available in the preface in the section "Scope of information".

When using "Web Option for OS" in an OS single-user system or OS multi-user system, note the following:

- The notes in the foreword to "Safety concepts and communication".
- The conditions and notes in the Function Manual *"Process Control System PCS 7 Web Option for OS"* in the section "Overview of the Web Option for OS".
 - An OS client that is configured as Web server, for example, can no longer be utilized as an operator station (OS client, SIMATIC BATCH client, etc.) within the PCS 7 system.
 - The Web client cannot be used as an additional PCS 7 station.

Requirements:

- OS:
 - "PCS 7 Web Option for OS" must be installed and set up on the OS.
 - "Web Option for OS" requires WinCC V7.4 or PCS7 V8.2 or higher.
- Web client
 - The "SafetyMatrix_WebPlugin" must be installed on the Web client. The plug-in is available for download and installation after the Web Client has logged onto the Web Navigator Server.
 - DotNet V4.6.1 and VC++ redistributable 2015 must be installed. This software is available from the Safety Matrix product DVD.
 - No Safety Matrix Viewer may be installed on the Web Client.

10.3 Starting online mode in the engineering tool

Introduction

Online operation in the Safety Matrix Engineering Tool allows for monitoring the status of a Safety Matrix that was downloaded to the F-CPU.

Starting and stopping online mode

To start/stop online mode, select the menu command **Monitor > Monitor On/Off**. Alternatively, click on the "Monitor On/Off" icon in the toolbar.

The Safety Matrix Engineering Tool establishes the connection to the Safety Matrix in the F-CPU. The current status of the Causes and Effects is displayed once the connection has been established.

The following example shows the Safety Matrix in online mode. The active Cause "LS100" and the associated, triggered Effects are highlighted in color.

SIMATIC Safety Matrix						
ReactorA						
Ack.driver		View Tags		View status		
Bypass		View events		Clear events		
		Bypass report				
SIF filter <input type="text" value="No filter used"/>						
Input tag	Values	Function	Limit / Trip	Unit	Name	Description
ESD_BUTTON	TRUE		FALSE		ESD_Button	0 = ESD pressed / gedrueckt
PT_110	12.12666	OR	H 18 D 1	bar	PT_110	Reactor pressure 1+2 / Reaktordruck 1+2
PT_111	11.52481					
LS_100	FALSE		FALSE		LS_100	S2/S3 (1 = Level OK / Fuellstand ok)
GT_100	TRUE		FALSE		GT_100	0 = gas detected / Gas erkannt

Output tag	Values	Name	Description
H_ESD	FALSE	H_ESD	0 = ESD active / aktiv
HS_103	TRUE	HS_103	1 = Stirrer start / Rührer an
XV_110	TRUE	XV110	1 = XV110 closed / zu
XV_121	FALSE	XV121	1 = XV121 open / offen
XV_131	FALSE	XV131	1 = XV131 open / offen
XV_140	TRUE	XV140	1 = XV140 closed / zu

10.4 Opening the Safety Matrix faceplates (Safety Matrix Viewer)

Introduction

During runtime, you can start the faceplates of the Safety Matrix Viewer from within WinCC. The faceplates of the Safety Matrix Viewer provide a visual representation of the Safety Matrix.

- The Safety Matrix block icon displays the entire configuration of a Safety Matrix (with Causes, Effects and intersections). The configuration cannot be changed.
- Block icons are also displayed for Causes and Effects.

Faceplates of the Safety Matrix Viewer allow simultaneous operation and monitoring of multiple matrices. In addition, the Safety Matrix Viewer supports simultaneous monitoring of a Safety Matrix on several client stations.

Note

When a WinCC user is changed, the currently opened Safety Matrix faceplate is automatically closed. It can be reopened only with the new authorizations of the logged-on user. If the Safety Matrix faceplate is open during a WinCC user change, e.g. due to changes in WinCC scripts, it must be closed manually before the new user logs on.

Note

If user settings for the block icon of a Safety Matrix are to be retained during OS compilation of an existing picture, you must clear the "Derive block icons from the plant hierarchy" option for this WinCC picture.

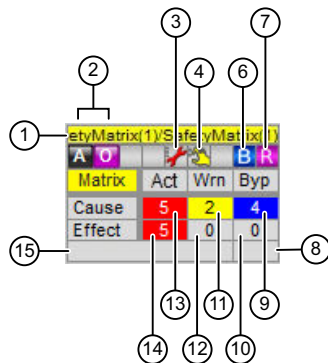
Requirements for generating block icons

Requirement for generating the block icons for the Safety Matrix described below is the corresponding configuration of the message blocks (see section "Message configuration (Page 67)") and transfer of the Safety Matrix with the "Positioning alarm blocks" option selected (see section "Transferring the Safety Matrix to the program (Page 130)").

Opening the Safety Matrix Viewer

1. Log on to the OS as a user with the required permissions.
2. Open the picture containing the desired Safety Matrix block icons. During OS compilation of the Safety Matrix, the corresponding block icons are generated for the configured message blocks F_MA_AL (Safety Matrix, 1 time), F_SC_AL or F_SC_AL2 (1 time for each Cause) and F_SE_AL (1 time for each Effect). It provides the following views:
 - Of the entire Safety Matrix;
 - Of an individual Case with associated intersections and Effects;
 - Of an individual Effect with associated intersections and Causes.
3. Click on the relevant block icon to open the Safety Matrix faceplate with the required view.

Safety Matrix block icon



The Safety Matrix block icon shows the following information for the Safety Matrix:

(1) Technological name of the Safety Matrix message block

(2) Group display

Meaning:

- "A" = Alarm
- "W" = Warning
- "T" = Tolerance
- "S" = Fault
- "F" = Error
- "M" = Preventive maintenance
- "O" = Operator prompt

(3) Display that at least one tag of the matrix has "Bad Quality".

(4) Display that at least one tag of the matrix is simulated.

(6) Display indicating whether there is at least one bypass.

(7) Display indicating whether re-integration of the fail-safe channel drivers is required.

(8) Number of the SIF group (if configured in the "Links" property as described below).

(9) Number of Causes with bypass

(10) Number of effects with bypass

(11) Number of active prewarnings for Causes (only active for current Safety Matrix library)

(12) Number of active prewarnings for effects (only active for current Safety Matrix library)

(13) Number of active Causes

(14) Number of active effects

(15) Description of the SIF group (if configured in the "Links" property as described below)

Attributes for filtering the display of the Safety Matrix faceplate

In the "SIF_Nr" attribute under the "Links" property of the Safety Matrix faceplate, you can enter the number of the safety instrumented function group (SIF group) whose assigned Causes and Effects are to be displayed when the Safety Matrix faceplate is opened. All other Causes and Effects are hidden, including those that are not assigned to an SIF group.

If a SIF group for filtering the display is configured in the "Links" property of the block icon, the description (15) and the number of the SIF group (8) are displayed in the Safety Matrix faceplate.

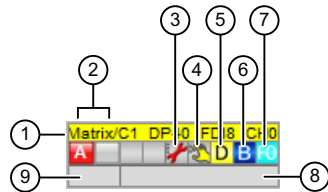
The following table provides an overview of the filter properties:

Designation in "Links" property	Description	Default
SIF_Nr	Numerical default setting of the SIF group in the Safety Matrix	0 = all Causes and Effects are displayed
SIF_Description	Textual default setting of the SIF group in the Safety Matrix	-

Attributes for setting the display colors

The block icon offers you the option of using attributes to change the background and text colors in the display.

Cause block icon



The Cause block icon shows the following information for a Cause:

(1) Technological name of the Cause message block

(2) Group display

Meaning:

- "A" = Alarm
- "W" = Warning
- "T" = Tolerance
- "S" = Fault
- "F" = Error
- "M" = Preventive maintenance
- "O" = Operator prompt

(3) Display that at least one tag has "Bad Quality".

(4) Display that at least one tag of the Cause is simulated.

(5) Shows whether there is a diagnostic interrupt/fault for the Cause

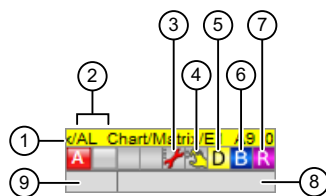
- (6) Display that there is at least one bypass for the Cause.
- (7) Indicates whether the acknowledgment of a First Out alarm is required.
- (8) + (9) Status display and text box

Status	Status display (9)	Display in the text box (8)
Prewarning pending for the Cause	"Yellow"	"Prewarning"
Cause active	"Red"	"Cause active"

Attributes for setting the display colors

The block icon offers you the option of using attributes to change the background and text colors in the display.

Effect block icon



The effect block icon shows the following information for an effect:

- (1) Technological name of the effect message block
 - (2) Group display
- Meaning:
- "A" = Alarm
 - "W" = Warning
 - "T" = Tolerance
 - "S" = Fault
 - "F" = Error
 - "M" = Preventive maintenance
 - "O" = Operator prompt
- (3) Display that at least one tag has "Bad Quality".
 - (4) Display that at least one tag of the effect is simulated.
 - (5) Display that a diagnostic interrupt/fault is pending for the effect.
 - (6) Display that there is at least one bypass for the effect.
 - (7) Display that the effect can be reset.

(8) + (9) Status display and text box

Status	Status display (9)	Display in the text box (8)
Prewarning pending for the effect	"Yellow"	"Prewarning"
Effect tripped	"Red"	"Effect active"

Attributes for setting the display colors

The block icon offers you the option of using attributes to change the background and text colors in the display.

10.5 Safety Matrix faceplate (Viewer)

10.5.1 Layout and views of a faceplate (Viewer)

Overview

A Safety Matrix faceplate consists of the following elements:

- The overview row.
- The so-called views to display different contents.

Overview row in all views

In the so-called overview row, a Safety Matrix faceplate has display and operator control elements, for example, group display, status displays and buttons for selecting the views.

You can find a detailed description on this in section "Layout of the faceplate overview row (Viewer) (Page 156)".

Views

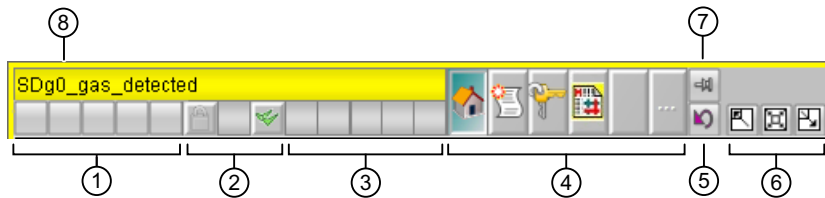
Different views can be selected with the buttons in the overview row:

- Safety Matrix faceplate, "Standard" view (Page 160)
- Safety Matrix faceplate, "Messages" view (Page 161)
- Safety Matrix faceplate, "User rights" view (Page 162)

10.5.2 Layout of the faceplate overview row (Viewer)

Overview

The following figure shows the general arrangement of the overview row elements. Functional dependencies in the display of elements are not taken into account.



The faceplate of the Safety Matrix, Cause and Effect provides the following display and operator control elements:

- (1) Group display
- (2) Lock, acknowledge messages
- (3) Status displays
- (4) Buttons for selecting the views
- (5) Back to the block icon
- (6) Display of the faceplate
- (7) Pin faceplate
- (8) Name of the faceplate

(1) Group display

The group display shows the current status.





The letters used, and the assignment to the specific buttons of the group display, are specified in the "Group display assignment" tab of the "Configure PCS 7 alarm logging" dialog box.

Standard setting:

- "A" = Alarm
- "W" = Warning
- "T" = Tolerance
- "S" = Fault
- "F" = Error
- "M" = Preventive maintenance
- "O" = Operator prompt
- "P" = process message








(2) Unlock/acknowledge messages

You can use the buttons in this area to manage the messages for this matrix.

Button	Description
	<p>You can use this button to lock or unlock block messages.</p> <p>The messages are displayed again in the group display when you enable messages. Messages generated in the locked phase are displayed when you enable the message function.</p> <p>The logged-on user must have authorization to access the area that the faceplate is assigned to so that the button and function are enabled.</p> <p>You can hide this button from specific users / user groups of the plant by using the operating authorizations in the PCS 7-OS. You will find additional information about this in the manual <i>"Process control system PCS 7; OS process control"</i>.</p>
	<p>You can acknowledge all messages from the block instance using this button.</p> <p>You can hide this button from specific users / user groups by using the authorization in the PCS 7 OS. You will find additional information about this in the manual <i>"Process control system PCS 7; OS process control"</i>.</p>

(3) Status displays

The status is displayed in this area.






Status display	Description
	"Good" state
	Display that at least one tag has "Bad Quality".
	Display that at least one tag is simulated.
	Display indicating whether a diagnostic interrupt/fault is pending for the effect.
	Display indicating whether there is at least one bypass.
	Display indicating whether the acknowledgment of a First Out alarm is required.
	<ul style="list-style-type: none"> • Display in the faceplate of the matrix: Re-integration of the fail-safe channel driver is required. • Display in the faceplate of the effect: The effect can be reset.

(4) Buttons for selecting the views

You can use this field to open the various views of a faceplate, or, for Cause/Effect, to switch to the overall view of the matrix.

Left-clicking shows the view in the same window. Right-clicking opens a new window.

The following buttons are available:

Button	Description
	"Standard" view This view also shows the following contents in the matrix display: <ul style="list-style-type: none">• The entire Safety Matrix• A Cause with associated Effects• An Effect with associated Causes
	"Messages" view This view shows the current messages of a Safety Matrix, a Cause or Effect.
	"User rights" view This view shows the current user rights that are in effect for the selected Safety Matrix, the Cause or Effect.
	"Overall view of the matrix" In the faceplate of a Cause/Effect, this button displays the overall view of the Safety Matrix in the faceplate.
	"Other buttons" Use this button to show other buttons. If there are no additional buttons, this button is disabled.

Note

The buttons are disabled when views cannot be selected.




(5) Back to the block icon

Use this button to return to the block icon in the process image of the corresponding faceplate. You use this function when you have pinned a block "(7)", for example, and have changed the process picture afterwards.



(6) Display of the faceplate

Use these buttons to change the display of the faceplate of the Safety Matrix.

Button	Description
	"Minimize" You can use this button to minimize the faceplate to the size of a standard faceplate. If the displayed matrix is smaller than a standard faceplate, then the size is adapted to the displayed matrix.
	"Optimize" You can use this button to optimize the size of the faceplate. The size is adapted to the matrix shown. If the display of the matrix is larger than the working area, the faceplate is adjusted in width or height to the working area, and the scroll bar is displayed.
	"Maximize" You can use this button to maximize the size of the faceplate so that the matrix is displayed over the entire working area.

(7) Pin faceplate

You can pin a faceplate on top of the user interface using this button. This allows you to change to another picture or area without closing the faceplate.



After the button has been clicked and a faceplate pinned, the button is displayed as follows:



A pinned faceplate remains pinned until the faceplate is closed or the button is clicked again.

(8) Name of the faceplate

The name of the faceplate is created from the following:

- For the faceplate of the Safety Matrix, the name is formed from the "Description" field in the properties of the matrix.
- For the faceplate for Cause or Effect, the name is formed from the string of the "M_Name" input of the associated message block F_SC_AL, F_SC_AL2 or F_SE_AL.

10.5.3 Safety Matrix faceplate, "Standard" view

Overview

This view shows the following faceplate contents in the matrix display, depending on the selected faceplate icon:

- The entire Safety Matrix.
- An individual Cause with associated intersections and Effects.
- An individual Effect with associated intersections and Causes.

Example

The following figure shows the "Standard" view of an individual Cause with associated intersections and Effects.

The overview line is not shown in the figure.

You can find information on the "Info" and "Legend" tabs in the section "Overview of the software user interface (Page 41)".

The screenshot displays the SIMATIC Safety Matrix interface for 'ReactorA'. It features a control panel with buttons for 'Ack.driver', 'View Tags', 'View status', 'Bypass', 'View events', 'Clear events', and 'Bypass report'. A 'SIF filter' dropdown is set to '03 - Level SIF'. Below the control panel is a table of input tags, with 'LS_100' selected. To the right, a vertical list shows output tags: 'H_ESD', 'XV_121', and 'XV_131'. A legend on the far right explains the values: 0 = ESD active / aktiv, 1 = XV121 open / offen, and 1 = XV131 open / offen.

Input tag	Values	Function	Limit / Trip	Unit	Name	Description
LS_100	TRUE		FALSE		LS_100	S2/S3 (1 = Level OK / Fuellstand ok)

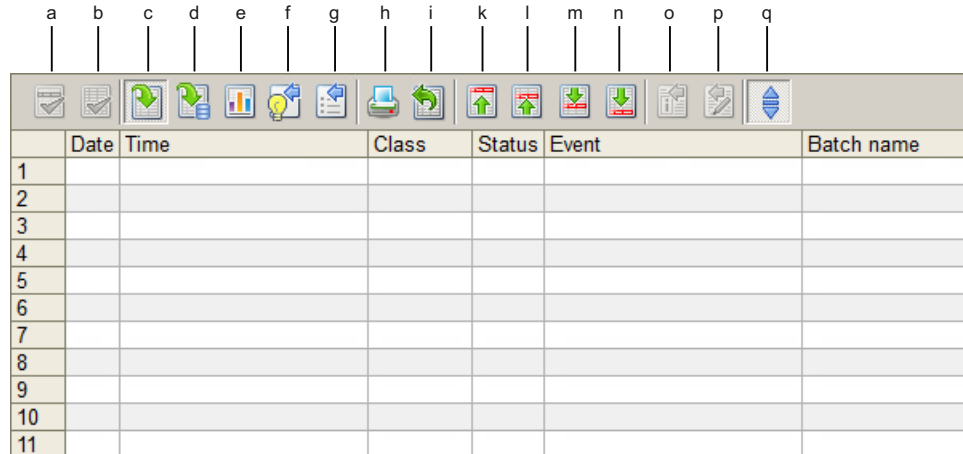
Output tag	Values	Name	Description
H_ESD	TRUE	H_ESD	0 = ESD active / aktiv
XV_121	TRUE	XV121	1 = XV121 open / offen
XV_131	TRUE	XV131	1 = XV131 open / offen

10.5.4 Safety Matrix faceplate, "Messages" view

Overview

This view shows the message window of the faceplate of a Safety Matrix faceplate, a Cause or Effect.

The overview line is not shown here.



Meaning of the buttons:

a	Acknowledge single message
b	Acknowledge all visible messages
c	Display message list
d	Short-term archive list
e	Hit list
f	Display options dialog
h	Selection dialog
i	Print page log
k	Display first message
l	Display previous message
m	Display next message
n	Display last message
o	Info text dialog
p	Comments dialog
q	Autoscroll

10.5.5 Safety Matrix faceplate, "User rights" view

Overview



This view shows the user rights that are in Effect for the logged-on user and the associated Safety Matrix, the Cause or Effect.

The user rights are shown in groups.

- "Enabled operation"
- "Operator roles"
- "Operator control functions"

Icons for the status of the user rights

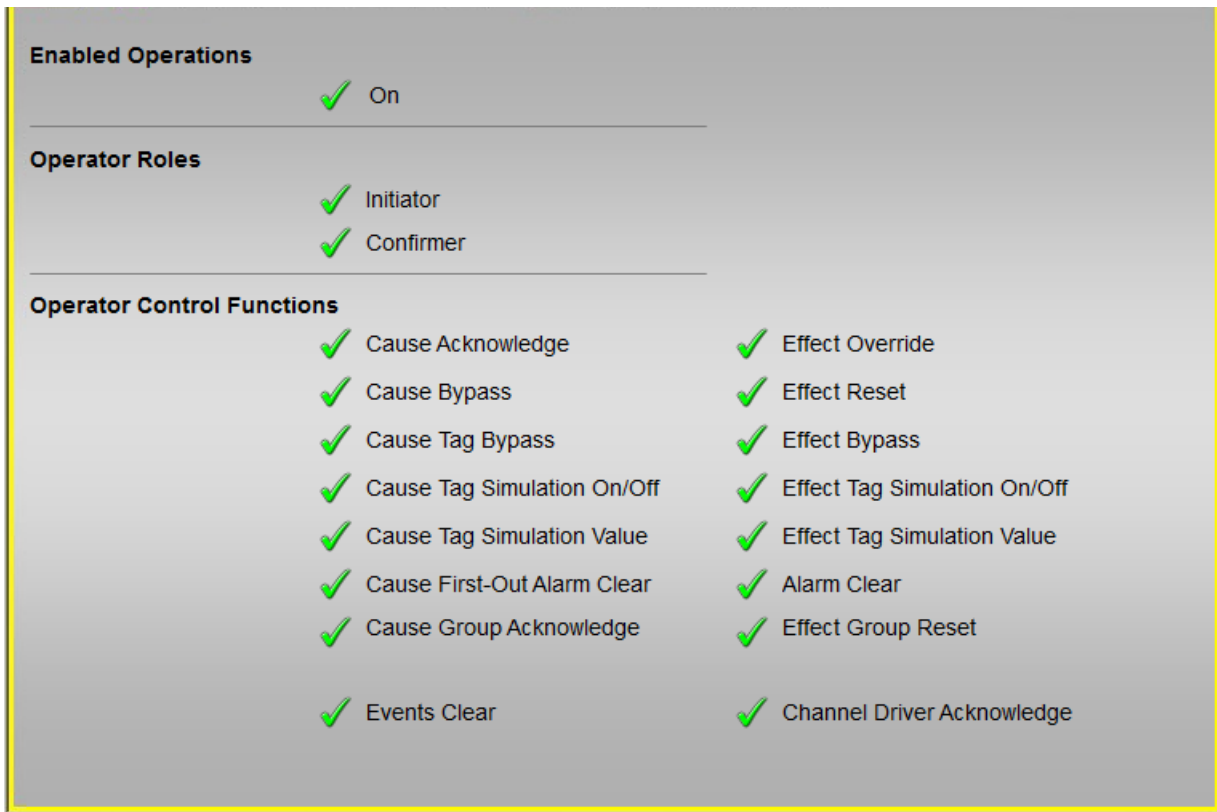
The current status of the user rights is indicated by the following icons.

Icon	Description
	The user has the user right for the listed operator control function or action.
	The user does not have the user right for the listed operator control function or action.

Example

The following figure shows the "User rights" view of the logged-on user.

The overview line is not shown here.



10.6 Monitoring the Safety Matrix (Engineering Tool / Viewer)

10.6.1 Color codes for status display in the Safety Matrix display

Colors

The status of Causes, intersections, and Effects are shown in different colors in online mode of the Safety Matrix.

These colors are preset and can be changed in the "Customize - Colors" dialog box (see section ""Customize" dialog boxes (Page 94)").

Assignment of status and color

Cause:

10.6 Monitoring the Safety Matrix (Engineering Tool / Viewer)

The following table shows the assignment of status and color for a Cause in descending order of priority.

Priority	Status	What is shown in color?	Color used (option in the "Customize - Colors" dialog box)
1	First Out active	Groups	"First Out"
2	Attention / acknowledgment required	Cause number	"Attention Required"
3	Cause trip requested	Cause number	"Active - Alarm profile"
4	Bypass active	All except Cause number and input tags	"Bypass, simulation"
5	Inhibit active	All except Cause number and input tags	"Inhibit"
6	Tag simulation active	Input tag	"Bypass, simulation"
7	Bad Quality with Degraded Voting	Input tag	"Attention Required"
8	Tag active	Input tag	"Active - Alarm profile"
9	Cause tripped	All apart from input tag	"Active - Alarm profile"
10	Tag prewarning active	Input tag	"Prewarning"

Note

If the function type of a Cause is "Comment only", no input tag values are displayed and there is no color.

Effect:

The following table shows the assignment of status and color for an effect in descending order of priority.

Priority	Status	What is shown in color?	Color used (option in the "Customize - Colors" dialog box)
1	Attention/channel driver acknowledgment required	Effect number	"Attention Required"
2	Bypass active	All except effect number	"Bypass, simulation"
3	Tag simulation active	Output tag	"Bypass, simulation"
4	Mask active	All except effect number	"Masking"
5	Prewarning override active	All except effect number	"Prewarning"
6	Override active	All except effect number	"Override"
7	OK to reset	All except effect number	"OK to reset"

Priority	Status	What is shown in color?	Color used (option in the "Customize - Colors" dialog box)
8	Override error	Effect number	"Active - Alarm profile"
9	Tag active	Output tag	"Active - Alarm profile"
10	Effect active	All (color depends on alarm profile)	"Active - Alarm profile"

Note

If the function type of an effect is "Comment only", no output tag values are displayed and there is no color.

