Choose certainty.
Add value.

Report

to the

Certificate

M6A 067803 0019 Rev. 00

Safety-Related Programmable Systems

SIMATIC Safety System

Manufacturer:

Siemens AG
Gleiwitzer Str. 555
D-90475 Nürnberg

Report No.: SN84635C
Revision 2.2 dated 2019-02-13

Testing Body:

TÜV SÜD Rail GmbH
Generic Safety Systems
Barthstraße 16
D-80339 München

Certification Body:

TÜV SÜD Product Service GmbH
Ridlerstraße 65
D-80339 München

Revision Log

Version	Name	Date	Changes/History
1.0	G. Greil	2013-11-06	Initial
1.1	P. Weiß	2013-11-14	New Certificate number Chapter 2.1, 2.2, 2.3, 4.1, and 4.2
1.2	G. Effenberger	2016-03-14	New certificate numbers (Z10 13 09 67803 007 to Z10 16 02 67803 010)
1.3	G. Effenberger	2016-06-08	update to IEC 62061: 2005 / A2: 2015 EN 62061 :2005/A2: 2015
1.4	C. Dirmeier	2016-06-30	ET200MP added
2.0	P. Weiß	2018-07-17	M6A certificate updated Chapter 2.1.1.2 modified Chapter 2.5 updated
2.1	C. Dirmeier	2018-08-29	New number of Z10 certificate Chapter 3.2 updated
2.2	C. Dirmeier	2019-02-13	Added SFF in chapter 1.1 and 2.1.1 Rev. added in certificate number

Content Page

1 Purpose and Scope

TÜV SÜD Rail GmbH has been contracted by Siemens AG to certify the Safety-Related Programmable System SIMATIC Safety System.

This report summarizes the user related results of the tests and inspections performed on the SIMATIC Safety System based on the certification requirements outlined under clause 3.1 and reported by the documentation listed under clause 3.2.

1.1 Definition of Terms

The following terms are used in this report with a meaning defined as follows:

Functional Safety	Part of the overall safety relating to the EUC (equipment under control) and the EUC control system that depends on the correct functioning of the E/E/PE (electrical/electro-nic/programmable electronic) safety-related systems and other risk reduction measures to achieve a (defined) safe state for the equipment under control (EUC) or to maintain the safe state for the EUC.
Multiple fault occurrence time	The multiple-fault occurrence period denotes a time frame, in which the probability for the appearance of combination-wise safety-critical multiple faults is sufficiently low for the considered requirement class. The period of time begins with the last point in time, at which the considered system was in a fault-free assumed condition according to the considered requirements class. The definition of this time is not system specific. A general recommendation is to assume this time to be magnitudes (2 to 3) below the specified MTBF time.
Fault tolerance time (process safety time)	The fault-tolerance time denotes a characteristic of the process and describes the period of time, in which the process can be controlled by a faulty control-output signal, without entering a dangerous condition.
Interference free	Property of a unit not to cause faulty state in connected units even if it fails.
Probability of Failure on Demand (PFD)	Safety unavailability of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.
Average frequency of a dangerous failure per hour (PFH)	Average frequency of a dangerous failure (per hour) of an E/E/PE safety related system to perform the specified safety function over a given period of time (in the case of high demand or continuous mode)
Profibus	Includes PROFINET-IO and PROFIBUS-DP/PA
SFF	Safe Failure Fraction
TIA Portal	Totally Integrated Automation Portal

Table 1: Definition of Terms

2 System Overview

The SIMATIC Safety System is a Safety-Related Programmable System suitable for safety-related applications with a high level of potential danger, e.g. controllers for machinery applications, chemical processes and offshore processes.

