



exida Certification S.A.
2 Ch. de Champ-Poury
CH-1272 Genolier
Switzerland

Tel.: +41 22 364 14 34
email: info@exidaCert.com

Results of the IEC 61508 Functional Safety Assessment

Project:
9203 Solenoid / Alarm Driver

Customer:
PR electronics
Rønde,
Denmark

Contract No.: 0709-02C
Report No.: 0709-02C R007 Assessment
Version V1, Revision R0, April 2010

Peter Müller

Management summary

The Functional Safety Assessment of the PR electronics, performed by *exida* Certification S.A. consisted of the following activities:

- *exida* Certification S.A. assessed the setup of the development process used by PR electronics for development projects against the relevant requirements of IEC 61508 parts 1 to 3.

Subject to this assessment were the Functional Safety Planning activities, the tailoring of the Verification and Validation activities and the realization of the technical safety aspects using the 9203 Solenoid / Alarm Driver development project.

- *exida* Certification S.A. audited the development process by a detailed development audit which investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the PR electronics 9203 Solenoid / Alarm Driver development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* Certification S.A. assessed the Safety Case prepared by PR electronics against the technical requirements of IEC 61508.



The result of the Functional Safety Assessment can be summarized by the following statements:

The audited PR electronics development process tailored and implemented by the 9203 Solenoid / Alarm Driver Software and Hardware development project, complies with the relevant safety management requirements of IEC 61508 SIL2.

The assessment of the FMEDA, which was performed according to IEC 61508, has shown that the 9203 Solenoid / Alarm Driver has a PFD_{AVG} within the allowed range for SIL2 (HFT = 0) according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of 91%.

The assessment has shown that the Software developed for the 9203 Solenoid / Alarm Driver, complies with the relevant safety requirements for design, implementation and verification for IEC 61508 SIL2.

This means that the 9203 Solenoid / Alarm Driver with version 9203-001 is capable for use in SIL2 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

	
Assessor Dipl.-Ing. (FH) Peter Müller	Certifying Assessor Rachel van Beurden-Amkreutz

Content

Management summary2

1 Purpose and Scope4

2 Project Description5

 2.1 Description of the Functional Safety Management System5

 2.2 Description of the System.....5

3 Project management5

 3.1 Assessment of the development process.....5

 3.2 Roles of the parties involved6

4 Results of the Functional Safety Assessment7

 4.1 Technical aspects of the 9203 Solenoid / Alarm Driver8

 4.2 Functional Safety Management.....8

 4.2.1 Safety Life Cycle.....9

 4.2.2 FSM planning.....9

 4.2.3 Documentation.....9

 4.2.4 Training and competence recording10

 4.2.5 Configuration Management10

 4.2.6 Tools (and languages)10

 4.3 Safety Requirement Specification11

 4.3.1 Safety Requirement Specification and traceability into design11

 4.4 Change and modification management.....11

 4.4.1 Change and modification procedure.....11

 4.5 Software Design12

 4.5.1 Software architecture design12

 4.5.2 Tools and languages13

 4.6 Hardware Design.....13

 4.6.1 Hardware architecture design.....13

 4.6.2 Hardware Design / Probabilistic properties.....14

 4.7 Verification & Validation.....15

 4.7.1 HW related V&V activities.....15

 4.7.2 SW related V&V activities16

 4.8 Safety Manual.....17

 4.8.1 Operation, installation and maintenance requirements17

5 Agreement for future assessment18

6 Reference documents19

7 Status of the document21

 7.1 Releases.....21

1 Purpose and Scope

This document describes the results of the

Full Functional Safety Assessment according to IEC 61508

of the product development processes according to the safety lifecycle phase 9 of IEC 61508-1. The purpose of the assessment was to investigate the compliance of:

- the 9203 Solenoid / Alarm Driver with the technical IEC 61508-2 and -3 requirements for SIL2 and the derived product safety property requirements

and

- the 9203 Solenoid / Alarm Driver development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL2.

It was not the purpose to assess the fulfillment of the statement of conformance from PR electronics for the following European Directives;

- EMC Directive
- Pressure Directive
- Low Voltage Directive
- ATEX Directive

The correct execution of all activities that lead to the statement of Conformance to these European Directives is in the responsibility of PR electronics and builds a basis for the certification.

It was not the purpose of the assessment / audits to investigate Company quality management system versus ISO 9001 and ISO 9000-3 respectively.