10.6.2 Status displays for selected Cause/Effect

"Display status" monitoring function in the control bar

The "Display status" button is available when a Cause or an Effect is selected. Click this button to open the "Cause status" or "Effect status" display window. These display windows contain information about the selected Cause or Effect.

The check box in front of the option indicates when the associated option is selected.

Cause status descriptions

Option/field	Description	Entry in event log
"Cause" area		
Cause active	Indicates that all configured criteria are satisfied for the active status (status, function logic, time delays, etc.).	X
Hysteresis active	Indicates that an active Cause no longer fulfills its trip condition but is still within the configured dead band.	
Inhibit active	Indicates that the inhibit tag is active.	X
Bypass active	Indicates that a bypass is active.	X
Soft bypass active	Indicates that the current bypass was set by means of an operator input.	X
Ackn. Cause required	Indicates that the Cause is held in active state until it is acknowledged by the user and the tripping condition is no longer met.	X
Trip requested	Indicates that linking of the tags according to the function logic is met. The active status of the Cause can be influenced by the configured time behavior or bypass, inhibit, and interlock functions.	X

10.6 Monitoring the Safety Matrix (Engineering Tool / Viewer)

Option/field	Description	Entry in event log
Degraded Voting active	Indicates that Degraded Voting is active in this Cause.	X
First Out active	Indicates that a First Out alarm is active in this Cause.	X
Discrepancy error (tag x – tag Y)	Indicates that the calculated tag delta (X - Y) has exceeded the configured delta value, and has not yet reached the "delta value - hysteresis".	X
Input trip alarm	For a Cause with multiple tags this status indicates that at least one tag has reached the trip condition and requests tripping, but not all conditions for tripping have been met yet.	X
Illegal Config	Error during internal diagnostic check of the FB (internal error; remedy: transfer, compile, and download again, if necessary).	
SDF error	Indicates that the Safety Matrix has detected an error in the safety data format in the DB. This error always causes the safety program to go to F-STOP.	X
Configuration changed	Shows that the Limit, Delta, or Hysteresis were changed via Secure Write.	
Bypass prewarning	Indicates that the prewarning is active for a timed soft bypass.	X
Bypass error: Timeout	Indicates that a soft-bypass was not removed within the configured time.	X
Maintenance operations reset error	Indicates that an error has occurred during reset of maintenance operations.	X
"Timed status" area		
• ON delay active	Indicates that a configured ON delay is active. The "active" bit is deleted after the time has expired.	
• OFF delay active	Indicates that a configured OFF delay is active. The "active" bit is deleted after the time has expired.	
• Time control active	Indicates that a configured time control is active. The "active" bit is deleted after the time has expired.	
• Associated "Time remaining" output field	Indicates the current time remaining of the following functions: <ul style="list-style-type: none"> • ON delay active • OFF delay active • Timed Cause active 	
• Timed soft bypass active	Indicates that a timed soft bypass is active for the tag.	
• Associated "Time remaining" output field	Shows the current remaining time of the active, timed soft bypass (status is displayed in the "Cause" area)	
"Tag x" area		
Ackn. channel driver required	Indicates that an acknowledgment of the F-channel driver is required.	
Bad Quality	Indicates that the F-channel driver of the configured tag signals a bad signal state.	X
Channel error	Indicates that the F-channel driver of the configured tag signals a channel error.	X
PROFIsafe error	Indicates that the F-channel driver of the configured tag signals a PROFIsafe failure that is caused by the F-module driver.	X
Loss of redundancy	Indicates that the redundancy for redundant input modules is no longer given.	
Value	Displays the tag value.	
Trip prewarning	Indicates that the configured tag meets the condition for the limit prewarning.	X
Trip requested	Indicates that the configured tag meets the condition for requesting a trip. This status includes the Energize-to-trip setting of the tag.	X

Option/field	Description	Entry in event log
Simulation active	Indicates that the tag is simulated.	X
Soft bypass active	Indicates that a soft bypass is active for the tag.	X


Effect status descriptions

Option/field	Description	Entry in event log
"Effect" area		
Effect active	Indicates that all configured criteria are satisfied for the active status (intersection status, bypass, etc.).	X
Mask active	Indicates that a mask is active.	X
N intersections	Indicates that an interconnected intersection type "N - Not Stored" is active.	
S intersections	Indicates that an interconnected intersection type "S - Stored" is active.	
V intersections	Indicates that an interconnected intersection type "V - Overridable" is active.	
R intersections	Indicates that an interconnected intersection type "R - Resettable and overridable" is active.	
Bypass active	Indicates that a bypass is active.	X
Soft bypass active	Indicates that the current bypass was set by means of an operator input.	X
Pass-through active	Indicates that "Process data pass through" is active in the effect logic.	X
Override input	Indicates that the effect is currently being overridden.	
OK to override	Indicates that the effect is ready to be overridden.	
OK to reset	Indicates that the effect is ready to be reset.	
Effect latched	Indicates that the effect is latched and must be reset.	X
Prewarning override	Indicates that the effect meets the time prewarning condition for the maximum override time.	X
Override failed: Cause	Indicates that the Effect override has been interrupted because a new Cause has become active.	X
Override failed: Timeout	Indicates that overriding of the effect was interrupted due to a timeout.	X
Illegal Config	Error during internal diagnostic check of the FB (internal error; remedy: transfer, compile, and download again, if necessary).	
SDF error	Indicates that the Safety Matrix has detected an error in the safety data format in the DB. This error always causes the safety program to go to F-STOP.	X
Maintenance operations reset error	Indicates that an error has occurred during reset of maintenance operations.	X
"Timed status" area		
• Output delay active	Indicates that an output delay is active.	
• Override active	Indicates that an override function is active.	X
• "Time remaining" output field	Indicates the current time remaining by which the effect can still be delayed. The times of the following functions are displayed: <ul style="list-style-type: none"> • Output delay active • Override active 	
"Tag x" area		

Option/field	Description	Entry in event log
Ackn. channel driver required	Indicates that an acknowledgment of the F-channel driver is required.	
Bad Quality	Indicates that the F-channel driver of the configured tag signals a bad signal state.	X
Channel error	Indicates that the F-channel driver of the configured tag signals a channel error.	X
PROFIsafe error	Indicates that the F-channel driver of the configured tag signals a PRO- FIsafe error that is caused by the F-module driver.	X
Loss of redundancy	Indicates that the redundancy for redundant input modules is no longer given.	
Value	Indicates the current status of the output tag.	
Simulation active	Indicates that the tag is simulated.	X

10.7 Operating

While all control bar functions are available without restrictions during online operation of the Safety Matrix Engineering Tools after the passwords for the safety program and the F-CPU have been entered, the available functions in the Safety Matrix Viewer on the PCS 7 OS depend on the assignment of the functions to a permission level at the block icon and the user permissions configured accordingly in the PCS 7 OS.

<p> WARNING</p> <p>Operator authorization for standard operator</p> <p>Make sure that you do not assign an operator authorization for the Safety Matrix to a standard operator, for example, Autologin.</p> <p>(SMW-013)</p>

10.7.1 Initiator and confirmer permission (Viewer)

2-operator scenario

During configuration of the Safety Matrix in the PCS 7 OS, you can select a 2-operator scenario (double-check principle). Two operator roles are defined for this purpose: initiator and confirmer. With the corresponding "Initiator" or "Confirmer" attributes, you determine which authorization the PCS 7 OS operator must have in order to be able to perform the operating functions on the Safety Matrix Viewer as an initiator or as a confirmer:

- Initiator permission: the operator may start an operation.
- Confirmer permission: the operator may confirm an operation.

If the confirmer permission and initiator permission is set to 0 (= no access protection), the 2-operator scenario is not being used. In this case, individual functions are governed solely by the permission level specified for the respective operator function.

In addition to the initiator and/or confirmer permission, users must have the specified permission level for each operator function to be performed.

Procedure

You configure the assignment of the Safety Matrix functions to a permission level in the PCS 7 OS in the "Properties" dialog box of the Safety Matrix, "Permissions OS" tab (see section ""Properties" dialog box of the Safety Matrix (Page 88)").

Note

The permission levels configured in the "Permissions OS" tab in the Safety Matrix must match the permission levels in the "User Administrator" editor of the PCS 7 OS; otherwise, no operator control function is possible in the Safety Matrix.

Setting up user permissions for operators

Create the following users based on whether the controls are to be operated by two operators or by one operator only:

Operation with two operators

If a Safety Matrix is to be operated by two operators, create two users:

- The initiator starts the Safety Matrix operation via Secure Write. This user must have the permission that is assigned to the "Initiator" attribute in the properties of the Safety Matrix. However, the initiator does not have permission to confirm the operation.
- The confirmer verifies and confirms the operation. This user must have the permission that is assigned to the "Confirmer" attribute in the properties of the Safety Matrix. However, the confirmer does not have permission to initiate the operation.

Operation with one operator

- If only one operator is to perform all of the operation steps, but with initiator/confirmer access protection, create a user who has both authorizations, which are assigned to the "Initiator" and "Confirmer" attributes in the properties of the Safety Matrix.

You create the users and their individual permission levels in the PCS 7 OS with the "User Administrator" editor.

Activating the OS

Activate the runtime system of the PCS 7 OS, e.g. by selecting **File > Activate** in WinCC Explorer.

Once the WinCC Runtime system is activated, the hierarchy levels appear as buttons in the runtime system of the OS. Click the button to display the block icons for this level.

Deactivating the OS

Close the Safety Matrix Viewer before deactivating the OS runtime system.

Deactivate the runtime system of the PCS 7 OS, e.g. by selecting **File > Deactivate** in WinCC Explorer.

See also

Chapter "Transaction for Secure Write (Page 170)"

10.7.2 Secure Write

10.7.2.1 Transaction for Secure Write

What is a transaction for Secure Write?

You perform a transaction for operation of a Safety Matrix via Secure Write in online mode of the Engineering Tool or on the OS by means of the Safety Matrix faceplate. The transaction consists of a sequence of operations that can be performed by one or two operators.

The transaction must be completed within a time interval specified by the user (timeout). If the transaction is not completed within this time interval, it is automatically canceled.

The time interval can be set in the "Properties" dialog box of the Safety Matrix, "Parameter" tab. The default setting is 60 s.

Requirements

- The Safety Matrix program is compiled and downloaded to the F-CPU, and the F-CPU is in RUN mode. See section "Compiling and downloading to the F-CPU (Page 143)".
- Operator input via the OS: The configuration of the faceplates is downloaded to the OS. See section "Compiling and downloading to the operator station (OS) (Page 144)".
- The operator(s) with the relevant permissions are set up. See section ""Properties" dialog box of the Safety Matrix (Page 88)".
- The EN_SWC input of the nested chart of the matrix logic for enabling Secure Write is set to TRUE. See section ""Properties" dialog box of the Safety Matrix (Page 88)".
- If operation is by means of the OS, you must prevent the OS user interface from being closed as is customary in *PCS 7* (by blocking the key combination).

General information

Note

You cannot make any operations in the Safety Matrix Viewer V6.3 that change the signature of the safety program, which means the values for the permitted delta, limit and hysteresis cannot be changed. The corresponding dialog is only available in the Safety Matrix Engineering Tool.

WARNING

The "Secure Write" functionality allows changes to the safety program to be made during RUN mode

As a result, the following safety measures are required:

- Make sure that changes that could compromise plant safety cannot be made. You can use the provided #EN_SWC input for this purpose, for example, by controlling it with a key-operated switch or on a process-specific basis via the safety program.
- Make sure that only authorized persons can make changes. You must not solely rely on the configured permissions here.

Examples:

- Control the EN_SWC input with a key-operated switch.
- Set up access protection at operator stations where the "Secure Write" function can be performed.

(SMW-014)

WARNING

Operating a Safety Matrix

Take organizational measures to ensure that only one transaction at a time can be initiated or confirmed for a Safety Matrix.


(SMW-015)


WARNING


Checking the technological assignment

When opening the faceplate, make sure that the technological assignment in the top line is appropriate for the environment in which the block icon was placed. In this way you make sure you are operating the correct Safety Matrix.

(SMW-018)

 WARNING
Secure Write: checking correct functioning of the operation
You must check the correct functioning of the operation. Immediately following an operation, the following must be true:
<ul style="list-style-type: none">• The expected reaction of the operation can be recognized as a change in the status display. or• The status of this operation corresponds to the entries in the "Events" report of the Safety Matrix.
(SMW-016)

 WARNING
Checking a transaction
As an operator, you may only accept the awaited information. If there are inconsistencies, you must cancel the transaction. You may only confirm the transaction assigned to you organizationally.
(SMW-017)

 WARNING
Cancellation of a transaction
You must always anticipate the cancellation of a transaction through unforeseeable events, e.g. communication errors; the safety of the system must not be endangered as a result.
(SMW-019)

Operator roles for Secure Write

A transaction can be performed by an individual operator who starts, verifies, and confirms the operation. However, a transaction can also be performed by two operators on the OS. One operator starts the operation (initiator) and the second operator checks and confirms it (confirmer).

Sequence of a transaction for Secure Write

A transaction consists of multiple dialog boxes that must be run through one after the other. After you have operated a dialog box, wait time may occur (depending on the load of the server or the communication channel to the F-CPU) until the follow-up dialog box opens.

To make this operation more transparent, a dialog box is opened at the start of each transaction and remains open until the end of the transaction. Additionally, this dialog box provides additional information such as the time remaining for the transaction and error messages.

Causes for the "Data error" message for aborted transaction:

An unsuccessful transaction can be caused by data corruption or the expiration of the time allowed for the transaction. Check the "Events" report of the Safety Matrix to draw conclusions about the cause.

10.7.2.2 Variants of Secure Write

Overview

Secure Write is available in 3 versions:

- Complete Secure Write (in online mode of the Safety Matrix Engineering Tool or from the PCS 7 OS via the Safety Matrix Viewer):
The operator has both initiator and confirmer authorizations, and can perform the transaction on their own.
- Secure Write for initiator (only via Safety Matrix Viewer on the PCS 7 OS):
If the operator has the initiator authorization, he/she can start the transaction as an initiator.
- Secure Write for confirmer (only via Safety Matrix Viewer on the PCS 7 OS):
If the operator has the confirmer authorization, he/she can confirm the transaction as a confirmer. Only after this confirmation does the operation in the safety program take effect.

10.7.3 Operations in the Safety Matrix

10.7.3.1 Operating over the control bar (Engineering Tool / Viewer)

Introduction

The following operator controls are available in online mode of the Safety Matrix Engineering Tool and in the Safety Matrix Viewer:

- Control bar
The control bar is described below.
- "SIF Filter" standard table
Using the "SIF Filter" standard table, the display of the Causes and Effects can be filtered for single or multiple safety instrumented function groups (SIF groups).
You can find additional information on this in section ""SIF Filter" drop-down list (Page 47)".

Dependency of available functions

For working with a Safety Matrix, the control bar is available in online mode of the Safety Matrix Engineering Tool and in the Safety Matrix Viewer. Once a Cause or an Effect is selected in the Safety Matrix, the control bar functions available for the Cause or Effect are displayed as control bar buttons. Control bar functions for which permission does not exist are desensitized.

Which functions can be used depends on the following factors:

- The selected element
- The configuration of the element

10.7 Operating

- The status of the element
- Operator permissions for the PCS 7 OS

The following example shows the Safety Matrix with a control bar, a highlighted, tripped Cause, and the associated tripped Effect.

SIMATIC Safety Matrix						
ReactorA						
<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="display: flex; gap: 10px;"> <div style="border: 1px solid gray; padding: 2px;">Ack.driver</div> <div style="border: 1px solid gray; padding: 2px;">View Tags</div> <div style="border: 1px solid gray; padding: 2px;">View status</div> </div> <div style="display: flex; gap: 10px;"> <div style="border: 1px solid gray; padding: 2px;">Bypass</div> <div style="border: 1px solid gray; padding: 2px;">View events</div> <div style="border: 1px solid gray; padding: 2px;">Clear events</div> <div style="border: 1px solid gray; padding: 2px;">Bypass report</div> </div> </div>						
SIF filter <input type="text" value="No filter used"/>						
Input tag	Values	Function	Limit / Trip	Unit	Name	Description
ESD_BUTTON	TRUE		FALSE		ESD_Button	0 = ESD pressed / gedrueckt
PT_110 PT_111	12.12666 11.52481	OR	H 18 D 1	bar	PT_110	Reactor pressure 1+2 / Reaktordruck 1+2
LS_100	FALSE		FALSE		LS_100	S2/S3 (1 = Level OK / Fuellstand ok)
GT_100	TRUE		FALSE		GT_100	0 = gas detected / Gas erkannt

Output tag	Values	Name	Description
H_ESD	FALSE	H_ESD	0 = ESD active / aktiv
HS_103	TRUE	HS_103	1 = Stirrer start / Rührer an
XV_110	TRUE	XV110	1 = XV110 closed / zu
XV_121	FALSE	XV121	1 = XV121 open / offen
XV_131	FALSE	XV131	1 = XV131 open / offen
XV_140	TRUE	XV140	1 = XV140 closed / zu

Description of control bar functions

Control bar functions	Function	Required permission level ^{*1)}
View events	The event log enables the Safety Matrix to store event-related information, e.g., based on status changes of a Cause and Effect. A maximum of 100 events are logged in a circular log. This ensures that the latest events are always displayed. Events of the Safety Matrix can be read from the F-CPU with the "View events" function and displayed in the Engineering Tool in the Reports window or in the Viewer. You can find additional information on which user actions and diagnostic events are recorded in section "Status displays for selected Cause/Effect (Page 165)".	-
View status	This button is available when a Cause or an Effect is selected. Click this button to open the "Cause status" or "Effect status" display window. This display window contains information about the selected Cause or Effect. You can find additional information on this in section "Status displays for selected Cause/Effect (Page 165)".	-
View tags	A click on this button shows a dialog box in which the values of Cause or Effect tags can be viewed. To simulate a Cause or Effect tag, you need the corresponding user permission.	-
Acknowledge Cause	The button is available when the selected Cause is active and is configured without automatic acknowledgment. An acknowledgment request is displayed and the Cause remains active until this "Acknowledge Cause" button is clicked and the trip conditions that have activated the Cause are no longer met. You can also acknowledge multiple Causes that have to be acknowledged in one step. <ul style="list-style-type: none"> To do so, the user must have the permission level "Cause group acknowledgment". To select the Causes, a row area can be selected in the current matrix display. 	"Cause Acknowledge" "Cause group acknowledgment"
Clear First Out	A color change indicates which Cause tripped the associated First Out Alarm Group first. This first Cause is highlighted in the selected color until the Cause and the "Clear First Out" button are clicked.	"Cause First-Out Alarm Clear"
Bypass	This button sets a bypass for a Cause or Effect, so that the Cause or Effect will not be triggered.	"Cause Bypass" or "Effect Bypass"
Clear events	This "Clear events" function deletes the event log in the F-CPU.	"Events Clear"
Clear alarm	The "Clear alarm" function becomes active if the number of a Cause or Effect has been selected for which an alarm is pending. Sample Causes of the alarm: <ul style="list-style-type: none"> The configured maximum override time has elapsed. The configured maximum bypass time has elapsed. 	"Clear alarm"
Reset/Override effect	This button is either labeled "Reset effect" or "Override effect", depending on the status of the selected effect and intersection type.	-

Control bar functions	Function	Required permission level *1)
<ul style="list-style-type: none"> Reset effect 	<p>If an Effect is tripped by an intersection type S (stored) or R (resettable and overridable), it remains active even if it is no longer tripped by the Cause. The effect can be reset if it is no longer tripped. To do so, click the "Reset effect" button.</p> <p>This function is only available when a reset is possible for the selected effect (shown in the selected color) and no reset/override tag is configured.</p> <p>You can also reset multiple tripped effects in one step.</p> <ul style="list-style-type: none"> To do so, the user must have the permission level "Effect group reset". To select the effects, a column area can be selected in the current matrix display. 	<p>"Reset effect"</p> <p>"Effect group reset"</p>
<ul style="list-style-type: none"> Override effect / Stop override 	<p>If an effect is tripped by an intersection type V (overridable) or R (resettable and overridable), the output tags of the effect can be set to the operating value even though the effect is still pending. This is referred to as the override function.</p> <p>The override function can only be activated with this button if no reset/override tag is configured.</p> <p>The effect is disabled for the set duration with a click on the "Override effect" button.</p> <p>After activation of the override function, the button is renamed to "Stop override".</p> <p>Override is stopped manually by clicking on the "Stop override" button.</p> <p>Note</p> <p>The duration of the override function cannot exceed the maximum time specified under options ("Override maximum time"). If the time is exceeded, an alarm is tripped and override is ended.</p> <p>If another Cause (that is interconnected with the Effect) becomes active during the override time, the override function stops immediately and an alarm is likewise triggered.</p>	<p>"Override effect"</p>
Acknowledge driver	<p>This button allows you to perform the necessary reintegration of the F-channel drivers during an F-startup after fault elimination.</p>	<p>"Acknowledge channel driver"</p>
Display colors	<p>With this button, you can display in the Safety Matrix Viewer the assignment of status or alarm profile to color in the Safety Matrix.</p>	-

*1) You can find additional information on operator functions and permissions in section ""Properties" dialog box of the Safety Matrix (Page 88)".

"Bypass report" control bar function

The "Bypass report" control bar function is only available in the engineering tool.

The "Bypass report" function generates a list with all Causes and Effects for which bypasses are set up and with all currently simulated tags. The results are displayed in the Reports window in the "Maintenance operations" tab.

Note

Simultaneous soft bypass and hard bypass

If a soft bypass and a hard bypass are active for a Cause or Effect, only the soft bypass is listed in the bypass report.

See also

Initiator and confirmer permission (Viewer) (Page 168)

Secure Write (Page 170)

10.7.3.2 Example: Reset effect with two operators (Viewer)

Operation with two operators

When resetting effects on the PCS 7 OS, you can configure a 2-operator scenario. Two operators with different permissions are required.

The sections below describe the necessary transaction steps for the two operators "Initiator" and "Confirmer".

Note

Sequence of the transaction with only one operator

The sequence is similar as when the operation is carried out with two operators, but one operator can perform all the steps. The difference is that there is no longer a wait for the "Confirmer". Instead, the operator can verify and confirm the operator input immediately. In addition to the initiator and/or confirmer permission, the operator must have the permission level for each operator function to be performed.

Requirements

- In addition to the initiator and/or confirmer permission, the operators must have the specified permission level for each operator function to be performed.
 - The "Effect Reset" permission level is required for resetting effects.
 - For resetting one or more effects, the "Effect group reset" permission level is required.
- The "Reset effect" function is only possible if an effect was tripped by an intersection type S (stored) or R (resettable and overridable). In addition, reset must be possible for the selected effect (in the configured color, e.g. in green) and no reset/override tag must be configured. You can find additional information on this in section "Operating over the control bar (Engineering Tool / Viewer) (Page 173)".

Initiator: Start operation

1. Log on to the OS as a user with the initiator permission and the specified permission level "Effect Reset" or "Effect group reset".
2. Open the screen in which the desired Safety Matrix block icon is contained.
3. Click the Safety Matrix block icon to open the faceplate.

4. Select the effect you want to reset.
This requires that the effect be shown in the configured color, e.g. in green (= reset possible).
Alternatively, a group reset of effects is possible with a multiple selection of tripped effects.
5. Click the "Reset effect" button in the control bar.
Result: The Safety Matrix Viewer sends the command to the Safety Matrix and reads the read back values. The timeout monitoring for the transaction is started.
6. The "Initiate Transaction" dialog box is displayed.
If multiple effects were selected, they are all displayed in a list in the "Transaction" area.
Check whether the specified change corresponds to the desired operation.
 - If it does, select the "Operation checked and to be activated" check box and click the "OK" button.
 - If it does not match, you must click "Cancel".

Result: The transaction for the initiator is now stopped; it can be continued by a confirmer.

Operation by the initiator is entered in the PCS 7 operation list and in the Safety Matrix event log.

Note

Depending on the operator control to be performed, you may be prompted to enter a reason that is logged together with the result.

Confirmer: Confirm operation

1. Log on to the OS as user with the Confirmer permission and the specified permission level "Reset effect".
You can be logged on to a second OS or to the same OS as the Initiator.
2. Open the screen in which the desired Safety Matrix block icon is contained.
3. Click the Safety Matrix block icon to open the faceplate.
4. Click the "Confirm" button in the control bar.
5. The "Confirm Transaction" dialog box is displayed.
If multiple effects were selected, they are all displayed in a list in the "Transaction" area.
Check whether the specified change corresponds to the desired operation.
 - If it does, select the "Operation checked and to be activated" check box and click the "OK" button.
 - If it does not match, you must click "Cancel".

