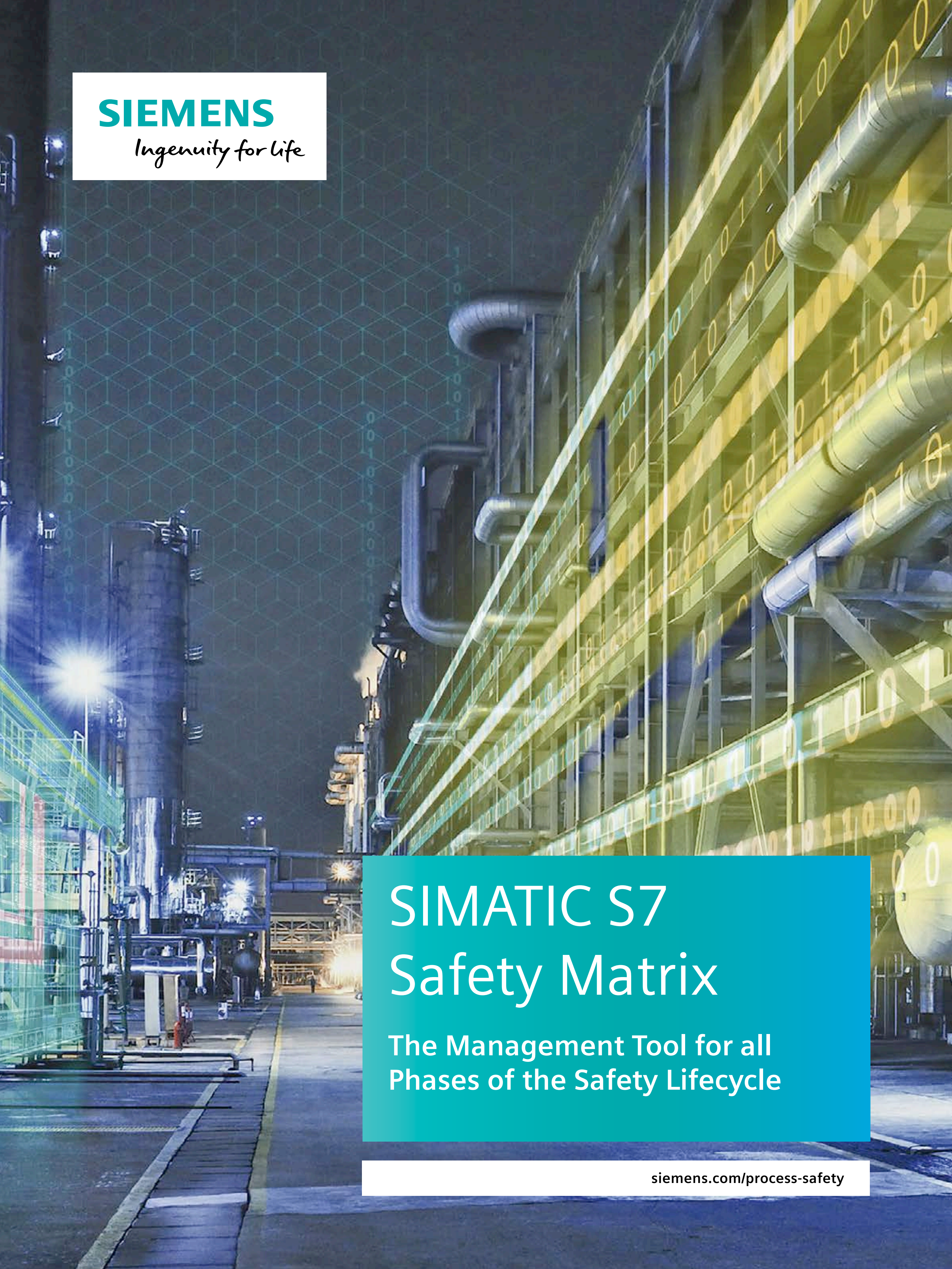
SIEMENS
Ingenuity for life



SIMATIC S7 Safety Matrix

The Management Tool for all Phases of the Safety Lifecycle

siemens.com/process-safety

Functional Safety and Safety Lifecycle Management

The installation and operation of potentially dangerous plants in the process industry are subject to the international standard IEC 61511, the standard for the functional safety of Safety Instrumented Systems.

The procedure for implementing functional safety is described in this standard in accordance with the safety lifecycle of the plant, which is usually divided into the following three phases: analysis, implementation and operation/maintenance.

All these phases and the associated activities for functional safety must generally be documented. The documents are the basis for proving the safety of the plant and the Safety Instrumented Systems used.

Following a modification, all phases of the safety lifecycle are run through again and documented.

Analysis phase

Process plants which are potentially dangerous must be specifically analyzed in order to identify possible dangers and to assess their risks.

One common technique used for this initial process hazard analysis is the HAZOP analysis (Hazard and Operability Analysis).

Using the knowledge gained from the analysis and its assessment, the existing protection layers are identified and any additional protection layers are defined. Safety tasks and functions are assigned to these protection layers. The Safety Instrumented System (SIS) is one of these protection layers.