The assessment has been carried out based on the quality procedures and scope definitions of *exida* Certification S.A..

2 Project Description

2.1 Description of the Functional Safety Management System

The functional management system is implemented by the use of the functional safety management plan and the related planning documents, which describes the activities in detail. The functional safety management plan shows the implementation of a safety life cycle model which adopts the V-model as described in IEC 61508.

The related planning documents are mainly the configuration management plan, the verification and validation plan and a set of guidelines.

Evidence for the fulfilment of the detailed requirements has been collected in a Safety Justification report, which was subject to the assessment.

2.2 Description of the System

The 9203 Solenoid / Alarm Driver shall provide the following Type-A safety function:

The 9203 Solenoid / Alarm Driver shall convert NPN/contact/PNP signals from safe area into digital drive signals in hazardous area.

Additionally, the 9203 Solenoid / Alarm Driver provide a Type-B safety function operating on the Type-A safety function which results in the consideration of the 9203 Solenoid / Alarm Driver as Type-B system:

The 9203 Solenoid / Alarm Driver shall provide a menu-configured possibility for inverting the output via the Output CPU

Evidence for the fulfilment of the detailed technical requirements has been collected in a Safety Justification report, which was subject to the assessment.

3 Project management

3.1 Assessment of the development process

The development audit was closely driven by requirements subsets filtered from the IEC 61508 content of the *exida* SafetyCaseDB database. That means that the Functional Safety Management related requirements were grouped together according their related objectives. The detailed answers to the requirements, i.e. the justification report, were subject to the assessment. This assessment of the justification report was supplemented by the prior review of documents.

The assessment was planned by *exida* Certification S.A. and agreed with PR electronics [R4].

The following IEC 61508 objectives were subject to detailed auditing at PR electronics:

- FSM planning, including
 - Safety Life Cycle definition
 - Scope of the FSM activities
 - Documentation

- Activities and Responsibilities (Training and competence)
- Configuration management
- Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic
- Hardware and system related V&V activities including documentation, verification
 - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

The project teams, not individuals were audited.

The safety relevant documents have been assessed off site.

The audits were performed in Rønne, Denmark at 2007.12.17 – 19, 2008.02.19 – 22, 2008.04.21 – 23 and 2008.10.08-10.

3.2 Roles of the parties involved

PR electronics

Represents the designer of the safety related 9203 Solenoid / Alarm Driver and the investigated organization. The following teams / responsible persons were audited:

- | | |
|-------------------------------|----------------------------|
| ● Project & Safety Management | Hans Jørgen Eriksen |
| ● Hardware development | Hans Jørgen Eriksen |
| ● Software development | Flemming Svanholm Sørensen |
| ● Test leader | Kaj Harbo |

exida Certification S.A.

Set up and structure of the assessment and audit process, extracted the requirements for the assessment and audit from the IEC 61508 standard and guided through the audit.

The activities were done by *exida* Certification S.A. as an independent organization. The assessment was performed by Peter Müller, who was not involved in the execution of the audited activities.

4 Results of the Functional Safety Assessment

exida Certification S.A. assessed the development process used by PR electronics for this development project against the objectives of IEC 61508 parts 1 to 3. The results of the pre-assessment are documented in [R1].

All objectives have been successfully considered in the PR electronics development processes for the 9203 Solenoid / Alarm Driver development.

exida Certification S.A. assessed the safety case prepared by PR electronics, a set of documents, against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements, before the development audit.

The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see [R1]) investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the PR electronics 9203 Solenoid / Alarm Driver.

The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited development process tailored and implemented by the 9203 Solenoid / Alarm Driver Software and Hardware development project, complies with the relevant safety management requirements of IEC 61508 SIL2.

The assessment of the FMEDA, which was performed according to IEC 61508, has shown that the 9203 Solenoid / Alarm Driver has a PFD_{AVG} within the allowed range for SIL2 (HFT = 0) according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of 91%.

The assessment has shown that the Software developed for the 9203 Solenoid / Alarm Driver, complies with the relevant safety requirements for design, implementation and verification for IEC 61508 SIL2.

This means that the 9203 Solenoid / Alarm Driver with version 9203-001 is qualified for use in SIL2 applications.