Result

If the transaction is completed within the specified time interval, the successful operation within the Safety Matrix can be seen in the status display (e.g. color change).

Operation by the confirmer is also entered in the PCS 7 operation list and in the Safety Matrix event log.

10.7.3.3 Example: Acknowledge Cause with two operators (Viewer)

Operation with two operators

When acknowledging Causes on the PCS 7 OS, you can configure a 2-operator scenario. Two operators with different permissions are required.

The sections below describe the necessary transaction steps for the two operators "Initiator" and "Confirmer".

Note

Sequence of the transaction with only one operator

The sequence is similar as when the operation is carried out with two operators, but one operator can perform all the steps. The difference is that there is no longer a wait for the "Confirmer". Instead, the operator can enter a reason for the operation immediately and confirm the operator input. In addition to the initiator and/or confirmer permission, the operator must have the permission level for each operator function to be performed.

Requirements

- In addition to the initiator and/or confirmer permission, the operators must have the specified permission level for each operator function to be performed.
 - The "Cause Acknowledge" permission level is required for acknowledging a Cause.
 - For acknowledging one or more Causes, the "Cause group acknowledgment" permission level is required.
- The "Acknowledge Cause" function is only possible when the selected Cause is active and the "Auto acknowledge active Cause" option is not activated in the "Options" tab of the Cause properties.

In addition, an acknowledgment request must be displayed in the row of the Cause. You can find additional information on this in section "Operating over the control bar (Engineering Tool / Viewer) (Page 173)".

Initiator: Start operation

1. Log on to the OS as a user with the initiator permission and the specified permission level "Cause Acknowledge" or "Cause group acknowledgment".
2. Open the screen in which the desired Safety Matrix block icon is contained.
3. Click the Safety Matrix block icon to open the faceplate.
4. Select the Cause you want to acknowledge.

This requires that an acknowledgment request be displayed.
Alternatively, a group acknowledgment of Causes is possible with a multiple selection of active Causes.

5. Click the "Acknowledge Cause" button in the control bar.
Result: The Safety Matrix Viewer sends the command to the Safety Matrix and reads the read back values. The timeout monitoring for the transaction is started.
6. The "Initiate Transaction" dialog box is displayed.
If multiple Causes were selected, they are all displayed in a list in the "Transaction" area. Check whether the specified change corresponds to the desired operation.
 - If it does, select the "Operation checked and to be activated" check box and click the "OK" button.
 - If it does not match, you must click "Cancel".

Result: The transaction for the initiator is now stopped; it can be continued by a confirmer.

Note

Depending on the operator control to be performed, you may be prompted to enter a reason that is logged together with the result.

Confirmer: Confirm operation

1. Log on to the OS as user with the Confirmer permission and the specified permission level "Cause Acknowledge".
You can be logged on to a second OS or to the same OS as the Initiator.
2. Open the screen in which the desired Safety Matrix block icon is contained.
3. Click the Safety Matrix block icon to open the faceplate.
4. Click the "Confirm" button in the control bar.
5. The "Confirm Transaction" dialog box is displayed.
If multiple Causes were selected, they are all displayed in a list in the "Transaction" area. Check whether the specified change corresponds to the desired operation.
 - If it does, select the "Operation checked and to be activated" check box and click the "OK" button.
 - If it does not match, you must click "Cancel".

Result

If the transaction is completed within the specified time interval, the successful operation within the Safety Matrix can be seen in the status display (e.g. color change).

Operation by the initiator is also entered in the PCS 7 operation list and in the Safety Matrix event log.

See also

Operating (Page 168)

10.7.3.4 Perform maintenance changes (Engineering Tool / Viewer)

Introduction

You can make the following maintenance changes in online mode of the Safety Matrix Engineering Tool or from the PCS 7 OS via the Safety Matrix Viewer.

Online mode of the Safety Matrix Engineering Tool	Safety Matrix Viewer
Simulate value of a Cause or Effect tag	Simulate value of a Cause or Effect tag
Set soft bypass for an input tag of a Cause	Set soft bypass for an input tag of a Cause
Change values for limit, hysteresis, and delta for analog input types	-
Change high and low range boundary of F-channel drivers for analog input tags ^{**1)}	-

^{**1)} A Secure Write transaction is not used for this operation.

Simulate value of a Cause or Effect tag

You can simulate the value of a Cause or Effect tag in online mode of the Safety Matrix Engineering Tool or from the PCS 7 OS via the Safety Matrix Viewer.

Note

In addition to the initiator and/or confirmer permission, operators on the PCS 7 OS must have the specified permission level for each operator function to be performed.

Procedure

1. Double-click the desired Cause/Effect, "Value" column, or click the "View Tags" button in the control bar for the selected Cause/Effect.
2. Select the check box labeled "Enable maintenance changes" in the "Values" tab of the "Display Tags" dialog box.
3. Click the (simulation) "Start" button for the relevant tag.
Result: A Secure Write transaction is started for starting the simulation. Either the current pending process data or the configured simulation value is used as the simulation value, depending on your configuration.
4. If you would like to change the value of the simulated tag, enter the desired value for the relevant tag in the "Simulation value" field (maximum of 7 characters, plus decimal separator and sign).
For analog values, also make sure to comply with the range limits indicated.

Note

The "V_MOD" column displays the analog or discreet input value received from the F-I/O (available in "S7 F Systems Lib" V1_3 and higher). If communication with the F-I/O is not possible or if a user acknowledgment has not yet occurred following an error, "0.0" is displayed.

5. Click on the "Write" button for the respective tag.
Result: A Secure Write transaction is started for writing the values.
 6. Click the (simulation) "Stop" button for the relevant tag to stop the simulation.
-

Note

You must take the following into consideration when simulating a tag:

- When the "Mutually locked maintenance operations" option is selected, only one tag of a Cause or Effect can be simulated in each case.
 - For 'internal F-channel drivers', the simulation affects all locations of use of the tag. This includes other matrices and each user-configured logic that uses this F-channel driver.
 - Tags provided with a prefix ("@") are external to this Safety Matrix and cannot be simulated.
 - For the Safety Matrix to also interconnect external F-channel drivers (except customer-specific F-channel drivers with the prefix "~") as "internal channel drivers", you must select the "Integrate external channel drivers" option for the transfer of the Safety Matrix to the project. This is necessary for the "Simulate tag" function to also act on these external F-channel drivers.
-

Set soft bypass for an input tag of a Cause

You can set a soft bypass for an input tag of a Cause.

For this purpose, the "Soft Bypass allowed" option must be enabled for the tag in the properties of the Cause, "Configure" tab.

Note

If the Cause has multiple input tags and the soft bypass is set for one input tag, this results in Degraded Voting.

You can find additional information on this in section "The "Degraded Voting" function (Page 60)".

Procedure

1. Double-click the desired Cause, "Values" column, or click the "View Tags" button in the control bar for the selected Cause.
2. Select the check box labeled "Enable maintenance changes" in the "Values" tab of the "Display Tags" dialog box.
3. Click the "Set" button for the desired tag in the "Bypass" area.
Result: A Secure Write transaction is started to set the soft bypass.

4. In the following prompt, enter a reason for the soft bypass and click the "Bypass" button. The following dialog shows the desired transaction again so you can check it.
5. Check whether the specified change corresponds to the desired operation.
 - If it does, select the "Operation checked and to be activated" check box and click the "OK" button.
 - If it does not match, you must click "Cancel".

Result: The set soft bypass is displayed in color in the "Input tag" column of the matrix display.

If the Cause has multiple input tags and the soft bypass was set for one input tag, this results in Degraded Voting. The resulting Cause logic is displayed here in the "Function" column of the relevant Cause.

Change values for limit, hysteresis and delta

You can also display and edit the values for limit, hysteresis, and delta for analog input types in online mode of the Safety Matrix Engineering Tool.

You can find additional information on hysteresis, and discrepancy (delta) in section ""Cause details" dialog - "Analog parameter" tab (Page 104)".

Procedure

1. Double-click the desired Cause with an analog input tag in the "Limit" column. Alternatively, you can click the "View Tags" button in the control bar for the selected Cause.
2. Select the check box labeled "Enable maintenance changes" in the "Analog parameter" tab of the "Display Tags" dialog box.
3. Enter the desired value for limit, hysteresis, and (in case of multiple analog input tags for a Cause) the permitted delta in the respective "New value" field in REAL format. You can find additional information on the REAL format in section "Overview of configuring the Causes (Page 97)".
4. Click the "Write" button.
Result: A Secure Write transaction is started for writing the values.

Changing high and low range boundaries

You can also display and edit the high and low range limits for analog input tags currently stored in the CFC chart in online mode of the Safety Matrix Engineering Tool.

Procedure

1. Double-click the desired Cause, "Values" column, or click the "View Tags" button in the control bar for the selected Cause.
2. Select the check box labeled "Enable maintenance changes" in the "Range limits" tab of the "Display Tags" dialog box.

3. Enter the desired value for the high or low range boundary in the respective "New value" field in REAL format.
You can find additional information on the REAL format in section "Overview of configuring the Causes (Page 97)".
4. Click the "Write" button for the input tag whose range limits have just been changed.
Result: The data is written to the relevant F-channel drivers by means of a CFC online change. For this purpose, you are prompted to deactivate safety mode.

Note

Note that safety mode will not be reactivated until you switch out of online mode of the Safety Matrix.

10.8 Events and messages

All alarms and operation messages triggered by the OS are logged in the PCS 7 message system.

The event log of the Safety Matrix contains the last 100 messages from the Safety Matrix.

10.8.1 Messages in the event protocol of the Safety Matrix

Entries in the event log

The Safety Matrix keeps an event log in which it logs the individual results and operator inputs in detail.

The event log is opened in the control bar of the Engineering Tool or Viewer with the "View events" function and displayed in the Reports window.

The event log is a circular buffer with a maximum capacity of 100 entries, which means the oldest entries are overwritten. The event log cannot be archived by the PCS 7 OS.

10.8.2 Operator messages of the Safety Matrix Viewer

If the Safety Matrix Viewer generates an operator input messaged in the PCS 7 operation list, it also enters the event in the event log.

Entries in the PCS 7 operation list

The Safety Matrix Viewer enters the operations into the PCS 7 operation list. All operation entries contain the following information:

- Time of operation
- Type of operation

- Reason for operation entered by the operator and output in the "Operation" column
- Logged on operator
- Depending on the type of operation, additional information is entered that is logged in the "Operation" column:

Safety Matrix control functions	Additional entries in "Operation" column
Cause Bypass	Cause number; Cause name
Reset FO alarm	Number of the FO alarm group
Override effect / Stop override	Effect number; effect name
Reset effect	Effect number; effect name
Start and stop Cause tag simulation	Cause number; Cause name; tag number; tag name, started or stopped
Simulating a Cause tag	Cause number; Cause name; tag number; tag name, previous value, new value
Effect bypass	Effect number; effect name
Start and stop effect tag simulation	Effect number; effect name; tag number; tag name, started or stopped
Simulating an effect tag	Effect number; effect name; tag number; tag name, previous value, new value
Reintegrating driver	-
Acknowledge Cause	Cause number; Cause name
Tag bypass	Cause number; Cause name, bypass, tag number; tag name, set/remove

10.8.3 PCS 7 alarm messages in the WinCC message system

Signaling of all process-relevant events

All process-relevant events can be signaled by means of a WinCC message so that it is possible to trace in a message archive, even after a long time, which events occurred in which order.

In WinCC, these messages appear like any other in the PCS 7 message system.

the "Loop-in-alarm" button is available on the left, next to the message line of the overview area of the PCS7 OS/WinCC and in all message lists (except in the operation list).



When the "Loop-in-alarm" button is clicked, the screen in which the block icon of the Safety Matrix belonging to the message is located is opened. Click this icon to open the faceplates in the Safety Matrix Viewer.

Requirements for generating block icons

To generate the block icons for the Safety Matrix, the message blocks must be configured appropriately and the Safety Matrix must be transferred with the "Position alarm blocks" option selected:

- In the "Properties" dialog box of the Safety Matrix, "Alarms" tab (see section ""Properties" dialog box of the Safety Matrix (Page 88)")
- In the "Cause details" dialog box, "Alarms" tab (see section ""Cause details" dialog box - "Alarms" tab (Page 108)")
- In the "Effect details" dialog box, "Alarms" tab (see section ""Effect details" dialog box - "Alarms" tab (Page 116)")
- In the "Transfer to project" dialog box, "Alarm blocks" area (see section "Transferring the Safety Matrix to the program (Page 130)")

See also

Section ""Properties" dialog box of the Safety Matrix (Page 88)"

10.8.4 Warning messages

Warning messages of the Safety Matrix

In online mode, the Safety Matrix outputs warning messages as red text above the control bar, for example:

- Transaction in progress
- Matrix stopped executing
- Communication error
- Maintenance operations are locked

10.8.5 Messages of the matrix message blocks

Overview

The messages of the matrix message blocks F_MA_AL, F_SC_AL, F_SC_AL2 und F_SE_AL that are displayed in the Safety Matrix Viewer in the PCS 7 alarm logging are described below.

Message blocks must be positioned and message classes must be configured for these messages.

- Message block for the matrix
The message block for the matrix F_MA_AL exists at least once in the Safety Matrix charts.
- Message blocks for Cause and Effect
If separate messages are to be output for individual Causes/Effects, a F_SC_AL / F_SC_AL2 or F_SE_AL message block must be positioned for each of these Causes/Effects.
This happens under the following requirements:
 - The "Positioning of Cause and Effect" option must be activated in the "Alarms" tab in the properties of the Safety Matrix.
 - For each Cause or Effect for which separate messages are to be output, the "Positioning" option must be activated in the "Alarms" tab in the properties of the respective Cause or Effect.
- The message classes and messages are configured as follows:
 - For the Safety Matrix in the properties of the matrix in the "Alarms" tab under the option "Enable Matrix messages".
 - For each Cause or Effect in the properties of the respective Cause or Effect in the "Alarms" tab under the option "Enable messages".

Messages of the F_MA_AL block

For the message block F_MA_AL of the Safety Matrix, the output messages depend on whether or not message blocks are positioned for Cause and Effects.

Both options are described in the following tables.

Message blocks are not positioned for Causes and Effects

The messages in this table are output by the F_MA_AL block when no F_SC_AL / F_SC_AL2 and F_SE_AL message blocks are positioned for Causes and Effects.

No.	Message class	Event	Single acknowledgment	With acknowledgment
1	Process control message - error	<\$\$BlockComment\$\$> Configuration changed		X
2	Operator prompt - general	<\$\$BlockComment\$\$> Acknowledgment request driver		
3	Alarm - high	<\$\$BlockComment\$\$> Cause(s) active		X
4	Warning - high	<\$\$BlockComment\$\$> Cause(s) prewarning(s) active		X
5	Preventive maintenance - general	<\$\$BlockComment\$\$> Cause(s) bypass(es) active		X
6	Alarm - high	<\$\$BlockComment\$\$> Effect(s) active		X

Table 1

No.	Message class	Event	Single acknowledgment	With acknowledgment
7	Warning - high	<\$\$BlockComment\$\$> Effect(s) prewarning(s) active		X
8	Preventive maintenance - general	<\$\$BlockComment\$\$> Effect(s) bypass(es) active		X

Key:

a) "<\$\$BlockComment\$\$>" = Path to the block instance + instance-specific comment in the block

Note

Dependency of messages of the Safety Matrix message block

The output of the message classes and events to the messages of the matrix message block depends on whether the message blocks for Cause and Effects are positioned.

The matrix message block outputs **various event texts** in the messages. If the Cause/Effect message blocks are positioned, a general event text is output by the matrix message block, because an additional detailed message is output by the Cause/Effect message block.

Example:

- Cause/Effect message blocks are not positioned.
This means table 1 above applies to the messages of the matrix message block.
With a bypass at a Cause, the matrix message block outputs message no. 5 "Preventive maintenance - general / **Cause(s) bypass(es) active**".
- Cause/Effect message blocks are positioned.
This means tables 2 and 3 above apply to the messages of the matrix message block.
 - With a bypass at a Cause, the matrix message block outputs message no. 6 "Preventive maintenance - general / **Cause Preventive maintenance(s) active**".
 - In addition, the message "Preventive maintenance - general / Cause [x] bypass active" (e.g. message no. 3 of the following table 4 of the F_SC_AL block) is output by the corresponding Cause message block.

Message blocks are positioned for Causes and Effects

The messages in this table are output by the F_MA_AL block for **all Causes** when the message blocks F_SC_AL / F_SC_AL2 and F_SE_AL are positioned for Causes and Effects .

Table 2

No.	Message class	Event	Single acknowledgment	With acknowledgment
1	Alarm - high	<\$\$BlockComment\$\$> Cause alarm(s) active		X
2	Warning - high	<\$\$BlockComment\$\$> Cause warning(s) active		X
3	Tolerance - high	<\$\$BlockComment\$\$> Cause tolerance(s) active		
4	AS process control message - fault	<\$\$BlockComment\$\$> Cause process control message(s) - Fault active		X

No.	Message class	Event	Single acknowledgment	With acknowledgment
5	AS process control message - error	<\$\$BlockComment\$\$> Cause process control message(s) - Error active		X
6	Preventive maintenance – general	<\$\$BlockComment\$\$> Cause preventive maintenance(s) active		X
7	Process message – with acknowledgment	<\$\$BlockComment\$\$> Cause process message(s) active		X
8	Operator prompt - general	<\$\$BlockComment\$\$> Cause operator prompt(s) active		

Key:

a) "<\$\$BlockComment\$\$>" = Path to the block instance + instance-specific comment in the block

The messages in this table are output by the F_MA_AL block for **all Effects** when the message blocks F_SC_AL / F_SC_AL2 and F_SE_AL are positioned for Causes and Effects .

No.	Message class	Event	Single acknowledgment	With acknowledgment
1	Alarm - high	<\$\$BlockComment\$\$> Effect alarm(s) active		X
2	Warning - high	<\$\$BlockComment\$\$> Effect warning(s) active		X
3	Tolerance - high	<\$\$BlockComment\$\$> Effect tolerance(s) active		
4	AS process control message – fault	<\$\$BlockComment\$\$> Effect process control message(s) - Fault active		X
5	AS process control message - error	<\$\$BlockComment\$\$> Effect process control message(s) - Error active		X
6	Preventive maintenance – general	<\$\$BlockComment\$\$> Effect preventive maintenance(s) active		X
7	Process message – with acknowledgment	<\$\$BlockComment\$\$> Effect process message(s) active		X
8	Operator prompt - general	<\$\$BlockComment\$\$> Effect operator prompt(s) active		

Key:

a) "<\$\$BlockComment\$\$>" = Path to the block instance + instance-specific comment in the block

Messages of the F_SC_AL block

The following messages are output for each Cause for which the message block is positioned in the Safety Matrix chart.

No.	Message class	Event	Single acknowledgment	With acknowledgment
1	Alarm - high	<\$\$BlockComment\$\$> Cause [x] active	X	X
2	Warning - high	<\$\$BlockComment\$\$> Cause [x] [Limit prewarning], [Delta] active		X
3	Preventive maintenance – general	<\$\$BlockComment\$\$> Effect [x] [Bypass], [Soft bypass], [Mask], [Override], [Pass-through] active		X
4	Operator prompt - general	<\$\$BlockComment\$\$> Cause [x] acknowledgment request		
5	Process message – with acknowledgment	<\$\$BlockComment\$\$> Cause [x] First Out Alarm group [y]		X
6	Warning - high	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] active [- T1:X, T2:Y, T3:Z]		X
7	Preventive maintenance – general	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] simulated [- T1:X, T2:Y, T3:Z]		X
8	AS process control message – fault	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] faulty [- T1:X, T2:Y, T3:Z]		X

Key:

- a) "<\$\$BlockComment\$\$>" = Path to the block instance + instance-specific comment in the block
- b) "[- T1:X, T2:Y, T3:Z]" = The tags [- T1:X, T2:Y, T3:Z] are added in the messages no. 6, 7, 8 if the option "Extend event by symbolic tag name" is activated in the "Message configuration" dialog box of the respective Cause.

Messages of the F_SC_AL2 block

The following messages are output for each Cause for which the message block is positioned in the Safety Matrix chart.

No.	Message class	Event	Single acknowledgment	With acknowledgment
1	Alarm - high	<\$\$BlockComment\$\$> Cause [x] active	X	X
2	Warning - high	<\$\$BlockComment\$\$> Cause [x] [Limit prewarning], [Delta] active		X
3	Preventive maintenance – general	<\$\$BlockComment\$\$> Effect [x] [Bypass], [Soft bypass], [Mask], [Override], [Pass-through] active		X
4	Operator prompt - general	<\$\$BlockComment\$\$> Cause [x] acknowledgment request		
5	Process message – with acknowledgment	<\$\$BlockComment\$\$> Cause [x] First Out Alarm Group [y]		X
6	Warning - high	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] active [- T1:X, T2:Y, T3:Z]		X

No.	Message class	Event	Single acknowledgment	With acknowledgment
7	Preventive maintenance – general	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] simulated [- T1:X, T2:Y, T3:Z]		X
8	AS process control message – fault	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] faulty [- T1:X, T2:Y, T3:Z]		X
9	Warning - high	<\$\$BlockComment\$\$> Cause [x] Soft bypass prewarning active		X
10	AS process control message – fault	<\$\$BlockComment\$\$> Cause [x] Error soft bypass timeout		X
11	Preventive maintenance – general	<\$\$BlockComment\$\$> Cause [x] Degraded Voting active		X
12	Preventive maintenance – general	<\$\$BlockComment\$\$> Cause [x] Tag [1], [2], [3] Bypass active [- T1:X, T2:Y, T3:Z]		X

Key:

a) "<\$\$BlockComment\$\$>" = Path to the block instance + instance-specific comment in the block

b) "[- T1:X, T2:Y, T3:Z]" = The tags [- T1:X, T2:Y, T3:Z] are added in the messages no. 6, 7, 8, 12 if the option "Extend event by symbolic Tag name" is activated in the "Message configuration" dialog box of the respective Cause.

Messages of the F_SE_AL block

The following messages are output for each effect for which the message block is positioned in the Safety Matrix chart.

No.	Message class	Event	Single acknowledgment	With acknowledgment
1	Alarm - high	<\$\$BlockComment\$\$> Effect [x] active	X	X
2	Warning - high	<\$\$BlockComment\$\$> Effect [x] Prewarning override active		X
3	Preventive maintenance – general	<\$\$BlockComment\$\$> Effect [x] [Bypass], [Soft bypass], [Mask], [Override], [Pass-through] active		X
4	AS process control message - error	<\$\$BlockComment\$\$> Effect [x] Stop override		X
5	Operator prompt - general	<\$\$BlockComment\$\$> Effect [x] [Acknowledgment request], [OK to reset] active		
6	Warning - high	<\$\$BlockComment\$\$> Effect [x] @Tag [1], [2], [3], [4] active [- T1:X, T2:Y, T3:Z, T4:W] Note: The message comes under the following conditions: <ul style="list-style-type: none"> • When Tag[x] is configured as Energized-to-trip and Tag[x] = TRUE. • When Tag[x] is configured as Deenergized-to-trip and Tag[x] = FALSE. 		X

No.	Message class	Event	Single acknowledgment	With acknowledgment
7	Preventive maintenance – general	<\$\$BlockComment\$\$> Effect [x] @Tag [1], [2], [3], [4] simulated [- T1:X, T2:Y, T3:Z, T4:W]		X
8	AS process control message – fault	<\$\$BlockComment\$\$> Effect [x] @Tag [1], [2], [3], [4] faulty [- T1:X, T2:Y, T3:Z, T4:W]		X

Key:

- a) "<\$\$BlockComment\$\$>" = Path to the block instance + instance-specific comment in the block
- b) "[- T1:X, T2:Y, T3:Z, T4:W]" = The tags [- T1:X, T2:Y, T3:Z, T4:W] are added in the messages no. 6, 7, 8 if the option "Extend event by symbolic Tag name" is activated in the "Message configuration" dialog box of the respective Cause.

See also

Overview for configuring messages (Page 67)

Documentation of a Safety Matrix

11.1 Print Safety Matrix

Overview

The menu command **File > Print** is available in the Safety Matrix Engineering Tool or, alternatively, the icon of the same name is available in the toolbar for printing a Safety Matrix.

Print settings

The print preview allows you to select different settings, for example:

- "Details"
In the selection field you determine the details of the Safety Matrix data to be printed:
 - "Brief overview"
 - "Detail overview"
- "Layout"
In the selection field you determine the page alignment of the printout:
 - "Portrait"
 - "Landscape"
- "Format"
In the selection field, select the page format for the printout, e.g. "A3":

Depending on these setting, the print data is displayed in the print preview.