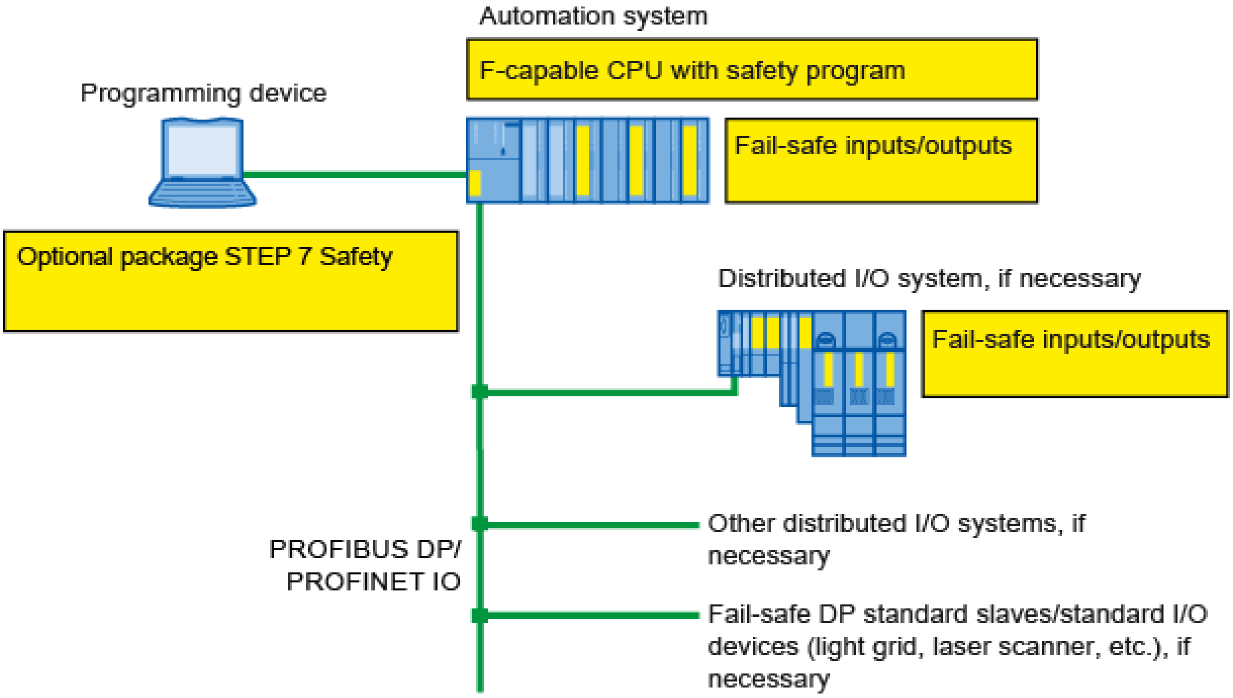
Automation system
F-capable CPU with safety program
Programming device
Fail-safe inputs/outputs
Optional package STEP 7 Safety
Distributed I/O system, if necessary
Fail-safe inputs/outputs
PROFIBUS DP/
PROFINET IO
Other distributed I/O systems, if necessary
Fail-safe DP standard slaves/standard I/O devices (light grid, laser scanner, etc.), if necessary

Figure 1: Hard and software components of SIMATIC Safety System

The SIMATIC Safety System consists of a F-CPU (central processing unit) and fail-safe I/O suitable for safety-related applications.

Safety critical input signals are read from the process with the fail-safe I/O or read from other F-CPU's via safety-related communication.

Safety critical output signals are sent from the F-CPU to the fail-safe I/O or to other F-CPU's via safety-related communication. The fail-safe I/O is responsible for the safety-related output to the process.

2.1 System Elements within the scope of this document

The following elements describe the system elements included in the above referenced certificate. These elements are tested, developed, and realized according to the standards mentioned in chapter 3.

2.1.1 F-CPU

The F-CPU implements a 1oo1D structure with diverse application software ("coded processing" according to IEC 61508-3) on single channel hardware and a non-safety relevant operating system.

Fault detection and control with SFF >> 99% is implemented by comparison of the diverse application software results within the CPU at different levels and the independent fail-safe I/O, internal self-tests and program and data flow monitoring in the CPU and fault monitoring of the CPU by the fail-safe I/O.

2.1.1.1 F-CPU S7-1500

The F-CPU's from S7-1500 system can be configured with central and de-central failsafe I/O modules.

