

SIEMENS

Ingenuity for life

Industry Online Support

Home

Guideline Functional Safety Management

Safety Integrated

<https://support.industry.siemens.com/cs/ww/en/view/109781708>

Siemens
Industry
Online
Support



Legal information

Use of application examples

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

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

Disclaimer of liability

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

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

Other information

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

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

Security information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit **Fehler! Linkreferenz ungültig..**

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: **Fehler! Linkreferenz ungültig..**

Table of contents

Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Risk evaluation	4
2 Functional Safety Management	7
2.1 Functional Safety Management plan.....	7
2.2 Safety Requirement Specification	9
2.3 Functional Design Specification	11
2.4 V&V specification	14
3 Summary and conclusion	19
4 Appendix	20
4.1 Service and support	20
4.2 Links and literature	21
4.3 Change documentation	21

1 Introduction

1.1 Overview

Before placing goods on the European market, the manufacturer or distributor must meet the requirements of the country of destination. Uniform requirements have been defined for the European Economic Area. The manufacturer must implement all applicable directives and declare their compliance by the CE marking. This essentially includes the documentation of the development process.

The entire CE process of a machine takes into account the fulfilment of the basic health and safety requirements for the design and construction of machines.

These indicate the preparation and implementation of a risk evaluation. The assessment results must be taken into account for the design and construction of the machine. To this end, it is recommended that harmonized standards designed to meet the essential requirements of the directives be applied.

To fully comply with the CE marking process, any appropriate directive must be taken into account. Compliance with the Machinery Directive 2006/42/EC is only one prerequisite for CE marking.

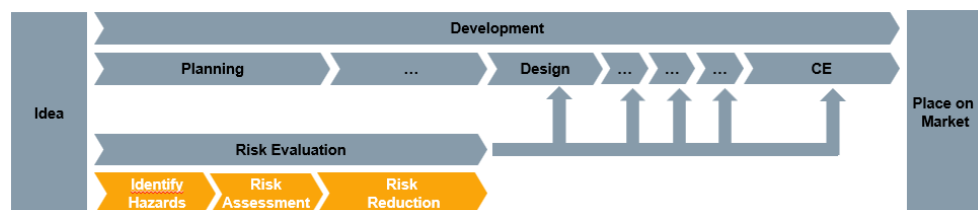
Relating to machine safety, this application example focuses on the fulfilment of the requirements for control-related measures. To this end, this document sets out the necessary minimum requirements for Functional Safety Management (FSM) and the benefits of this additional effort to facilitate fulfillment of the requirements.

1.2 Risk evaluation

The risk evaluation process in this application example is based on the DIN EN ISO 12100 standard. Performing the risk evaluation comprises various steps that are necessary to fulfil the specified process.

- Identify hazards
- Risk estimation
- Risk assessment and risk reduction

Figure 1-1 Classification of the risk evaluation in the development process from the idea to placing a machine on the market



Identification of hazards

Once the limits of the machine have been defined, potential hazards are analyzed on this basis, for each phase of its life, and for each mode of operation.

Risk estimation

The risks arising from the hazards identified must be considered. The risk is a combination of

- extent of damage and
- the probability of the occurrence of damage

Risk assessment and reduction

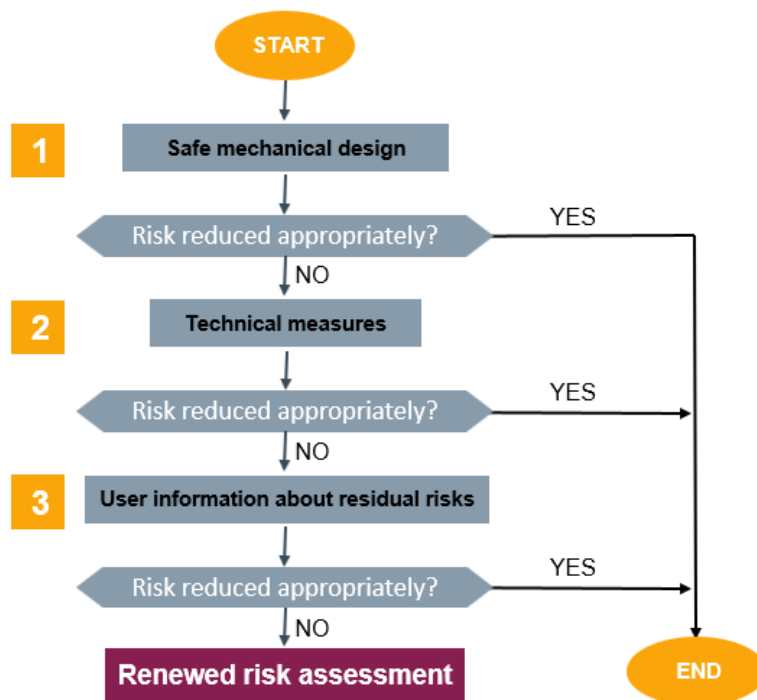
Once the risk estimation has been completed, an assessment of the identified risks takes place to determine whether a reduction is necessary.