Buttons

- "Print" button
After selecting the desired settings, you use the "Print" button to open a selection dialog for the printer.
If necessary, you can select specific settings of the printer.
You also start the print process in this dialog.
- "Help" button
The button opens the associated help.

Data in the print preview

The following description applies to the "Brief overview". Deviations from the "Detail overview" are highlighted.

The following data of a Safety Matrix is shown in the print preview or printed.

- General information
 - Safety Matrix name
 - S7 program path
 - Plant hierarchy
 - Version
 - Time stamp (main/minor file revision)
 - Current signature
 - Date of the last transfer
- Overall view of the Safety Matrix on one page.
The representation is similar to the one in the Safety Matrix Engineering Tool.
- Additionally for "Detail view":
Separate pages are displayed or printed for the Causes and Effects in the detail view. For larger matrices, Causes and Effects are broken down into several pages.
- Legend
 - Intersection types
 - Cause/Effect options
- SIF groups
- User notes
- Version information
 - Time stamp of the last main revision and minor revision
 - Matrix version (main revision and minor revision)

11.2 Comparing Safety Matrices

Introduction

Using the menu command "Compare Safety Matrix with" you can compare the following Safety matrices with each other and show and print out deviations:

- The current Safety Matrix with another, open Safety Matrix.
- The current Safety Matrix with the last saved version of the Safety Matrix.
- The current Safety Matrix with the last Safety Matrix transferred to the program.
- The current Safety Matrix with the Safety Matrix downloaded to the F-CPU.

Procedure

Select the menu command **Options > Compare Safety Matrix with** and then select the desired comparison:

- **Safety Matrix**
Both Safety matrices you want to compare must be opened in the Safety Matrix Engineering Tool for this purpose.
- **Storage**
Here the Safety Matrix is compared with its saved version. The comparison shows you the changes you have made after the last save.
- **Program**
Compares the Safety Matrix with the program from the last transfer, and displays the existing differences.
- **CPU**
Compares the Safety Matrix with the program loaded in the F-CPU, and displays the existing differences.

Result of comparison

The result of comparison is displayed in the reports window. The following differences are shown:

- Safety Matrix signature
- Parameter values
- Causes, Effects, and intersections

You can save and print the result of comparison via the reports window using the corresponding commands.

11.3 Comparing CFCs

Introduction

The "Compare Programs" dialog box enables you to compare all CFC charts of a chart folder, which have been created during transfer by the Safety Matrix Engineering Tool, and to display and print out differences. This comparison is useful during commissioning and for the system acceptance test.

The result of the comparison shows whether the following are different:

- Collective signature
- Safety Matrix signature
- Parameter values
- Causes, Effects, and intersection types
- Tag names and tag properties

To check whether a safety program has been changed, compare the safety program with the original program status, which you have saved, for example, as a reference.

Starting the comparison

Select the **Tools > Compare programs** menu command. The "Compare programs" dialog box will appear.

"Reference" area

- "Saved on:" output field
The output field shows the time stamp of the reference to which the comparison is made if "Reference" has been selected as the comparison object.
- "Save Reference" button
Using this button, you can save the current program (i.e. all Safety Matrix charts in the S7 program) as a reference. This reference represents a subset of the reference program, which is created in the "Safety Program" dialog of S7 F Systems using the "Save Reference" button.
The reference for the "Safety program" dialog in S7 F Systems is saved in a separate file independently of Safety Matrix.

"Comparable objects" area

- "Program" and "Reference" option buttons
Select one of these options to specify whether you want to compare the current program or the reference program.
Use this selection box to specify the second safety program to use for the comparison.

Program	Compare with ...	
	"Reference"	The current program is compared with the last saved reference.
	"Other Project"	The current program is compared with another program. Use the "Browse" button to select the offline program.
Reference	Compare with ...	
	"Current safety program"	The last saved reference is compared with the current safety program ("Backward comparison").
	"Other Project"	The last saved reference is compared with another program. Use the "Browse" button to select the offline program.

- "Browse" button
You can use this button and the "Open" dialog to select the offline program of any project to be compared, if you have selected the "Other project" option under "Comparable objects".

"Start" button

Click this button to start the comparison.

Result

The result of the comparison shows whether a Cause/Effect is new or has been changed or deleted.

- For elements from the source for which no element is found in the reference, 'Cause/Effect x new' is output (x refers to the source).
- For elements from the reference for which no element is found in the source, 'Cause/Effect x deleted' is output (x refers to the source).
- For elements for which a difference is found, 'Cause/Effect x changed' is output (x refers to the source and is determined from the number of the preceding element).

Finally, the intersection types are compared on the basis of the assigned Cause/Effect pairs.

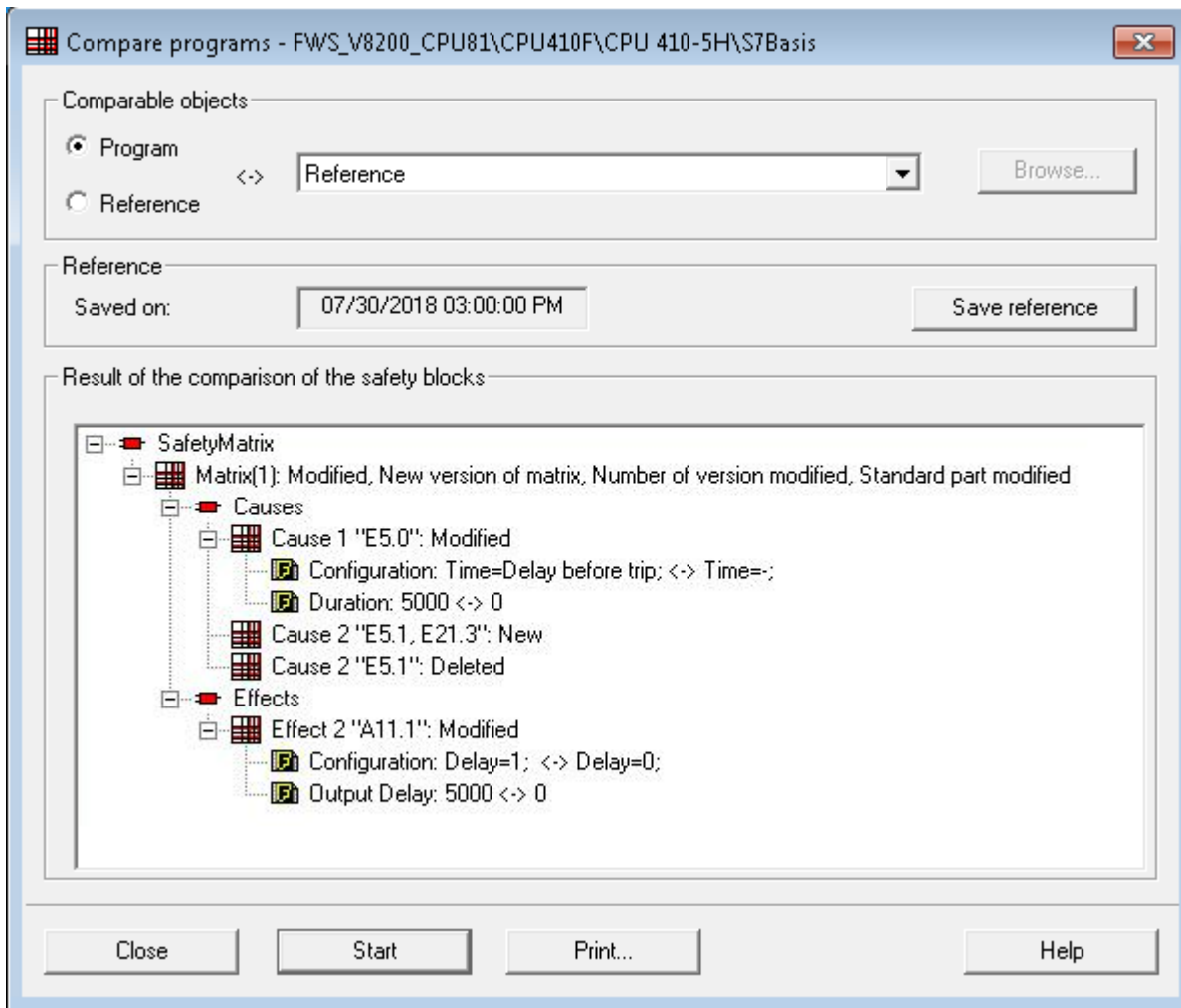
- If an intersection type is found in the reference for a Cause/Effect pair, then this is compared with the corresponding intersection type of the source. If a difference is detected, the 'Intersection type of Cause x and Effect y changed' is output (x and y refer to the source).
- If no intersection type is found for this pair, the 'Intersection type of Cause x and Effect y new' is output (x and y refer to the source).
- All deleted intersection types whose Cause and Effect have not been deleted are shown.

The differences between Safety Matrix charts are displayed in a hierarchical format similar to Windows Explorer.

11.4 Configuration report

The following figure shows an example comparison. In this example, the following changes were made in the Safety Matrix:

- The time response in Cause 1 has been changed.
- Tag 2 in Cause 2 has been newly assigned.
- The delay in effect 2 has been changed.



11.4 Configuration report

Overall display of the complete configuration

The configuration report contains the complete configuration of the Safety Matrix.

Creating a configuration report

Select the menu command **Options > Create report > Configuration**.

The configuration report is opened in the Reports window in a separate tab.

Contents of the configuration report

The configuration report contains the following information:

- Logical path to S7 program
- Plant hierarchy
- Detailed information on all Causes
- Detailed information on all effects
- Detailed information on all intersections
- List of user notes
- List of versions
- List of Safety instrumented function groups (SIF)
- List of essential properties of the Safety Matrix:
 - Name of the Safety Matrix
 - Size (number of rows and columns) of the Safety Matrix
 - Usage statistics of Causes, Effects, intersections (number of configured Causes, Effects, intersections)
 - Paths (to SIMATIC project, S7 program)
 - Title
 - Project
 - Description
 - General note
 - Main revision and minor revision (with time stamp)
 - File revision (with time stamp)
 - File path
 - Cycle time
 - Task OB
 - Safety Matrix signature

Printing out the configuration report

You can save and print the configuration report via the reports window using the corresponding commands.

Print the configuration report after completing the Safety Matrix and store it in a safe location. It is part of the documentation for acceptance of the safety program and the plant.

11.5 Validation report

Plausibility check of the complete configuration

The validation report shows the result of the plausibility check of the Safety Matrix configuration in form of errors and warnings.

Creating a validation report

Select the menu command **Options > Create report > Validation**.

The validation report is opened in the Reports window in a separate tab.

Contents of the validation report

The validation report contains the following information:

- Name of the Safety Matrix
- Logical path to S7 program
- Plant hierarchy
- Errors and warnings, such as:
 - Missing intersection configurations
 - Effects without reset tags
 - Multiple effects with the same output tag

Printout of the validation report

You can save and print the validation report via the reports window using the corresponding commands.

Acceptance test for a Safety Matrix

Introduction

During the system acceptance test, all relevant application-specific standards must be adhered to as well as the following procedures. For the acceptance test, you must consider the systems in the Certification Report.

As a general rule, the acceptance test of an F-System is performed by independent experts.

Acceptance test same as for S7 F/FH Systems

The acceptance test of a Safety Matrix is conducted basically the same as for S7 F/FH Systems. For this reason, you must observe and comply with the section "System Acceptance Test" of the *"S7 F/FH Systems, Configuring and Programming"* Programming and Operating Manual (or the corresponding section in the relevant manual for older versions of S7 F/FH Systems). Additional information on this document is available in the preface.

The procedures described there are also valid for the Safety Matrix as a subset of S7 F/FH Systems. The manual also contains additional details about each step of the acceptance test.

The following detailed description includes only those actions that must be carried out **additionally** for the Safety Matrix.

Initial acceptance test of a safety program

The following specific extensions for the Safety Matrix must be taken into account in addition to the testing activities described in S7 F/FH systems:

1. Preliminary test of the configuration of the F-CPU and F-I/O (optional).
2. Backup of the safety program
 - **Before** backing up your safety program, you must **transfer** and **compile** all matrices (see sections "Transferring a Safety Matrix (Page 129)" and "Compiling and downloading (Page 143)").
 - Check the result of the transfer using the **Tools > Compare Matrix with > Program** menu command. There must not be any differences displayed.
3. Inspection of the printout
 - Print the configuration report for each matrix and inspect it (see section "Configuration report (Page 198) ").
Check if all information is complete and conforms to the desired configuration. Check the configuration of times, and check for unintended interconnections.
 - Validate the signatures and initial value signatures of the Safety Matrix F-blocks in the printout of the safety program. The signatures and initial value signatures must match those in Annex 3 of the Certificate Report.

4. Downloading the S7 program to the F-CPU.
5. Execution of a complete function test

Acceptance test of safety program changes

The following specific extensions for the Safety Matrix must be taken into account in addition to the testing activities described in S7 F/FH systems:

1. Back up your safety program.
 - **Before** backing up your safety program, you must **transfer** and **compile** all matrices (see sections "Transferring a Safety Matrix (Page 129)" and "Compiling and downloading (Page 143)")
 - Check the result of the transfer using the **Tools > Compare Matrix with > Program** menu command. There must not be any differences displayed.
2. Compare your new safety program with your accepted safety program.
 - **Identify** the matrices that have been changed using the "Compare programs" dialog box ("Safety program" dialog box in S7 F/FH Systems).
The result of the comparison is a list of changed F-runtime groups including their F-blocks. All F-blocks of Safety Matrices are contained in a common F-runtime group in the default setting for each OB. Modified F-blocks contain the name of the modified Safety Matrix.
 - **Identify** the changes in the tag pre-processing: The preprocessing of a tag is performed in the chart "Matrix name\PP_Chart\PP_<tag name>".
 - **Compare** the modified Safety Matrices one after the other as follows:
 - Comparison in the "Compare programs" dialog box of the Safety Matrix (see section "Comparing CFCs (Page 195) ")
 - Comparison using the **Compare Matrix with > Safety Matrix** menu command (see section "Comparing Safety Matrices (Page 194) ")
3. Inspect the changes in the printout.
 - **Print** the configuration report for each matrix and **inspect** it (see section "Configuration report (Page 198) "). Check that all information is complete and conforms to the desired configuration. Check the configuration of times, and check for unintended interconnections.
4. Download your modified safety program to the F-CPU.
5. Perform a function test of your changes.
 - If both comparisons performed in Item 2 list changes that match the ones you have made in the Safety Matrix, you only have to test these changes.
 - If the two comparisons list additional changes or if the changes identified by the two comparisons differ, or if "Safety Matrix modified" is displayed, you must test the entire Safety Matrix.

Explanation of parameter assignment options

The following section contains the time diagrams that show you the behavior of Causes and Effects for different configurations.

Please note that one discrete tag each was selected with Deenergize-to-trip (DTT) in the following examples.

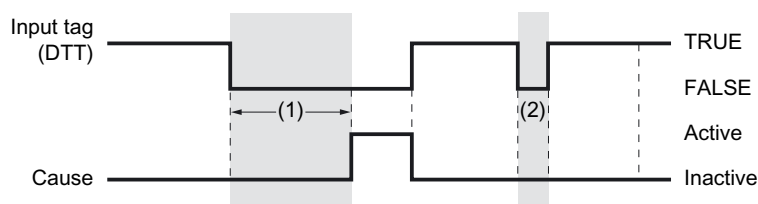
13.1 Parameter assignment options for causes

13.1.1 Time response

Time response of a Cause

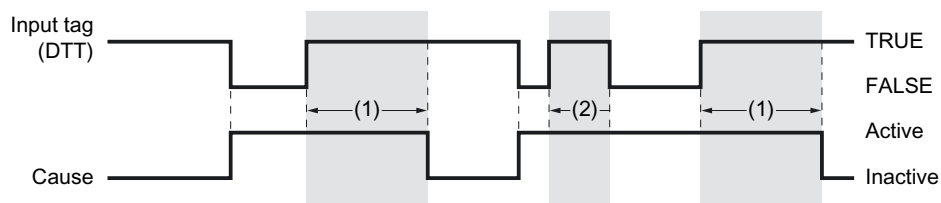
Only one configuration can be made for each Cause regarding the time response.

ON delay



- Gray level: Time running
- (1): ON delay
- (2): ON delay canceled by change of the input tag.
- Delayed activation of the Cause
- The input tag must stay tripped throughout the ON delay time for the Cause to become active.

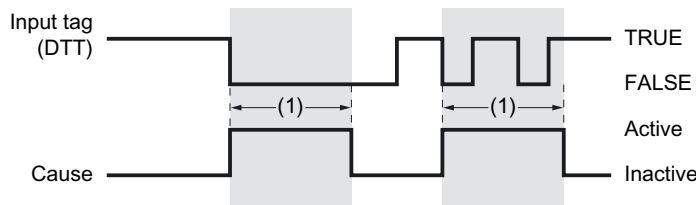
OFF delay



13.1 Parameter assignment options for causes

- Gray level: Time running
- (1): OFF delay
- (2): OFF delay canceled by change of the input tag.
- The Cause is still active for the configured time of the OFF delay after the input tag has become TRUE. Any potentially configured acknowledgment requirement of the Cause has no effect on this behavior.
- The timer of the OFF delay is canceled when the input tag becomes FALSE again.

Timed Cause

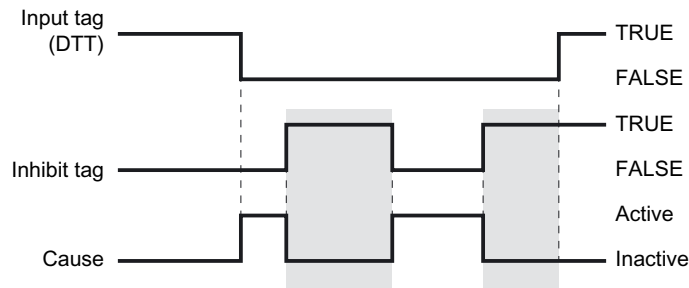


- Gray level: Time running
- (1): Time for timed Cause
- If the input tag becomes FALSE, the timer of the timed Cause is started and the Cause becomes inactive again after expiration of the timer, regardless of the state which the input tag assumes in the meantime. Any potentially configured acknowledgment requirement of the Cause has no effect on this behavior.

13.1.2 Inhibit

Characteristics during inhibit of a Cause

The inhibit tag is used to inhibit the Cause during start-up of a system. The Cause is inhibited, which means it is inactive, when the inhibit tag is TRUE.

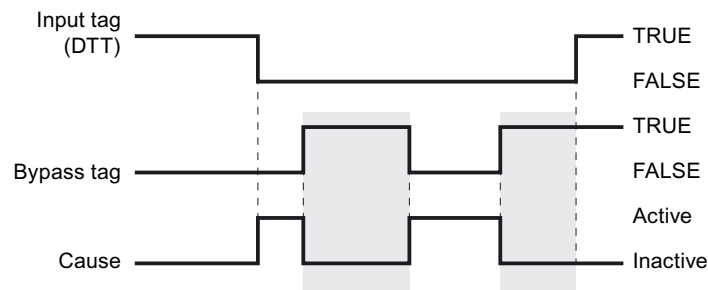


- Gray level: Inhibit of the Cause is active
- ON delay, OFF delay and timed Cause have no effect on the function of the inhibit tag. They act independently of one another.
- If "Auto acknowledged active Cause" is not set, a manual acknowledgment is required to deactivate the Cause. The inhibit tag merely inhibits an activated Cause without acknowledging it.

13.1.3 Bypass

Response to bypass

Bypass and inhibit basically have the same function. The difference is only in how they are used. The bypass is used for maintenance purposes. The Cause becomes inactive when the value of the bypass tag is TRUE.



- Gray level: Bypass for Cause active
- ON delay, OFF delay and timed Cause have no effect on the function of the bypass tag. They act independently of one another.
- If "Auto acknowledge active Cause" is not set, a manual acknowledgment is required to deactivate the Cause. The bypass tag merely inhibits an activated Cause without acknowledging it.
- In addition to the bypass tag, the soft bypass can also be allowed in the configuration. The user can control the bypass via operator input. The soft bypass can also be configured as time-controlled. The bypass is then removed automatically when the configured time has elapsed.

13.1.4 Auto acknowledge active cause

Behavior with Auto acknowledge active cause

If "Auto acknowledge active cause" is configured, the cause will become inactive automatically as soon as the tripping conditions are no longer satisfied. If "Auto acknowledge active cause" is not configured, the operator must manually acknowledge an active cause. The cause remains active until it has been acknowledged.

13.1 Parameter assignment options for causes

If an OFF delay or timed cause is configured, the configured Auto acknowledge active cause has no effect.

13.1.5 "Bad Quality" Voting

Behavior on Bad Quality

In the properties of a Cause, various options can be selected for behavior in case of a bad signal status ("Bad Quality") of the input tags:

- 'Ignore "Bad Quality"'
If the "Ignore "Bad Quality"" option is activated, then the bad signal status ("Bad Quality") of the input tags is not evaluated.
- 'Trip on "Bad Quality"'
If "Trip on Bad Quality" is activated, the quality errors signaled by the F-channel driver ("Bad Quality") force the input tag to assume the tripped state.
- 'Degraded voting at "Bad Quality"'
If 'Degraded Voting at "Bad Quality"' is activated, then the input tag with a bad signal status ("Bad Quality") is taken out of the evaluation for the Cause.

See also

"Cause details" dialog box - "Options" tab (Page 105)

13.1.6 Alarm on input trip

Alarm behavior with multiple input tags

If a Cause is configured with more than one input tag, you can choose whether an alarm is indicated as soon as one of the inputs satisfies the tripping criteria. By default, the alarm is enabled for discrete and analog inputs.

13.2 Parameter assignment options for effects

13.2.1 Reset/override

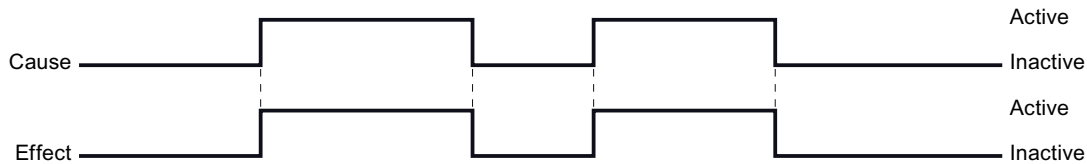
Behavior during reset/override of an effect as a function of the intersection type

Reset/override takes place either via an operation, via the button in the Safety Matrix Engineering Tool online mode or in the Safety Matrix Viewer, or by setting and resetting the reset/override tag.

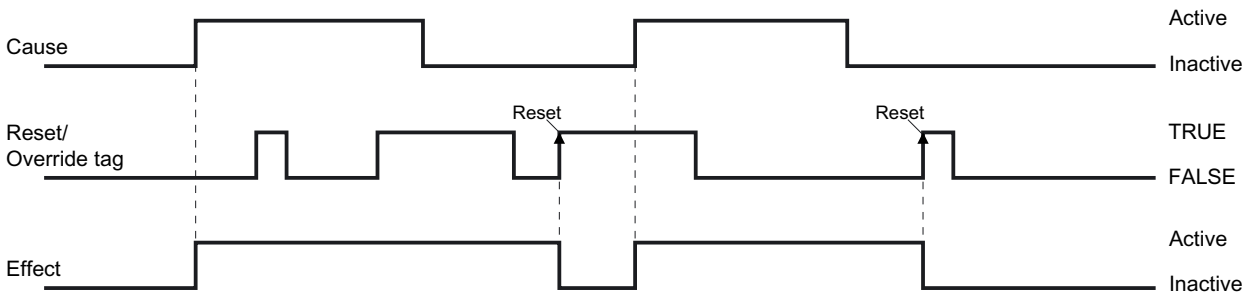
Reset/override tag and maximum override time have no effects on the effect.

Reset/override of an effect for intersection type "N - Not stored"

Reset/override is not relevant for effects for intersection type "N - Not stored".

