Rail

Add value.
Inspire trust.

Report

to the

Certificate

Z10 16 06 20080 004

Safety-Related Programmable Systems

SIMATIC S7 F/FH Systems

Manufacturer

Siemens AG
PD PA AE R&D
Östliche Rheinbrückenstr. 50
D-76187 Karlsruhe

Report No. SN87148C
Revision 1.6.1 of 2019-10-22

Test Body

TÜV SÜD Rail GmbH
Rail Automation
Barthstraße 16
D-80339 München

Certification Body

TÜV SÜD Product Service GmbH
Ridlerstraße 65
D-80339 München

List of Contents page

List of Tables page

List of Figures page

Modification History

Version	Status	Date	Author	Changed chapters	Reason of change
1.0	final	2015-12-17	C. Dirmeier		Initial version based on the report to the certificate Z10 09 07 67803 004
1.1	final	2016-04-18	G. Effenberger	2.1 2.3.3, 2.3.4, 2.4	Adopted figures 1 and 2, correction of text passages text corrections corrections in wording ET 200 SP safety manual added
1.2	final	2016-04-21	G. Effenberger	3.1	correction of wording (3.1) and correction after Siemens review
1.3	final	2016-06-23	G. Effenberger	3.6	update to EN ISO 13849-1: 2015 update to IEC 62061: 2005/A2: 2015 update to IEC 61511-1: 2016 update of certificate number Z10 16 06 20080 004
1.4	final	2016-09-20	P. Weiß	3.6	update to UL 1998 update to ANSI/ISA-84.00.01 update to VDI VDE 2180 update to NFPA 72 update to NFPA 85 (SK89909T)
1.5	final	2017-02-01	G. Effenberger	3.6	Update to EN 54-2 (SK 90484T)
1.6	final	2019-10-08	P. Weiß	1, 3.6, 5.1	Update including burner standards (SK94376T)
1.6.1	final	2019-10-22	P. Weiß	-	Formal Update

Table 1: Modification history

1 Target of Evaluation (ToE)

In April and May 2015 Siemens AG assigned TÜV SÜD for testing and certifying of the Safety-Related Programmable Systems SIMATIC S7 F/FH Systems according to the 2nd edition of the IEC 61508 series (SIL 3), ISO 13849-1 (Category 4 PL e) and IEC 62061 (SILCL 3). The SIMATIC S7 F/FH Systems have already been certified for the 1st edition of the IEC 61508 series with certificate Z10 09 07 67803 004.

This report summarizes the user related results of the tests and inspections performed on the SIMATIC S7 F/FH Systems based on the certification requirements outlined under clause 3.1 and reported by the documentation listed under clause 3.2.

In June 2019 Siemens AG assigned TÜV SÜD for testing and certifying the Safety-Related Programmable Systems SIMATIC S7 F/FH Systems in accordance to the burner standards referenced in clause 3.6.

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/electronic/programmable electronic) safety-related systems and other risk reduction measures to achieve a (defined) safe state for the 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).
1oo2D	This architecture consists of two channels connected in parallel. During normal operation, both channels need to demand the safety function before it can take place. In addition, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that

	the overall output state then follows that given by the other channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either channel, then the output goes to the safe state. In order to detect a discrepancy between the channels, either channel can determine the state of the other channel via a means independent of the other channel.
1oo1D	This architecture consists of a single channel connected to an independent diagnostic circuit (not self-diagnostics). If the diagnostic circuit detects a hidden fault in the channel it asserts the safe state via a means independent of the channel.

Table 2: Definitions and Terms

2 System overview

2.1 System Architecture

SIMATIC S7 F/FH Systems are safety-related fail safe programmable electronic systems (PES) suitable for safety-related applications with a high level of potential danger, e.g. controllers for chemical processes, offshore processes and machinery applications.

SIMATIC S7 F/FH Systems consist of 1 or 2 "S7-400 CPUs" (central processing units) respectively that are suitable for safety-related applications and "Fail-Safe I/O Modules" (F-I/O).

