

**Assessment Report about the conformity
according to IEC 61508 of the
FSC Fail-Safe Controller System Family**

Manufacturer:

Honeywell Safety Management Systems
Rietveldenweg 32
NL-5222 AR 's-Hertogenbosch
Netherlands

Report No.: HH80661T
Revision 1.0 of 13. May 2003

Testing and Certification Center
TÜV AUTOMOTIVE GMBH
Automation, Software and Electronics - IQSE
Ridlerstraße 65
80339 München

This Report to the Certificate may not be duplicated **other than in its entirety** without the prior written consent of the TÜV AUTOMOTIVE GMBH, IQSE.

Contents	Page
1 Objective of the assessment	3
2 Functional safety management	3
2.1 Life cycle	3
2.2 Change Management	4
2.3 Objectives Management of Functional Safety	6
2.4 Documentation	6
2.4.1 Objectives Documentation - Part 1	7
2.4.2 System documentation	8
2.4.3 Hardware documentation	10
2.4.4 Software documentation	11
3 Objectives IEC 61508	13
3.1 Part 1 General Requirements	13
3.2 Part 2 Hardware requirements	18
3.3 Part 3 Software requirements	20
4 Overall Results	24

1 Objective of the assessment

The FSC Fail-Safe Controller System Family has been certified by TÜV PRODUCT SERVICE / AUTOMOTIVE IQSE (following named TÜV PS/TA IQSE) according to DIN V VDE 0801 and other applicable standards (see report to the certificate SH99495C). The objective of this paper is to show how the DIN V VDE 0801 compliant system can be related with Safety Integrity Level 3 according to IEC 61508:2000, Part 1 to 4 and to show that additional measures introduced are suitable to give conformity with the objectives of IEC 61508. It needs to be stated that the development of new modules and/or components is carried out according to IEC 61508 and is not part of the assessment described in this document.

The general additional requirements for existing certified (DIN V VDE 0801) safety related systems are:

- preparation of a functional safety management
- composition of documentation corresponding to SIL3
- evidence of proven in use for Hardware and Software
- probabilistic calculation according to the requirements of SIL3

2 Functional safety management

2.1 Life cycle

Status: The V-model life cycle approach, defined by TÜV PS/TA IQSE for their functional safety certification since 1990 (see Figure 1), is very similar to the approach specified by IEC 61508 today. The scope of the TÜV PS/TA IQSE safety certification goes far beyond the scope defined by IEC 61508. The TÜV PS/TA IQSE safety certification includes in addition all basic safety aspects and EMC as required by the European Directives on Low Voltage Appliances and EMC.

TÜV PS/TA IQSE has not, explicitly, carried out functional safety management audits. The skill of the vendor's design and test engineers has been demonstrated - and if needed increased - during the project and the skill of the TÜV PS/TA IQSE test engineers is recorded. The EN 45011 approach of independence and peer-to-peer review of test and analysis team versus technical certifier replaced the functional safety assessment.

Conclusion: For certified devices / systems where the development or the certification followed the TÜV PS/TA IQSE life-cycle approach nothing has to be improved in order to comply with the requirements of IEC 61508.