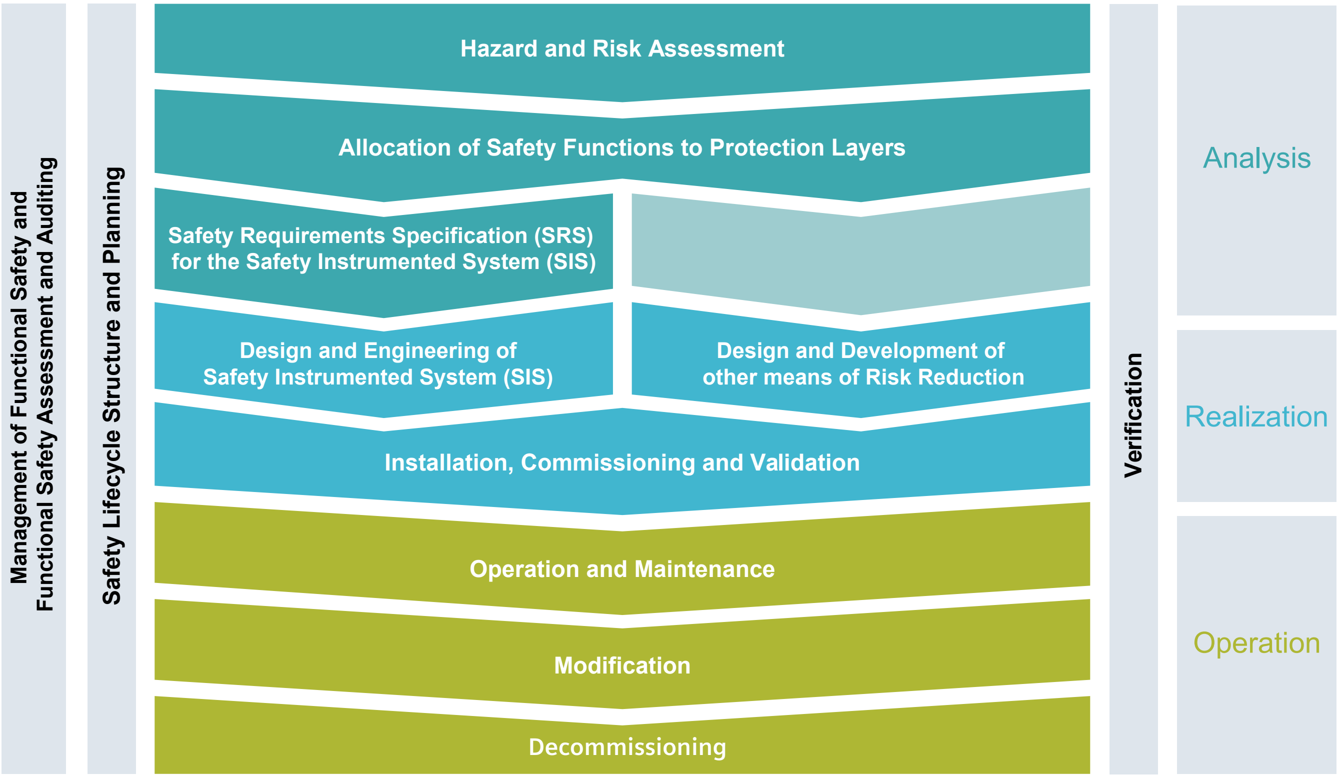
An important output from the analysis phase is the Safety Requirement Specification (SRS) for the Safety Instrumented System. The SRS describes all Safety Instrumented Functions (SIF) including the demands placed on them, and specifies the required Safety Integrity Level (SIL). The SIL is a measure of the reduction in risk that the SIF has to deliver.

Implementation phase

The SRS is the basis for further planning of the plant, especially for the design of the Safety Instrumented System (SIS) and its safety functions as well as for other measures for reducing the risk.
It helps decide the selection of the SIS technology and the selection of the hardware, architecture and software for implementing the safety functions.

Design and planning are followed by installation, commissioning, and validation of the plant. Since the SRS includes the associated tests and test criteria in addition to the safety functions and requirements, it also forms the basis for verification and validation.

In accordance with the guidelines for functional safety, the results achieved


Management of Functional Safety and Functional Safety Assessment and Auditing
Safety Lifecycle Structure and Planning
Hazard and Risk Assessment
Allocation of Safety Functions to Protection Layers
Safety Requirements Specification (SRS) for the Safety Instrumented System (SIS)
Design and Engineering of Safety Instrumented System (SIS)
Design and Development of other means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning
Verification
Analysis
Realization
Operation

The Safety Lifecycle Model in accordance with IEC 61511

when testing to the SRS requirements must be documented. These documents are required for subsequent acceptance of the safety functions and the safety system.

Operation and maintenance phase

This phase comprises operation and optimization of the plant up to the time it is decommissioned.

The SIMATIC S7 Safety Matrix offered by Siemens is a TÜV-certified safety lifecycle management tool for safety applications up to SIL 3 in accordance with IEC 61508.

The SIMATIC S7 Safety Matrix can be used in all phases of the safety lifecycle.The benefits achieved by its use make a significant contribution toward reduction of capital expenditure (CAPEX) and operational expenses (OPEX) of the plant.

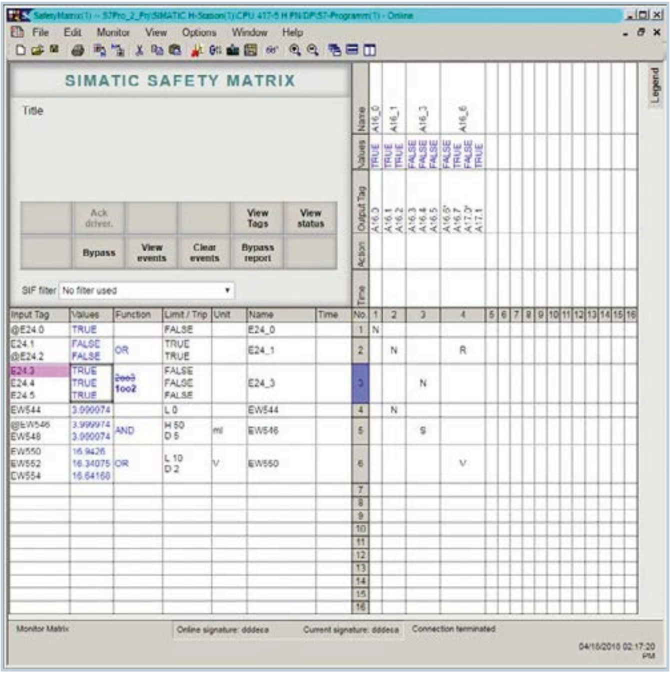
The SIMATIC S7 Safety Matrix consists of the following individual products which have different functionalities and fields of application:

- Safety Matrix Engineering Tool
- Safety Matrix Viewer

SIMATIC S7 Safety Matrix

Products	Supports safety lifecycle phases	Field of application	Operating modes
Safety Matrix Engineering Tool	Analysis phase, implementation phase, operation and maintenance phase	Creation, configuration, and compilation of a safety matrix Importing/exporting of a CEM matrix file Transferring to the project, compilation, downloading, operation, and monitoring of the safety-related CFC program Comparison of safety matrices on the basis of CEM matrix files and CFCs Configuration report and plausibility check with validation report	Online and offline operation
Safety Matrix Viewer	Operation and maintenance phase	Operation and monitoring of the safety-related CFC program	Online operation

Field of application of the SIMATIC S7 Safety Matrix products



SafetyMatrix(1) -- S7Pro_2_Prj\SIMATIC H-Station(1)\CPU 417-5 H PN/DP\S7-Programm(1) - Online
File Edit Monitor View Options Window Help
SIMATIC SAFETY MATRIX
Title
Ack driver.
View Tags
View status
Bypass
View events
Clear events
Bypass report
Legend
Name
Values
Output Tag
Action
Time

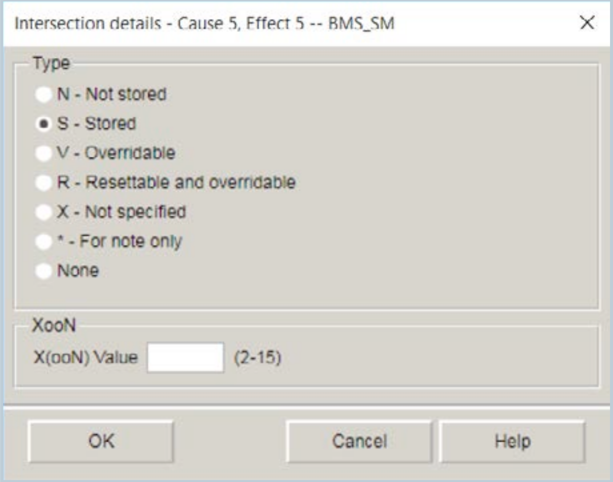
SIF filter: No filter used

Input Tag	Values	Function	Limit / Trip	Unit	Name	Time	No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
@E24.0	TRUE		FALSE		E24_0		1	N															
E24.1 @E24.2	FALSE FALSE	OR	TRUE TRUE		E24_1		2		N		R												
E24.3 E24.4 E24.5	TRUE TRUE TRUE	2oo3 1oo2	FALSE FALSE FALSE		E24_3		3			N													
EW544	3.999074		L 0		EW544		4		N														
@EW546 EW548	3.999974 3.999074	AND	H 50 D 5	ml	EW546		5			S													
EW550 EW552 EW554	16.9426 16.34075 16.64160	OR	L 10 D 2	V	EW550		6				V												
							7																
							8																
							9																
							10																
							11																
							12																
							13																
							14																
							15																
							16																

Monitor Matrix | Online signature: dddeca | Current signature: dddeca | Connection terminated

04/16/2018 02:17:20 PM

Safety Matrix Editor



Intersection details - Cause 5, Effect 5 -- BMS_SM

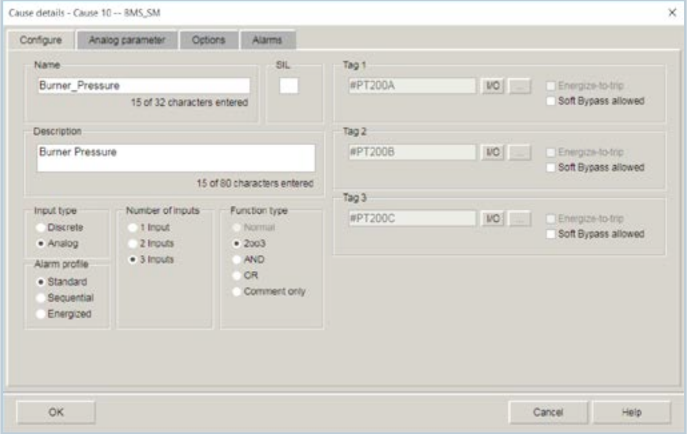
Type

○ N - Not stored
● S - Stored
○ V - Overridable
○ R - Resettable and overridable
○ X - Not specified
○ * - For note only
○ None

XooN

X(ooN) Value: (2-15)

Definition of the cause logic operations and functions



Cause details - Cause 10 -- BMS_SM

Name: Burner_Pressure
15 of 32 characters entered

SIL:

Description: Burner Pressure
15 of 80 characters entered

Input type: ○ Discrete ● Analog

Alarm profile: ● Standard ○ Sequential ○ Energized

Number of inputs: ○ 1 Input ○ 2 Inputs ● 3 Inputs

Function type: ○ Normal ● 2oo3 ○ AND ○ OR ○ Comment only

Tag 1: #PT200A — I/O — □ Energize-to-trip □ Soft Bypass allowed

Tag 2: #PT200B — I/O — □ Energize-to-trip □ Soft Bypass allowed

Tag 3: #PT200C — I/O — □ Energize-to-trip □ Soft Bypass allowed

Definition of a cause

Safe Highlights

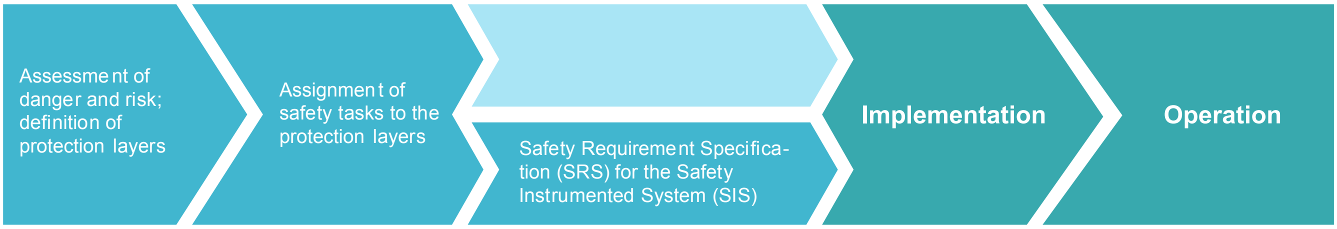
- 128 causes per matrix
- 128 effects per matrix
- 1024 intersections per matrix
- Up to 3 inputs per cause
- Up to 4 outputs per effect

Advantages

- No programming knowledge required
- Readily understandable for everyone involved
- Quick and precise overview of the safety function in engineering and operation

SIMATIC S7 Safety Matrix in the analysis phase

It is important in the analysis phase to identify and analyze known and potential safety risks, e.g. using the HAZOP method. This serves to filter out non-tolerable risks, to evaluate the probability of a hazard occurring, and to estimate possible consequences.


Assessment of danger and risk; definition of protection layers
Assignment of safety tasks to the protection layers
Safety Requirement Specification (SRS) for the Safety Instrumented System (SIS)
Implementation
Operation

The safety concept for the plant is subsequently produced. During this, the safety tasks are assigned to the various protection layers of the plant.

The Safety Instrumented System (SIS) plays an important role within the safety concept. The SIS requirements defined and described in the form of a safety requirement specification (SRS) are the basis for planning, engineering, and acceptance of the plant. Since different people have to work in accordance with this specification during different phases of the safety lifecycle, it is important to formulate the safety requirements in a readily understandable manner.

Safety Requirement Specification (SRS)

The requirements placed on the safety system are defined in the SRS. The SRS includes the functional description of the safety functions as well as all the conditions that cause them to be triggered. In addition, determination of the Safety Integrity Level (SIL) is part of the detailed consideration of each individual safety function.

Cause & Effect matrix

The Cause & Effect method has proven to be an extremely effective option for the description of safety functions and for the definition of marginal and shut-down conditions. The method specified by the American Petroleum Institute in the API RP 14C guideline is currently employed in many sectors of the process industry.

Siemens has implemented the Cause & Effect method defined by the American Petroleum Institute in the SIMATIC S7 Safety Matrix.

During the analysis phase, the SIMATIC S7 Safety Matrix allows safety functions to be consistently recorded, described, and formulated in a format which is easily understood by everyone involved. No special programming knowledge is required for this so process specialists can also directly define their requirements with the SIMATIC S7 Safety Matrix.

The causes can include the logical connection of up to 3 digital or analog signals. Additional aspects can also be considered, e.g. time delays and bypassing.

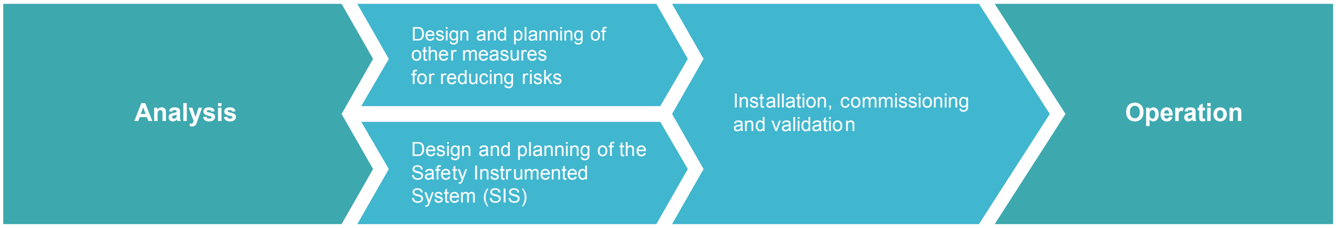
The effects are defined in the columns of the matrix table. An effect can include connections to up to 4 different actuators.

The linking of several causes and the definition of the relationship between causes and effects is carried out at the intersections of the rows and columns, along with any requirements for latching, resets and overrides.

Causes can also be combined in selection groups. For example, it is possible to implement a 2 out of 3 (2oo3) vote in this manner.

SIMATIC S7 Safety Matrix in the implementation phase

The implementation phase starts with the design and detailed planning of the safety-related system and other measures for reducing the risk. This is followed by installation, commissioning, and validation.


Analysis
Design and planning of other measures for reducing risks
Design and planning of the Safety Instrumented System (SIS)
Installation, commissioning and validation
Operation

The specified safety functions are implemented during the planning phase. When using the SIMATIC S7 Safety Matrix, the safety functions defined during the analysis phase are presented in the form of a Cause & Effect matrix, which can be used directly to generate the logic required within the SIS.

There is no need to transpose the requirements described in the SRS into a form that the SIS can use. This is done by the Safety Matrix giving considerable savings in engineering costs.

Connection to the plant field level is established by assigning the causes and effects to the inputs and outputs of the SIMATIC S7-400F/FH controller. Further extension functions and parameter settings can also be carried out in SIMATIC S7 Safety Matrix. These include the setting of limits and hysteresis for analog values, as well as the definition of the maximum discrepancy for alarming when linking several analog measured values.