From the standard DIN EN ISO 12100, the following measures can be defined and applied:

1. Inherently safe mechanical design (elimination of hazard due to design modification)
2. Technical measures (use of safety components or protective devices)
3. User information about residual risks

After applying any risk reduction measures, a further risk assessment must be carried out to check whether the risk has been reduced to an acceptable level. If this is not the case, further risk reduction measures must be defined.

Figure 1-2 Three-step procedure



Details on technical measures

Technical measures with monitoring ($\hat{=}$ safety functions or control-related measures) are implemented with suitable devices, such as safety relays or fail-safe controls. If the monitored limits or limit values are violated, the machine is automatically transferred to a safe state, as well as in the event of a malfunction of the protective devices.

In order to select suitable safety-relevant equipment, a quantitative degree of safety-relevant performance must be determined. The following levels can be used for this purpose.

- Safety Integrity Level (SIL) according to EN 62061
- Performance level (PL) according to EN ISO 13849

The result of this evaluation forms the basis for the definition and implementation of the safety functions.

To ensure high quality during the implementation and design phase, a suitable process must be established. For the description, several steps are necessary to

1 Introduction

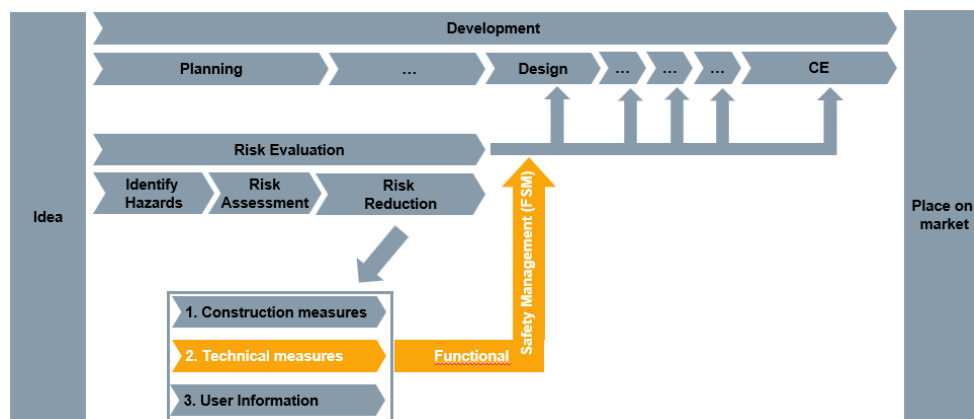
meet the requirements. With these steps the phases specification, implementation, verification and validation can be fulfilled. The entire process is called Functional Safety Management (FSM).

2 Functional Safety Management

According to the requirements of the Machinery Directive, it is necessary to ensure a high quality of each individual machine component. With regard to the part of functional safety used to ensure the safe operation of the machine, the following two points should be considered in order to achieve an acceptable level.

- Use of reliable hardware
- Ensuring a reliable and correct implementation

Figure 2-1 Classification of Functional Safety Management in the process



From the risk assessment, the risk reduction measures must be defined in the form of technical, specifically control-related measures by the Functional Safety Management framework. The Functional Safety Management process defines, among other things, the following steps and their execution.