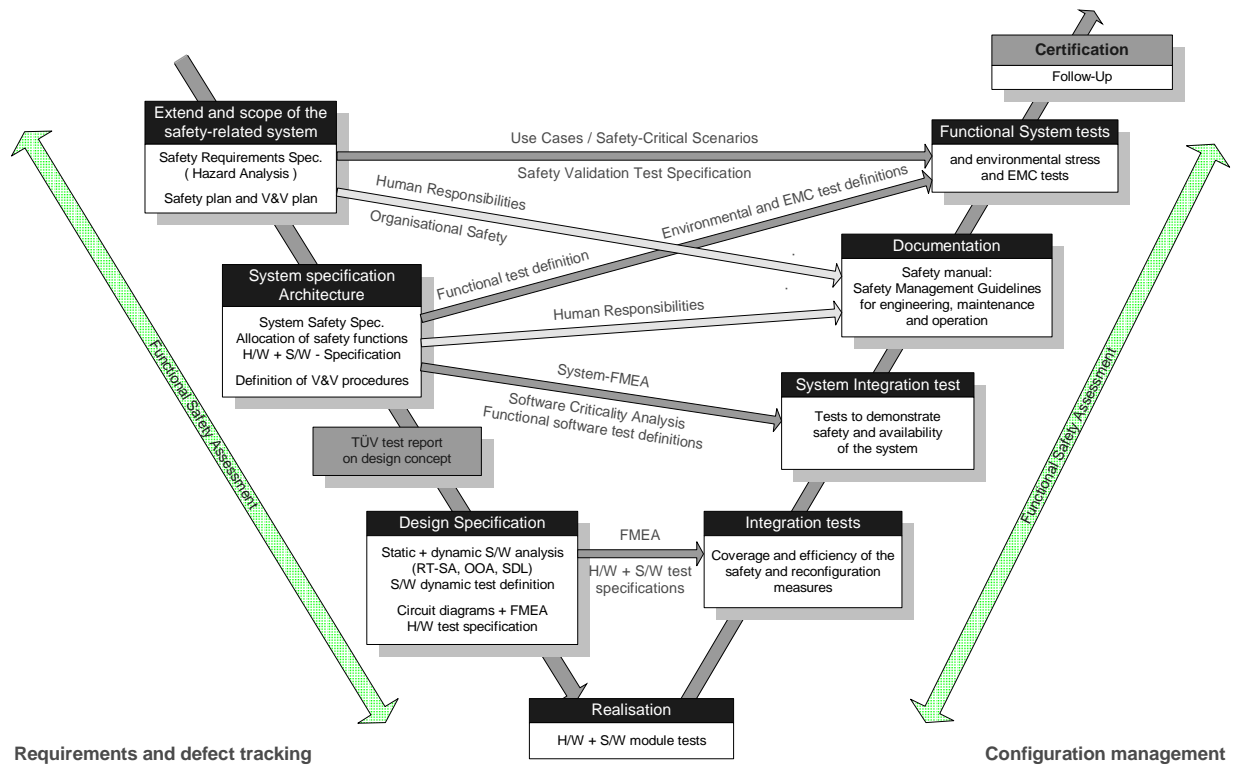


Figure 1. V&V model

2.2 Change Management

Status: The modification process recommended by TÜV PS/TA IQSE since 1996 (see Figure 2) is very similar to the process specified by IEC 61508.

The follow-up procedure of TÜV PS/TA IQSE goes beyond the scope of IEC 61508. It includes in addition electrical safety aspects as defined by the Harmonisation Documents (HD) of CENELEC and auditing of the field reporting procedures at the vendor.

Conclusion: For the FSC Fail-Safe Controller System Family the change management is implemented as shown in Figure 2 and is in accordance with IEC 61508.