Complex calculations can also be integrated into the Safety Matrix using function blocks for signal preprocessing, e.g. for conversion of an input value. The corresponding function blocks can be selected in the channel driver of the I/O signal.

It is also possible to configure simulations and bypasses with corresponding access privileges for commissioning and subsequent operation.

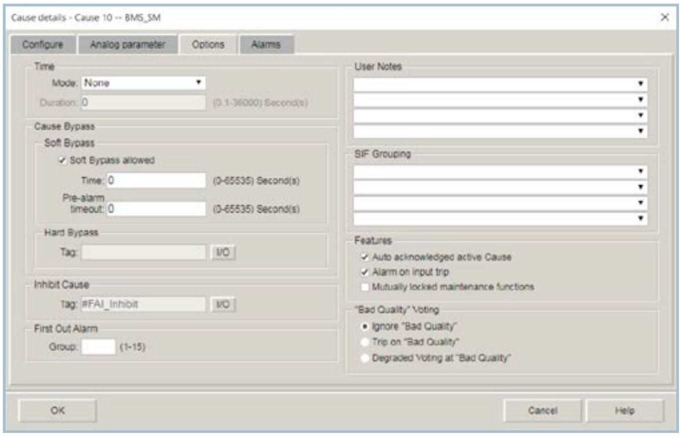
A bypass can be controlled, for example, directly using the SIMATIC S7 Safety Matrix or via an input signal (key switch).

The option for assigning causes and effects to 3 alarm profiles each improves the overview for displaying alarms and enables plant operators to recognize problems more rapidly and to react accordingly. The reduction in shutdown times makes a significant contribution to increasing plant availability.

The conversion into executable program logic is carried out automatically. Using CFC (Continuous Function Chart), the SIMATIC S7 Safety Matrix Engineering Tool generates program logic for each matrix with function blocks from the F-library in SIMATIC S7 F Systems, and generates the channel drivers for all fail-safe I/O channels. The CFC program logic can subsequently becompiled and downloaded to the controller. Automatic generation of the CFC program logic has been approved and certified by TÜV.

The Safety Matrix Engineering Tool can be switched directly to the online view for test purposes. Alternatively, the Safety Matrix Viewer on the SIMATIC PCS 7 Operator Station or SIS compact Operator Station can also be used.

Functions integrated in the SIMATIC S7 Safety Matrix for plausibility checking, documentation, and simulation as well as for comparison of files and charts effectively support the planning, commissioning and test engineers during the testing and acceptance of the safety application.



Time
Mode: None
Duration: 0 (0.1-36000) Second(s)

Cause Bypass
Soft Bypass
☑ Soft Bypass allowed
Time: 0 (0-65535) Second(s)
Pre-alarm timeout: 0 (0-65535) Second(s)
Hard Bypass
Tag:

Inhibit Cause
Tag: #FAI_Inhibit

First Out Alarm
Group: (1-15)

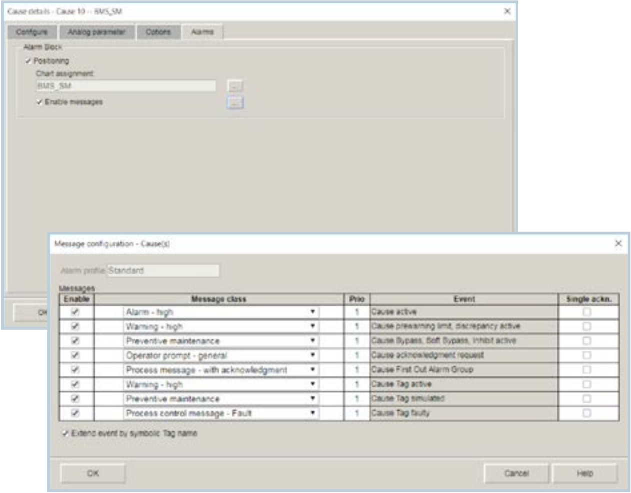
User Notes

SIF Grouping

Features
☑ Auto acknowledged active Cause
☑ Alarm on input trip
□ Mutually locked maintenance functions

"Bad Quality" Voting
● Ignore "Bad Quality"
○ Trip on "Bad Quality"
○ Degraded Voting at "Bad Quality"

Cause details


Cause details - Cause 10 -- BMS_SM
Configure
Analog parameter
Options
Alarms
OK
Message configuration - Cause(s)
OK
Cancel
Help

Alarm Block
☑ Positioning
Chart assignment
BMS_SM
☑ Enable messages

Alarm profile: Standard

Messages

Enable	Message class	Prio	Event	Single ackn.
☑	Alarm - high	1	Cause active	□
☑	Warning - high	1	Cause prewarning limit, discrepancy active	□
☑	Preventive maintenance	1	Cause Bypass, Soft Bypass, Inhibit active	□
☑	Operator prompt - general	1	Cause acknowledgment request	□
☑	Process message - with acknowledgment	1	Cause First Out Alarm Group	□
☑	Warning - high	1	Cause Tag active	□
☑	Preventive maintenance	1	Cause Tag simulated	□
☑	Process control message - Fault	1	Cause Tag faulty	□