2.1.1.2 F-CPU S7-1200

The F-CPU's from S7-1200 system can be configured with central and de-central[1] failsafe I/O modules..

2.1.2 Safety application programming

Safety application programming is performed by editing the safety program using the F-FBD or F-LAD language (a subset of FBD respectively LAD) and certified function blocks out of the library.

Coded processing is added by a special compiler included in the optional package STEP 7 Safety.

Edit, compile and load functions for application programs are using the standard STEP7 Safety programming environment of the SIMATIC. The STEP7 Safety programming environment can also be used within the functionality of the TIA portal.

The software STEP7 Safety V13 SP1 or higher for the Engineering Station (ES) allows the user to configure, maintain and operate the failsafe application for the S7-1200 F system (see chapter 2.1.1.2 and 2.1.5.2).

2.1.3 Safety Hardware configuration

Safety Hardware configuration is necessary for installation and modification of a SIMATIC Safety System using STEP7 Safety too.

2.1.4 Communication

Safety-related communication between F-CPUs and fail-safe I/O is based on the PROFIsafe protocol via any network medium but implements an additional safety shell on top.

[1] From STEP 7 Safety V14.0

2.1.5 Fail-safe Modules

The fail-safe I/O modules of SIMATIC Safety System are build in a 1oo2D structure. They are located in the central rack or ET 200 distributed I/O racks. The safety-related communication between the CPU and the fail-safe I/O is utilizing the PROFIsafe profile.

2.1.5.1 Failsafe Modules ET200SP and ET200MP

The ET200SP and ET200MP failsafe modules can be located in the central rack or ET 200 distributed I/O racks.

2.1.5.2 Failsafe Modules S7-1200

The S7-1200 failsafe I/O modules shall be located in central rack positions only.

2.2 Hardware Components under Certification

The safety-related system components belonging to this certificate are listed in the current revision of the Annexes of the Report to the Certificate Z10 067803 0020. This allows the components to be used to process safety critical signals and functions.

All other components of the SIMATIC Safety system are interference free and allowed to be used; however, they are not certified for process safety critical signals and functions. Using these components does not interfere with the proper functioning of the safety related modules.

2.3 Software Elements under Certification

A list of the software elements with the valid version numbers is shown in the actual revision of the Annexes of the Report to the Certificate Z10 067803 0020.

2.3.1 Safety-related Software Components

The following software components have been certified ‘safety-related’ allowing the software components to be used for processing safety critical signals and executing critical functions:

- Safety-related parts of SIMATIC Safety System optional package especially
  - Safety library

For the specific versions see the actual revision of the Annexes of the Report to the Certificate Z10 067803 0020.

2.3.2 Interference free Software Components

Other software components than those mentioned in 2.3.1 are not the subject of this certification. Absence of impact of not certified components on ‘safety-related’ components is enforced due to the intrinsic safety features provided by the coded processing followed by the fail-safe I/O.

2.4 Certified System Elements not in the scope of this document

The following elements can be used with the system elements described in chapter 2.1. These elements of the S7 Distributed Safety system are tested, developed, and realized according to the standards mentioned in the related reports and certificates. A system can be built up, using elements of SIMATIC Safety (see chapter 2.1) and elements of SIMATIC S7 Distributed Safety (see chapter 2.2). As a result, the safety functions of these combined system elements shall be used in the certification scope of SIMATIC S7 Distributed Safety only.

2.4.1 F-CPU

The F-CPU S7 Distributed Safety implements a 1oo1D structure with diverse application software (“coded processing” according to IEC 61508-3) on single channel hardware and a non-safety relevant operating system. Fault detection and control is implemented by comparison of the diverse application software results within the CPU at different levels and the independent fail-safe I/O, internal self-tests and program and data flow monitoring in the CPU and fault monitoring of the CPU by the fail-safe I/O.

2.4.2 Fail-safe Modules

The fail-safe I/O modules of S7 Distributed Safety are build in a 1oo2D structure. They are located in the central rack or ET 200 distributed I/O racks. The safety-related communication between the CPU and the fail-safe I/O is utilizing the PROFIsafe profile.