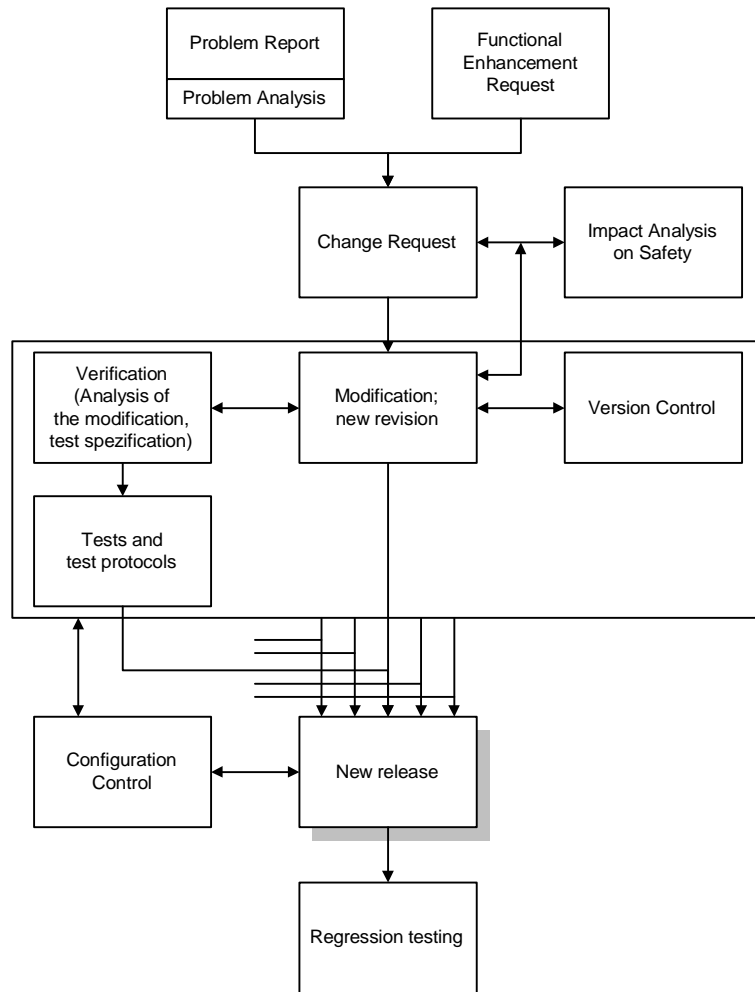


Figure 2. change process

2.3 Objectives Management of Functional Safety

Table 1. Objective Management of Functional Safety Part 1

Par.	Objective	Judgement
6.1.1	The first objective of the requirements of this clause is to specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.	The existing Functional Safety Management System complies with the criteria specified in IEC 61508. The results of the examination are presented in the assessment report "Functional Safety Management Certificate" dated 20. May 1999
6.1.2	The second objective of the requirements of this clause is to specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.	The existing Functional Safety Management System complies with the criteria specified in IEC 61508. The results of the examination are presented in the assessment report "Functional Safety Management Certificate" dated 20. May 1999

2.4 Documentation

Status: The documentation requirements of IEC 61508 go beyond the requirements specified by DIN V VDE 0801 and TÜV PS/TA IQSE. The documentation requirements of IEC 61508 versus DIN V VDE 0801 correspond as follows.

Conclusion: The safety-related system and hardware documentation of a DIN V VDE 0801 certified system should be in line with or close to the documentation requirements of IEC 61508-1 and -2.

The safety-related software documentation of a DIN V VDE 0801 certified system might need further investigation. This is addressed in the tables of paragraph 2.4.2, 2.4.3 and 2.4.4.

2.4.1 Objectives Documentation - Part 1

Par.	Objective	Judgement
5.1.1	The first objective of the requirements of this clause is to specify the necessary information to be documented in order that all phases of the overall E/E/PES and software safety lifecycles can be effectively performed.	This objective is addressed by the tables in paragraphs 2.4.2, 2.4.3, and 2.4.4 that will give an overview of how the documentation requirements of IEC 65108 are addressed.
5.2.1	The second objective of the requirements of this clause is to specify the necessary information to be documented in order that the management of functional safety (see clause 6) verification (see 7.18) and the functional safety assessment (see clause 8) activities can be effectively performed.	This objective is met because all documents are written using the QA procedures [ISO 900x, Quality Handbook].

