Choose certainty.
Add value.

Report

to the

Certificate

M6A 17 05 67803 014

Safety-Related Programmable Systems

SIMATIC S7 Distributed Safety

Manufacturer:

Siemens AG
DF FA AS
Gleiwitzer Str. 555
D-90475 Nürnberg

Report No.: SN84627C
Revision 3.2 dated 2019-02-13

Testing Body:

TÜV SÜD Rail GmbH
Generic Safety Systems
Ridlerstraße 57

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	2012-10-25	Initial
2.0	C. Dirmeier	2015-12-18	Modification regarding • IEC 62061(ed.1);am1 and • reference to new certification number Z10 15 11 67803 009 because of upgrade of certification to IEC 61508 (ed.2)
3.0	C. Dirmeier	2016-06-06	Modification regarding • EN ISO 13849-1:2015 (SN88739T) • reference to new certification number Z10 16 06 67803 012 because of upgrade of certification to EN ISO 13849-1:2015 • EN 62061:2005/A2:2015
3.1	G. Effenberger	2019-02-13	Updated type examination number due to validity date. • New Certificate number is: M6A 17 05 67803 014 • Reference to new certificate Z10 17 05 67803 015
	P. Weiß		Added SFF in chapter 1.1 and 2.1.1

Content

Page

1 Purpose and Scope

TÜV Rail GmbH has been contracted by Siemens AG to certify the Safety-Related Programmable System SIMATIC S7 Distributed Safety.

This report summarizes the user related results of the tests and inspections performed on the SIMATIC S7 Distributed 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	The ability of a safety-related system to carry out the actions necessary 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.
Process safety time	The process safety 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)	Average probability of failure of a system to perform its design functions on demand.
Probability of dangerous failure per hour (PFH)	The probability of a dangerous failure per hour (in the case of high demand or continuous mode).
Profibus	Includes PROFINET-IO and PROFIBUS-DP/PA
SFF	Safe Failure Fraction

Table 1: Definition of Terms

2 System Overview

2.1 System Architecture

The SIMATIC S7 Distributed Safety 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.

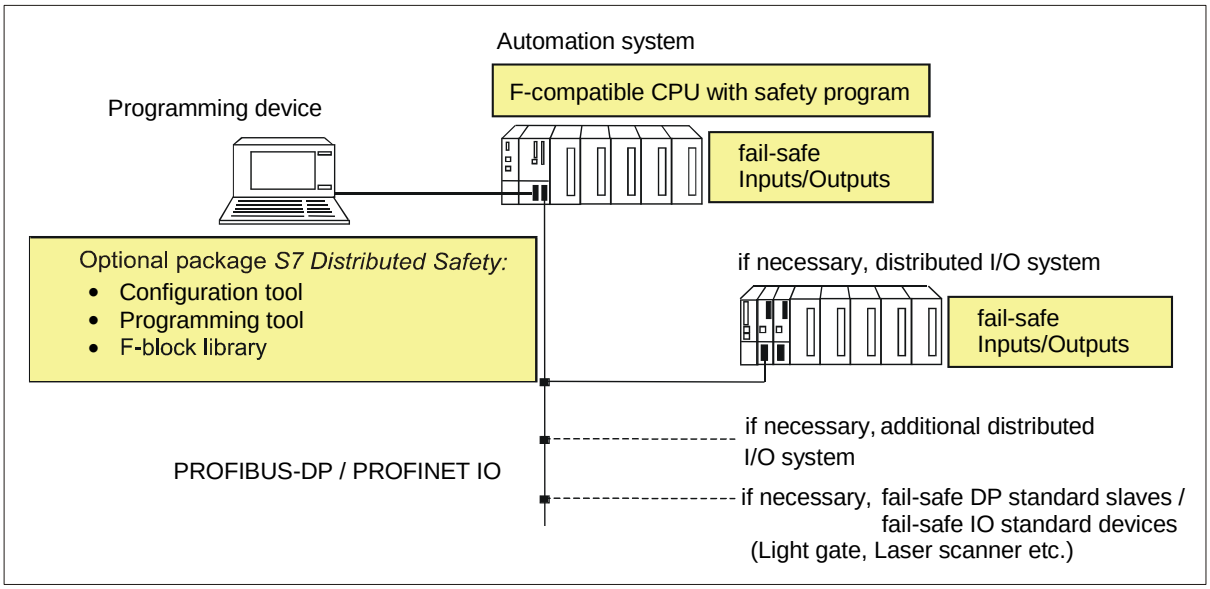

Figure 1: Hard- and software components of SIMATIC S7 Distributed Safety

The SIMATIC S7 Distributed Safety 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.

2.1.1 SIMATIC S7 Distributed Safety F-CPU

The SIMATIC S7 Distributed Safety 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.

2.1.2 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 “Distributed Safety (V1)".

Coded processing is added by a special compiler included in the optional package SIMATIC S7 Distributed Safety.

Edit, compile and load functions for application programs are using the standard STEP7 programming environment of the S7.

2.1.3 Safety configuration

Safety configuration is necessary for installation and modification of a SIMATIC S7 Distributed Safety System using STEP7 too.

2.1.4 COM PROFIsafe

COM PROFIsafe allows integration of fail-safe DP standard slaves / fail-safe IO standard devices from other companies into the SIMATIC S7 Distributed Safety system after proving and setting of all safety-related slave specific configuration data’s.

The scope of the certification only covers the software interface to those fail-safe DP standard slaves / fail-safe IO standard devices. For safety related use of those slaves the compliance to the safety standards need to be shown.