- Listing of a Safety Requirements Specification (SRS) with all relevant safety information
- Design and selection of the required hardware and software
- Verification of compliance with all required safety values
- Creation of a suitable program
- Testing of hardware and software

The FSM process ensures the necessary independence between all persons involved in the process. The completion of the process shows that all safety requirements have been implemented and are functioning properly.

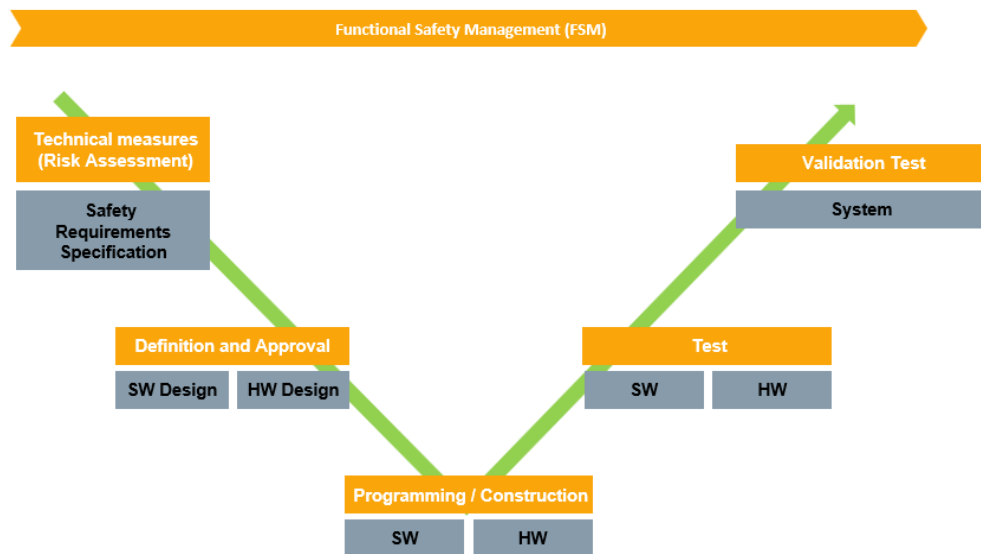
By using basic documents, these requirements of the FSM process can be documented as well as tracked at all times.

2.1 Functional Safety Management plan

The FSM plan is at the heart of the Functional Safety Management process and thus represents a process description for the structured implementation of all safety requirements.

For example, the respective process can be represented with a V model and shows the chronological sequence of the development steps.

Figure 2-2 Simplified FSM plan using a V model



Depending on the size and complexity of the system to be developed, the level of detail of the FSM plan may vary, but always follows the same principle.

The most important contents to be defined as well as an exemplary implementation of these contents are presented in the following.

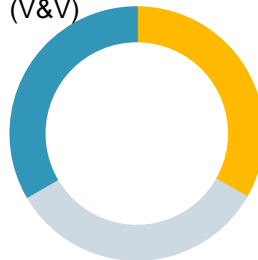
Figure 2-3 Components of the FSM plan

Documentation

- Description of the process
- Safety Requirements Specification (SRS)
- Functional Design Specification (FDS)
- Validation/Verification (V&V)

Roles of the persons

- Persons and their qualification
- Activities of each role (tasks, responsibility)
- Definition of a division of roles (e.g. designer, tester, manager)



Development process

- Order of activities (V model)
- Requirements of the activities
- Verification and validation procedures
- Configuration management

Figure 2-4 Exemplary documentation FSM plan

FSM-Plan

Project: Project name
 Version: XY of xx.yy.zz
 Author: NAME (Functional Safety Manager)

1. Project Description

Brief description of project target.

2. Personen und ihre Qualifikationen

In this chapter the roles can be defined and described.

Table 0-1: Definition und description of roles

Role	Name	Qualification
Project Manager		- Several years of experience in functional safety projects - Further <u>training xy</u>
Funktional Safety Manager		
Designer		
V&V Manager		
.....		

3. Area of responsibility of the roles

This chapter describes the activities of the roles and their areas of responsibility.

Figure 0-1: Exemplary representation of the process and the roles

4. ...