2.4.2 System documentation

IEC 61508-1	Level	DIN V VDE 0801 and TÜV PS/TA IQSE	Judgement
Hazard and risk analysis	EUC ¹	Not applicable. AK6 is defined for the safety system according to DIN V VDE 0801. The safety system is classified for SIL 3 according to IEC 61508. This is a customer requirement to have the system SIL 3 certified	OK
Safety requirements	EUC	Not applicable on EUC level. Identification of safety functions and safety integrity. The customer has this information in the form of marketing requirements. They define their market and therefore they know what kind of system they need to build. This is part of the Safety Requirement Specification.	OK
Safety requirements allocation	E/E/PE safety-related systems; other technology safety-related systems; external risk reduction facilities.	Not applicable. On EUC level. The above identified safety functions and safety integrities are allocated on EUC level to E/E/PE safety related systems, other technology safety-related system, or external risk reduction facilities. The safety system is designed to control up to SIL 3 safety functions utilising different engineering solutions.	OK
Operation and maintenance plan and procedures	System	Addressed by the 'Safety Manual' which is shipped with the product to the user.	OK
Installation and commissioning plan and procedures	System	To the extend applicable, addressed by the 'Safety Manual'.	OK

¹ EUC = equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities [IEC61508]

IEC 61508-1	Level	DIN V VDE 0801 and TÜV PS/TA IQSE	Judgement
Safety validation	System	To the extend applicable, addressed by the 'Safety Manual'.	OK
E/E/PE design documents	Hardware, Software	See tables below	See tables below
Hardware / software integration test	Hardware, Software	See tables below	See tables below
E/E/PES integration test	System Hardware, Software	This is on E/E/PES level, i.e., sensors, logic solver, and valves together (see "Safety Manual").	OK
Verification documents	System Hardware, Software	As applicable this is available. Verification activities need to be carried out after each phase of the safety lifecycle. Many phases are on plant level and do not apply directly to the safety system development. The safety system development follows the V&V plan which inherently has verification. See tables below for documentation.	OK
E/E/PES functional safety assessment	System Hardware, Software	As applicable this is available. Safety assessment activities need to be carried out for the complete safety system including sensors and valves. In this case on the logic solver of the safety system has been assessed by TÜV PS/TA IQSE. See tables below for documentation.	OK

Conclusion: The system level documentation for TÜV PS/TA IQSE certification following DIN V VDE 0801 A1 also fulfil the requirements of IEC 61508-1.

2.4.3 Hardware documentation

IEC 61508-2	Level	DIN V VDE 0801 and TÜV PS/TA IQSE	Judgement
Safety requirements	(Sub)System	A Safety Requirements Specification is available which results eventually to detailed hardware requirements.	OK
Hardware design documents	Hardware	Available documents are block diagrams, parts lists, circuit diagrams, printed boards, assembly drawings, inspection provision.	OK
E/E/PES integration test	(Sub)System Hardware, Software	This documentation is available.	OK
E/E/PES safety validation	(Sub)System Hardware, Software	This is reflected in the work task (project plan) as offered by TÜV PS/TA IQSE quotation.	OK
E/E/PES Installation, commissioning, operation and maintenance	(Sub)System Hardware, Software	Addressed by the 'Safety Manual' which is shipped with the product to the user.	OK
Verification documents	(Sub)System Hardware, Software	Following documents are available: System-FMEA, H/W-FMEA, FIT, Probabilistic and Reliability calculations	OK

Conclusion: The Hardware documentation for a TÜV PS/TA IQSE certification following DIN V VDE 0801 A1 fulfils the requirements of IEC 61508-2.

2.4.4 Software documentation

IEC 61508-3	Level	DIN V VDE 0801 and TÜV PS/TA IQSE	Judgement
Software safety requirements spec.	Software system	Honeywell Safety Management Systems has besides an SRS several other detailed software specification available which can be judge to be safety related as all activities have the target to create a safety system.	OK
Software safety validation	Software system	This is reflected in the work task (project plan) as offered by TÜV PS/TA IQSE quotation.	OK
Software design and development	Architecture	Documentation of Software Architecture is available.	OK
	Software architecture integration test	Available for the new developed software parts. The old software is addressed by functional and black box testing and the evidence of proven in use.	OK
	Selection of support tools and programming languages Coding standards	The programming tools are proven in use and the development team is familiar with the tools and programming language. Coding standards were used, verification was carried out in the certification process.	OK
	Detailed software system design	Documentation of Software System Design is available.	OK
	Software system integration test	Available for the new developed software parts. The old software is addressed by functional testing and the evidence of proven in use.	OK