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

The S7-400 F-CPU implements a 1oo1D structure with diverse application software on single channel hardware. Fault detection is implemented by comparison of the diverse application software results in the CPU and the independent F-I/O, internal self-tests and program and data flow monitoring in the CPU and fault monitoring by the F-I/O.

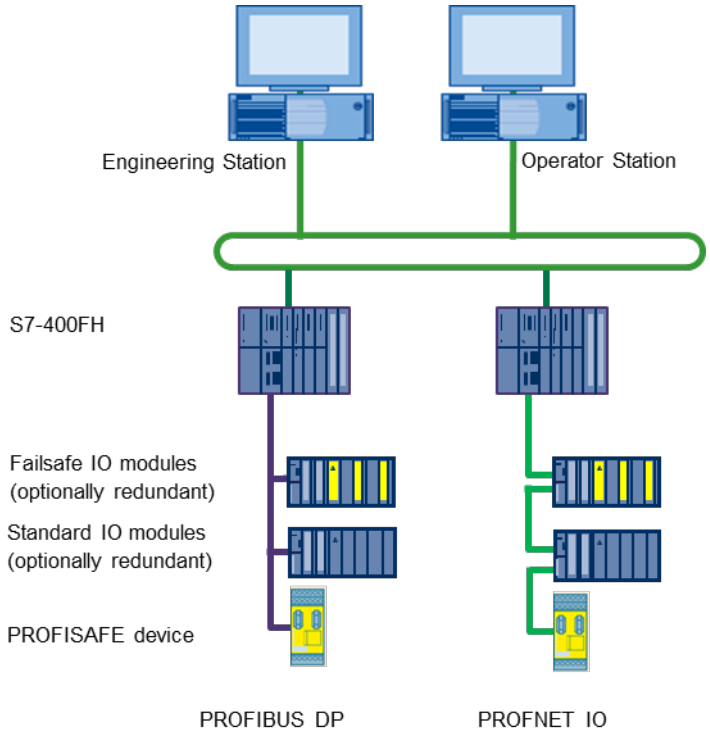

Figure 1: System Architecture for S7 F/FH Systems (single architecture)

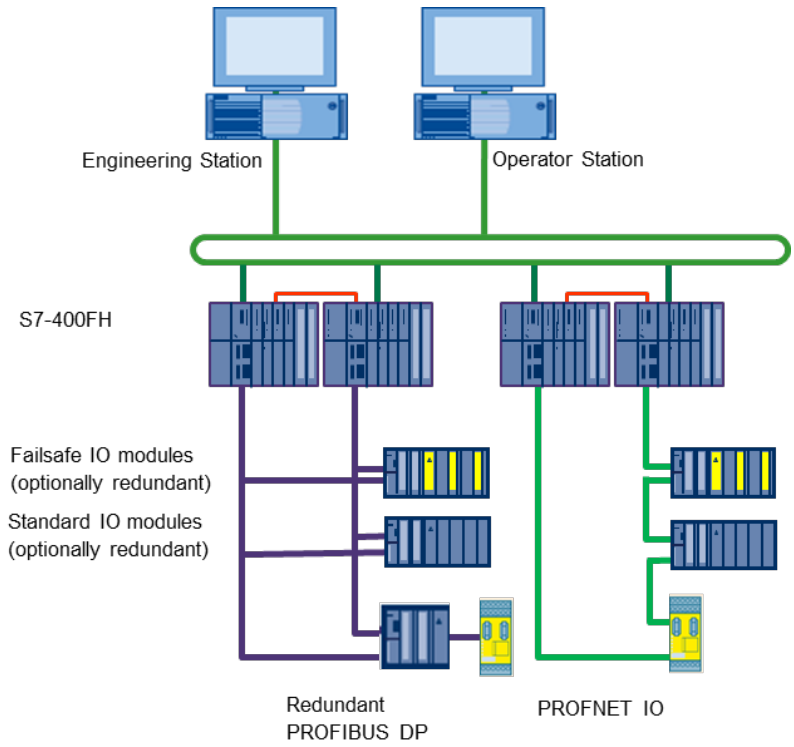

Figure 2: System Architecture for S7 F/FH Systems (redundant architecture)

The following fault control measures are implemented in the CPU:

- redundant execution with data and code redundancy, diversity and comparison of the diverse results
- self-test of safety-related operations in each cycle
- program and data flow monitoring

Checking of this and fault reaction is done directly by the CPU itself as well as indirectly by the recipients of the CPU's safety-related outputs, i.e. the fail-safe output modules and other CPUs.