2.5 Safety manuals

The conditions and rules for safe use of the SIMATIC Safety System are laid down within the user documentation:

- SIMATIC Safety - Configuring and Programming (Programming and Operating Manual)
- SIMATIC ET 200SP Distributed I/O system, System manual and Manuals for the Fail-Safe Modules
- SIMATIC ET 200eco PN, Manuals for the Fail-Safe Modules
- SIMATIC S7-1200 Functional Safety Manual and updates
- SIMATIC S7-1500/ET200MP Automation system, System manual and Manuals for the Fail-Safe Modules
- SIMATIC S7-1200/S7-1500 F-CPUs product information

3 Certification Requirements

3.1 Basis of Certification

The certification of SIMATIC Safety System will be according to the regulations and standards listed in clause 3.3 of this document. This certifies the successful completion of the following test segments:

I. Functional safety
   - Analysis of the system structure (FMEA system)
   - Analysis of the hardware (FMEA component, quantitative analysis)
   - Analysis of the software
   - Fault simulations and software tests
   - Test of the fault prevention measures
   - Functional test

II. Electrical safety

III. Susceptibility to environmental errors
   - Climate and temperature
   - Mechanical effects

IV. Electromagnetic compatibility

V. Safety information in the product documentation (safety manual, operating instructions)

VI. Product-related Quality Management in manufacturing and product care.

Certification is dependent on successful completion of all of the above test segments. The testing follows the basic certification scheme for safety-related programmable electronic systems of TÜV SÜD Rail GmbH.

3.2 Certification Documentation

Documentation of this certification is based in the following reports:

- Testing documentation
  The Technical Reports SN83930T, SA85222T, SF86498T, SN88221T, SN90355T, SN90962T and SN92804T are summarizing the assessment activities related to functional safety. The certification report is a mandatory part of the certificate, whereas publication of the Technical Report is facultative.
- Manual, see chapter 2.5

Based on the specified purpose of use of the SIMATIC Safety System in safety critical process protection applications the certification is based on the following set of standards. The issuance of the certificate states compliance with these references unless specifically noted otherwise.

3.3 Standards Machinery (MD)

The assessment of the safety related system has been performed in accordance to the following guideline, reference and title of the harmonized standards. This component specific information is given in the current revision of the Annexes of the Report to the Certificate Z10 067803 0020.

Because of the expected applications of the system following additional standards and regulations should be considered:

Directive 2006/42/EC	Base: Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) OJ No L 157, 9 June 2006 Modification: Regulation (EC) N° 569/2009 - adaptation to the regulatory procedure with scrutiny [OJ L 188, 18 July 2009] Directive 2009/127/EC amending Directive 2006/42/EC with regard to machinery for pesticide application [OJ L 310, 25 November 2009]
ISO 13849-1:2015 EN ISO 13849-1: 2015	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design
EN 62061 :2005/A2: 2015 IEC 62061: 2005 / A2: 2015	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

Table 2: Standards

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the SIMATIC Safety System in conjunction with their system software comply with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections, and is suitable for safety-related use in accordance with ISO 13849-1 up to PL e and CAT 4 and in accordance with IEC 61508 (ed2) and IEC 62061:(ed1); am1; am2 up to SIL3, for intermittent or continuous operation, as well as for operation with or without continuous supervision, on condition that the "0 state" (closed-circuit principle) is defined as the safe state for the binary inputs and outputs.

4.1.1 Fault Reaction and Timing

Fault reactions of F-CPU:

1. Faults in the cyclic communication between the F-CPU and the fail-safe input modules are detected by the F-CPU. Either ‘0’ or configured substitute values are handed to the application program. The application program developer must implement a specific fault reaction.
2. Faults in the cyclic communication between the F-CPU and the fail-safe output modules are detected by the F-DQ. If a fault occurs, all outputs of the affected fail-safe modules are driven to ‘0’.
3. Faults in the cyclic communication between two F-CPU’s are detected by the receiving F-CPU. If a fault occurs the application program is notified and configured substitute values are handed to the receiving application program. The application program developer must implement a specific fault reaction.
4. Faults within the safety-related data or code, within data or control flow of the application program and faults detected by built-in tests lead at first to standard stop reactions of the CPU. The safety-related propagation of the detectability of those failures to the fail-safe I/O and other CPU’s lead to a safe state (see fault reactions 1., 2. and 3.).