	Module design	Available in several documents related to the different functions.	OK
	Detailed code implementation Code review	Source code of the FSC-Software is available. The source code of the system software was verified by code inspection. Reviews of all software changes was carried out.	OK
	Module test	Tests were traced to the module design and the test coverage was judged to be sufficient.	OK
PE Hardware / Software integration test	Hardware, Software	Test specifications are available (TÜV S/W analysis and FMEA documents).	OK

Conclusion: TÜV PS/TA IQSE considers the documentation to be sufficient because the connection between the proven in use of the old modules and the new developed modules (according to IEC 61508) represents the objectives of IEC 61508 to achieve safe operating software.

3 Objectives IEC 61508

The following table gives an overview of the objectives of the different lifecycles and follows the structure of the IEC 61508 standard. Figure 2 box number refers to the figure of the lifecycle in IEC 61508. One important column to keep in mind is the scope, which describes where this phase of the lifecycle applies.

3.1 Part 1 General Requirements

Table 2. Objectives part 1

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 2 box number	Title			
1	Concept	To develop a level of understanding of the EUC and its environment (physical, legislative etc) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	EUC and its environment (physical, legislative etc).	To the extend applicable this is addressed in the Safety Manual.
2	Overall scope definition	To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc).	EUC and its environment.	Not applicable. Not applicable.

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 2 box number	Title			
3	Hazard and risk analysis	<p>To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse;</p> <p>To determine the event sequences leading to the hazardous events determined;</p> <p>To determine the EUC risks associated with the hazardous events determined.</p>	<p>The scope will be dependent upon the phase reached in the overall, E/E/PES and software safety lifecycles (since it may be necessary for more than one hazard and risk analysis to be carried out). For the preliminary hazard and risk analysis, the scope will comprise the EUC, the EUC control system and human factors.</p>	<p>To the extend applicable this is addressed in the Safety Manual.</p>
4	Overall safety requirements	<p>To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.</p>	<p>EUC, the EUC control system and human factors.</p>	<p>To the extend applicable this is addressed in the Safety Manual.</p>

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 2 box number	Title			
5	Safety requirements allocation	<p>To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities;</p> <p>To allocate a safety integrity level to each safety function.</p>	EUC, the EUC control system and human factors.	To the extend applicable addressed in the Safety Manual.
6	Overall operation and maintenance planning	To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	To the extend applicable addressed in the Safety Manual.
7	Overall safety validation planning	To develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	To the extend applicable addressed in the Safety Manual.
8	Overall installation and commissioning planning	<p>To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved;</p> <p>To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.</p>	EUC and the EUC control system; E/E/PE safety-related systems.	<p>To the extend applicable addressed in the Safety Manual.</p> <p>To the extend applicable addressed in the Safety Manual.</p>

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 2 box number	Title			
9	E/E/PE safety-related systems: realisation	To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).	E/E/PE safety-related systems	See table for part 2 and 3.
10	Other technology safety-related systems: realisation	To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other technology safety-related systems.	Not applicable.
11	External risk reduction facilities: realisation	To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities (outside the scope of this standard).	External risk reduction facilities.	Not applicable.
12	Overall installation and commissioning	To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems.	EUC and the EUC control system; E/E/PE safety-related systems.	To the extent applicable as addressed in the safety manual.

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 2 box number	Title			
13	Overall safety validation	To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.	EUC and the EUC control system; E/E/PE safety-related systems.	To the extend applicable as addressed in the safety manual.
14	Overall operation, maintenance and repair	To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.	EUC and the EUC control system; E/E/PE safety-related systems.	To the extend applicable as addressed in the safety manual.
15	Overall modification and retrofit	To ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.	EUC and the EUC control system; E/E/PE safety-related systems.	To the extend applicable as addressed in the safety manual.
16	Decommissioning or disposal	To ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.	EUC and the EUC control system; E/E/PE safety-related systems.	Not applicable. Should be addressed by the plant owner and might depend on local legal requirements.