In addition, the CPU performs self-tests in the background and uses two independent time bases. One CPU is sufficient to achieve the certified functional safety. In the S7 FH two redundant CPUs (each 1oo1D) are used to increase availability.

The F-I/O modules are in an internal 1oo2D structure (two channels with comparison). One F-I/O module is sufficient to achieve the certified functional safety. Optionally two redundant F-I/O modules (each 1oo2D) are used to increase availability.

2.2 Hardware/Firmware Components under Certification

The system components which are certified ‘safety-related’ are listed in the current revision of the Annexes to this report. This allows the components to be used to process safety critical signals and functions.

All other components of the S7-400 and S7-300 family 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.

For details on architectural, configuration and implementation requirements please refer to the manuals (see chapter 2.4).

2.3 Software Components under Certification

A list of the software components with the valid version numbers is shown in the actual revision of the Annexes to this report.

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:

- SIMATIC S7 F Systems
- SIMATIC S7 Safety Matrix

For the specific versions see the actual revision of the Annexes to this report.

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 diverse logic implementation followed by the 1oo2D F-I/O modules.

2.3.3 Communication

Safety-related communication between F-CPUs and F-I/O is based on the Profibus and ProfiNET protocol but implements an additional safety layer on top (PROFIsafe).

Safety-related communication between F-CPUs is based on standard protocols like MPI, Profibus-DP/PA or Ethernet but implements an additional safety layer on top.

2.3.4 Programming environment

Safety application programming is performed by the connection of function blocks using the SIMATIC CFC language. CFC is a limited variability language which offers certified function blocks to realize safety functions. These fail safe function blocks utilise particular safety data types to prevent the usage of standard function blocks for safety applications. To edit, compile and load the application program the standard SIMATIC Manager programming environment of the S7-400 and S7-300 family is used. The add-on option package S7 F Systems provides the following properties required to extend the standard programming environment for safety programming:

- Library with safety-related function blocks (F-FBs)
- Integration of fault detection measures (self-tests, program and data flow monitoring, data redundancy) into the application program
- Additional access protection for the safety-related parts of the application program and configuration data in SIMATIC Manager and in the F-CPU
- Add-on option package S7 F Systems consistency checks
- Use in virtual environments and the use of remote access

2.4 Safety manual

The conditions and rules for safe use of the SIMATIC S7 F/FH Systems are laid down within the user documentation:

- SIMATIC Industrial Software Safety Engineering in SIMATIC S7, System Manual
- SIMATIC Industrial Software S7 F/FH Systems Software - Configuring and Programming, Programming and Operating Manual
- SIMATIC Industrial Software Safety Matrix, Configuration Manual
- SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-Safe Signal Modules, Hardware Installation and Operating Manual
- SIMATIC Distributed I/O System Fail-Safe Engineering ET 200S Distributed I/O System, Installation and Operating Manual
- SIMATIC ET 200eco Distributed I/O Station - Fail-Safe I/O Module Operating Instructions
- SIMATIC Distributed I/O fail-safe engineering ET 200pro Distributed I/O System - Fail-Safe Modules, Operating Instructions

- SIMATIC Distributed I/O, ET 200iSP Distributed I/O Device – Fail-safe Modules Operating Instructions
- SIMATIC ET200SP Distributed I/O system, System Manual and Manuals for the Fail-Safe Modules
- ET200M, Marshalled Termination Assemblies, Remote I/O Modules Commissioning Manual
- SIMATIC Industrial software PFD_{avg} and PFH values for components with use in SIMATIC Safety, Distributed Safety and F/FH Systems, Product Information

3 Certification Requirements

3.1 Basis of Certification

The certification of the SIMATIC S7 F/FH Systems was conducted according to the regulations and standards listed in clause 3.3 to 3.6 of this document. The assessment confirms 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.