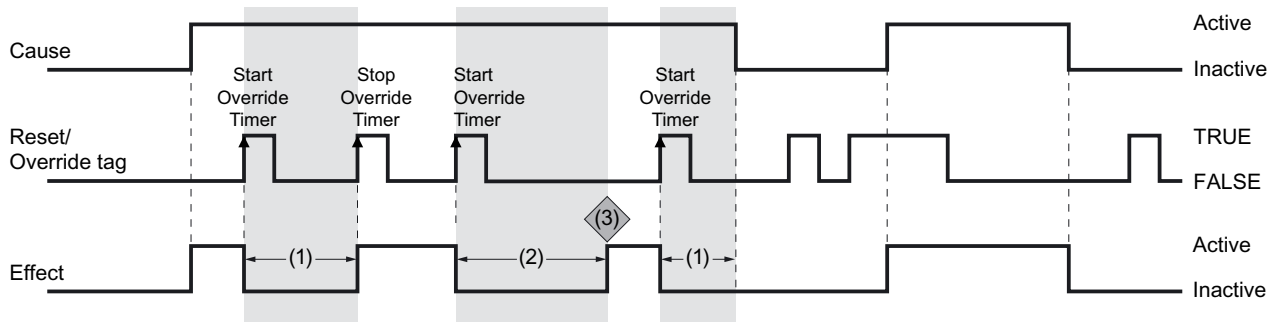


Reset/override of an effect for intersection type "S - Stored"



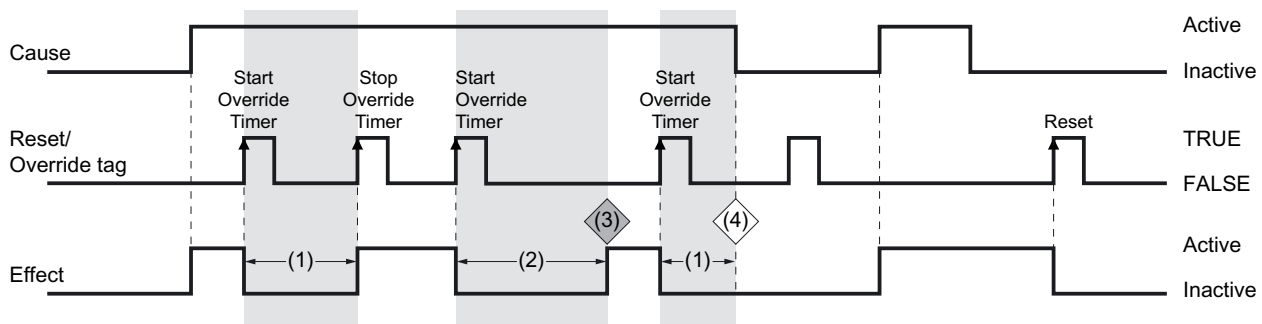
- After the Cause has become inactive, a reset is required to disable the Effect.
- A rising edge is required for the reset.

Reset/override of an effect for intersection type "V - Overridable"



- Gray level: Override timer runs
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm:** Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- A rising edge of the override tag both starts and stops the override timer.
- The timer is automatically stopped as soon as the maximum override time has been reached.
- If the Cause becomes inactive, the override timer is also stopped.

Reset/override of an effect for intersection type "R - Resettable and overridable"



- Gray level: Override timer runs
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm:** Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- This intersection type forms the combination of the intersection types S and V with the special feature that no reset is necessary if the override timer is still running when the Cause becomes inactive (4).

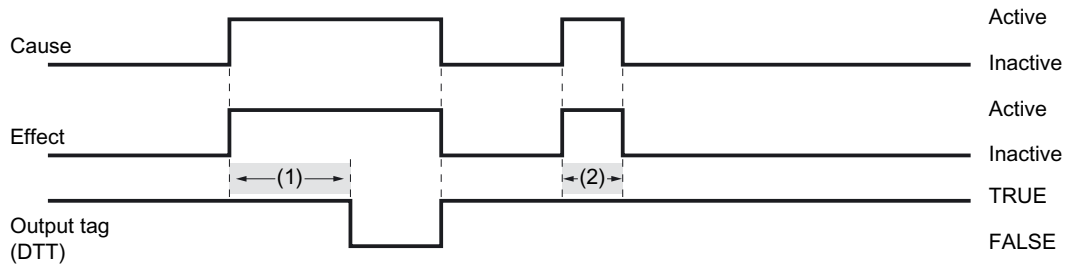
13.2.2 Reset/override with output delay

Behavior during reset/override with output delay as a function of the intersection type

After the effect becomes active, the output delay delays the change of the output tags.

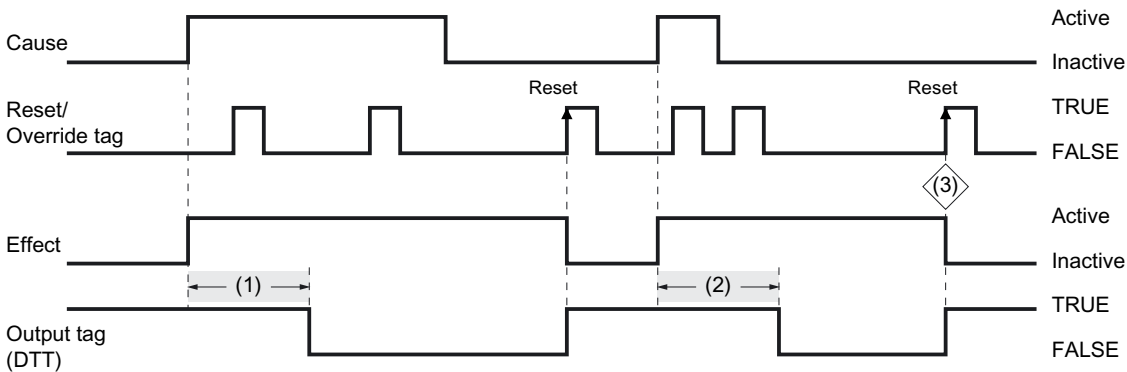
Reset/override of an effect with output delay for intersection type "N - Not stored"

Reset/override tag and maximum override time have no effects on the effect for intersection type "N - Not stored".



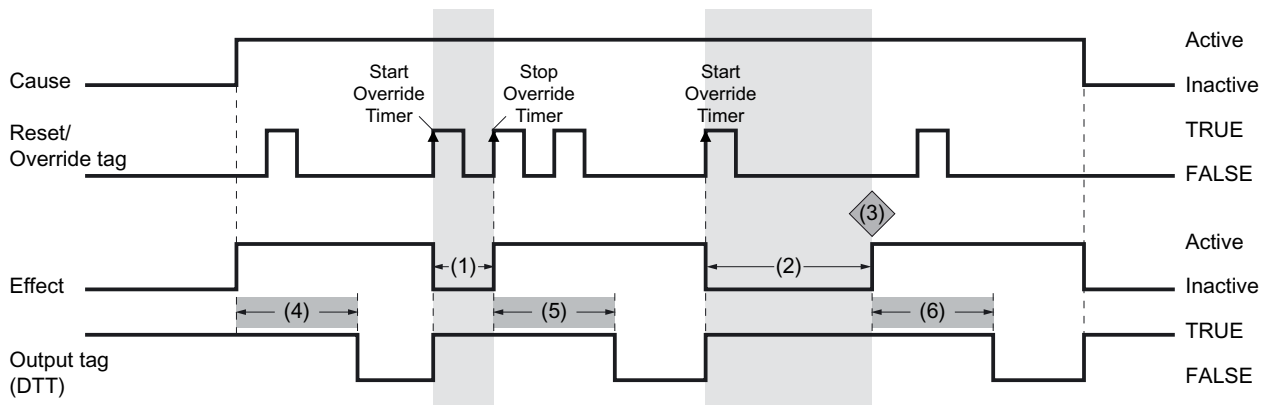
- (1): Time \geq Configured duration for the output delay
- Gray level: Output delay timer runs
- (2): If the Cause becomes inactive, the output delay timer is also stopped.

Reset/override of an effect with output delay for intersection type "S - Stored"



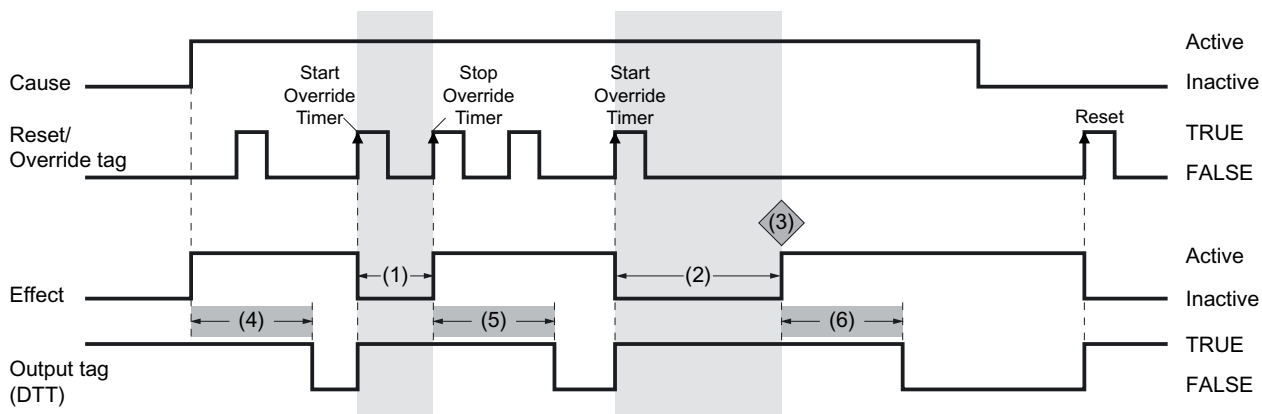
- (1): Time \geq Configured duration for the output delay
- Gray level: Output delay timer runs
- After the Cause has become inactive, a reset is required to also disable the Effect.
- A rising edge is required for the reset.
- Reset has no effect as long as the Cause is active or the output delay timer is running.
- (2): If the Cause becomes inactive, the output delay timer is **not** stopped. Only after the output delay timer has expired can the reset take place (3).

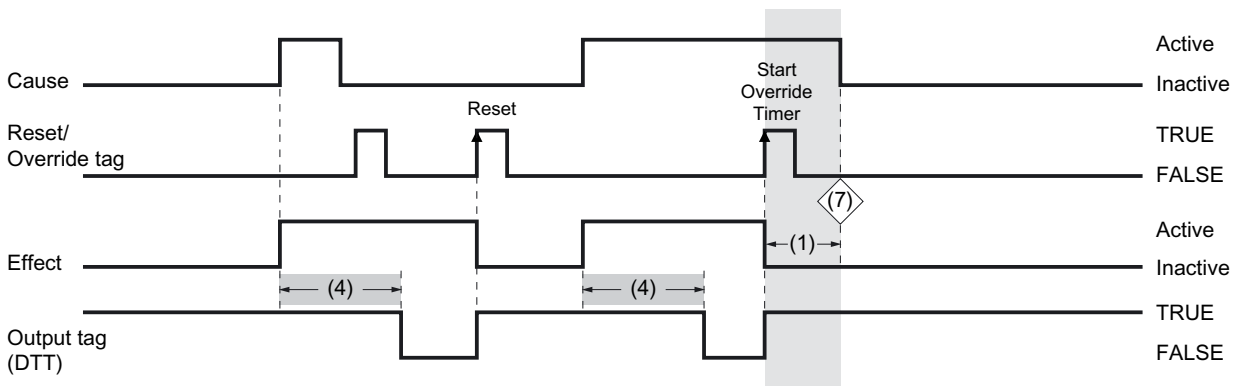
Reset/override of an effect with output delay for intersection type "V - Overridable"



- (4), (5), (6): Output delay timer runs
- (1), (2): Override timer runs
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm:** Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- (4): As soon as the effect becomes active, the output delay timer is started. After it expires, the output tag is also changed.
- (5): The output delay timer is also started when the override is stopped or (6) the maximum override time is exceeded.
- If the Cause becomes inactive, the Effect will also become inactive regardless of whether the output delay timer or the override timer is running.
- The override tag has no effect as long as the output delay timer is running or the Cause is inactive.

Reset/override an effect with output delay for intersection type "R - Resettable and overridable"





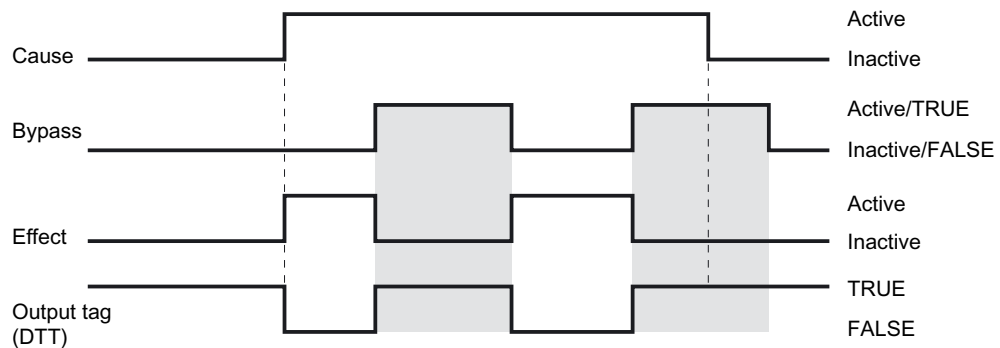
- (4), (5), (6): Output delay timer runs
- (1), (2): Override timer runs
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm**: Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- This intersection type forms the combination of the intersection types S and V with output delay with the special feature that no reset is necessary if the override timer is still running when the Cause becomes inactive (7).

13.2.3 Bypass

Behavior during bypass as a function of the intersection type configuration

In addition to the reset/override tag, the bypass tag is now also taken into consideration.

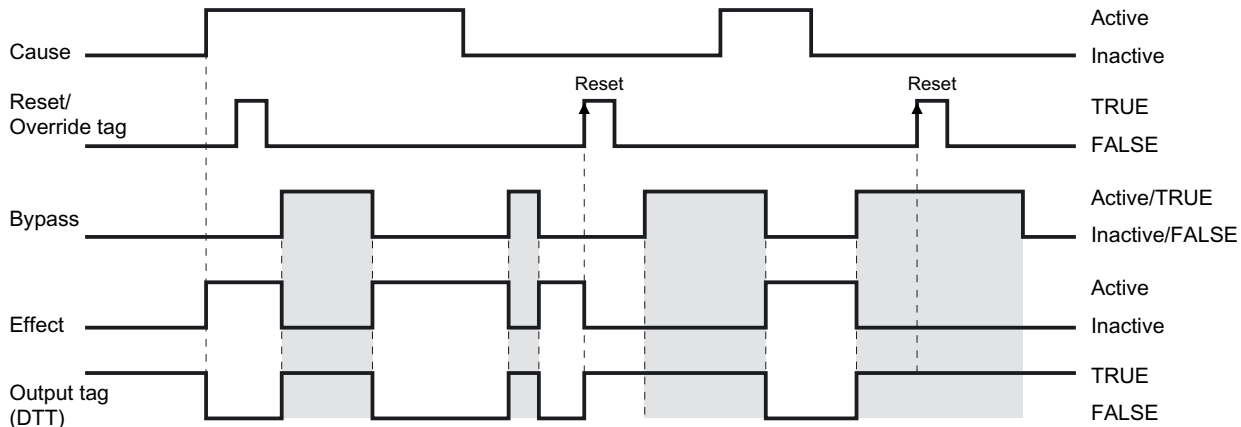
Bypass of an effect for intersection type "N - Not stored"



13.2 Parameter assignment options for effects

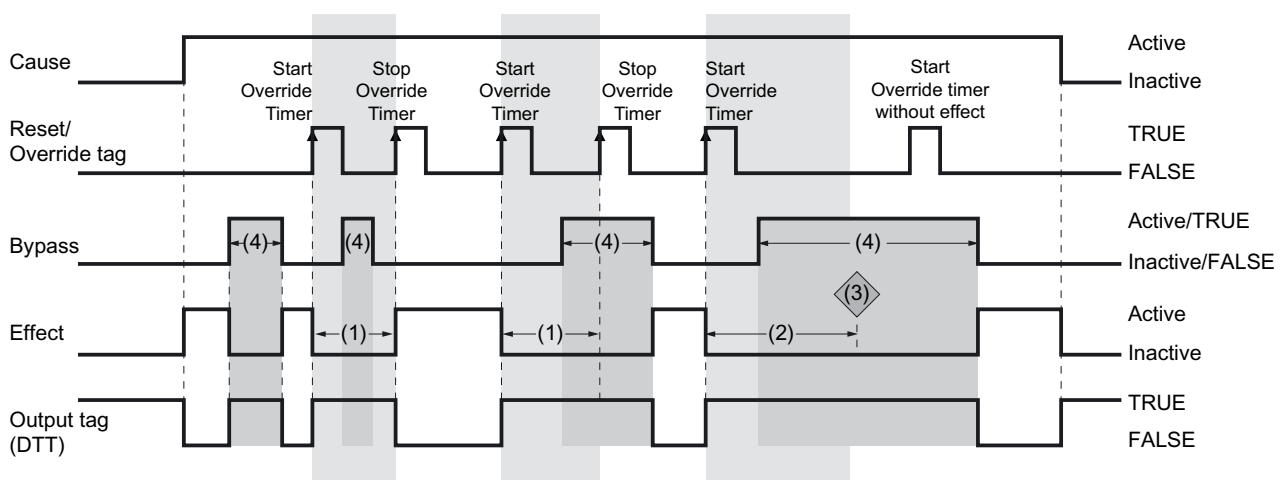
- Gray level: Bypass active
- As soon as bypass becomes active, the effect becomes inactive. This has an immediate effect on the output tag for intersection type N.
- If the Cause becomes inactive, the bypass tag has no Effects on the Effect or output tag any longer.

Bypass of an effect for intersection type "S - Stored"



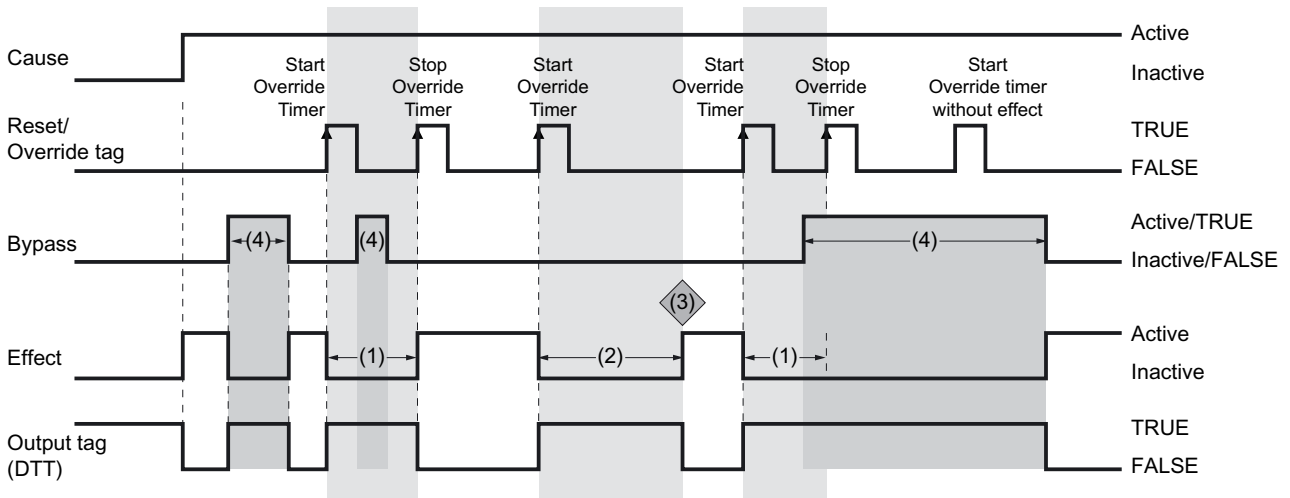
- Gray level: Bypass active
- Reset has no effect when Cause is active.
- Only when the Cause becomes can the reset be performed.
- If the Cause is inactive, the bypass has an Effect on the activity of the Effect and thus on the output tag as long as the Effect has not been reset by a positive edge of the reset/override tag.

Bypass of an effect for intersection type "V - Overridable"

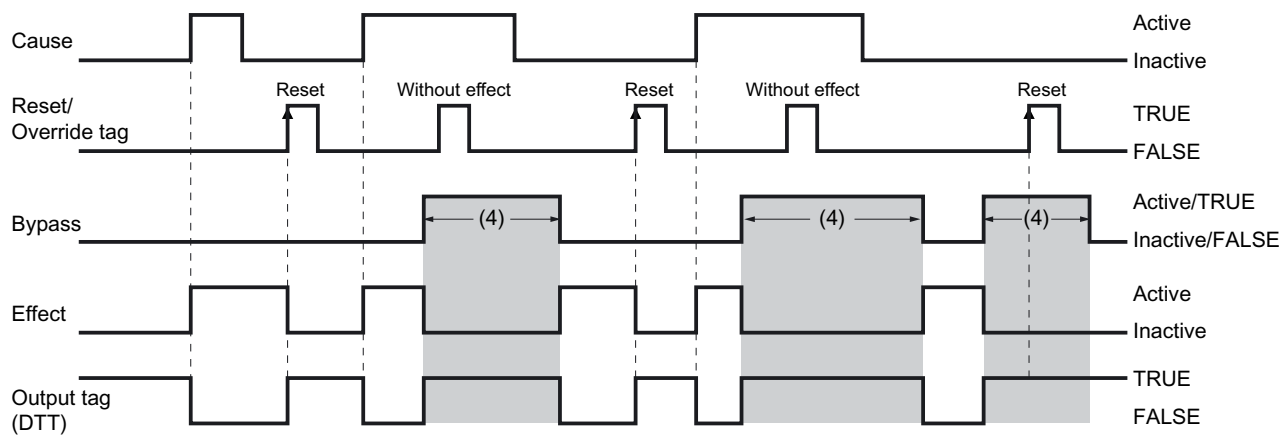


- (1), (2): Override timer runs
- (4): Bypass active
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm**: Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- A rising edge of the reset/override tag both starts and stops the override timer.
- The timer is automatically stopped as soon as the maximum override time has been reached (3).
- If the Cause becomes inactive, the override timer is also stopped.
- Activation of the bypass does not stop the override timer.
- A started override timer can always be stopped again by a positive edge of the reset/override tag regardless of the bypass state.
- The override timer cannot be activated if bypass is active.

Bypass of an effect for intersection type "R - Resettable and overridable"



13.2 Parameter assignment options for effects



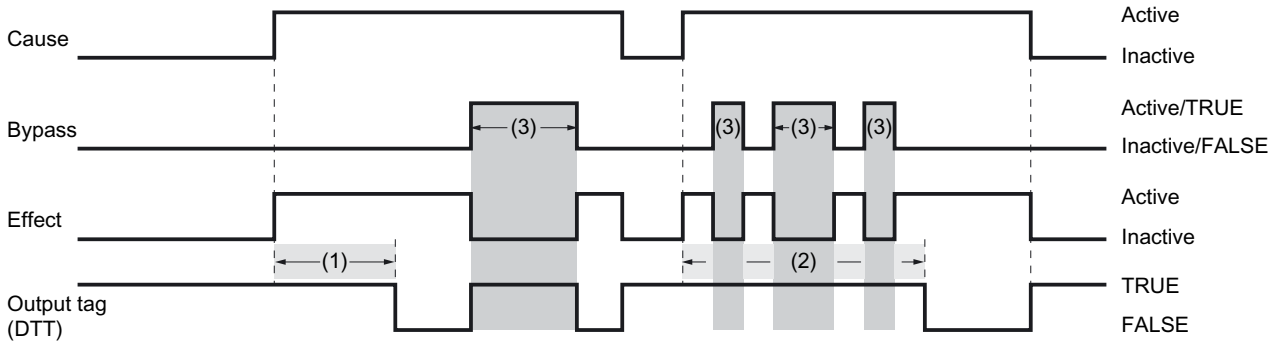
- (1), (2): Override timer runs
- (4): Bypass active
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm:** Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- A rising edge of the reset/override tag both starts and stops the override timer.
- The timer is automatically stopped as soon as the maximum override time has been reached (3).
- If the Cause becomes inactive, the override timer is also stopped.
- If the Cause becomes inactive while the override timer is running, no reset is required to make the Effect inactive.
- Activation of the bypass does not stop the override timer.
- A started override timer can always be stopped again by a positive edge of the reset/override tag regardless of the bypass state.
- The override timer cannot be activated if bypass is active.
- If the Cause has become inactive, the Effect can be reset by a positive edge of the reset/override tag.
- If the Cause is inactive, the bypass has an Effect on the activity of the Effect and thus on the output tag as long as the Effect has not been reset by a positive edge of the reset/override tag.