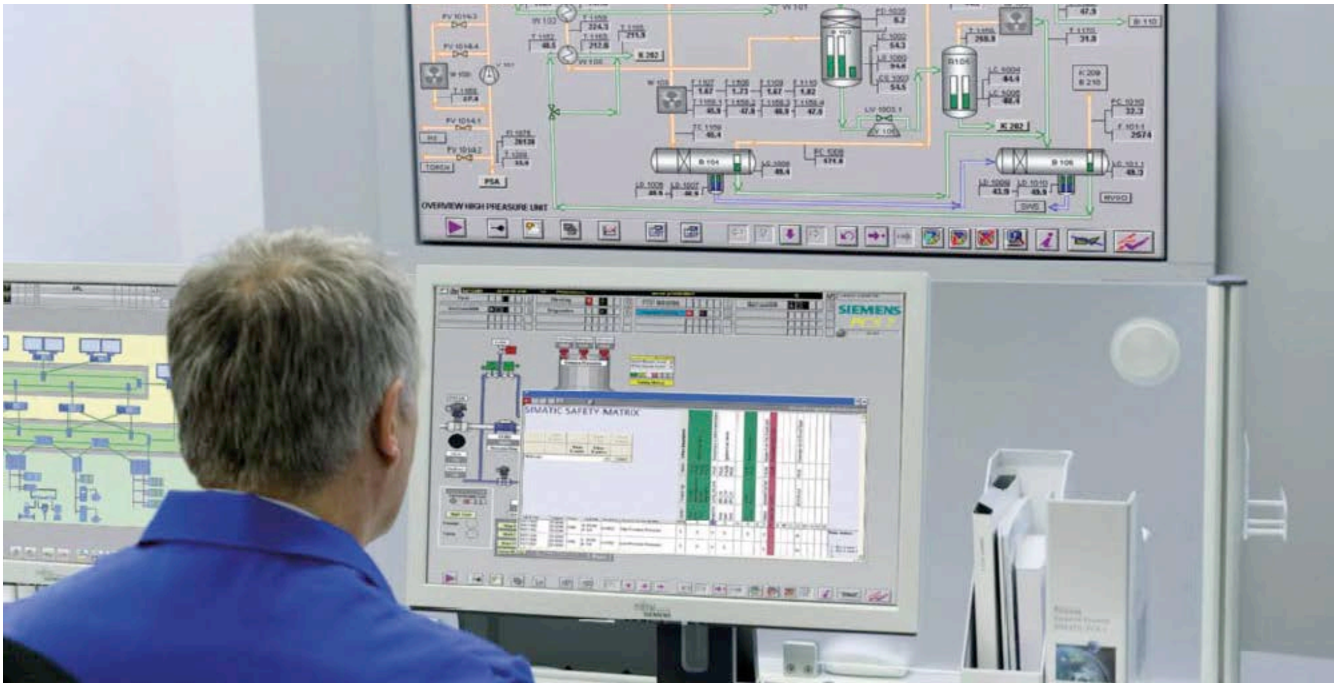
☑ Extend event by symbolic Tag name

Alarm definition and assignment

Acceptance of the safety application is usually carried out by authorized authorities. Since such persons do not normally have special programming knowledge, they greatly benefit from the use of the SIMATIC S7 Safety Matrix. The auditor can reproduce the safety functions specified in the SRS almost 1:1 on the screen in online mode.
Interpretation of a specific programming language is unnecessary. This shortens the acceptance times, and productionin the plant can be started earlier.

SIMATIC S7 Safety Matrix Highlights

- Processing functions within causes such as 2oo3, AND, OR
- Degraded voting scheme in Causes
- Definition of trip values when processing causes
- Consideration of time requirements for causes and effects
- Easy implementation of "sequential control" for e.g. plant start-up sequences
- Consideration of signal and module faults
- Preprocessing of values
- Effect can directly drive up to 4 actuators
- Integral simulation and bypass functions
- Integral limitation of simulation to 1 transmitter within a voting group
- Triggering upon active cause, no latching
- Triggering upon active cause, latching, reset necessary
- Triggering upon active cause, bypassing possible
- XooN selection
- Generation of safety groups
- Alarm groups
- Preliminary and discrepancy alarms
- OS Web-Client support for Safety Matrix Viewer
- Remote monitoring and control via Web connection



Additional functions

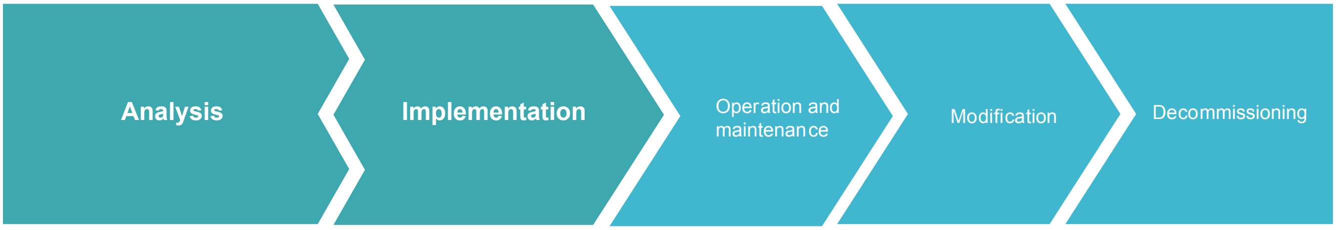
- Comparison of matrices for tracking modifications
- Integral validation report
- Configuration report, matrix documentation
- Modification report

Advantages

- Direct linkage to the Safety Requirement Specification (SRS) during generation of program
- Identical display of matrix in configuration, operation, and documentation
- Common understanding for all involved persons
- Reduction in planning, implementation, and acceptance times
- Bulk Engineering based on spreadsheets
- Cause & Effect matrix can be imported and exported
- Usable standalone, with SIMATIC PCS 7 and SIMATIC SIS compact

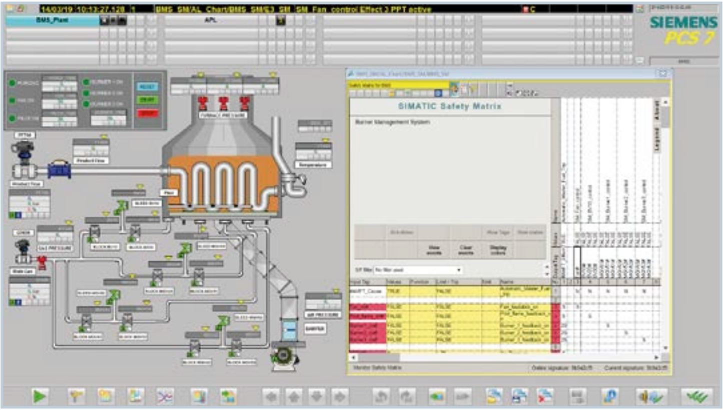
SIMATIC S7 Safety Matrix in the operating phase

During process control it must be possible for the operator to recognize relevant deviations early and to react rapidly. Simple and intuitive operation of the automation plant is therefore necessary. This particularly applies to safety-critical processes where the plant will be switched off if the operator cannot locate the cause of an alarm rapidly enough and initiate appropriate measures.