Fault reactions of fail-safe I/O:

Faults detected by built-in self-tests or diagnostics are either fail-safe communicated to the application program or in case communication is affected faults are detected as described in section 1. and 2. above. If the faulty module is an input module, the process data transmitted to the F-CPU is set to ‘0’ with binary inputs for all inputs or the faulty inputs. If the faulty module is an output module, all outputs or the faulty outputs are driven to ‘0’.

The fault tolerance period of the process controlled by the SIMATIC Safety System shall be greater than the worst case response time. Additional information is given in the manuals (see clause 2.5).

4.1.2 Evaluation of fault prevention measures

For the avoidance of failures the following techniques and measures were used:

- Project management
- Documentation
- Structured specification
- Inspection of the specification or walk-through of the specification
- Observance of relevant guidelines and standards
- Structured design
- Modularization
- Use of well tried components
- Inspection of the hardware
- Functional testing (also under environmental conditions)
- Operational and maintenance instructions
- User- and maintenance friendliness

The individual measures for the avoidance of failures provide the required degree of effectiveness and are specified in the relevant documents

4.1.3 Analysis of the hardware safety integrity

The Failure Mode Effect Analysis (FMEA) showed that the occurrence of multiple faults, fault accumulation and common cause failures do not lead to loss of the safe functioning.

4.1.4 Application Development

The SIMATIC Safety System can treat and execute programmed safety and non-safety-related functions independently from each other at the same time. An intended safety function of the SIMATIC Safety System can be enforced either by application programmed functions or by built in fault reaction functions. The application programmed safety function lies with the application program developer.

During planning and engineering of applications the developers should regard the certification requirements defined in the chapters 3.3 and the element specific information detailed in the current revision of the Annexes.

Acceptance of programmed safety function requires complete functional testing. After that complete functional testing is only necessary for changed parts of the programmed safety function.

Loading and changing of safety-related programs in the CPU need authorization by password. Non safety-related programs can be changed at any time without impact on programmed and built-in safety functions of the SIMATIC Safety System.

4.1.5 Online loading of safety applications

In general, responsibility for monitoring the process during and after the on-line modification lies entirely with the organization and person responsible for the on-line modification. Since on-line modifications are generally associated with an increased level of risk the approval of on-line modifications is at the discretion of the testing and inspection center responsible for approval of the system’s application.

The procedure for on-line modifications and existing restrictions are described in the manuals ‘SIMATIC Safety, Configuring and Programming’.

Loading of safety program changes and changes of safety related constant parameters while the process is running in observed mode requires at least:

- off-line verification and / or
- simulation and / or
- online testing and / or
- similar IEC 61508 compliant verification activities within a well defined modification procedure

of the changes prior to downloading them into the CPU controlling the safety critical process.

4.2 Basic Safety and Electromagnetic Compatibility

4.2.1 Electrical Safety

The results about the electrical safety are documented by the certificates and test reports of an accredited test centre. The documentation of the tests has been reviewed for completeness.

These certificates show that the standards specified in clause 3 are covered.

4.2.2 Environmental Testing

The environmental stress tests are documented by the certificates of an accredited test centre.

The above mentioned certificates and tests and the quality assurance measures implemented by the manufacturer have shown that the SIMATIC Safety System complies with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections.

4.2.3 Electromagnetic Compatibility

The tests of the electromagnetic compatibility are documented by the certificates and test reports of an accredited test centre. The documentation of the tests has been reviewed for completeness.

These certificates show that the standards specified in clause 3 are covered.

4.3 Product Specific Quality Assurance and Control

All software and hardware elements developed and manufactured in course of the safety evaluation are governed by an ISO 9001 certified quality assurance and control system.