The testing follows the basic certification scheme for Safety Components of TÜV SÜD Rail GmbH.

3.2 Certification Documentation

Documentation of this certification is based on the following reports:

- Testing documentation:
  The technical reports SN87148T and SN87345T 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.
- Manuals see chapter 2.4.

Based on the specified purpose of use of SIMATIC S7 F/FH Systems in safety critical process 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 Functional Safety

The testing for functional safety is to be performed using the following standards and guidelines:

IEC 61508-1 (ed.2) (SIL3) (= IEC 61508-1: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
IEC 61508-2 (ed.2) (SIL 3) (= IEC 61508-2: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems
IEC 61508-3 (ed.2) (SIL 3) (= IEC 61508-3: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements
IEC 61508-4 (ed.2) (SIL 3) (= IEC 61508-4: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations
IEC 61508-5 (ed.2) (SIL 3) (= IEC 61508-5: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 5: Examples of methods for the determination of safety integrity levels
IEC 61508-6 (ed.2) (SIL 3) (= IEC 61508-6: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC 61508-7 (ed.2) (SIL 3) (= IEC 61508-7: 2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 7: Overview of techniques and measures

Table 3: Standards functional safety

3.4 Basic Safety and Environmental Safety

To complete and to specify the technical requirements resulting from the essential requirements of the directives listed above the testing of Basic Safety is to cover the following standards:

IEC 60204-1 (ed.5) EN 60204-1: 2006 / A1:2009, AC:2010	Safety of machinery – Electrical equipment of machines Part 1: General requirements
EN 61131-2:2007	Programmable controllers Part 2: Equipment requirements and tests

Table 4: Standards Basic safety and environmental safety

3.5 Electromagnetic Compatibility

To complete and to specify the technical requirements resulting from the essential requirements of the directives listed above, the testing of Electromagnetic Compatibility is to cover the following standards:

EN 61131-2:2007 IEC 61131-2 (ed.3)	Programmable controllers – equipment requirements and tests
EN 61000-6-2:2005	Electromagnetic compatibility (EMC) Part 6-2: Generic standards – Immunity standard for industrial environments
EN 61000-6-4:2007	Electromagnetic compatibility (EMC) Part 6-4: Generic standards – Emission standard for industrial environments
EN 61326-3-1:2008	Electrical equipment for measurement, control and laboratory use – EMC requirements Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications

Table 5: Standards Electromagnetic Compatibility

3.6 Application

IEC 60204-1 (ed.5) EN 60204-1: 2006 / A1:2009, AC:2010	Safety of machinery – Electrical equipment of machines Part 1: General requirements
IEC 61511, Part 1 - 3:2003	Functional safety - Safety instrumented systems for the process industry sector Part 1: Framework, definitions, system, hardware and software requirements Part 2: Guidelines for the application of IEC 61511-1 Part 3: Guidance for the determination of the required safety integrity levels
EN 62061/A1:2013, IEC 62061 (ed.1), am2 (SILCL 3) (=IEC 62061:2005 / AMD2:2015)	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
ISO 13849-1: 2015 EN ISO 13849-1:2015 (Cat. 4 PL e)	Safety of machinery — Safety-related parts of control systems Part 1: General principles for design
IEC 61511-1: 2016	Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements
UL 1998	Standard for Safety for Software in Programmable Components
ANSI/ISA-84.00.01: 2004	Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements
VDI VDE 2180: 2007 Part 1	Safeguarding of industrial process plants by means of process control engineering – Introduction, terms, comments