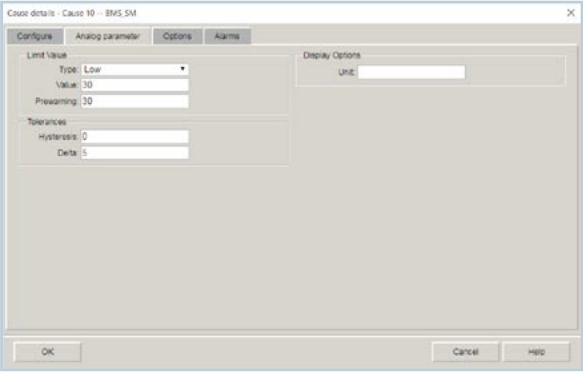

Analysis
Implementation
Operation and maintenance
Modification
Decommissioning

The SIMATIC S7 Safety Matrix can make the operator aware of imminent critical situations by means of a preliminary alarm, and can display the cause with the associated effect. The operator can then directly recognize an anomalous or faulty sensor and immediately initiate checking or other steps for elimination of the cause.

Maintenance functions integrated in the SIMATIC S7 Safety Matrix support checking of sensors. They allow brief bypassing of the sensor for replacement or external testing. Plant downtimes or shutdowns can be avoided in this manner. A pending proof test can also be the reason for temporarily bypassing sensors or actuators.



Process image of an operator station with Safety Matrix Viewer displayed

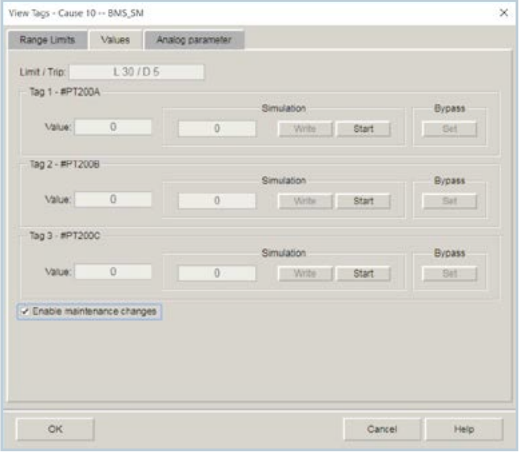

Cause details - Cause 10 -- BMS_SM

Limit Value
Type: Low
Value: 30
Prewarning: 30

Tolerances
Hysteresis: 0
Delta: 5

Display Options
Unit:

Limit Value



Limit / Trip: L 30 / D 5

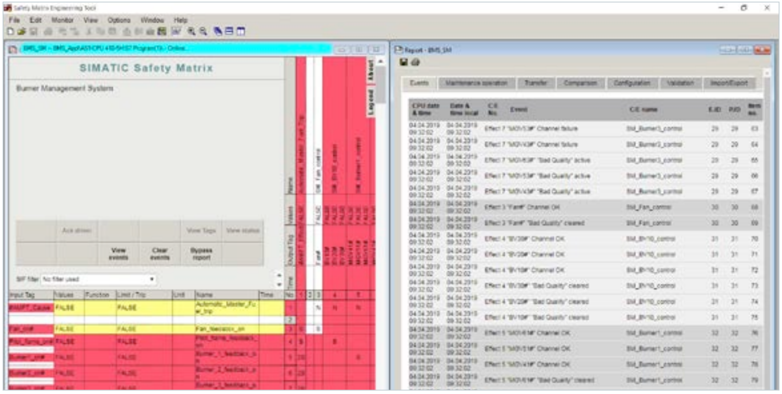
Tag 1 - #PT200A — Value: 0 — Simulation: 0

Tag 2 - #PT200B — Value: 0 — Simulation: 0

Tag 3 - #PT200C — Value: 0 — Simulation: 0

☑ Enable maintenance changes

Maintenance



CPU date & time	Date & time local	C/E No.	Event	C/E name	E-ID	P-ID	Item no.
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 7 "MOV53#" Channel failure	SM_Burner3_control	29	29	63
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 7 "MOV43#" Channel failure	SM_Burner3_control	29	29	64
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 7 "MOV63#" "Bad Quality" active	SM_Burner3_control	29	29	65
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 7 "MOV53#" "Bad Quality" active	SM_Burner3_control	29	29	66
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 7 "MOV43#" "Bad Quality" active	SM_Burner3_control	29	29	67
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 3 "Fan#" Channel OK	SM_Fan_control	30	30	68
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 3 "Fan#" "Bad Quality" cleared	SM_Fan_control	30	30	69
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 4 "BV30#" Channel OK	SM_BV10_control	31	31	70
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 4 "BV20#" Channel OK	SM_BV10_control	31	31	71
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 4 "BV10#" Channel OK	SM_BV10_control	31	31	72
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 4 "BV30#" "Bad Quality" cleared	SM_BV10_control	31	31	73
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 4 "BV20#" "Bad Quality" cleared	SM_BV10_control	31	31	74
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 4 "BV10#" "Bad Quality" cleared	SM_BV10_control	31	31	75
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 5 "MOV61#" Channel OK	SM_Burner1_control	32	32	76
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 5 "MOV51#" Channel OK	SM_Burner1_control	32	32	77
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 5 "MOV41#" Channel OK	SM_Burner1_control	32	32	78
04.04.2019 09:32:02	04.04.2019 09:32:02		Effect 5 "MOV61#" "Bad Quality" cleared	SM_Burner1_control	32	32	79

Documentation of operator interventions and events

Maintenance can be optimized even further through integration of the fail-safe sensor system into the asset management system.