3.2 Part 2 Hardware requirements

Safety lifecycle phase or activity		Objectives	Scope	Judgement
Figure 2 box number	Title			
9.1	E/E/PES safety requirements specification	To specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.	E/E/PE safety-related systems	Is addressed in the SRS.
9.2	E/E/PES Safety validation planning	To plan the validation of the safety of the E/E/PE safety-related systems	E/E/PE safety-related systems	Is addressed by the certification process specified by TÜV PS/TA IQSE
9.3	E/E/PES design and development	To design the E/E/PE safety-related systems to meet the requirements for safety functions and safety integrity.	E/E/PE safety-related systems	Is addressed by the design documents and the assessment of TÜV PS/TA IQSE.
9.4	E/E/PES integration	To integrate and test the E/E/PE safety-related systems.	E/E/PE safety-related systems	Is addressed by the integration test documents and the assessment of TÜV PS/TA IQSE.
9.5	E/E/PES operation and maintenance procedures	To develop procedures to ensure that the functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.	E/E/PE safety-related systems; EUC	Is addressed by the safety manual.
9.6	E/E/PES safety validation	To validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the required safety integrity.	E/E/PE safety-related systems	Is addressed by the certification process of TÜV PS/TA IQSE.
-	E/E/PES modification	To make corrections, enhancements or adaptations to the E/E/PE safety-related systems, ensuring that the required safety	E/E/PE safety-related systems	Is addressed by the safety manual. Any changes are reported to TÜV PS/TA IQSE

Safety lifecycle phase or activity		Objectives	Scope	Judgement
Figure 2 box number	Title			
		integrity level is achieved and maintained.		and leads to an update of the related certification documents that after successful completion leads to a new approval of the safety system.
-	E/E/PES verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.	E/E/PE safety-related systems	This is addressed by the V&V model and the certification process ² .
-	E/E/PES functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems.	E/E/PE safety-related systems	This is addressed by the certification process of TÜV PS/TA IQSE. Results see "Assessment Report to support the Functional Safety Management Certificate", dated 20.May 1999

² In addition to DIV V VDE 0801 a probabilistic calculation was carried out according to IEC 61508 for the complete System by TÜV PS/TA IQSE. The results are documented in "AUDIT REPORT, Honeywell SMS – SIL / reliability calculations", dated 13.June 2001

3.3 Part 3 Software requirements

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 3 box number	Title			
9.1	Software safety requirements specification	To specify the requirements for software safety in terms of (1) the requirements for software safety functions and (2) the requirements for software safety integrity; To specify the requirements for the software safety functions for each E/E/PE safety-related system necessary to implement the required safety functions; To specify the requirements for software safety integrity for each E/E/PE safety-related system necessary to achieve the safety integrity level specified for each safety function allocated to that E/E/PE safety-related system.	PES; Software system.	Is addressed by the SRS and other specification documents.
9.2	Software safety validation planning	To develop a plan for validating the software safety.	PES; Software system.	This is addressed by the certification process of TÜV PS/TA IQSE and controlled by the requirement management tool "Requisite Pro" by Honeywell SMS
9.3	Software design and development	Architecture: To create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level; To review and evaluate the requirements placed on the software by the hardware architecture of the E/E/PE safety-related system, including the significance of E/E/PE hardware/software interactions for safety of the equipment under control.	PES; Software system.	This is addressed by the high level software design