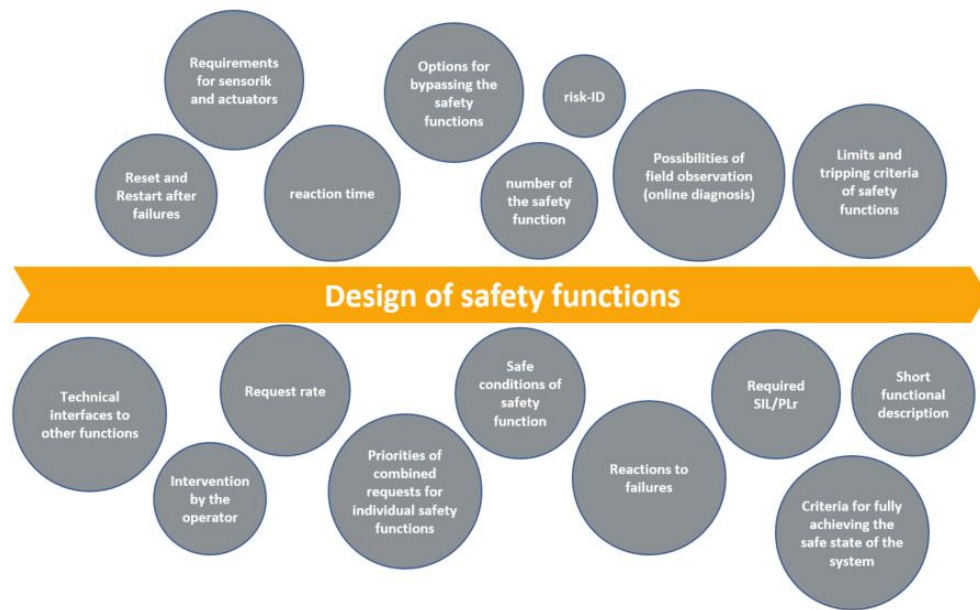
© Siemens AG 2020. All rights reserved

2.2 Safety Requirement Specification

After a risk assessment and the definition of measures, the specification of each individual safety function must be determined. It comprises the part of the risk-reducing measures from this risk assessment that must be implemented by using safety technology (control-related measures).

The design of the hardware and software of control-related measures can be described with the following parameters.

Figure 2-5 Overview of definition of control-related measures



Based on a detailed description, the hardware and software can subsequently be described and defined.

Figure 2-6 Exemplary documentation SRS

Safety Requirement Specification

Project: Project name
Version: XY of xx.yy.zz

Author: NAME (Project Manager)
Releaser: NAME (Functional Safety Manager)

1. System und function description
General description and definition of safety targets.

2. Specific description of safety functions

Number: Serial. Nr.	Risk ID:	Name: Name of safety function
1. Description		<i>Safety function description</i>
2. Required Performance Level		<i>Description of the basis on which the required PL was defined.</i>
3. Safe state		<i>Description of how the safe state is defined and assumed</i>
4. Measures to be taken when an error occurs		<i>Description of the measures to be taken in the event of errors occurring</i>
5. Limit values and tripping criteria of the safety function		<i>Definition of limit values and their associated machine reaction</i>
6. Acknowledgement and restart after error		<i>Description of the conditions which have to be fulfilled for restarting and the granting of the operational release.</i>
7. Possibilities to bypass the safety function		<i>Description of any conditions that allow the safety function to be bypassed</i>
8. Requirement rate		<i>Definition of requirement rate</i>
9. Used sensors		<i>Description of required sensor technology</i>
10. Used actuators		<i>Description of defined actuator technology</i>
11. Reaction time		<i>Definition of max. tolerable reaction time</i>
12. Operator intervention		<i>Definition and description of a possibly necessary intervention of the operating personnel</i>
13. Mutual influencing of the safety functions		<i>Description of a possible mutual influence</i>
14. Interface to non-safe functions		<i>Description</i>

3. ...

© Siemens AG 2020. All rights reserved

2.3 Functional Design Specification

The Functional Design Specification (FDS) describes the complete functional scope of the overall system to be created and contains a breakdown of the functionalities into subsystems/subprojects. In order to implement these, a hardware and software design process is necessary. The degree of detail of the FDS depends on the respective project complexity and is largely determined by the scope of supply and services.