Some areas for improvement were nevertheless identified. The recommended improvements given are generally required to formally show the compliance to IEC 61508. However, because of the size of the project (limited number of people) and the low complexity / limited size of the products, PR electronics was able to demonstrate that the *objectives of the related areas have been successfully met*. More details can be found in the chapters below.

4.1 Technical aspects of the 9203 Solenoid / Alarm Driver

The following figure shows the principle product architecture of the 9203 Solenoid / Alarm Driver:

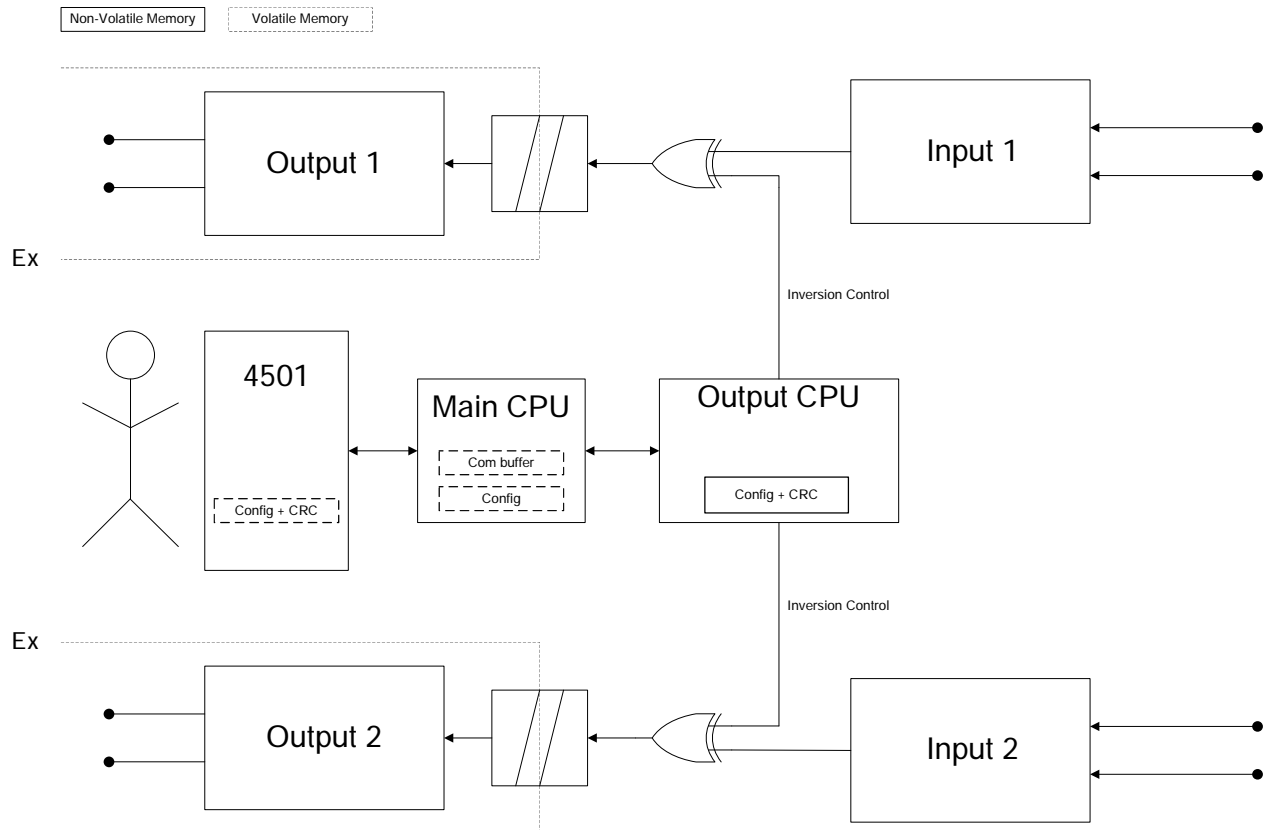


Figure 1 Product architecture of the 9203 Solenoid / Alarm Driver

It can be seen, that the complex electronics (Type B) are only used to control the direct / invert setting of the output. The read back of the Output CPU's control signal by the Main CPU for diagnostic purposes and the possible second independent shutdown path are available, but not shown in this diagram.

In the high current version there is only one channel available.

The two channels on the device shall not be used in the same safety function, e.g. to increase the hardware fault tolerance of the device (to achieve a higher SIL), as they contain common components. The two channels may be used in separate safety instrumented functions if due regard is given to common cause failures.