2.1.5 Fail-safe I/O

The fail-safe I/O modules of SIMATIC S7 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.

2.2 Hardware/Firmware Components under Certification

The safety-related system components belonging to this certification are listed in the current revision of the Annexes of the Report to the Certificate Z10 17 05 67803 015. This allows the components to be used to process safety critical signals and functions.

All other components of the S7 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 components.

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 of the Report to the Certificate Z10 17 05 67803 015.

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 S7 Distributed Safety optional package especially
- Distributed Safety library
- COM PROFIsafe

For the specific versions see the actual revision of the Annexes of the Report to the Certificate Z10 17 05 67803 015

2.3.2 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.

2.3.3 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 Safety manual

The conditions and rules for safe use of the SIMATIC S7 Distributed Safety are laid down within the user documentation:

- Industrie Software
  Safety Engineering in SIMATIC S7
  System Manual
- S7 Distributed Safety
  Configuring and Programming
  Programming and Operating Manual
- Distributed I/O system, ET200SP,
  System Manual and Manuals for the Fail-Safe Modules
- Automation System S7-300
  ET 200M
  Distributed I/O Device
  Fail-safe signal modules
  Installation and Operating Manual
- Distributed I/O System Fail-Safe Engineering
  ET 200S
  Distributed I/O System
  Fail-Safe Modules
  Installation and Operating Manual
- ET 200eco
  Distributed I/O Station
  Fail-Safe I/O Module
  Manual
- Distributed I/O fail-safe engineering
  ET 200pro
  Distributed I/O System – Fail-Safe Modules
- Distributed I/O
  ET 200iSP
  Distributed I/O Device – Fail-safe Modules

3 Certification Requirements

3.1 Basis of Certification

The certification of SIMATIC S7 Distributed Safety will be according to the regulation and harmonized standards listed in clause 3.3 of this document. This will certify the successful completion of the following test segments:

I. Functional Safety

   A. Safe failure fraction (reached due to coded processing) analysis related to the hardware of the components as described in the manuals (see chapter 2.4) also used for defining input values used by the probability of failure on demand calculation.

   B. Software analysis for the safety-related software components.

   C. Descriptive safety as given by the safety sections of the user documentation, indicated in section 2.4 of this report.

II. Basic Safety including electrical safety according to EN 61131-2

III. Environmental Stress Testing

   A. Climatic and temperature stress

   B. Mechanical stress

IV. Electromagnetic Compatibility

   A. Electromagnetic susceptibility

   B. Electromagnetic emission

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

Certification is dependent on successful completion of all of the above test segments.

3.2 Certification Documentation

Documentation of this certification is based on the following reports:

- Testing documentation

  The Technical Reports SN87345T and SN87148T summarize 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 the SIMATIC S7 Distributed 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 17 05 67803 015

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]
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	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 S7 Distributed Safety Safety-Related Programmable System in conjunction with its 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 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.

4.1.1 Safety of machinery

The text of ISO13849-1:2006 has been taken over as EN ISO 13849-1:2008 without any modification and supersedes EN ISO 13849-1:2006. Only the informative Annex ZB in regard to the essential requirements of the MD-Directive was added. Therefore no further testing activities are necessary.

Our assessment activities regarding EN ISO 13849-1:2015 are summarized in the Technical Report SN88739T.

4.1.2 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-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 process safety time of the process controlled by the SIMATIC S7 Distributed Safety shall be greater than the worst-case response time. Additional information is given into the manual 'Safety Engineering in SIMATIC S7'.

4.1.3 Application Development

The SIMATIC S7 Distributed Safety can treat and execute programmed safety-related functions. An intended safety function of the SIMATIC S7 Distributed Safety 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 and the component specific information detailed in the current revision of the Annexes of the Report to the Certificate Z10 17 05 67803 015.

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.

4.1.4 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 centre responsible for approval of the system's application.

The procedure for on-line modifications and existing restrictions are described in the Manuals: 'S7 Distributed 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 Basic Safety

The tests of the electrical safety and the environmental stress tests are executed by the accredited laboratory of Siemens AG.

For details refer to Report to the Certificate Z10 17 05 67803 015.

4.2.2 Electromagnetic Compatibility

The documentation of the electromagnetic compatibility tests are executed by the accredited laboratory of Siemens AG.

For details refer to Report to the Certificate Z10 17 05 67803 015.

5 Implementation Conditions and Restrictions

The use of the SIMATIC S7 Distributed Safety shall comply with the current version of the Safety parts of the manuals (see chapter 2.4) and the following implementation and installation requirements have to be followed if the SIMATIC S7 Distributed Safety system is used in safety-related installations.

The SIMATIC S7 Distributed Safety is a safety-related product 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

5.1.1. Only components certified for safety-related operation, as shown in the Annexes of the Report to the Certificate Z10 17 05 67803 015 shall be used for safety-critical signals. Not certified standard components (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 shutdown 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.

5.2 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 components 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 components 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 S7 Distributed Safety 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.

5.4 Specific application conditions

For specific application conditions refer to the Report to the Certificate Z10 17 05 67803 015.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of the Safety-Related Programmable System SIMATIC S7 Distributed Safety by Siemens AG to the certificate:

M6A 17 05 67803 014

Munich, 2019-02-13

Digital unterschrieben von Christian Dirmeier
Datum: 2019.02.13 15:24:54 +01'00'

Christian Dirmeier

Technical Certifier