For more complex projects, it is advisable to make a further division. For example, an elementary description of a function can be defined in the FDS. A more detailed description can then be made in a respective Detailed Design Specification (DDS).

Note

It is important that references to the Safety Requirements Specification are provided for specification points relating to control-related measures in order to ensure traceability.

Hardware design

The design and selection of hardware plays an essential role in the implementation of a safety function. Here, the results of the risk evaluation must be taken into account and applied. If a combination of safety-relevant parts is required, suitable qualified components must be selected. These include

- certified,
- non-certified or
- combined

hardware.

The designer must ask himself various questions in order to achieve the required safety level on the one hand and to select suitable hardware on the other hand.

- Does the hardware meet the safety requirements?
- Can the hardware cover the functional range?
- Can each subsystem be implemented with hardware?
- Which architecture is suitable?
- How reliable must the safety function be?
- What diagnostics is required?
- Resistance to external influences?
- Suitable process available?
- Are further measures needed?
 - Diagnoses?
 - Settings?

Note

Fail-safe modules offer the necessary quality due to integrated structures and diagnostic measures and are certified accordingly for use in the implementation of safety functions. When using non-certified hardware, please note that additional measures may be required to qualify it for use.

After selecting the safety-relevant components, they can be verified by means of the TIA Selection Tool Safety Evaluation in accordance with the standards EN 62061 and EN ISO 13849-1. Taking these into account, a designer can quickly and easily evaluate the safety functions of the machine.

Through early verification of the achievable safety levels with the selected components, the designer can avoid the selection and ordering of hardware that is not suitable for the safety requirements.

Software design

Based on the SRS and the selected hardware, it may be necessary to design a suitable user software. For the software program, detailed planning of its designs is

helpful. In order to realize this, a designer must work out a specification of the program. The following points may help in this respect.

- Description of the function
- Semiformal representation of the program flow
 - Cause-effect diagram
 - Detailed state machine
 - Signal flow chart
 - Program flow charts for state transitions
- General textual description
- Description of the interface
- Address ranges

These points can help the software programmer to implement the program for the safety functions. With increasing quality of the design planning, e.g. through detailed state diagrams, the quality of the subsequently created software and its traceability also increases.

Figure 2-7 Exemplary FDS

Functional Design Specification (HW / SW)

Project: Project name
Version: XY of xx.yy.zz

Author: NAME (Designer)
Releaser:NAME (Functional Safety Manager)

1. System overview

1.1 Hardware description
General description of the used hardware / Possible restrictions

▲ **1.2 Safety components of the system**
Description and presentation of the logical connection of the used components, including derivation and calculation to achieve the required PI / SIL

1.3 General conditions
Description of possible basic conditions like reaction times, request rates, diagnostic test intervals, address ranges.....

2. Technical description

1.4 Function 1
Content:
- Description of the range of functions
- Detailed functional description (flow diagrams, time diagrams, state diagram...)
- Definition of interfaces
- Interaction of individual functions
- Description of individual detection measures
- Error reactions

1.5 Function n

3. Calculation of safety level
Verification with TIA Selection Tool Safety Evaluation

2.4 V&V specification

The V&V specification defines the process with regard to validation and verification. It is specified how these measures have to be carried out and which documents may be created in the process. A high quality of document creation helps to comply with the burden of proof.

Note

The V&V steps to be defined are also largely derived from the scope of supply and services. However, it is also important here, analogous to the FDS, that V&V steps relating to control-related measures must be identified by means of references to the SRS in order to prove their completeness

Validation

The aim of validation is to check whether the implemented safety functions make the required contribution to risk reduction. In the case of deviations from the expected results, corrections must be made to the technical implementation and an appropriate repeat test must be carried out.

The validation process can be divided into the following phases:

Safety Requirements Specification (SRS), derived from the risk assessment

Once the SRS has been defined and prepared, it is checked whether all risks identified in the risk evaluation are met by the specification. Furthermore, in addition to checking the content, the completeness, contradictions and correctness of the information are also examined.

Hardware and software specification, derived from the SRS

During the hardware and software validation, it is checked whether all requirements specified in the SRS have been covered. This includes, for example, comparing the implemented software and its description with the hardware used. It has to be proven that they comply with the required measures to implement risk reduction.