4.2 Functional Safety Management

Objectives of the Functional Safety Management

The main objectives of the related IEC 61508 requirements are to:

- Structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

- Structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- 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.
- 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.
- Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
- Document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.
- Document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.
- 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.
- Select a suitable set of tools, for the required safety integrity level, over the whole safety lifecycle which assists verification, validation, assessment and modification.

4.2.1 Safety Life Cycle

The development process is well structured and described in the 9000 FSM Plan. It describes all relevant phases for development, integration, verification, validation and modification. The related activities including inputs and outputs assumed for each phase are described.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.2.2 FSM planning

The 9000 FSM Plan defines for the different work items the required input documents, guidelines and templates. The phases are specified in the 9000 FSM Plan and the 9000 V&V plan. All major activities related to specification, verification and validation are planned in the 9000 FSM Plan. The different roles and responsibilities of people are defined in the 9000 RACI chart. The modification procedure after product release is part of this document.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.2.3 Documentation

All V&V specifications and reports are kept under version control together with the associated design and product documents.

The test specification templates describes precisely how to document the validation and integration tests, their specifications, their execution and the results. The templates enables the re-execution of tests by requiring the relevant information.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.2.4 Training and competence recording

The FSM Plan have been specified, reviewed and approved by the responsible people for the specified activities of the project.

The responsibility for the documents are tracked in the RACI chart.

The FSM plan requires to collect the evidence documentation regarding the competence of the involved parties in the project. This is documented in the competence matrix document.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.2.5 Configuration Management

All work products are part of a Visual Source Safe based version management system.

The HW and SW modules building the subsystem can be identified by a naming / numbering convention as described in the Q-system (KMH). The project documents are listed / defined in the RACI-chart together with their version and revision.

The connection between these named items, their version / revision and (internal) releases (baselines, labels, builds, etc) can be generated out of the SourceSafe database. In the Correction sheet for each product the connection between the firmware and hardware version is listed.

There is a set of master copy(ies) / Baselines available that contains all work products that were used as an argument for demonstrating safety integrity of a certain version.

Which versions of a work product was part of which test run is documented in the respective test reports.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.2.6 Tools (and languages)

The 9000 FSM Plan and the "9000 Confidence from Use of Software tools" lists the selected set of tools and argues for their suitability.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.3 Safety Requirement Specification

Objectives of the Safety Requirement Specification

The main objective of the related IEC 61508 requirements is 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.

4.3.1 Safety Requirement Specification and traceability into design

The FSM plan requires the SRS to be developed before any other design and development activity as input for the architecture design of the system / product. For the System9000 project, the final SRS and Safety concept iterations was developed partly in parallel with the development activities.

For each product (sometimes product pairs) one SRS is existing covering all technical safety requirements, both for system and SW, with a clear identification of safety and non-safety related requirements.

The structure and consistency of the SRS is achieved through use of a template back-end, which is based on the IEC 61508 standard.

During the architectural system and software design, the SRS is reviewed by designers for completeness and understandability. The target of the review is always to detect inconsistencies and incompatibilities of the requirements.

The safety concept contains references to the requirements in the SRS. This enables a verification of that the architecture is addressing all applicable requirements in the SRS.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.4 Change and modification management

Objectives of change and modification management

The main objective of the related IEC 61508 requirements is to:

- Ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

4.4.1 Change and modification procedure

The FSM plan includes a section which describes the modification process. This includes:

- (1) Change request either by a fault found during integration / validation, functional enhancement request or by a (field) failure investigation;
- (2) Impact analysis of the proposed change to the PES itself;
- (3) Specification of the change;
- (4) The impact analysis determines the appropriate re-entry point of the safety life cycle;
- (5) Implement the specified change;
- (6) Re-verification of changed modules and affected modules.
- (7) Re-validation of affected requirements and regression tests;
- (8) Procedures and decision to inform customers upon detection of safety critical faults in released products, these are part of the normal company quality procedures.

(9) The modification process shall be used starting with formal integration test.

For the product version 9203-001 it was demonstrated that the change procedure has been followed. This was possible as the product is based on another certified product. The change requests with an embedded impact analysis were assessed. The changes are documented in the HW description and the tests/regression tests are adequately defined in the Acceptance Test document and the Routine Test Specification.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.5 Software Design

Objectives of software design

The main objectives of the related IEC 61508 requirements are to:

- Create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level.
- 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.
- Design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analyzable and verifiable, and which is capable of being safely modified.

