TÜV SÜDDEUTSCHLAND

Report

to the

Certificate

Z2 03 04 38282 002

Safety-Related Programmable Systems

SIMATIC S7 F/FH Systems

(formerly S7-400F and S7-400FH)

Manufacturer:

Siemens AG
Werner-von-Siemens Str. 50
D-92224 Amberg

Report No.: 10042360
Revision 1.6 dated 30. June 2005

Testing Body:
TÜV Automotive GmbH
TÜV Süddeutschland Group
Automation, Software and Electronics - IQSE

Certification Body:
TÜV Product Service GmbH
TÜV Süddeutschland Group
Ridlerstraße 65
D-80339 München

Revision Log

Version	Name	Date	Changes/History
1.0	R. Faller	30.11.1999	Initial
1.1	P. Müller	18.12.2000	LS 2
1.3	P. Müller	15.11.2001	Section 5.4 added and modified
1.4	A. Beer M.Weber	23.04.2003	Product name Definition of terms; 1oo1D and 1oo2D added Section 2.2 General application condition added New software version V5.2 added Restriction 5.4.1 modified
1.5	A. Beer M.Weber	03.06.2004	Make reference to “Annexes” (instead a particular annex) when the annex refers to a software component revision information.
1.6	F. Rauch	30.06.2005	SP2: The standards EN 54-2:1997, EN 54-4:1997, NFPA72:2002 and NFPA 85:2004 were included and EN 298 was updated to 2003 in section 3.7.

TÜV SÜDDEUTSCHLAND

Content Page

1 Purpose and Scope

TÜV Automotive GmbH has been contracted by Siemens AG to certify the Safety-Related Programmable Systems SIMATIC S7 F/FH Systems.

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.

1.1 Definition of Terms

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

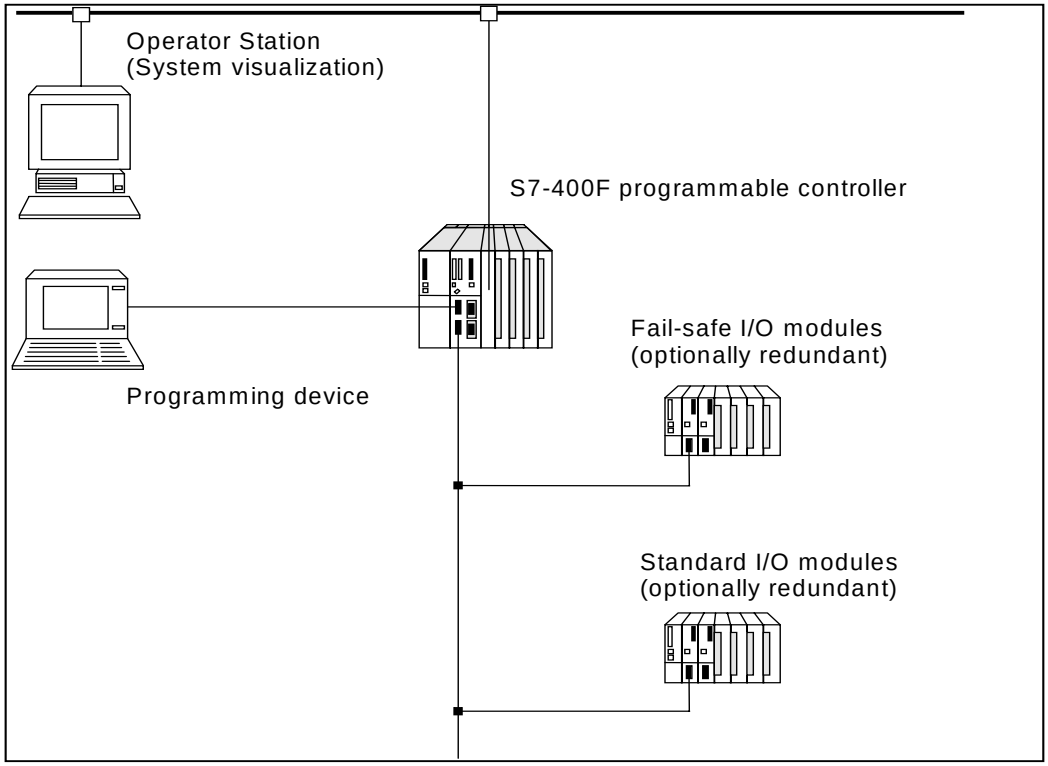
Functional Safety	The ability of a safety-related system to carry out the actions necessary to achieve a (defined) safe state for the equipment under control (EUC) or to maintain the safe state for the EUC.
CFC	Continuous Function Chart
Degraded operation	Denotes the system operating mode when a fault has been detected and localized in one of the critical components.
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	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)	Average probability of failure of a system to perform its design functions on demand.
Proven-in-use Proven-by-operation Field tested	A sufficient number of installations in various application fields with available fault history of the installed systems did not show the presence of a safety-related systematic error