VDI VDE 2180: 2007 Part 2	Safeguarding of industrial process plants by means of process control engineering (PCE) – Management system
VDI VDE 2180: 2007 Part 3	Safeguarding of industrial process plants by means of process control engineering (PCE) – Plant engineering, realization and operation
VDI VDE 2180: 2010 Part 4	Safeguarding of industrial process plants by means of process control engineering (PCE) – Calculating methods of reliability characteristics of safety instrumented systems
VDI VDE 2180: 2010 Part 5	Safeguarding of industrial process plants by means of process control engineering (PCE) – Recommendations for practical use
VDI VDE 2180: 2013 Part 6	Safeguarding of industrial process plants by means of process control engineering (PCE)-Application of functional safety in the context of explosion protection
NFPA 72: 2016	National Fire Alarm and Signaling Code
NFPA 85: 2015	Boiler and Combustion Systems Hazards Code
EN 54-2:1997/A1:2006 [1]	Fire detection and fire alarm systems – Part 2: Control and indicating equipment
DIN EN 50156-1: 2016-03 [1]	Electrical equipment for furnaces and ancillary equipment - Part 1: Requirements for application design and installation
DIN EN 50156-2: 2016-03 [1]	Electrical equipment for furnaces and ancillary equipment - Part 2: Requirements for design, development and type approval of safety devices and subsystems

Table 6: Standard Applications

[1] Only valid for marked components (with restrictions) as documented in Annex I.

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that SIMATIC S7 F/FH Systems 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 EN ISO13849-1 up to PL e and CAT 4, and in accordance with IEC 61508:2010 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.
Systematic safety integrity (SC 3) has been achieved by applying suitable techniques and measures for fault prevention and fault reaction according to Route 1_S.
Route 1_H has been applied during development to achieve the required hardware safety integrity.

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-DO. 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 data types, within data or control flow of the application program lead to blocking of the cyclic transmissions to output modules and other F-CPUs or signaling of the fault to them. If a fault occurs all outputs of the affected output modules are driven to ‘0’ and the affected receiving F-CPUs use the configured substitute values.
5. Faults detected by built-in self-test lead to blocking of the cyclic transmissions to output modules and other F-CPUs or signaling of the fault to them. If a transmission fault occurs all outputs of the affected output modules are driven to ‘0’ and the affected receiving F-CPUs use the configured substitute values.
6. In the FH-system structure one of the CPUs is running as master whereas the other CPU is running as standby. Faults in the Master-CPU detected by self-tests or other fault control mechanism inside the CPU lead to master changeover before failure effects the F-DO. Faults in the Standby-CPU detected by self-tests or other fault

control mechanism inside the CPU lead to blocking of master changeover before failure effects the F-DO.

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 process safety time of the process controlled by the SIMATIC S7 F/FH Systems shall be greater than the worst-case response time. Additional information is given in the manual ‘Safety Engineering in SIMATIC S7’.

4.1.2 Evaluation of fault prevention measures

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

- Safety 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

SIMATIC S7 F/FH Systems can treat and execute programmed safety and non-safety-related functions independently from each other at the same time. An intended safety function of SIMATIC S7 F/FH Systems can be enforced either by application-programmed functions or by built in fault reaction functions. Responsibility of application programmed safety functions are within the scope of the developers.

During planning and engineering of applications the developers should regard the certification requirements defined in the chapters 3.3. to 3.6 and the element specific information detailed in the current revision of the Annexes.

Acceptance of programmed safety function requires its 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 S7 F/FH Systems.

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: 'S7 F/FH Systems, 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 on a hot standby CPU and / or
- similar IEC 61508 compliant verification activities within a well defined modification procedure (e.g. activities acc. application standard IEC 61511) of the changes prior to downloading them into the CPU controlling the safety critical process.

4.1.6 Simulation of safety applications

Offline simulation of safety applications can be performed on a virtual CPU, emulated by an additional software package either on the programming station or the engineering station. If an online connection to a running safety system exists, the "safety mode" shall not be deactivated and the password protected access to the S7-F-CPU shall not be granted.