Objectives of tools and languages

The main objective of the related IEC 61508 requirements is 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.

4.5.1 Software architecture design

The design is described by the used UML model in combination with the detailed design description.

The UML subset used addresses the following objectives:

1. Static design - Deployment and Component diagrams
2. Dynamic behavior - State transition diagrams;
- Sequence diagrams or Object interaction diagrams.
3. Link to the source code - Class diagrams with each .c/.h. pair modeled by a class;

The use of UML supports the need for transparency, abstraction and modularity as required by the "9000 Safety Concept Design using UML".

The use of this design method is supported by the software tool Enterprise Architect which is used for safety related projects.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.5.2 Tools and languages

For the System 9000 the compiler vendor provides a statement of the compliance with well accepted test suites like Plum Hall (ANSI C). This is documented in the "Confidence from use of software tools" document.

The "9000 Style Guide for Firmware Coding" describes the coding standard for this project. It is based on the MISRA coding standard together with some PR electronics defined stricter rules. The source is checked by PC-Lint, a static code analysis tools together with the applied MISRA rules. Rules that cannot be automatically checked are part of the checklist for manual source code review.

The "9000 Style Guide for Firmware Coding" additionally describes the "style guides" for the source code files / documentation regarding description, inputs and output. Also naming conventions, information requirements and layout of the files are described here

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.6 Hardware Design

Objectives of hardware design

The main objectives of the related IEC 61508 requirements are 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).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.

Objectives of hardware design / probabilistic properties

The main objective of the related IEC 61508 requirements is to:

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.

4.6.1 Hardware architecture design

There is a description of the HW architecture in the safety concept document.

The sub-systems with their HW / SW and SW / SW interactions are specified and documented together with their safety relevance in the Safety Criticality Analysis report (in the System-FMEA) / architecture description.

The HW/HW interactions are described in more detail in the different circuit description documents. This serves both as input to specification of integration tests and as information about which functions and interfaces that can be used by safety functions.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.6.2 Hardware Design / Probabilistic properties

The detailed hardware design is described by Circuit Diagrams, layout drawings and a related parts list. As required by IEC 61508, an FMEDA with probabilistic calculations and the related fault insertion tests will be carried out for the safety related products, as planned by the 9000 FSM plan.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.6.2.1 FMEDA - 9203 Solenoid / Alarm Driver

In addition to the results of the Type B FMEDAs shown below, a FMEDA was carried out for the Type A safety function, to show the use of the CPU's (only controlling and supervising the inversion bit) does not improve the SFF of the Type A hardware too much. That means evidence was given that the Type A requirements are fulfilled without taking the Type B parts into account.

The Type A Safety Function fulfills the requirements with good margins. Also, fault injection testing supports the claim of SFF >90%.

For both variants, it can be concluded, that the faults that impacts the SFF most are, faults that are detectable by the simple Offline Proof Test with a very high coverage (>99%).

4.6.2.1.1 FMEDA - 9203 Solenoid / Alarm Driver, low current

Table 1 Failure rates according to IEC 61508

I_s^1	I_{dd}	I_{du}	SFF	DC _D
416 FIT	61 FIT	43 FIT	91,7%	58,7%

Table 2 PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 2.73E-04	PFD _{AVG} = 4.52E-04	PFD _{AVG} = 9.89E-04

¹ Note that the SU category includes failures that do not cause a spurious trip

4.6.2.1.2 FMEDA - 9203 Solenoid / Alarm Driver, high current

Table 3 Failure rates according to IEC 61508

I_s^2	I_{dd}	I_{du}	SFF	DC _D
419 FIT	61 FIT	46 FIT	91,2%	57,0%

Table 4 PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 2.92E-04	PFD _{AVG} = 4.84E-04	PFD _{AVG} = 1.06E-03

4.7 Verification & Validation

Objectives of HW related verification & validation activities

The main objectives of the related IEC 61508 requirements are to:

- Demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- 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.
- Integrate and test the E/E/PE safety-related systems.
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.
- 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 safety integrity.

4.7.1 HW related V&V activities

The V&V Plan specifies the techniques and the project specific tools / test SW which are used in the verification activities for each phase and each product. The criteria are addressed wherever applicable, e.g. for test coverage.