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.

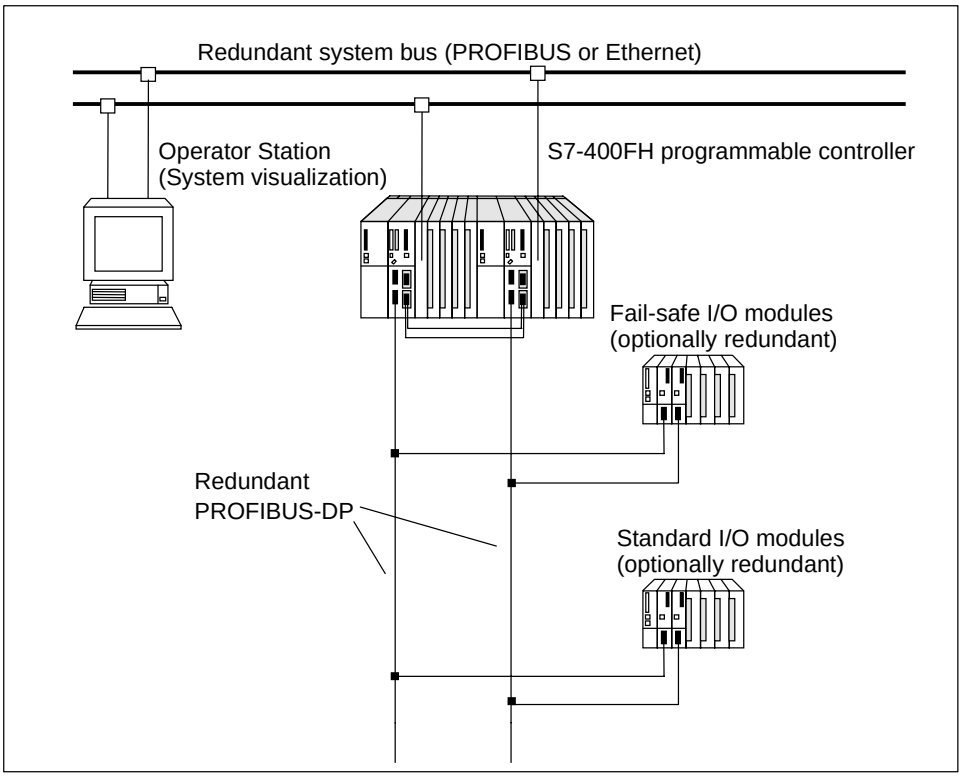
2 System Overview

2.1 System Architecture

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



System Architecture for S7 F



System Architecture for S7 FH

The 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-SM or 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 a 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.

The following failure control measures are implemented in the CPU:

- redundant execution with data and code redundancy and 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 are used in 2oo2 of 1oo1D configuration to increase availability. The second channel of the I/O module implements an independent comparison and diagnostic entity and allows the D designator for the 1oo1 hardware CPU architecture.