13.2.4 Bypass with output delay

Behavior during bypass with output delay as a function of the intersection type configuration

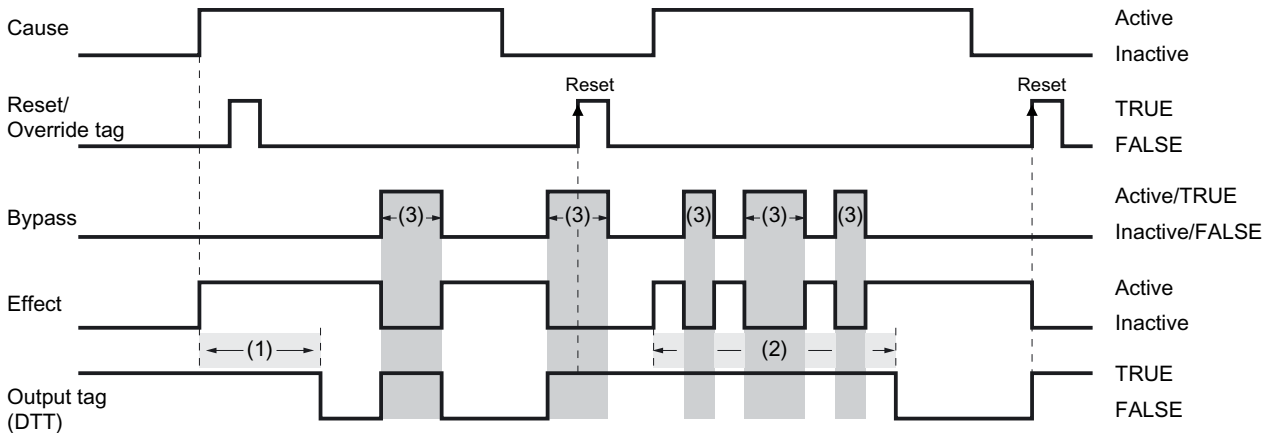
The bypass tag with output delay will be examined below.

Bypass of an effect with output delay for intersection type "N - Not stored"



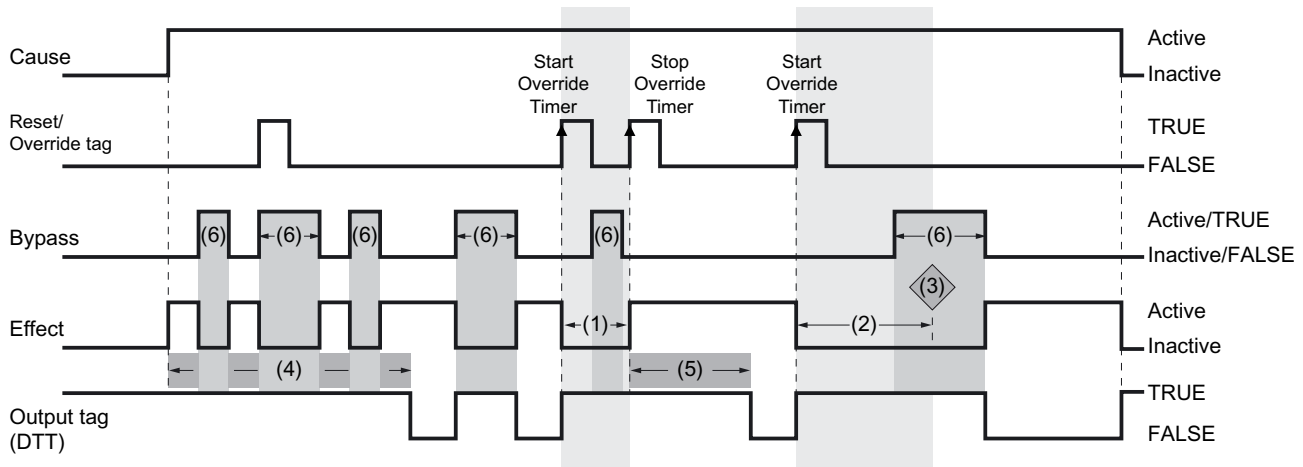
- (1), (2): Output delay timer runs
- (3): Bypass active
- If the Cause becomes inactive, the output delay timer is also stopped.
- (2): Bypass interrupts the output delay timer. Thus, the output delay can be delayed by an additional time.

Bypass of an effect with output delay for intersection type "S - Stored"



- (1), (2): Output delay timer runs
- (3): Bypass active
- The Effect becomes active as a result of an active Cause. The output delay timer starts. After it expires, the output tag is also set (to FALSE if DTT; to TRUE if ETT).
- (2): Bypass interrupts the output delay timer. Thus, the output delay can be delayed by an additional time.
- The output delay timer is only restarted if the Cause has become active.
- Once the Cause has become inactive, the Effect must be reset; otherwise, it remains active and the bypass can be in Effect.

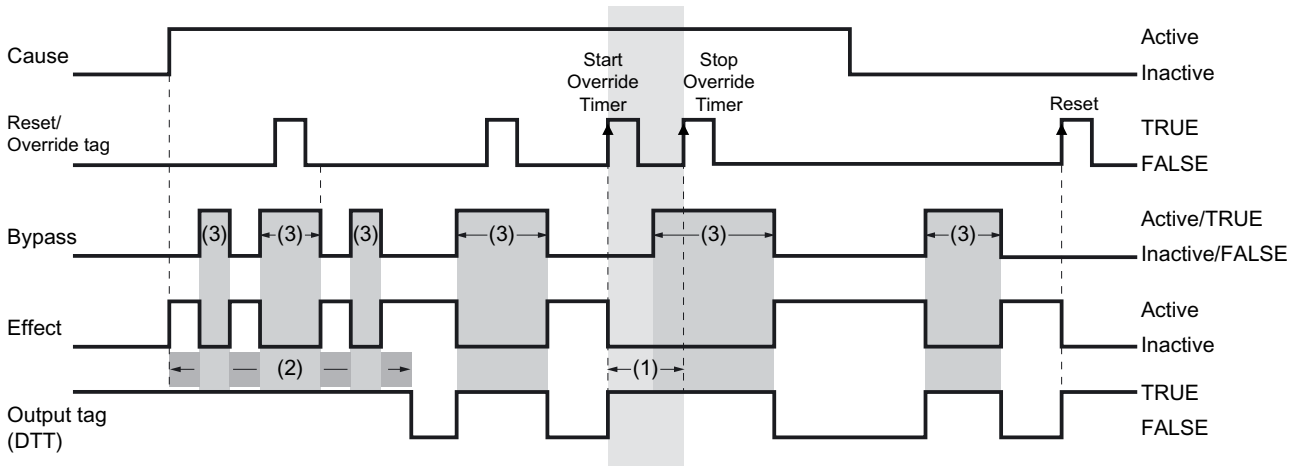
Bypass of an effect with output delay for intersection type "V - Overridable"



- (1), (2): Override timer runs
- (4), (5): Output delay timer runs
- (6): Bypass active
- (1): Time < Maximum override time
- (2): Time >= Maximum override time
- (3): **Alarm:** Time-out when the effect is overridden; the alarm is cleared either via an operator input or through a restart of the override timer.
- The Effect becomes active as a result of an active Cause. The output delay timer starts. After it expires, the output tag is also set (to FALSE if DTT; to TRUE if ETT).
- (4): The output delay timer can be interrupted by the bypass.
- (4), (5): The output delay timer is only started if the Cause has become active or the override timer has been stopped while no bypass was active.
- If the Cause becomes inactive, the Effect will also become inactive immediately. All timers are reset.
- A rising edge of the reset/override tag both starts and stops the override timer.
- (3): The override timer is stopped as soon as the maximum override time has been reached.
- (1): Activation of the bypass does not stop the override timer.
- If the override timer is started and bypass is then activated, the override timer can be stopped again by a positive edge of the reset/override tag.
- The override timer cannot be activated if bypass is active.

Bypass of an effect with output delay for intersection type "R - Resettable and overridable"

Because intersection type R is a combination of intersection types S and V, the properties of these intersections are also represented here.



- (1): Override timer runs
- (2): Output delay timer runs
- (3): Bypass active
- The Effect becomes active as a result of an active Cause. The output delay timer starts. After it expires, the output tag is also set (to FALSE if DTT; to TRUE if ETT).
- (2): The output delay timer can be interrupted by the bypass.
- The output delay timer is only started if the Cause has become active or the override timer has been stopped while no bypass was active.
- A rising edge of the reset/override tag both starts and stops the override timer.
- The override timer is automatically stopped as soon as the maximum override time has been reached.
- Activation of the bypass does not affect the override timer.
- If the override timer is started and bypass is then activated, the override timer can be stopped again by a positive edge of the reset/override tag.
- The override timer cannot be activated if bypass is active.
- Once the Cause has become inactive, the Effect must be reset; otherwise, it remains active and the bypass can be in effect.
- If the Cause becomes inactive while the override timer is running, the Effect will not be stored, i.e., it will become inactive immediately without the need for a reset.
- If the Cause becomes inactive while the output delay timer is running, the Effect will be stored and will become inactive only when a reset has taken place.

13.2.5 Pass through process data and mask enable

Behavior for "Pass through process data" and mask enable

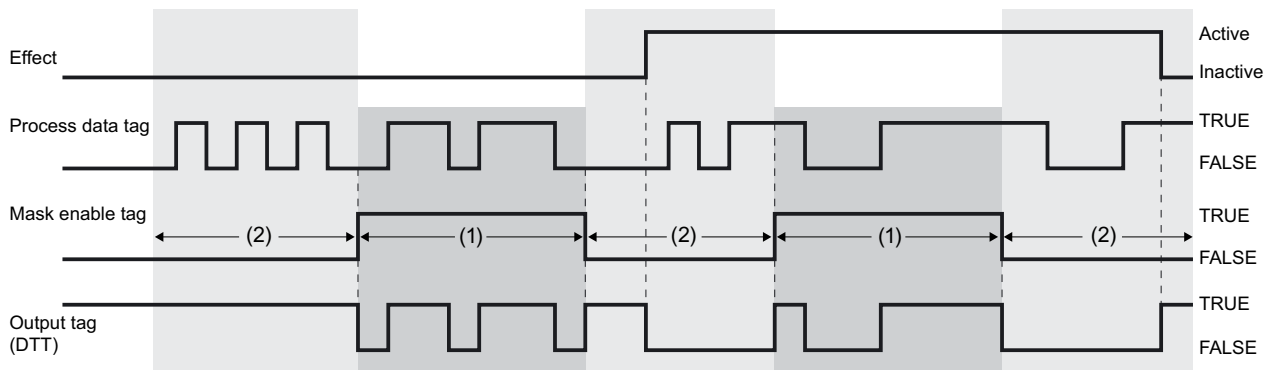
The effects of the different combination of the two options on the output tags of the effect are discussed in detail below with the help of diagrams.

Dependencies between "Pass through process data" and mask enable

Pass through process data	Mask enable tag	Result
Not activated	Not configured	No effect
Not activated	Configured	See below: "Mask" configuration
Enabled	Not configured	See below: "Pass through process data" configuration
Enabled	Configured	See below: "Pass through process data" configuration and "Mask" simultaneously

"Mask" configuration

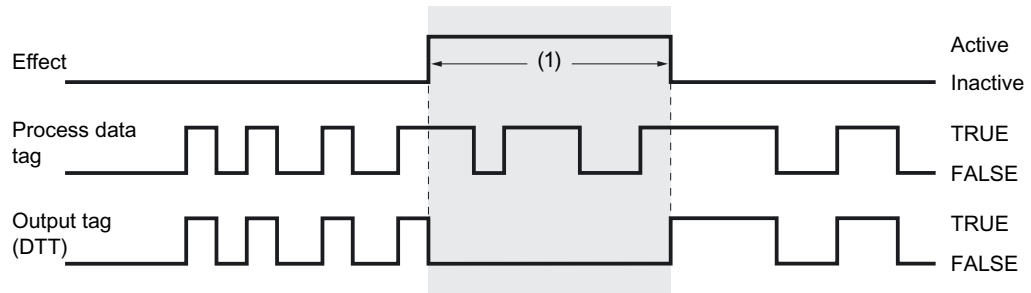
Process data tag and mask enable-tag are configured, "Pass through process value" is not activated, which means the output tag follows the following logic:



- The value of the mask enable tag specifies whether the effect logic or an externally controlled process tag (the process data tag) is interconnected to the output tags of the effect.
- (1): If the mask enable tag is TRUE, the value of the process data tag is transferred to the output tags.
- (2): If the mask enable tag is FALSE, the effect logic is applied to the output tags.

"Pass through process data" configuration

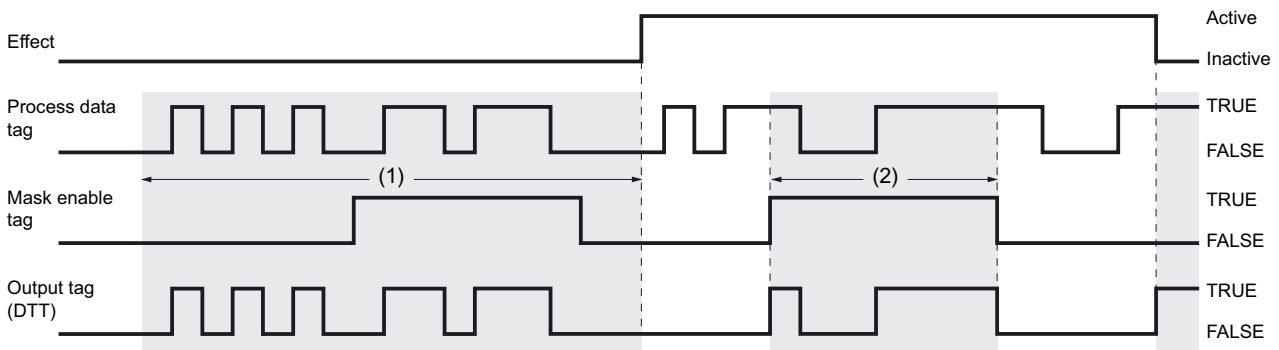
"Pass through process data" and process data tag configured, mask enable tag not configured:



- The passing through of the process value is controlled by the state of the effect.
- The value of the process data tag is transferred to the output tags when the effect is not active.
- (1): If the effect becomes active, the output tags are controlled by the state of the effect.

"Pass through process data" configuration and "Mask" simultaneously

Process data tag and mask enable-tag are configured, "Pass through process value" is activated, which means the output tag follows the following logic:



- (1): If the effect is not active, the value of the process data tag is always connected to the output tags regardless of the value of the mask enable tag.
- (2): If the effect is active, the value of the process data tag is only switched to the output tags when the mask enable tag is TRUE.

Requirements for virtual environments and remote access



A.1 Overview

Operating conditions, restrictions, enables

SIMATIC S7 F/FH Systems with S7 F Systems V6.0 and higher and SIMATIC Safety Matrix V6.1 SP1 and higher enable use in virtual environments for ES and OS under the following conditions.

All restrictions and notes in the corresponding releases of S7 F Systems and Safety Matrix, as well as of STEP 7 and PCS 7 continue to be valid for virtual environments and remote access.

Virtual environments

In information technology, a virtual machine refers to the emulation of a real computer system (hardware) on an abstraction layer which can execute multiple virtual machines at the same time. The abstraction layer is known as a hypervisor. Well-known manufacturers are Microsoft (Microsoft Hyper-V), VMware (VMware vSphere Hypervisor (ESXi)) and Citrix (XenServer).

A virtual environment enables, for example, very convenient test environments, simplifies the transfer of systems and saves space.

Remote Access and Control

In information technology, "remote access" designates the takeover of a graphical user interface and can be employed for different types of access. In this document, "remote access" refers to the unique access to the graphical user interface and the transfer of keyboard actions and mouse movements of an Engineering Station or Operator Station. Well-known software products include Microsoft Remote Desktop Protocol (RDP) and the RealVNC Open Source Software VNC (RFC 6143).

Recommended software requirements

SIMATIC STEP 7 and PCS 7 are released for virtual environments and remote access and can be integrated in your plant under the environment descriptions linked here.

Products	Product news
PCS 7 V8.0 SP2: <ul style="list-style-type: none">• VMware vSphere V5.0• VMware vSphere V5.1	https://support.industry.siemens.com/cs/ww/en/view/102378876c (https://support.industry.siemens.com/cs/ww/en/view/102378876c)
PCS 7 V8.1: <ul style="list-style-type: none">• VMware vSphere V5.5	https://support.industry.siemens.com/cs/ww/en/view/93997453 (https://support.industry.siemens.com/cs/ww/en/view/93997453)

A.2 Configuration and operation

Products	Product news
PCS 7 V8.2: • VMware vSphere V5.5	https://support.industry.siemens.com/cs/ww/en/view/109737952 (https://support.industry.siemens.com/cs/ww/en/view/109737952)
PCS 7 V9.0 SP1: • VMware vSphere V6.5	https://support.industry.siemens.com/cs/ww/en/view/109755764 (https://support.industry.siemens.com/cs/ww/en/view/109755764)
Service Pack 4 for STEP 7 V5.5 and STEP 7 Professional Edition 2010 ^{*1)} : • VMware vSphere Hypervisor ESX(i) 5.5 • VMware Workstation 10.0 • VMware Player 5.02 • Microsoft Windows Server 2012 Hyper-V	https://support.industry.siemens.com/cs/ww/en/view/93842005 (https://support.industry.siemens.com/cs/ww/en/view/93842005)

*1) Only configuration, programming and operation in STEP 7 Engineering.


Note

Siemens provides preconfigured virtualization solutions with its "SIMATIC Virtualization as a Service".

For more information, see the following entry: <https://support.industry.siemens.com/sc/ww/en/sc/3095> (<https://support.industry.siemens.com/sc/ww/en/sc/3095>)

A.2 Configuration and operation

A.2.1 Virtual environments

 WARNING
<p>Use of virtual environments in ES/OS</p> <p>Note that a HYPERVISOR or the client software of a HYPERVISOR is not permitted to perform functions that reproduce recorded frame sequences with correct time behavior on a network with connected plants.</p> <p>Ensure that this is the case when using the following functions, for example:</p> <ul style="list-style-type: none"> • Reset of captured states (snapshots) of the virtual machine (VM) • Suspending and resuming the VM (suspend & resume) • Replay of recorded sequences in the VMs (replay) • Moving of VMs between hosts in productive operation (e.g. Fault Tolerance (FT)) • Digital twins of VMs in the virtual environment <p>If in doubt, disable these functions in the settings (HYPERVISOR administrator console).</p> <p>(SMW-020)</p>

Note

How do you use VMware vSphere Client to assign operator permissions for a virtual machine?

<https://support.industry.siemens.com/cs/ww/en/view/90142228> (<https://support.industry.siemens.com/cs/ww/en/view/90142228>)

Note

How do you use a controller to load from a VM (VMware Player/Workstation) via a PROFIBUS/MPI CP connected via PCI or PCIe?

<https://support.industry.siemens.com/cs/ww/en/view/100450795> (<https://support.industry.siemens.com/cs/ww/en/view/100450795>)

Note

Configure Hyper-V for Role-based Access Control

[https://technet.microsoft.com/en-us/library/dd283076\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd283076(v=ws.10).aspx) ([https://technet.microsoft.com/en-us/library/dd283076\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd283076(v=ws.10).aspx))

A.2.2 Remote Access and Control

 WARNING**Remote access from higher-level control room and Engineering Center**

Make sure that the plants are clearly distinguished from other accessible plants connected on the network before you start making changes or start operation.

Examples:

- Specify optical distinguishing marks (plant designation) at your operator stations.
- Specify unique descriptions for title and project in the properties of the Safety Matrix for all the plants connected on the network and check this before starting operation.
- Specify Active Directory access limitations in the corporate directory service and use SIMATIC Logon for accessing projects and for logging on to operator stations.

(SMW-021)

Carefully choose the persons who may have remote access to the plant and authorize them accordingly:

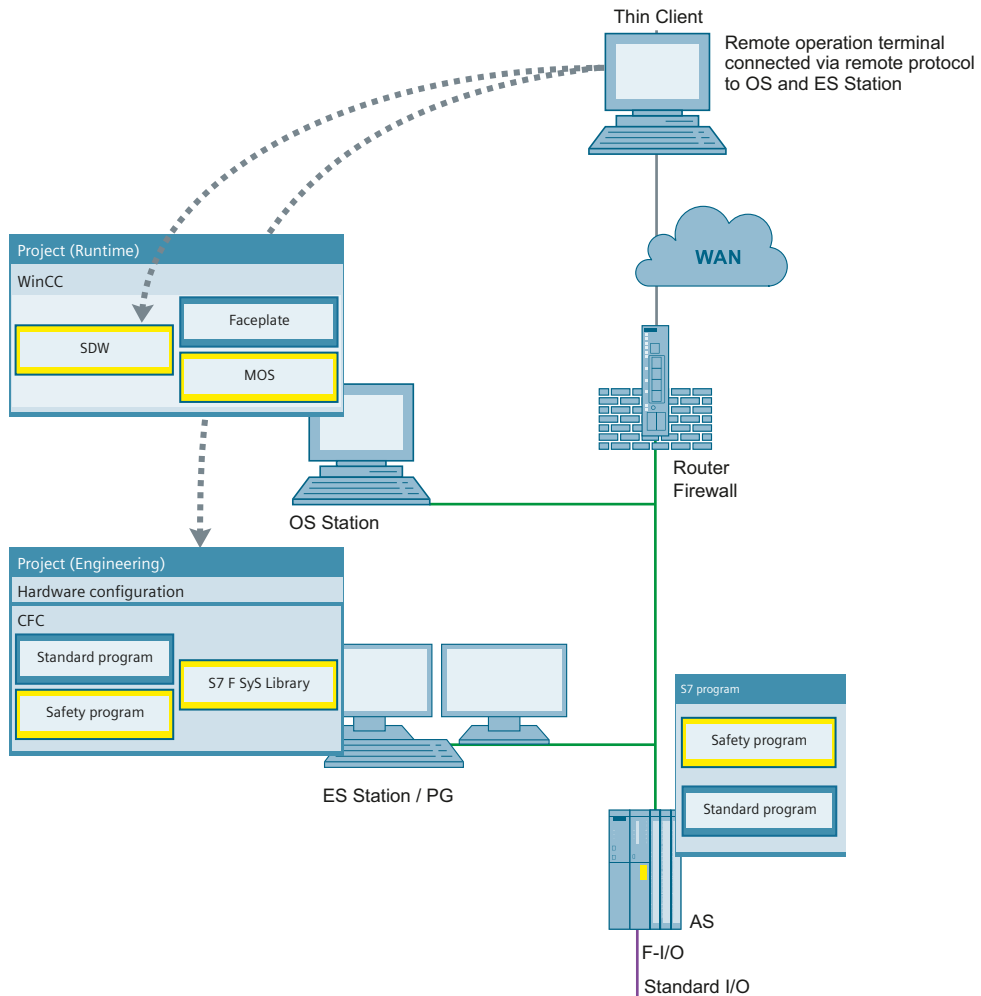
- Locally on the target computer "Remote Desktop User" (Workgroups)
OR
- In the Active Directory, and inherit permissions to the target computer "Remote Desktop User" (Domain).

A.2 Configuration and operation

As required, make a distinction in the WinCC authorizations between:

- Process control
- Higher process control
- Safety application control (SIF)

Fig. A-1: Diagram of Engineering Station and Operator Station in projects with safety applications



ES station

Physical location	Installed software
At the same location as the AS station and connected to the plant/terminal bus.	SIMATIC PCS 7 (package: PCS 7 Engineering) or STEP 7

OS station

Physical location	Installed software
At the same location as the AS station and connected to the plant/terminal bus.	SIMATIC PCS 7 (package: OS Client or OS Single Station)

Thin Client

Physical location	Installed software
Not at the same location as the AS station and not connected to the plant bus.	No SIMATIC software installed.

Note

SIMATIC Process Control System PCS 7 - PC Configuration - Section 5.8.2

<https://support.industry.siemens.com/cs/ww/en/view/90635791> (<https://support.industry.siemens.com/cs/ww/en/view/90635791>)

Note

Whitepaper; Security concept PCS 7 and WinCC - Basic document

<https://support.industry.siemens.com/cs/ww/en/view/26462131> (<https://support.industry.siemens.com/cs/ww/en/view/26462131>)

Note

How do you access WinCC and PCS 7 plants with "RealVNC"?