All planned test levels, module-, integration-, fault insertion- and validation-test are specified in accordance to the selected Safety Integrity Level.

All analytical verification activities are described by the combination of FSM plan and V&V Plan.

All validation activities are documented as required by the planning documents. This includes the techniques and methods to be used, e.g. procedural (review) and technical (functional test). The purpose is to show that the system and SW requirements are successfully met. The selected Requirements Tracking methodology shows traceably the link between safety requirements, validation tests and design. The target is 100% coverage of the safety

² Note that the SU category includes failures that do not cause a spurious trip

requirements. The test cases (called test objectives) are reviewed against the validation objectives and the corresponding requirement. The test execution results are reviewed against expected results.

E.g. the 9202 Requirement traceability matrix contains all requirements for the product, both safety and non-safety. This matrix is used to ensure completeness of the test cases versus all requirements.

Each validation test case defines a test objective, test preparation, test steps and expected output including additional acceptance criteria (typically for performance / usability requirements) where applicable.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.7.2 SW related V&V activities

Objectives of SW related verification and validation activities

The main objectives of the related IEC 61508 requirements are to:

- To the extent required by the safety integrity level, 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.
- Verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved.
- Integrate the software onto the target programmable electronic hardware. 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.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

The V&V Plan specifies the techniques and the project specific tools / test SW which are used in the verification activities for each phase and each product. The criteria are addressed wherever applicable, e.g. for test coverage.

All planned test levels, module-, integration-, fault insertion- and validation-test are specified in accordance to the selected Safety Integrity Level.

All analytical verification activities are described by the combination of FSM plan and V&V Plan.

The integration test strategy for the integration levels SW-SW and SW-HW are planned and described in the FSM and V&V plan.

The details regarding the tests, test type, test data and expected result / pass-fail criteria are all described in the test specifications (reports).

In the review of the test report, the test results are reviewed against the expected result / pass-fail criteria leading to a conclusion regarding successful completion of test.

The integration test specification uses the safety concept and the UML model together with the interface description defined therein as input documents in order to define the actual integration tests.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

4.8 Safety Manual

Objectives of the Safety Manual

The main objective of the related IEC 61508 requirements is to:

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

4.8.1 Operation, installation and maintenance requirements

The Safety Manual is part of the User Manual and will, for some important information, contain pointers to information in the User manual instead of repeating it.

The Safety Manual of the product documents the following aspects / characteristics in order to enable the end-user to integrate, operate and maintain the "Compliant Item" in his application:

- Limitations of the product and its application / operational environment;
- The highest achievable SIL of each sub-system (based on the techniques and measures documented in the safety justification reports);
- Useful lifetime, i.e. components as identified by the FMEDA, where the estimated PF is valid;
- Guidance on recommended periodic (offline) proof test activities / interval for the product;
- Information as provided by the FMEDA:
 - HW fault tolerance;
 - $\Lambda(du)$, $\Lambda(dd)$, $\Lambda(su)$, $\Lambda(sd)$, $\Lambda(\text{no effect, i.e., on dangerous or safe})$;
 - safe failure fraction (SFF);
 - diagnostic coverage derived according to IEC61508-2, annex C;
 - diagnostic test interval.
- All system functions and parameters accessible by the user to implement the safety functions;
- User configuration and programming of the safety functions;
- All safety-related interfaces (I/O, communication, HMI) and their performance characteristics;
- All safety-related aspects regarding installation, commissioning, modification and decommissioning of the product;
- Guidance on operation of the product including assumed organizational measures to protect against operator mistakes;

FMEDA has been chosen as the systematic method to identify failures which are revealed or unrevealed by the cyclic diagnostics. Periodic proof test procedures are developed for any dangerous undetected faults and documented in the Safety Manual.

Conclusion: The objectives of the standard are fulfilled by the PR electronics functional safety management system.

5 Agreement for future assessment

Areas of possible improvements have been identified during the assessment. However, these are assessed not to be in contradiction to an overall positive judgment of the subject.

Recommendations have been given by *exida* Certification S.A. to PR electronics as confidential information for the following lifecycle phases:

- Functional Safety Management
- Safety Requirement Specification
- SW Design
- HW Design
- Verification & Validation

6 Reference documents

The services delivered by *exida* Certification S.A. were performed based on the following standards.