Verification

During verification, it must be checked whether the hardware or software used in each case meets the respective specifications. This verification can be provided by means of analyses, reviews or various test scenarios.

For the safety functions, it must be demonstrated accordingly that the requirements from the SRS, if necessary by means of an FDS, are complied with in relation to the hardware and software implementation. This can be done in two test stages. It is strongly recommended to carry out a function test. Here the entire function is tested against the specification.

For function modules that are used repeatedly in defined functions, it may be useful to perform a module test.

Module test

This test includes the analysis of the user software with the corresponding hardware configuration. For this purpose, the basic functions of the modules, usually function blocks, are tested. This can be done by means of, for example, parameter checks, black/white box tests, etc. In addition, general tests, as listed below, are also conceivable.

- Hardware setup test in the control cabinet
- Analysis of the address ranges between the modules
- Limit value analysis (memory test, etc.)
- Compliance with programming guidelines

Function test

The function test concerns the program functionality in detail. Various tests are conceivable, such as process simulations, parameter checks, and limit value tests. To investigate the functionality of the software, among other things, various tests and analyses are available.

- IO test
- Acceptance test
- Function test
- Response time test
- Signal path test

Factory Acceptance Test

The acceptance of a safety function in the plant is completed within the scope of a Factory Acceptance Test (FAT). You can find sample documentation for this in Industry Online Support under the entry ID [109758262](#).

Figure 2-8 Exemplary V&V Specification

V&V Specification

Project: Project name
Version: XY of xx.yy.zz

Author: NAME (V&V Manager)
Releaser: NAME (Functional Safety Manager)

1. Module test

This chapter describes the test procedure for testing the individual modules..

1.1 Test execution

Hardware
Description of used hardware to perform the module test.

Software
Description of used software to perform the module test.

Procedure
Description of the test procedure

Test structure
Description of how the test cases are defined (flowcharts, state graphs...)

1.2 Overview project parameter

The following parameters are documented before the testing:

- Data name of the test project
- Symbolic block name
- Object number
- Block signature
- Password

1.3 Module Test checklist

The test cases with the expected results are shown here

1.4 Test case 1

Serial Nr.	IN1	IN2	IN3	IN4	Q		Test OK
					Expection	Real	
1.							
2.							
3.							
4.							

1.5 Test case n

2. Function test

This chapter describes the test execution of the entire system in the interaction of the individual modules.

2.1. Test execution

Hardware

Description of used hardware to perform the module test.

Software

Description of used software to perform the module test.

Procedure

Description of the test procedure

Hardware parameter

Specifications for the parameterization of the hardware

Test structure

Description of how the test cases are defined (flowcharts, state graphs...)

Block linking

Describes the interaction and signal characteristics between the individual blocks

1.6 Overview project parameter

The following parameters are documented before the testing:

- Data name of the test project
- Symbolic block name
- Object number
- Project signature
- Block signature
- Password

2.2. Description of test documentation

Serial Nr.	FDS cuncion, step	Test case	Test requirements	Test description/execution	Required result	Test result / tester / date
1.						
2.						
3.						
4.						
5.						
6.						

3. Summary test result

Summary of test result des Testergebnis|or list of defect to be remedied

3 Summary and conclusion

Every machine manufacturer must provide proof that the products he places on the market meet all legal requirements. The Functional Safety Management process provides a means of doing this.

With the process described, all necessary tasks can be carried out step by step, through a defined organizational structure. Various phases such as specification, implementation, verification and validation are run through and worked out. The responsibilities for activities, documents and milestones are also defined.

This helps to avoid systematic errors, to increase the quality of the products, and to integrate a structured working method into the workflow.

The user himself is responsible for the respective level of detail as well as the scope of this process shown. Here, it is always important to ensure that a suitable degree is found for the respective project scope.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

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

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

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

support.industry.siemens.com

Technical Support

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

www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

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

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

www.siemens.com/sitrain

Service offer

Our range of services includes the following:

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

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

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

Fehler! Linkreferenz ungültig.

4.2 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support Fehler! Linkreferenz ungültig.
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109781708
\3\	

4.3 Change documentation

Table 4-2

Version	Date	Modifications
V1.0	09/2020	First version