<https://support.industry.siemens.com/cs/ww/en/view/55422236> (<https://support.industry.siemens.com/cs/ww/en/view/55422236>)

Note

IP-based Remote Networks

<https://support.industry.siemens.com/cs/ww/en/view/26662448> (<https://support.industry.siemens.com/cs/ww/en/view/26662448>)

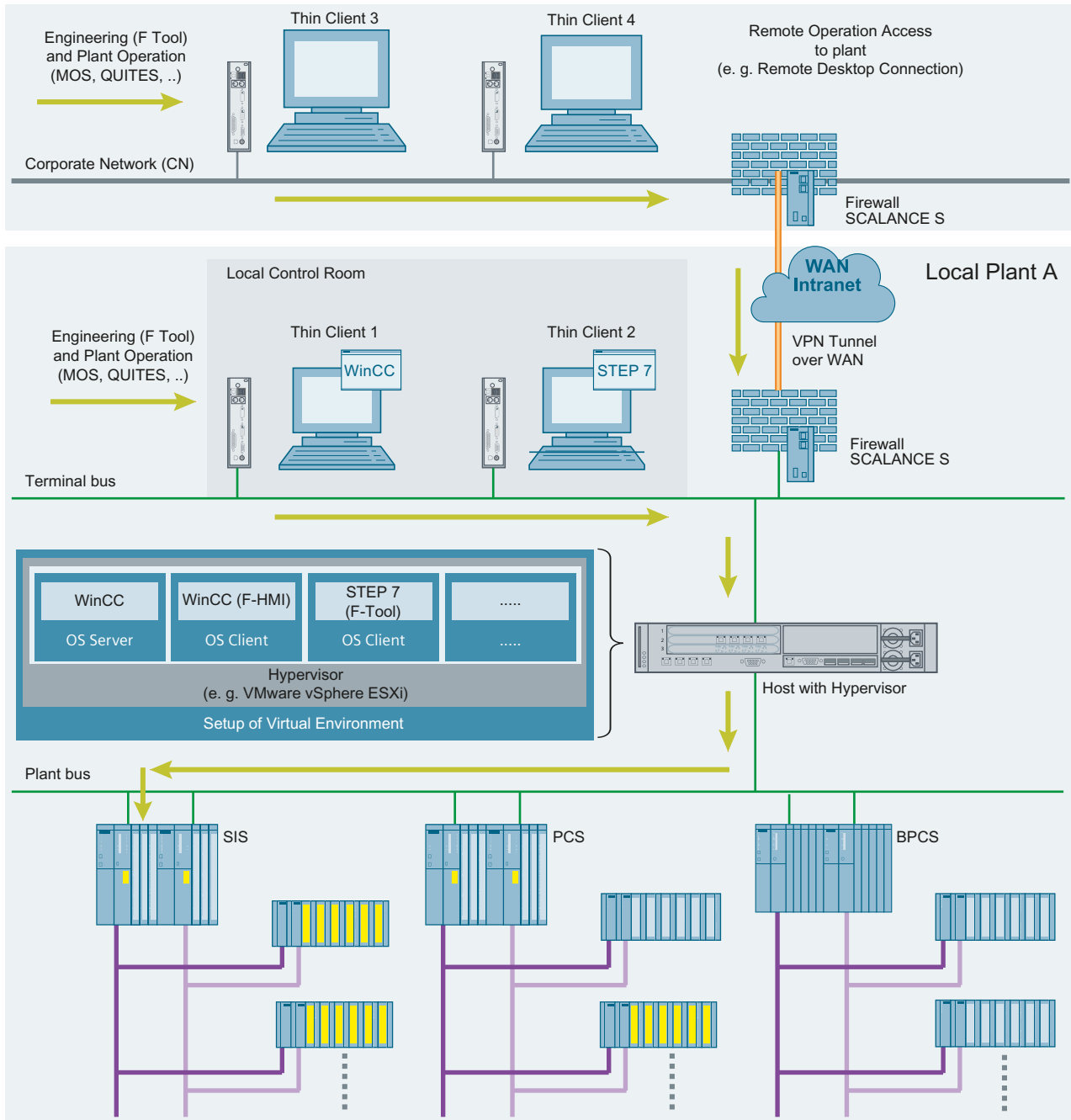
A.3 Examples of valid configurations in PCS 7

A.3.1 Example 1

The following figure shows a virtual environment for engineering and plant operation of safety applications including remote control.

A.3 Examples of valid configurations in PCS 7

Fig. A-2:



A.3.2 Example 2

The following figures show a configuration for remote access for configuration and maintenance operations as well as plant operation from higher-level control room in real and virtual environments.

Fig. A-3a:

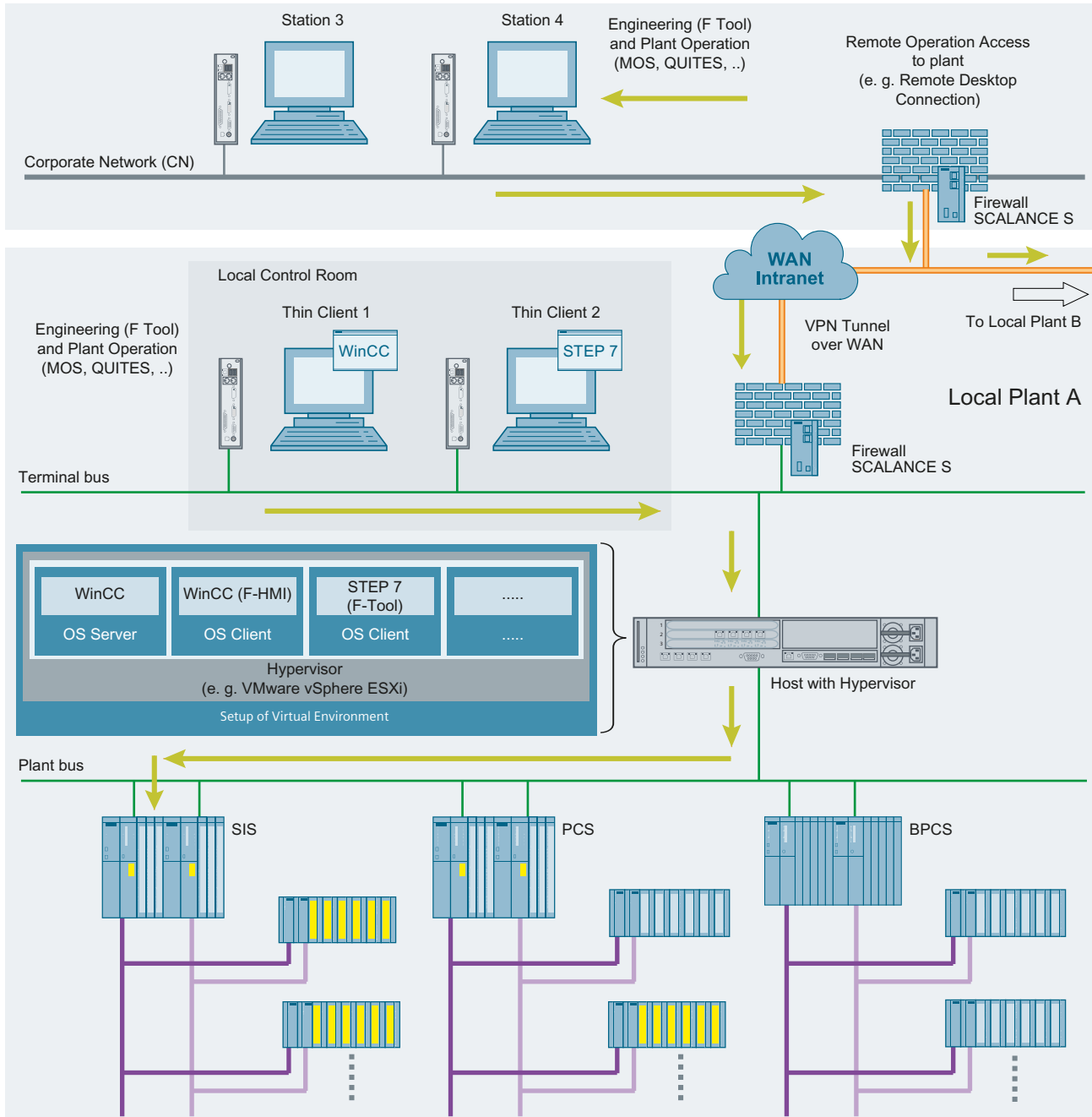
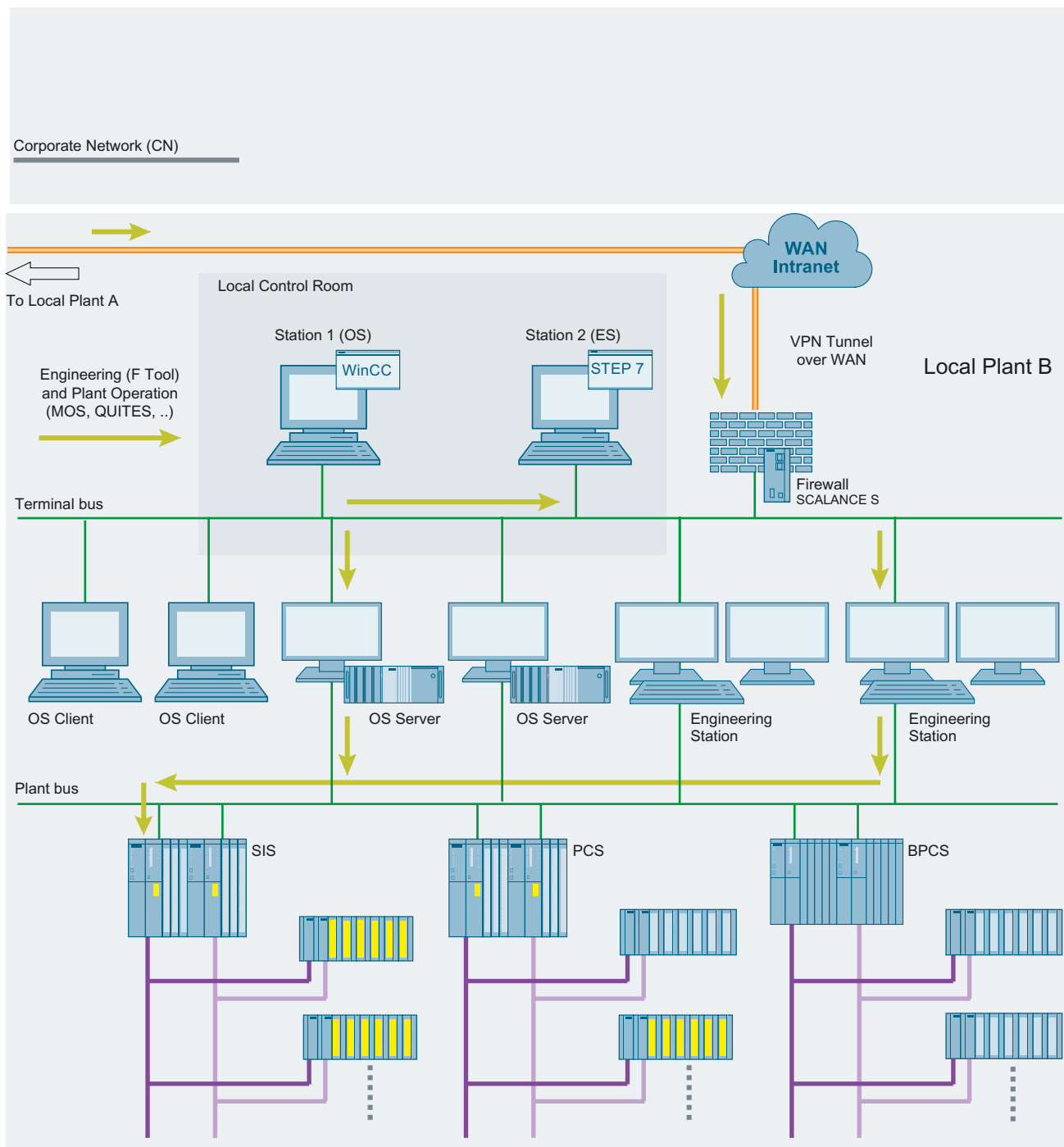


Fig. A-3b:

A.3 Examples of valid configurations in PCS 7



A.4 Abbreviations and explanations of terms

Abbreviation	Explanation of term
AD	Active Directory
BPCS	Basic Process Control System
CN	Corporate Network (company network/intranet)
ES	Engineering Station
LCR	Local Control Room
LER	Local Engineering Room
MOS	Maintenance Override Switch
OS	Operator Station
PCS	Process Control System
QUITES	Acknowledgment via ES/OS
ROC	Remote Operation Center (higher-level control than LCR)
SDW	Safety Data Write
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
VM	Virtual Machine (guest operating system)
WAN	Wide Area Network

A.5 References

	Subject area	Link
\1\	SIMATIC Industrial Software Safety Engineering in SIMATIC S7	https://support.industry.siemens.com/cs/ww/en/view/12490443 (https://support.industry.siemens.com/cs/ww/en/view/12490443)
\2\	SIMATIC Industrial Software S7 F/FH Systems - Configuring and Programming	https://support.industry.siemens.com/cs/ww/en/view/109742100 (https://support.industry.siemens.com/cs/ww/en/view/109742100)
\3\	SIMATIC Industrial Software Safety Matrix	https://support.industry.siemens.com/cs/ww/en/view/100675874 (https://support.industry.siemens.com/cs/ww/en/view/100675874)
\4\	SIMATIC PCS 7 technical documentation	www.siemens.com/pcs7-documentation (www.siemens.com/pcs7-documentation)
\5\	SIMATIC PCS 7 OS Software Client V7.1 + SP2 and higher released for use in virtual operating environments	https://support.industry.siemens.com/cs/ww/en/view/51401737 (https://support.industry.siemens.com/cs/ww/en/view/51401737)
\6\	SIMATIC Virtualization as a Service	https://support.industry.siemens.com/sc/ww/en/sc/3095 (https://support.industry.siemens.com/sc/ww/en/sc/3095)

A.5 References

	Subject area	Link
\7\	VMware vSphere Documentation V5.5	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html (https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html)
\8\	Microsoft Hyper-V	https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview (https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview)
\9\	XenServer Documentation Index	http://docs.vmd.citrix.com/XenServer/6.5.0/1.0/en_gb/ (http://docs.vmd.citrix.com/XenServer/6.5.0/1.0/en_gb/)

Resulting cause logic for Degraded Voting

B.1 Function type "OR" with 2 input tags (1oo2)

Introduction

The tables below show the resulting Cause logic for a Cause with two input tags and the function type "OR" (1oo2).

The configured options at the Cause are listed in the tables.

Table 1

The following option is configured at the Cause for ""Bad Quality" Voting":

- Trip on "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	1oo2	Inactive
2	Not tripped	Tripped/Bad Quality	1oo2	Active
3	Not tripped	Bypass	1oo1	Inactive
4	Tripped/Bad Quality	Tripped/Bad Quality	1oo2	Active
5	Tripped/Bad Quality	Bypass	1oo1	Active
6	Bypass	Bypass	Bypass	Inactive

Table 2

The following option is configured at the Cause for ""Bad Quality" Voting":

- Degraded Voting at "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	1oo2	Inactive
2	Not tripped	Tripped	1oo2	Active
3	Not tripped	Bad Quality	1oo1	Inactive
4	Not tripped	Bypass	1oo1	Inactive
5	Tripped	Tripped	1oo2	Active
6	Tripped	Bad Quality	1oo1	Active
7	Tripped	Bypass	1oo1	Active
8	Bad Quality	Bad Quality	(1oo1)	Active
9	Bad Quality	Bypass	(1oo1)	Active
10	Bypass	Bypass	Bypass	Inactive

B.2 Function type "AND" with 2 input tags (2oo2)

Table 3

The following option is configured at the Cause for ""Bad Quality" Voting":

- 'Ignore "Bad Quality"' = 1

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	1oo2	Inactive
2	Not tripped	Tripped	1oo2	Active
3	Not tripped	Bypass	1oo1	Inactive
4	Tripped	Tripped	1oo2	Active
5	Tripped	Bypass	1oo1	Active
6	Bypass	Bypass	Bypass	Inactive

B.2 Function type "AND" with 2 input tags (2oo2)

Introduction

The tables below show the resulting Cause logic for a Cause with two input tags and the function type "AND" (2oo2).

The configured options at the Cause are listed in the tables.

Table 1

The following option is configured at the Cause for ""Bad Quality" Voting":

- Trip on "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	2oo2	Inactive
2	Not tripped	Tripped/Bad Quality	2oo2	Inactive
3	Not tripped	Bypass	1oo1	Inactive
4	Tripped/Bad Quality	Tripped/Bad Quality	2oo2	Active
5	Tripped/Bad Quality	Bypass	1oo1	Active
6	Bypass	Bypass	Bypass	Inactive

Table 2

The following option is configured at the Cause for ""Bad Quality" Voting":

- Degraded Voting at "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	2oo2	Inactive
2	Not tripped	Tripped	2oo2	Inactive

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
3	Not tripped	Bad Quality	1oo1	Inactive
4	Not tripped	Bypass	1oo1	Inactive
5	Tripped	Tripped	2oo2	Active
6	Tripped	Bad Quality	1oo1	Active
7	Tripped	Bypass	1oo1	Active
8	Bad Quality	Bad Quality	(1oo1)	Active
9	Bad Quality	Bypass	(1oo1)	Active
10	Bypass	Bypass	Bypass	Inactive

Table 3

The following option is configured at the Cause for ""Bad Quality" Voting":

- 'Ignore "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	2oo2	Inactive
2	Not tripped	Tripped	2oo2	Inactive
3	Not tripped	Bypass	1oo1	Inactive
4	Tripped	Tripped	2oo2	Active
5	Tripped	Bypass	1oo1	Active
6	Bypass	Bypass	Bypass	Inactive

B.3 Function type "OR" with 3 input tags (1oo3)

Introduction

The tables below show the resulting Cause logic for a Cause with three input tags and the function type "OR" (1oo3).

The configured options at the Cause are listed in the tables.

Table 1

The following option is configured at the Cause for ""Bad Quality" Voting":

- Trip on "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	1oo3	Inactive
2	Not tripped	Not tripped	Tripped/Bad Quality	1oo3	Active
3	Not tripped	Not tripped	Bypass	1oo2	Inactive
4	Not tripped	Tripped/Bad Quality	Tripped/Bad Quality	1oo3	Active
5	Not tripped	Tripped/Bad Quality	Bypass	1oo2	Active

B.3 Function type "OR" with 3 input tags (1oo3)

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
6	Not tripped	Bypass	Bypass	1oo1	Inactive
7	Tripped/Bad Quality	Tripped/Bad Quality	Tripped/Bad Quality	1oo3	Active
8	Tripped/Bad Quality	Tripped/Bad Quality	Bypass	1oo2	Active
9	Tripped/Bad Quality	Bypass	Bypass	1oo1	Active
10	Bypass	Bypass	Bypass	Bypass	Inactive

Table 2

The following option is configured at the Cause for ""Bad Quality" Voting":

- Degraded Voting at "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	1oo3	Inactive
2	Not tripped	Not tripped	Tripped	1oo3	Active
3	Not tripped	Not tripped	Bad Quality	1oo2	Inactive
4	Not tripped	Not tripped	Bypass	1oo2	Inactive
5	Not tripped	Tripped	Tripped	1oo3	Active
6	Not tripped	Tripped	Bad Quality	1oo2	Active
7	Not tripped	Tripped	Bypass	1oo2	Active
8	Not tripped	Bad Quality	Bad Quality	1oo1	Inactive
9	Not tripped	Bad Quality	Bypass	1oo1	Inactive
10	Not tripped	Bypass	Bypass	1oo1	Inactive
11	Tripped	Tripped	Tripped	1oo3	Active
12	Tripped	Tripped	Bad Quality	1oo2	Active
13	Tripped	Tripped	Bypass	1oo2	Active
14	Tripped	Bad Quality	Bad Quality	1oo1	Active
15	Tripped	Bad Quality	Bypass	1oo1	Active
16	Tripped	Bypass	Bypass	1oo1	Active
17	Bad Quality	Bad Quality	Bad Quality	(1oo1)	Active
18	Bad Quality	Bad Quality	Bypass	(1oo1)	Active
19	Bad Quality	Bypass	Bypass	(1oo1)	Active
20	Bypass	Bypass	Bypass	Bypass	Inactive

Table 3

The following option is configured at the Cause for ""Bad Quality" Voting":

- 'Ignore "Bad Quality"' = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	1oo3	Inactive
2	Not tripped	Not tripped	Tripped	1oo3	Active
3	Not tripped	Not tripped	Bypass	1oo2	Inactive

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
4	Not tripped	Tripped	Tripped	1oo3	Active
5	Not tripped	Tripped	Bypass	1oo2	Active
6	Not tripped	Bypass	Bypass	1oo1	Inactive
7	Tripped	Tripped	Tripped	1oo3	Active
8	Tripped	Tripped	Bypass	1oo2	Active
9	Tripped	Bypass	Bypass	1oo1	Active
10	Bypass	Bypass	Bypass	Bypass	Inactive

B.4 Function type "2oo3"

Introduction

The tables below show the resulting Cause logic for a Cause with three input tags and the function type "2oo3".

The configured options at the Cause are listed in the tables.

Table 1

The following option is configured at the Cause for ""Bad Quality" Voting":

- Trip on "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	2oo3	Inactive
2	Not tripped	Not tripped	Tripped/Bad Quality	2oo3	Inactive
3	Not tripped	Not tripped	Bypass	1oo2	Inactive
4	Not tripped	Tripped/Bad Quality	Tripped/Bad Quality	2oo3	Active
5	Not tripped	Tripped/Bad Quality	Bypass	1oo2	Active
6	Not tripped	Bypass	Bypass	1oo1	Inactive
7	Tripped/Bad Quality	Tripped/Bad Quality	Tripped/Bad Quality	2oo3	Active
8	Tripped/Bad Quality	Tripped/Bad Quality	Bypass	1oo2	Active
9	Tripped/Bad Quality	Bypass	Bypass	1oo1	Active
10	Bypass	Bypass	Bypass	Bypass	Inactive

Table 2

The following option is configured at the Cause for ""Bad Quality" Voting":

- Degraded Voting at "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	2oo3	Inactive
2	Not tripped	Not tripped	Tripped	2oo3	Inactive

B.4 Function type "2oo3"

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
3	Not tripped	Not tripped	Bad Quality	1oo2	Inactive
4	Not tripped	Not tripped	Bypass	1oo2	Inactive
5	Not tripped	Tripped	Tripped	2oo3	Active
6	Not tripped	Tripped	Bad Quality	1oo2	Active
7	Not tripped	Tripped	Bypass	1oo2	Active
8	Not tripped	Bad Quality	Bad Quality	1oo1	Inactive
9	Not tripped	Bad Quality	Bypass	1oo1	Inactive
10	Not tripped	Bypass	Bypass	1oo1	Inactive
11	Tripped	Tripped	Tripped	2oo3	Active
12	Tripped	Tripped	Bad Quality	1oo2	Active
13	Tripped	Tripped	Bypass	1oo2	Active
14	Tripped	Bad Quality	Bad Quality	1oo1	Active
15	Tripped	Bad Quality	Bypass	1oo1	Active
16	Tripped	Bypass	Bypass	1oo1	Active
17	Bad Quality	Bad Quality	Bad Quality	(1oo1)	Active
18	Bad Quality	Bad Quality	Bypass	(1oo1)	Active
19	Bad Quality	Bypass	Bypass	(1oo1)	Active
20	Bypass	Bypass	Bypass	Bypass	Inactive

Table 3

The following option is configured at the Cause for ""Bad Quality" Voting":

- 'Ignore "Bad Quality"' = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	2oo3	Inactive
2	Not tripped	Not tripped	Tripped	2oo3	Inactive
3	Not tripped	Not tripped	Bypass	1oo2	Inactive
4	Not tripped	Tripped	Tripped	2oo3	Active
5	Not tripped	Tripped	Bypass	1oo2	Active
6	Not tripped	Bypass	Bypass	1oo1	Inactive
7	Tripped	Tripped	Tripped	2oo3	Active
8	Tripped	Tripped	Bypass	1oo2	Active
9	Tripped	Bypass	Bypass	1oo1	Active
10	Bypass	Bypass	Bypass	Bypass	Inactive

B.5 Function type "AND" with 3 input tags (3oo3)

Introduction

The tables below show the resulting Cause logic for a Cause with three input tags and the function type "AND" (3oo3).

The configured options at the Cause are listed in the tables.