- N1 IEC 61508-1:1998 Functional Safety of E/E/PES; General requirements
- N2 IEC 61508-2:2000 Functional Safety of E/E/PES; Hardware requirements
- N3 IEC 61508-3:1998 Functional Safety of E/E/PES; Software requirements

The pre-assessment delivered by *exida* Certification S.A. were performed based on the audit of the following documents.

- D1 Functional Safety Management Plan Project System 9000 V5R0
- D2 Functional Safety Management Justification Report in System 9000 IEC61508 FSM SafetyCaseDB
- D3 9000 Verification & Validation Plan V2R0
- D4 Technical Justification Report in 9202 SafetyCaseDB – Requirements & Solutions V0R23
- D5 Technical Justification Report in 9202 SafetyCaseDB – Validation Objectives V0R23
- D6 9000 Configuration Management Plan
- D7 9202 Safety Requirement Specification V4R1
- D8 9202 Safety Concept V3R0
- D9 9202 System FMEA / Safety Criticality Analysis V1R0

In addition, the following documents were presented by PR electronics during the audit or given to the assessor for review after the audit:

- D10 9000 SRS Review Record
- D11 Requirements Traceability Matrix Review Template
- D12 9000 Baseline Log V0R59
- D13 9000 RACI Chart
- D14 9000 Competence of People
- D15 9000 Confidence From-Use of Software Tools V2R0
- D16 Supplier Statements Regarding ANSII Compliance (ZIP file)
- D17 9000 Product History Document V1R51
- D18 Quality Handbook - Kvalitets og miljø handbog
- D19 Quality Procedure: Calibration
- D20 9000 Safety Concept Design using UML V1R0
- D21 9000 Style Guide for Firmware Coding V1R0
- D22 9000 Code Review Template

- D23 9000 Integration Test Report Template
- D24 9000 Firmware Design Specification Review Template
- D25 Acceptance Test Report Review Template
- D26 9203 Acceptance Test Report V8R0
- D27 9000 Change Request Template
- D28 920262xx Software Module Test Report
- D29 9202 Software Fault Insertion Test Report V3R0
- D30 9203 Integration Test Report V4R0
- D31 9203 Requirement Traceability Matrix
- D32 9203-1-03 Correction Sheet V1R17
- D33 9203 Circuit Description V6R0
- D34 9203 Safety Manual Solenoid / Alarm Driver V3R0
- D35 92026xxx Firmware Design Specification (UML model)
(920260xx V7R0; 920261xx V2R0; 920262xx V2R0; 920264xx V3R0)
- D36 9203 FMEDA Report V1R1
- D37 9203 FMEDA High current V6R0 – Excel sheets
- D38 9203 FMEDA Low current V6R0 – Excel sheets
- D39 9203 FMEDA Low current A version V6R0 – Excel sheets
- D40 9000 LED and Error Indications V4
- D41 9203 De-rating Analysis V6R0
- D42 9203 Schematics 9203-1-06
- D43 9203 Hardware Fault Insertion Report V4R0
- D44 9203 Hardware Module Test report V7R0
- D45 9203 Input to Requirement Specification V4R1
- D46 9203 SRS V3R1 Review 28-08-2008
- D47 Creation of “9203 A type FMEDA”
- D48 9203 Routine Test Specification V5R0
- D49 9203 Requirement Specification V2R0
- D50 9203 Change Requests 9203SCR01 – 07
- D51 9203 Analytic Validation Report V0R3

The supporting services delivered by *exida* were documented by the following documents.

- R1 Document Review & Assessment Comments, Version 1, Revision 10, February 2010.
Report No.: 0709-02C R002
Confidential Report
- R2 Results of the IEC 61508 Functional Safety Assessment 9203 (this document).
- R3 Minutes of Meeting, 2007.09.4 -7, System 9000 Assessment Preparation
- R4 Assessment Plan, Version 2, Revision 2, February 2008
- R5 Recommendations caused by the IEC 61508 Functional Safety Assessment V1R3,
February 2010. Report No.: 0709-02C R005
Confidential Report

7 Status of the document

7.1 Releases

Version History: V0, R1: Initial Report February, 2010
V1, R0 updated after Review, FMEDA report number updated,
March 26, 2010
SCR 07 added, Reference to Safety Manual updated,
April 22, 2010

Author: Peter Müller

Review: V0, R1 Rachel Amkreutz (*exida*); March 23, 2010

Release status: released