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 3 box number	Title			
9.3	Software design and development	Support tools and programming languages: To select a suitable set of tools, including languages and compilers, for the required safety integrity level, over the whole safety lifecycle of the software which assists verification, validation, assessment and modification.	PES; Software system; Support tools; Programming language.	This is addressed by the use of Assembler Language (structured programming) and tools that are well known and selected based on the experience of the users at Honeywell Safety Management Systems.
9.3	Software design and development	Detailed design and development (software system design): To design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analysable and verifiable, and which is capable of being safely modified.	Major components and subsystems of software architectural design.	This is addressed by a high level software design description and structured assembler programming in combination with the proven in use demonstration ³ .
9.3	Software design and development	Detailed design and development (individual software module design): To design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analysable and verifiable, and which is capable of being safely modified.	Software system design.	This is addressed by a high level software design description and structured assembler programming in combination with the proven in use demonstration.
9.3	Software design and development	Detailed code implementation: To design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analysable and verifiable, and which is capable of being safely modified.	Individual software modules.	This is addressed by a high level software design description and structured assembler programming in combination with the proven in use demonstration.

³ It is not necessary to fulfil all the requirements of IEC 61508 for proven in use demonstration (52.000 Years of operation; evidence for all software functions) because the safety of software is mainly based on the carried out measures required by IEC 61508.

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 3 box number	Title			
9.3	Software design and development	Software module testing: To verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved – to show that each software module performs its intended function and does not perform unintended functions.	Software modules.	This is addressed by the Verification and Validation tests and carried out for the safety related software functions.
9.3	Software design and development	Software integration testing: To verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved – to show that all software modules, components and subsystems interact correctly to perform their intended function and do not perform unintended functions.	Software architecture; Software system.	This is addressed by the Verification and Validation tests and carried out for the safety related software functions and fulfils the requirements in combination with the proven in use demonstration..
9.4	Programmable electronics integration (hardware and software)	To integrate the software onto the target programmable electronic hardware; To combine the software and hardware in the safety-related programmable electronics to ensure their compatibility and to meet the requirements of the intended safety integrity level.	Programmable electronics hardware; Integrated software.	This is addressed by the Verification and Validation tests (like FIT) and carried out for the safety related software functions.
9.5	Software operation and modification procedures	To provide information and procedures concerning software necessary to ensure that the functional safety of the E/E/PE safety-related system is maintained during operation and modification.	As above.	This is addressed by the safety manual.

Safety lifecycle phase		Objectives	Scope	Judgement
Figure 3 box number	Title			
9.6	Software safety validation	To ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.	As above	This is addressed by the Verification and Validation tests and carried out for the safety related software functions. Traceability is given with the requirement management tool "Requisite Pro" by Honeywell SMS
9.5	Software modification	To make corrections, enhancements or adaptations to the validated software, ensuring that the required software safety integrity level is sustained.	As above	This is addressed by ISO 9000 and the V&V activities by TÜV PS/TA IQSE. Any modification needs to be reported to TÜV PS/TA IQSE and will lead to a re-assessment of the product according to the certification process.
-	Software verification	To the extent required by the safety integrity level, to test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.	Depends on phase	This is addressed by the V&V model and fulfils the requirements in combination with the proven in use demonstration.
-	Software functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems.	All above phases	This is addressed by the certification process of TÜV PS/TA IQSE. Results see "Assessment Report to support the Functional Safety Management Certificate", dated 20.May 1999

4 Overall Results

The assessment has shown, that the FSC Fail-Safe Controller System Family is suitable for Safety Integrity Level 3 according to IEC 61508:2000, Part 1 to 4 under the assumption that the development of new modules and components is carried out in accordance with IEC 61508. The capability of Honeywell to follow this requirement has been approved with this assessment.

Functional Safety management and the corresponding V&V procedures comply with the requirements for IEC 61508.

In connection with existing measures, the probabilistic calculation of the hardware and the evidence of proven in use for the software has shown that the main objectives of the IEC 61508 are fulfilled.

TÜV Automotive GmbH
TÜV Süddeutschland Group
Automation, Software and Electronics – IQSE


Beer