Table 1

The following option is configured at the Cause for ""Bad Quality" Voting":

- Trip on "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	3oo3	Inactive
2	Not tripped	Not tripped	Tripped/Bad Quality	3oo3	Inactive
3	Not tripped	Not tripped	Bypass	2oo2	Inactive
4	Not tripped	Tripped/Bad Quality	Tripped/Bad Quality	3oo3	Inactive
5	Not tripped	Tripped/Bad Quality	Bypass	2oo2	Inactive
6	Not tripped	Bypass	Bypass	1oo1	Inactive
7	Tripped/Bad Quality	Tripped/Bad Quality	Tripped/Bad Quality	3oo3	Active
8	Tripped/Bad Quality	Tripped/Bad Quality	Bypass	2oo2	Active
9	Tripped/Bad Quality	Bypass	Bypass	1oo1	Active
10	Bypass	Bypass	Bypass	Bypass	Inactive

Table 2

The following option is configured at the Cause for ""Bad Quality" Voting":

- Degraded Voting at "Bad Quality" = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	3oo3	Inactive
2	Not tripped	Not tripped	Tripped	3oo3	Inactive
3	Not tripped	Not tripped	Bad Quality	2oo2	Inactive
4	Not tripped	Not tripped	Bypass	2oo2	Inactive
5	Not tripped	Tripped	Tripped	3oo3	Active
6	Not tripped	Tripped	Bad Quality	2oo2	Active
7	Not tripped	Tripped	Bypass	2oo2	Active
8	Not tripped	Bad Quality	Bad Quality	1oo1	Inactive
9	Not tripped	Bad Quality	Bypass	1oo1	Inactive
10	Not tripped	Bypass	Bypass	1oo1	Inactive
11	Tripped	Tripped	Tripped	3oo3	Active
12	Tripped	Tripped	Bad Quality	2oo2	Active

Resulting cause logic for Degraded Voting

B.5 Function type "AND" with 3 input tags (3oo3)

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
13	Tripped	Tripped	Bypass	2oo2	Active
14	Tripped	Bad Quality	Bad Quality	1oo1	Active
15	Tripped	Bad Quality	Bypass	1oo1	Active
16	Tripped	Bypass	Bypass	1oo1	Active
17	Bad Quality	Bad Quality	Bad Quality	(1oo1)	Active
18	Bad Quality	Bad Quality	Bypass	(1oo1)	Active
19	Bad Quality	Bypass	Bypass	(1oo1)	Active
20	Bypass	Bypass	Bypass	Bypass	Inactive

Table 3

The following option is configured at the Cause for ""Bad Quality" Voting":

- 'Ignore "Bad Quality"' = 1

Case	Status tag 1	Status tag 2	Status tag 3	Resulting Cause logic	Cause status
1	Not tripped	Not tripped	Not tripped	3oo3	Inactive
2	Not tripped	Not tripped	Tripped	3oo3	Inactive
3	Not tripped	Not tripped	Bypass	2oo2	Inactive
4	Not tripped	Tripped	Tripped	3oo3	Inactive
5	Not tripped	Tripped	Bypass	2oo2	Inactive
6	Not tripped	Bypass	Bypass	1oo1	Inactive
7	Tripped	Tripped	Tripped	3oo3	Active
8	Tripped	Tripped	Bypass	2oo2	Active
9	Tripped	Bypass	Bypass	1oo1	Active
10	Bypass	Bypass	Bypass	Bypass	Inactive

Glossary

2-operator scenario

During configuration of the Safety Matrix in the PCS 7 OS, you can select a 2-operator scenario (4-eyes principle). Two operator roles are defined for this purpose: initiator and confirmer.

- Initiator: the operator may start an operation.
- Confirmer: the operator may confirm an operation.

In addition to the initiator and/or confirmer permission, users must have the specified permission level for each operator function to be performed.

Access protection

Fail-safe systems must be protected against dangerous, unauthorized access. Access protection for F-systems is implemented by assigning two passwords (for the F-CPU and for the safety program).

Active

A Cause or Effect can be active, which means that it has been tripped.

Whether or not a Cause is active and when it becomes active is determined by the input tags, the function type, and the options for the Cause.

The activation of an Effect depends on the relationship (defined by intersections) to the Causes and the options for the Effect. If an effect is active, the output tags are set to "0" or "1", depending on the "Energize-to-trip" option.

Bypass

Bypass function that is normally used for maintenance purposes (e.g., to check effect logic or to replace a sensor).

- Bypass for the entire Cause or Effect:
A bypass for the entire Cause/Effect can be set by means of a so-called "hard bypass" or "soft bypass".
- Bypass for individual tags of a Cause:
A "soft bypass" can also be permitted for the individual tags of a Cause. The operator can manually set a bypass for individual tags of a Cause.

Category

Category to ISO 13849-1:2015 or EN ISO 13849-1:2015

S7 F systems can be used in safety mode up to Category 4.

Cause

A Cause represents a process event.

Conditions configured in the Cause must be fulfilled in order for the Cause to become active and thus to trigger an Effect defined by an intersection.

Analog or discrete values can be selected as the input type. The values of at least one but no more than three input tags together with the function type represent a Cause.

Channel error

Channel-specific error, such as a wire break or a short-circuit

Collective signatures

Collective signatures uniquely identify a particular state of the safety program. They are important for the preliminary acceptance test of the safety program, e.g., by assessors.

CRC

Cyclic Redundancy Check, see CRC signature

CRC signature

The validity of the process values in the safety message frame, the accuracy of the assigned address references, and the safety-related parameters are validated by means of the CRC signature in the safety message frame.

Deactivated safety mode

Periodic deactivation of safety mode for making changes in the safety program during operation.

Whenever safety mode is deactivated, the safety of the system must be ensured by other organizational measures, such as operation monitoring and manual safety shutdown.

Deenergize-to-trip (DTT)

Trip if FALSE: The Cause is active if input tag = "0" (low-active). The output tag is "0" if the effect is active. This negative logic is the default setting for the inputs and outputs of the Safety Matrix.

Degraded Voting

The "Degraded Voting" function allows you to take the individual input tags of a Cause "out of the evaluation" for the Cause in case of a bad signal status ("Bad Quality") or with an active soft bypass.

Depassivation

See reintegration

Effect

An effect represents the reaction that the Safety Matrix exerts on the process.

Certain conditions must be fulfilled in order for the effect to be triggered and thus have an effect on the process by means of its output tags.

The values of at least one but no more than four discrete output tags define the action to be performed on the process. The activation of an Effect depends on various factors (status of the assigned Causes, type of intersection, specified options for the Effect).

Energize-to-trip (ETT)

Trip on TRUE: The Cause is active if input tag = "1" (high-active). The output tag is "1" if the effect is active.

ES

Engineering system (ES): Configuration system that enables convenient, visual adaptation of the process control system to the task at hand.

Fail-safe systems

Fail-safe systems (F-systems) remain in a safe state or immediately assume another safe state as soon as particular failures occur.

Fault reaction function

See user safety function

F-block type

F-block types are ready-made program sections that can be used in a CFC chart (e.g., fail-safe addition block F_ADD_R, fail-safe multiplexer F_MUX2_R, etc.). Block instances are generated on insertion. Any number of block instances can be created by one F-block type.

The F-block type specifies the characteristics (algorithm) for all applications of this type. The name of the F-block type is specified in the symbol table.

F-blocks

The following fail-safe blocks are designated as F-Blocks:

- Blocks selected by the user from an F-Library.
- Blocks that are automatically added in the safety program.

F-CPU

An F-CPU is a central processing unit with fail-safe capability that is permitted for use in *S7 F Systems*. For *S7 F Systems*, the F-Runtime license allows the user to operate the central processing unit as an F-CPU. That is, a safety program can be run on it. A standard user program can also be run in the F-CPU.

F-Cycle time

Cyclic interrupt time for OBs with F-runtime groups

F-Data type

The standard user program and safety program use different data formats. Safety-related F-Data types are used in the safety program.

F-I/O

Group designation for fail-safe inputs and outputs or I/O modules available in *SIMATIC S7* for integration in *S7 F systems*, among others. The following are available for *S7 F Systems*:

- ET 200S fail-safe I/O modules
- ET 200SP fail-safe I/O modules
- S7-300 fail-safe signal modules in ET 200M (distributed configuration)
- ET 200eco fail-safe I/O modules
- ET 200pro fail-safe I/O modules
- ET 200iSP fail-safe I/O modules
- Fail-safe DP standard slaves
- Fail-safe IO standard devices
- Fail-safe PA field devices

F-runtime group

When the safety program is created, the F-blocks cannot be inserted directly into tasks/OBs; rather, they must be inserted into F-runtime groups. The safety program consists of multiple F-runtime groups.

F-shutdown groups

F-shutdown groups contain one or more F-runtime groups. F-shutdown group communications blocks are required between the F-blocks in the various F-shutdown groups.

If an error is detected in an F-Shutdown group, this F-Shutdown group is shut down. Additional F-Shutdown groups are shut down according to the configuration of F_SHUTDN.

F-SMs

S7-300 fail-safe signal modules that can be used for safety-related operation (see safety mode) as centralized modules in an S7-300 or as distributed modules in the ET 200M distributed I/O system. F-SMs are equipped with integrated safety functions.

F-Startup

An F-Startup is a restart following an F-STOP or an F-CPU STOP. *S7 F Systems* do not distinguish between a cold restart and warm restart of the F-CPU.

F-Systems

Fail-safe systems

Inactive

A Cause or Effect can be inactive, which means that the conditions for activation are not fulfilled.

Whether or not the Cause is inactive is determined by the input tags, the function type, and the options for the Cause.

The deactivation of an Effect depends on the relationship (defined by intersections) to the Causes and the options for the Effect. If an effect is inactive, the output tags are set to "0" or "1", depending on the "Energize-to-trip" option.

Initiator/confirmer

If the operation of a Safety Matrix is to be transacted by two operators, create two users:

- The initiator starts the Safety Matrix operation via Secure Write. This user must have the permission assigned to the "InitiatorLevel" attribute in the properties for the block icon. However, the initiator does not have permission to confirm the operation.
- The confirmer verifies and confirms the operation. This user must have the permission assigned to the "ConfirmerLevel" attribute in the properties for the block icon. However, the confirmer does not have permission to initiate the operation.

Intersection

Intersections form the link between the Causes and Effects and specify which Causes have an effect on the respective Effects. The properties of the link are specified with the intersection type.

OS

Operator station (OS): A configurable operator station used to operate and monitor machines and systems.

Partial shutdown

Only the F-shutdown group in which the error was detected is shut down.

Passivation

Passivation of digital output channels means that the outputs are de-energized.

Digital input channels are passivated when the inputs transmit a value of "0" to the F-CPU (by means of the fail-safe drivers), irrespective of the current process signal.

Analog input channels are passivated when the inputs transmit a fail-safe value or the last valid value to the F-CPU (by means of the fail-safe drivers), irrespective of the current process signal.

Process safety time

The process safety time of a process is the time interval during which the process can be left on its own without risk to life and limb of the operating personnel or damage to the environment.

Within the process safety time, any type of F-system process control is tolerated. That is, during this time, the F-system can control its process incorrectly or it can even exercise no control at all. The process safety time depends on the process type and must be determined on a case-by-case basis.

PROFIsafe

Safety-related bus profile of PROFIBUS DP/PA and PROFINET IO for communication between the safety program and the fail-safe I/Os in a fail-safe system.

Proof-test interval

Period after which a component must be forced to fail-safe state, that is, it is either replaced with an unused component, or is proven faultless.

Reintegration

Switchover from fail-safe values (0) to process data (reintegration of an F-I/O module) occurs automatically or, alternatively, only after user acknowledgment at the F-channel driver.

The reintegration method depends on the following:

- Cause of passivation of the F-I/O or channels of the F-I/O
- Parameter assignment for the F-channel driver

For an F-I/O with inputs, the process values pending at the fail-safe inputs are provided again at the output of the F-channel driver after reintegration. For an F-I/O with outputs, the F-System again transfers the output values pending at the input of the F-channel driver to the fail-safe outputs.

S7-PLCSIM

The *S7-PLCSIM* application enables you to execute and test your S7 program on a simulated automation system on your ES/OS. Because the simulation takes place entirely in STEP 7, you do not require any hardware (CPU, F-CPU, I/O).

Safe state

The basic principle of the safety concept in a fail-safe system is the existence of a safe state for all process variables. For the digital F I/O, the safe state is always "0".

Safety class

Safety Integrity Level (SIL) in accordance with IEC 61508. The higher the Safety Integrity Level, the more rigid the measures for prevention of systematic faults and for management of systematic faults and random hardware failures.

S7 F Systems can be used in safety mode up to safety class SIL3.

Safety function

Safety function is a mechanism integrated in F-CPU and F-I/O, which enables them to be used in fail-safe systems.

According to IEC 61508, the function is implemented by a safety device in order to maintain the system in a safe state or to place it into a safe state in the event of a particular fault (see user safety function).

Safety instrumented function groups (SIF groups)

You can create your own safety instrumented function groups for your application, that is, by dividing your application into function groups that you can then monitor and change selectively in the *Safety Matrix Engineering Tool* and *Safety Matrix Viewer* (e.g., "level measurement and shut off").

In order to use this function, you must assign the individual Causes and Effects of the safety program to your safety instrumented functions groups. Then, you can display one or more (or all) safety-instrumented function groups.

Safety message frame

In the safety mode, data is transferred in a safety message frame between the F-CPU and the F-I/O or, in safety-related CPU-to-CPU communication, between the F-CPU.

Safety mode

1. An operating mode for F I/Os in which safety-oriented communication using safety message frames is possible.
2. Operating mode of the safety program. In safety mode of the safety program, all safety mechanisms for fault detection and fault reaction are activated. In safety mode, the safety program cannot be modified during operation. Safety mode can be deactivated by the user (see deactivated safety mode).

Safety program

Safety-related user program

Safety protocol

See safety message frame

Safety-related communication

A type of communication for safe exchange of fail-safe data.

Signature

See collective signatures

Standard communication

Communication used to exchange non-safety-related data.

Standard mode

Operating mode of the F-I/O in which only standard communication, but no safety-oriented communication via safety message frames is possible.

Standard user program

Non-safety-related user program

User safety function

The safety function for the process can be provided through a user safety function or a fault reaction function. The user only has to program the user safety function. In the event of a fault, if the F-system can no longer execute its actual user safety function, it executes the fault reaction function: For example, the associated outputs are deactivated and the F-CPU switches to F-STOP mode if necessary.

Index

@

@MatrixName, 130, 137, 140

2

2-operator scenario, 148, 168

A

Acceptance test, 201

Configuration report, 199

Access protection, 127

ACK_NEC, 66

Active, 22

AL_Chart, 130, 138, 140

Alarm on input trip, 106, 206

Alarm profiles

Configuring, 92, 108, 117

Customize colors, 96

Group messages, 92

Matrix, 92

ALM, 27

Any signals from the safety program, 52, 54

Assignment of functions to user permissions, 92

Auto acknowledge active cause, 205

B

Block icons, 86

Bypass, 105, 205

Effect, 113, 211

for entire Cause/Effect, 24

for individual input tag of a Cause, 24

Bypass report, 176

C

Cause, 21

adding and editing, 100

Alarms, 108

Create/edit, 100

Inhibit, 106

Options, 105

Time function, 105

Time function for soft bypass, 105

Time lapse diagram for time functions, 107

Cause details

Alarms, 108

Analog parameter, 104

Configuring, 102

Options, 105

Cause/Effect matrix, 17

Cause/Effect matrix file, (See CEM file)

CEM file

Importing, 124

CH_STATx

F_SC_AL, 75

F_SC_AL2, 81

F_SE_AL, 85

Change limit, 104

Changes in safety program

Acceptance test, 202

Changes only

Transfer option, 132

Changing limit, 183

Changing range limits, 102, 183

Changing the delta, 104, 183

Changing the hysteresis, 104, 183

Channel driver

Acknowledgment, 66

Channel drivers, 64

Clean nested chart connections

Transfer option, 133

Color codes for status display, 163

Colors, 96

Column for effect, 109

Compare

Programs (CFC charts), 195

Safety Matrices, 194

Compilation of the program, 143

Compiling and downloading to the OS, 144

CONFIG_V

F_SC_AL, 72

F_SC_AL2, 78

F_SE_AL, 82

Configuration and data storage, 144

Configuration areas of the Safety Matrix user interface, 41

Configuration report, 198

Confirmer, 173, 178, 180

Continuous Function Chart (CFC)

Notes, 139

Control bar functions, 168, 175

Critical changes, 90, 97
Customer-specific channel driver, 54
Customer-specific F-channel drivers, 52, 54

D

Deenergize-to-trip (DTT), 23
Degraded Voting, 24
 Activation, 60
 at 'Bad Quality',
 Display, 60
 Implementation at function type "AND"
 (2oo2), 232
 Implementation at function type "AND"
 (3oo3), 237
 Implementation at function type "OR" (1oo2), 231
 Implementation at function type "OR" (1oo3), 233
 Implementation at function type '2oo3', 62, 235
DIAG_V
 F_SC_AL, 74
 F_SC_AL2, 80
 F_SE_AL, 84
Downloading the program to the F-CPU, 143
Driver acknowledgment, 66
DTT, 23, 97

E

Editing permission levels, 92
Editing the properties
 Customize, 96
Effect, 22
 Alarms, 116
 creating, 109
 Edit, 109
 Shortcut menu, 109
Effect details
 Alarms, 116
 Configuring, 111
 Options, 113
EN_GDM, 63
EN_SWC, 137
Energize-to-trip (ETT), 23
Entries in the event log, 184
ETT, 23
Event log, 184
Executable sequence, 139
Export of a Safety Matrix, 120

F

F_FBO_SM, 65
F_MA_AL, 92, 134
 Connections, 68
F_SC_AL, 91, 108, 134
 Connections, 70
F_SC_AL2, 91, 108, 134
 Connections, 76
F_SE_AL, 91, 116, 134
 Connections, 81
Faceplate
 Messages view, 161
 Overview row, 156
 Standard view, 160
 User rights view, 162
Faceplate overview row, 156
Fail-safe systems
 Access protection, 127
F-channel drivers, 64
F-channel drivers from S7 F Systems, 136
Floating-point number, 99
Function type, 23
 Cause, 98, 103
 Effect, 112

G

Group acknowledgment, 52
Group deactivation of maintenance operations, 63

H

Hard bypass, 24

I

Ignore "Bad Quality", 107
Import of a Safety Matrix, 120, 124
Inactive, 22
Information areas of the Safety Matrix user
interface, 41
Inhibit tag, 204
Initial acceptance test of a safety program, 201
Initiator, 173, 177, 179
Input and output tags, 52, 54
Installing
 Requirements, 27
 Safety Matrix components, 28

- Integrate external channel drivers
 - Transfer option, 133
- Interface assignment according to the majority principle, 120
- Internal references, 52, 54
- Intersection, 22
 - Editing/changing, 117
- Intersection details - Configuring, 118

- L**
- Layout, 94
- Limit prewarning, 104, 166

- M**
- Maintenance changes
 - Online mode, 181
- Mask, 116
- Mask enable, 114, 218
- MatrixName, 130, 136, 140
- MatrixSig, 137
- Measures after upgrading, 36
 - User scenario 3, 38
- Menu bar, 43
- Menu commands, 44
- Message block
 - Message configuration, 67
 - output messages, 186
- Message blocks, 91, 134
- Migration, 33, 129
- Monitoring functions
 - without access protection, 92
- Mutual dependencies of the Cause parameters, 98

- N**
- Nested chart of the F-channel drivers, 136
- Nested chart of the matrix logic, 137
- Nested chart of the Safety Matrix, 130
- Non-critical changes, 97

- O**
- OFF delay, 105, 203
- ON delay, 105, 203
- Online communication, 51
- Online mode
 - Color codes, 163
 - Maintenance changes, 181
 - Starting/stopping, 149
 - Status displays, 165
- Opening the Safety Matrix Viewer, 151
- Operation
 - with one operator, 169
 - with two operators, 169
- Operation with two operators, 177, 179
- Operational safety
 - Safety aspects, 15
 - Safety concepts and communication, 15
- Operator control and monitoring
 - 2-operator scenario, 168
 - Control bar functions, 168, 175
 - Dependency of available functions, 173
 - Differences between ES and OS, 148
 - Example, 177, 179
 - Overview of the functions, 93
 - Requirements, 147
 - User permissions, 92
- Operator control functions
 - with access protection, 92
- Operator input messages, 184
- Operator roles
 - for Secure Write, 172
 - with access protection, 92
- Optimizing the length of the code area, 140
- Optional packages, 20
- OS
 - Client, 147
- Output delay, 113
 - Bypass, 214
 - Reset/override, 209
- Override
 - Pre-alarm timeout, 114
 - Time, 114

- P**
- Pass through process data, 114, 115, 218
- PASS_ON, 136
- Password
 - for F-CPU, 127
 - for safety program, 127
- PCS 7 signaling system, 184
- PCS 7 operation list, 184
- Plausibility check, 200
- Positioning alarm blocks
 - Transfer option, 134
- PP_Chart, 130, 138, 140
- Prefix #, 52
- Prefix *, 53, 56
- Prefix @, 54

Prefix ~, 54, 64
 Preprocessing for input tag, 53, 56, 102
 Print, 193
 Print Preview, 193
 Process data pass through, 115, 218
 Process data tag, 114, 218
 Project structure, 49
 Properties

- Customize, 94
- Safety Matrix, 88
- Track changes, 97

R

R, 99
 REAL, 99
 Remote access, 221
 Reports window, 44, 135
 Requirements for configuration, 49
 Reset/override tag, 113, 207
 Rows for Cause, 100
 Runtime groups following a transfer, 139

S

Safe state, 23
 Safety Instrumented Function Groups, 89
 Safety Matrix

- Acceptance test, 201
- Basic chart, 135, 138
- Basic mode of operation, 19
- Block icon, 87, 92
- Cause block icon, 153
- Compare, 194
- Effect block icon, 154
- Exporting, 120
- Faceplates, 151
- Importing, 120, 124
- Matrix block icon, 152
- Menu commands, 44
- Name, 51
- Object, 50
- Optional packages, 20
- Order numbers, 9
- Pasting, 50
- Range of functions, 20
- Tags, 52, 54
- The name contains incorrect characters, 51
- Transfer option, 130
- Upgrading, 31

User interface, 41
 Warning messages, 186
 Safety Matrix Viewer, 150

- Faceplate, 147

 Safety program

- Comparing, 195

 Safety-instrumented function groups, 24
 SafetyMatrix Lib

- Backup of the pre-processing charts, 30
- Preprocessing charts, 56

 Secure Write, 24

- Enable for Secure Write transaction, 91
- Time for Secure Write transaction, 91
- Transaction, 170
- Transaction for, 25

 Sequence of a transaction for Secure Write, 172
 Set soft bypass for an input tag, 182
 SET_GDM, 63
 Shortcut menu

- Cause, 100
- Effect, 109
- Intersection, 117

 SIF, (See Safety Instrumented Function Groups),
 (See Safety-instrumented function groups)
 SIF Filter, 43, 47
 Signaling of process-relevant events, 185
 Signature, 44
 Simulating

- Mutually locked, 106, 115
- Simulating a tag, 102, 111, 181

 Simulating a tag, 102, 111, 181

- Mutually locked, 106, 115

 Simultaneous soft bypass and hard bypass, 176
 Soft bypass, 24
 Special circumstances when downloading single-user systems, 145
 STATE_V

- F_SC_AL, 73
- F_SC_AL2, 79
- F_SE_AL, 83

 Status bar, 44
 Status descriptions

- Cause, 165
- Effect, 167

 Suffix #, 53
 Syntax rules

- For message configuration, 68
- for tag names, 54

T

Tag

- with prefix, 64
- with prefix #, 52, 54
- with prefix *, 53, 56
- with prefix @, 54
- with prefix ~, 54
- with suffix #, 52, 54

Tags

- Analog input tags, 98
- Any signals from the safety program, 52
- Customer-specific F-channel drivers, 52, 54
- Discrete input tags, 97
- Internal references, 52, 54
- of Safety Matrix, 52, 54
- Syntax rules, 54

The entire Safety Matrix

- Transfer option, 131

Timed Cause, 105, 204

Toolbar, 43

Transaction for Secure Write, 25, 170

Transfer, 129, 140, 141, 142

- one matrix/multiple matrices, 129

Transfer option, 130

- Changes only, 132
- Clean nested chart connections, 133
- Integrate external channel drivers, 133
- Positioning alarm blocks, 134
- The entire Safety Matrix, 131

Transferring

- Status display at the matrix icon, 129

Transferring changes in a Safety Matrix to the OS, 144

Trip on 'Bad Quality', 107, 206

U

Upgrading, 31, 33, 38, 129

V

Validation report, 200

View of a Safety Matrix in online mode, 149

View status, 165

Virtual environment, 221

W

Warning notices

- Directory, 16

Web client, 148

Web Option for OS, 148

WinCC alarm, 185