The F-I/O modules are in an internal 1oo2 structure (two channels with comparison). One F-I/O module is sufficient to achieve the certified functional safety. Optional two redundant F-I/O modules are used in 2oo2 of 1oo2 configuration to increase availability.

2.2 Hardware Components under Certification

The system components which are certified 'safety-related' are listed in the current revision of the Annex 1 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' ('rückwirkungsfrei') 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 of the SIMATIC S7 F/FH Systems documentation package.

2.3 Software Components under Certification

A list of the software components with the valid version numbers is shown in the current revision of the applicable 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:

- Add-on option package S7 F Systems
- F-FBs
- Firmware of the Failsafe I/O modules

For the specific versions see the current 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 non certified components on 'safety-related' components is enforced due to the intrinsic safety features provided by the diverse logic implementation followed by the 1oo2 F-I/O modules.

2.3.3 Communication

Safety-related communication between F-CPUs and F-I/O is based on the Profibus DP/PA protocol but implements an additional safety shell on top (ProfiSafe).
Safety-related communication between F-CPUs is based on a standard protocol like MPI, Profibus or Ethernet but implements an additional safety shell on top.

2.3.4 Programming environment

Safety application programming is performed by connection of function blocks using the Step7 CFC language. Only special certified function blocks shall be used for safety applications. Use of standard function blocks for safety applications is prevented by their own safety data types. Edit, compile and load use the standard STEP7 programming environment of the S7-400 and S7-300 family. An add-on option package S7 F Systems provides the following properties required to improve 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 program in the F-CPU
- Add-on option package S7 F Systems checks

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:

- Programmable Controllers, S7 F/FH Systems
- ET 200S Distributed I/O System, Fail-Safe Modules
- Automation System S7-300, Fail-Safe Signal Modules

3 Certification Requirements

3.1 Basis of Certification

The certification of the controller will be according to the regulations and standards listed in clause 3.3 to 3.6 of this document. This will certify the successful completion of the following test segments:

I. Functional Safety

   A. Fault investigations for the hardware components listed in the current revision of the Annex 1 to this report and of the system configurations as described in the manuals of the SIMATIC S7 F/FH Systems and S7 Distributed Safety documentation packages.

   B. Software analysis for the software components listed in the current revision of the Annexes to this report

   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- 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. The testing follows the basic certification scheme for safety-related programmable electronic systems of TÜV Product Service GmbH.

3.2 Certification Documentation

Documentation of this certification is based in the following reports:

- Technical Report
  Report No.: SA58199
  Report No.: SA60720
  Report No.: T-10042360-01
  Report No.: SA66281

- EMC Test Report
  Report No.: 10.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 11.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 12.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 25.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 21.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 22.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 33.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 38.00 prepared by Siemens and reviewed by TÜV PS IQSE

- Environmental Test Report
  Report No.: 10.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 11.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 12.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 25.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 21.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 22.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 33.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 38.00 prepared by Siemens and reviewed by TÜV PS IQSE

- Test Report on IEC 1131-2
  Report No.: 10.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 11.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 12.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 25.99 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 21.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 22.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 33.00 prepared by Siemens and reviewed by TÜV PS IQSE
  Report No.: 38.00 prepared by Siemens and reviewed by TÜV PS IQSE

- Calculation of Probability of Failure on Demand:
  Internal Report of the "Probability-of-Failure-on-Demand" of S7-F Safety-Programmable-System, Rev. 4.1 from 12. December 2000

- Manuals: " Programmable Controllers, S7 F/FH Systems" and "S7-300 Programmable Controller, Fail-Safe Signal Modules"

Based on the specified purpose of use of the SIMATIC S7 F/FH Systems in safety critical process protection applications the certification is based on the following set of standards. The issu-

ance of the certificate states compliance with these references unless specifically noted otherwise.

3.3 European Directives

The fulfillment of the essential requirements of the following European Directives is mandatory for an electronic device such as the SIMATIC S7 F/FH Systems.