The SIMATIC S7 Safety Matrix can be operated and monitored both in online mode of the Safety Matrix Engineering Tool and by using the Safety Matrix Viewer on the operator station of the SIMATIC PCS 7 process control system and SIMATIC SIS compact system.

Operator interventions are documented and can be archived for Safety Lifecycle Management.

The facilities in the SIMATIC S7 Safety Matrix Viewer which are available to an operator depend on the operator privileges defined in the SIMATIC PCS 7 or SIMATIC SIS compact. This guarantees that only authorized persons can bypass or simulate field devices.

Process-relevant events and alarms are transferred to the operator system of the SIMATIC PCS 7 process control system and SIMATIC SIS compact system, and integrated into the signaling system. This enables joint archiving of alarms and messages by the Basic Process Control System (BPCS) and the safety system.

Matrices are called using block symbols positioned on the user interface of SIMATIC PCS 7 or SIMATIC SIS compact. These can apply to the complete matrix or just to a specific cause or effect. The view focused on a cause or effect can be switched over to the total view of the matrix at any time, and vice versa.

Group displays on the block symbol for the matrix allow the operator to already recognize whether warnings, alarms or maintenance functions are active. Further detailed information is then made available by opening the associated matrix view.

Highlights

- Integral maintenance functions such as bypass and simulation
- Display of all relevant process values, also during maintenance
- All relevant information can be seen at a glance in the template

Advantages

- Optimum operator prompting
- Process-independent maintenance of sensors and actuators
- Reduction in downtimes

SIMATIC S7 Safety Matrix – the Safety Lifecycle Management Tool

Consistent use of the SIMATIC S7 Safety Matrix across all phases of the safety lifecycle reduces the capital expenditure (CAPEX) and operational expenses (OPEX). The advantages of the SIMATIC S7 Safety Matrix provide convincing arguments in all phases.

Analysis phase

The SIMATIC S7 Safety Matrix does not require programming knowledge. It can therefore equally be used by process, test and planning engineers.

Safety functions are defined using the Cause & Effect method.

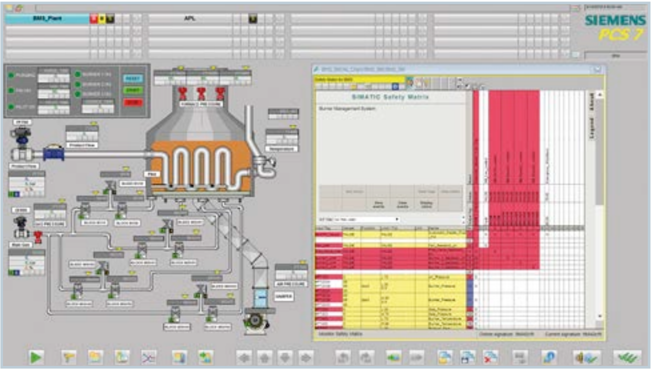
The Cause & Effect representation is compact, clear, and easy to understand.

Implementation phase

The safety functions defined using the SIMATIC S7 Safety Matrix can be imported directly. It is only necessary to carry out the system-specific settings of the AS 410F/FH and SIS compact safety system. Planning engineers, operators and test engineers always share a consistent and readily understandable view. The safety functions are represented identically during configuration and operation and in the documentation. Signal states and supplementary information are displayed in different colors during operation. All this results in a significant reduction in engineering, test and acceptance times.

Operating phase

The optimized operator prompting of the SIMATIC S7 Safety Matrix guarantees that operators can react rapidly and specifically to events during operation. They can also simulate sensor and actuator systems, particularly during maintenance. The SIMATIC S7 Safety MatrixViewer can be used to reduce plant downtimes.



Safety Matrix Viewer

Advantages at a glance

- No programming knowledge required
- Readily understandable for all involved persons
- Concise overview of all safety functions
- Direct linkage to the Safety Requirement Specification (SRS) during generation of program
- Identical display of matrix in configuration, operation, and documentation
- Uniform view and understanding of all involved persons
- Reduction in planning, implementation, and acceptance times
- Optimum operator prompting
- Process-independent maintenance of sensors and actuators
- Reduction in downtimes

Additional information

For further details, see SIMATIC Manuals Guide:
siemens.com/simatic-docu

You can order further documents on the subject of SIMATIC from:
siemens.com/simatic/printmaterial

In-depth technical documentation is available from our Service&Support Portal: siemens.com/automation/support

For a personal discussion, you can locate your nearest contact at: siemens.com/automation/partner

In the Industry Mall you can place orders electronically via the Internet:
siemens.com/industrymall

You can find details on the SIMATIC PCS 7 and SIMATIC SIS compact process control system at: siemens.com/simatic-pcs7

You can find details on the Siemens Process Safety solution at:
siemens.com/process-safety

Digital Industries
Process Automation
Oestliche Rheinbrueckenstr 50
76187 Karlsruhe, Germany

Subject to change
Order No.: E86060-A4678-A261-A1-7600
3P.8315.15.01 / Dispo 09508
BR 1110 6.0 ROT 12 En
Printed in Germany
Siemens AG 2019

siemens.com/process-safety

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.