4.2 Basic Safety and Electromagnetic Compatibility

4.2.1 Basic Safety and Environmental Safety

The results of the electrical safety and the environmental stress tests are documented by the certificates and test reports of an accredited test laboratory of Siemens AG. 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 Electromagnetic Compatibility

The tests of the electromagnetic compatibility are documented by the certificates and test reports of an accredited test center. 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

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

5 Implementation Conditions and Restrictions

The use of SIMATIC S7 F/FH Systems shall comply with the current version of the safety parts of the user manuals (see chapter 2.4), and the following implementation and installation requirements have to be followed if SIMATIC S7 F/FH Systems are used in safety-related installations.

SIMATIC S7 F/FH Systems are safety-related products and the recommendations based on the experience and judgment 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

- The guidelines specified in the instruction manuals shall be followed. Specifically the safety notes in the user's manuals shall be followed.
- Only modules (hardware and software) certified for safety-related operation, as shown in the Annexes to this report shall be used for safety-critical functions. Not certified standard components (defined as "interference-free") may be used for non-safety-critical signals only.
- The fault tolerance period of the process controlled by the system shall be greater than the worst-case response time of the system.
- A well defined shutdown procedure shall be specified.
- Non-safety-related blocks in the application program shall not control or affect data used by any safety-critical block unless with safety-related function blocks for data conversion and plausibility checks in the safety-related program.
- 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 shutdown conditions quicker than achievable with manual intervention or installations running unsupervised shall incorporate an automatic fault reaction procedure.
- The operating conditions as specified in the user manuals shall be met.
- The components – marked with « 1 » (in annex SN87148C-A1) – comply with the application standards DIN EN 50156-1:2016 and DIN EN 50156-2:2016 in case:

  - for open air installations a cabinet with minimum of IP 40 – or IP 54 shall be used and

  - the modules shall be supplied by a power supply which backs up power failures of >20 ms.

5.2 General Commissioning Conditions

- 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.
- All timing requirements shall be validated, including fault detection time, fault reaction time, throughput delay for shutdown logic and cycle time.
- 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.
- 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

- Failed components that are safety-related and in redundant configurations should be replaced as quickly as practical to minimize the probability of multiple fault accumulation and potential (safe) nuisance shutdown. As a maximum, failed components should be replaced within the multiple fault occurrence time. The calculations in the Internal Report of the Probability-of-Failure-on-Demand of the safety-related programmable System SIMATIC S7 F/FH are based on a mean time to repair of 100h.
- Application program modification during run-time should only be permitted under end-user responsibility.
- The procedure described in the user manual has to be followed.
- The application program modifications shall be limited and simple to verify and validate.
- The modifications and their interaction with existing program sections shall be thoroughly tested, e.g. using simulation.
- The modification shall be granted by the approval authority for the plant assessment.
- The use of F-Function Blocks for SIMATIC S7 F/FH Systems is only permitted if for the specific target system (F or FH system) an official S7 F Systems RT License with the order number 6ES7 833 1CC00 6YX0 is available.

  The S7 F Systems RT License consists of:

  - a S7 F Systems RT License contract
  - a copy of the TUV-Certificate
  - two labels to mark up the CPU (or CPU´s on a FH system) of the used S7 F Systems RT License

5.4 Product related Conditions

Purpose of the Safety Protector is to isolate the failsafe modules from over- voltages up to a maximum of 250 Volt AC/DC caused by not-safety related standard modules. No field voltage higher than 250V is allowed.

For the rules for using the Safety Protector please refer the warning notice in the Safety Manual SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-Safe Signal Modules, Installation and Operating Manual, chapter for configuration with F-SMs in Safety Mode.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of SIMATIC S7 F/FH Systems to the certificate:

Z10 16 06 20080 004

Munich, 2019-10-22

TÜV SÜD Rail GmbH
Rail Automation

Guido Neumann
(Technical Certifier)

Digital unterschrieben von Guido Neumann
Datum: 2019.10.22 13:02:34 +02'00'