73/23/EEC 93/68/EEC	Council Directive of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits.
98/37/EEC	Council Directive of 22 June 1998 on the approximation of the laws of the Member States relating to machinery (to the extend applicable to programmable electronic safety devices)

3.4 Functional Safety

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

DIN V 19250: 1994, AK6	Fundamental aspects to be considered for measurement and control equipment
DIN V VDE 0801: 1990, AK1-6, including amendment A1: 1994	Principles for computers in safety-related systems
IEC 61508-1: 12/1998 IEC 61508-2: 05/2000 IEC 61508-3: 12/1998 IEC 61508-4: 11/1998 IEC 61508-5: 11/1998 IEC 61508-6: 04/2000 IEC 61508-7: 03/2000 SIL1-3 (as applicable to PES)	Functional safety; Safety-related systems
prEN 50159-1:1996 (as applicable)	Railway Applications; Safety-Related Communication In Closed Transmission Systems (as applicable)
prEN 50159-2:1996 class 1 to 5 (as applicable)	Railway Applications; Safety-Related Communication In Open Transmission Systems (as applicable)

3.5 Basic 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:

EN 61131-2: 1995	Programmable controllers - equipment requirements and tests
EN 50178: 1997	Electronic equipment for use in power installations
DIN VDE 0110: 1989	Insulation co-ordination for equipment within low-voltages systems
EN 60068	Environmental Testing
QSH IQSE Version 1.4	Quality Manual of TÜV Product Service IQSE

3.6 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: 1995	Programmable controllers - equipment requirements and tests
EN 55011: 1997	Limits and methods of measurement of radio disturbance characteristics of industrial, scientific and medical (ISM) radio-frequency equipment.
EN 50081-2: 1993	Electromagnetic compatibility (EMC); Generic emission standard Part 2: Industrial environment
EN 50082-2: 1995	Electromagnetic compatibility (EMC); Generic immunity standard - Part 2: Industrial environment

3.7 Application Standards

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

Machinery Applications	
EN 60204-1: 1997 (as applicable) prEN 60204-1/ prA1: 1998	Safety of machinery - Electrical equipment of machines
EN 954-1: 1997 categories 2 to 4	Safety of machinery; Safety-related parts of control systems Part 1 "General principles for design"
Process Industry	
DIN V 19251: 1995	Process control technology- MC protection equipment- Requirements and measures for safeguarded function
VDI / VDE 2180: 1996 part 1, 2 and 5	Safeguarding of industrial processing plants by means of instrumentation and control technology
NE 31: 1993	NAMUR Recommendation
ANSI - ISA S84.01: 1996 (as applicable)	Application of safety instrumented system for the Process Industry
Burner Systems	
EN 230: 1991 clause 7.3	Monobloc oil burners
EN 298: 2003 (clause 7.3, 8, 9 and 10)	Automatic gas burner control systems for gas burners and gas burning appliances with or without fans
ENV 1954: 1996 (as applicable)	Internal and external fault behavior of safety-related electronic parts of gas appliances
DIN VDE 0116: 1989 clause 8.7	Electrical equipment of furnaces
prEN 50156-1: 1997 (as applicable)	Electrical equipment of furnaces

NFPA 85:2004	Boiler and Combustion Systems Hazards Code
Fire Detection and Fire Alarm Systems	
EN 54-2:1997	Fire detection and fire alarm systems - Part 2: Control and indicating equipment
EN 54-4:1997	Fire detection and fire alarm systems - Part 4: Power supply equipment
NFPA 72: 2002	National Fire Alarm Code

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the SIMATIC S7 F/FH Systems 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 are suitable for safety-related use in applications of requirement classes AK 1 to 6 in accordance with DIN V 19250:1994, categories 2 to 4 in accordance with EN 954, and safety integrity levels SIL 1 to 3 in accordance with IEC 61508, 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 F-I/O input modules are detected by the F-CPU. Either ‘0’ or configured substitute values are handed to the application program. A specific fault reaction must be implemented by the application program developer.
2. Faults in the cyclic communication between the F-CPU and the F-I/O output modules are detected by the F-DO. If a fault occurs all outputs of the affected F-I/O are driven to ‘0’.
3. Faults in the cyclic communication between two F-CPUs 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. A specific fault reaction must be implemented by the application program developer.
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 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 F-I/O:

Faults detected by built-in self-test or diagnostics are either safely 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 and 7FFFH with analog 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 S7 F/FH Systems shall be greater than the worst case response time, determined with the help of the Excel-Sheet S7ftime?.xls (? is a letter for language coding)

The results of the concept and the technical requirements analysis of the Profibus based communication safety shell (Profisafe) are subject of the Evaluation Report PK55299T, revision 1.0 of 30. March 1999.

4.1.2 Application Development

The 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 the SIMATIC S7 F/FH Systems 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.

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 S7 F/FH Systems.

4.1.3 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 of the SIMATIC S7 F/FH Systems and S7 Distributed Safety documentation packages.

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

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

4.1.4 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

The tests of the electrical safety and the environmental stress tests executed by TÜV Product Service show that the standards specified in clause 3 are covered.

The tests performed and the quality assurance measures implemented by the manufacturer have shown that the 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.

4.2.2 Electromagnetic Compatibility

The documentation of the electromagnetic compatibility tests executed by independent test laboratories has been reviewed for completeness. The testing executed has covered the requirements of the standards specified in clause 3.

4.3 Product Specific Quality Assurance and Control

All 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. Some older components have been developed under the manufacturer's internal quality procedures.

The European procedures for demonstrating conformity (93/465/EEC "Council Resolution of 22 July 1993 on the modules to be used in the technical harmonization directives for the various phases of conformity assessment procedures and the rules for attaching and using CE conformity marks") provide similar significance to the type testing and the manufacturer's quality assurance in production and product maintenance. 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 identifiably (follow-up service).

5 Implementation Conditions and Restrictions

The use of the SIMATIC S7 F/FH Systems shall comply with the current version of the Safety parts of the manuals of the SIMATIC S7 F/FH Systems and S7 Distributed Safety documentation packages., and the following implementation and installation requirements have to be followed if the SIMATIC S7 F/FH Systems are used in safety-related installations.

5.1 General application conditions

5.1.1. The guidelines specified in the user's manuals shall be followed. Specifically the safety notes in the user's manuals shall be followed.

5.1.2. Only hardware modules certified for safety-related operation, as shown in Annex 1 of this report shall be used for safety-critical signals. Not certified standard modules (defined as "interference-free") may be used for non-safety-critical signals only.

5.1.3. Only software modules listed in Annexes of this report shall be used to process safety critical data.

5.1.4. The fault tolerance period of the process controlled by the system shall be greater than the worst-case reaction time of the system, determined with the help of the Excel-Sheet s7ftime?.xls (? is a letter for language coding).

5.1.5. A well defined shutdown procedure shall be specified.

5.1.6. 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.

5.1.7. 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.

5.1.8. 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 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, including fault detection time, fault reaction time, throughput delay for shutdown logic and cycle time.

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 F-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 modules 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 modules should be replaced within the multiple fault occurrence time.

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. TUV certification does not cover output override.

5.3.8. The use of F-Function Blocks for SIMATIC S7 F/FH Systems F/FH is only permitted if for the specific target system (F or FH system) an official F-Copy License with the order number 6ES7 833 1CC00 6YX0 is available.
The F-Copy License consists of:
- the F-Copy License contract
- the copy of the TUV-Certificate
- two labels to mark up the CPU (or CPU´s on a FH system) of the used F-Copy License

5.4 Product-Related conditions

5.4.1. The Safety Protector allows use of failsafe-modules in combination with standard-modules. 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.

TÜV SÜDDEUTSCHLAND

6 Certificate Number

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

Z2 03 04 38282 002

Munich, 30. June 2005

TÜV Automotive GmbH
TÜV SÜD Group
Automation, Software and Electronics - IQSE
(Technical Certifier)

J. Blum