As part of the certification process TÜV Product Service also performs a procedure that is tailored to the assessed product in order to assess the consistency of product quality while accounting for product modifications and their identifiability (follow-up service).

5 Implementation Conditions and Restrictions

The use of the SIMATIC Safety System shall comply with the current version of the Safety parts of the manual (see chapter 2.5) and the following implementation and installation requirements shall be followed if the SIMATIC Safety System are used in safety-related installations.

The SIMATIC Safety System is a safety-related product and the recommendations based on the experience and judgement of the Siemens AG documented in the manuals shall therefore be carefully followed. The information, recommendations, specifications and safety instructions given in the belonging manuals shall be read and understood.

5.1 General application conditions

5.1.1. Only elements certified for safety-related operation, as shown in the Annexes of the Report to the Certificate Z10 067803 0020 shall be used for safety-critical signals. Not certified standard elements (defined as ”interference-free”) may be used for non-safety-critical signals only.

5.1.2. The fault tolerance period (process safety time) of the process controlled by the system shall be greater than the worst-case response time of the system.

5.1.3. A well-defined shutdown procedure shall be specified.

5.1.4. Non-safety-related blocks in the application program shall not control or affect data used by any safety-critical block unless in case of plausibility checks in the safety-related program.

5.1.5. Operator alarms as exclusive means of shutdown are only permitted under supervised operation and if the fault tolerance time of the controlled process is sufficiently long to ensure a safe manual reaction and shutdown and the operator has sufficient independent means to supervise the process. Installations that must react to shut down conditions quicker than achievable with manual intervention or installations running unsupervised shall incorporate an automatic fault reaction procedure.

5.1.6. The operating conditions as specified in the user manuals shall be met.

5.1.7. The elements listed in the Annex of the S7 Distributed Safety system certification can be used with the system elements described in chapter 2.1. The elements of the S7 Distributed Safety system are tested, developed, and realized according to the standards mentioned in the related reports and certificates. As a result, the safety functions of these combined system elements shall be used in the certification scope of SIMATIC S7 Distributed Safety only.

5.2 General commissioning conditions

5.2.1. Prior to commissioning, a complete functional test of all safety-relevant programmed application functions shall be performed. The programming of the application shall ensure that modules are small and self contained, sufficient to permit full functional testing.

5.2.2. All timing requirements shall be validated.

5.2.3. Any application software modification after commissioning shall result in a re-validation of the entire application software system. The commissioning can be reduced if the change can be shown by use of a revision checker to be limited to a specific area of program.

5.2.4. The proper fail-safe configuration of all safety-critical fail-safe I/O shall be verified. Only configurations covered by the User’s manual are covered by the certification.

5.3 General run-time conditions

5.3.1. Failed elements that are safety-related should be replaced as quickly as practical to minimize the probability of multiple fault accumulation and potential (safe) nuisance shutdown. As a maximum, failed elements should be replaced within the multiple fault occurrence time. The calculations in the Internal Report of the Probability-of-Failure-on-Demand of safety-related programmable System SIMATIC Safety System are based on a mean time to repair of 100h.

5.3.2. Application program modification during run-time should only be permitted under end-user responsibility.

5.3.3. The procedure described in the user manual has to be followed.

5.3.4. The application program modifications shall be limited and simple to verify and validate.

5.3.5. The modifications and their interaction with existing program sections shall be thoroughly tested, e.g. using simulation.

5.3.6. The modification shall be granted by the approval authority for the plant assessment.

5.3.7. Maintenance override is to be limited (time-restriction and number) of logical points. The TÜV guidelines for maintenance overrides are to be followed. TÜV certification does not cover output override.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of the Safety-Related Programmable Systems SIMATIC Safety System by Siemens AG to the certificate:

M6A 067803 0019 Rev. 00

Munich, 2019-02-13

Digital
unterschrieben
von Christian
Dirmeier
Datum:
2019.02.13
15:27:30 +01'00'

Christian Dirmeier

Technical Certifier