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:

9116 Universal Converter

Customer:

PR electronics

Rønde,
Denmark

Contract No.: 0709-02C

Report No.: 0709-02C R014 Assessment

Version V1, Revision R0, July 2010

Peter Müller

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

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 9116 Universal Converter 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 9116 Universal Converter 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 9116 Universal Converter 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 9116 Universal Converter 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 >90%.

The assessment has shown that the Software developed for the 9116 Universal Converter complies with the relevant safety requirements for design, implementation and verification for IEC 61508 SIL2.

This means that the 9116 Universal Converter with version 9116-001 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

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 9116 Universal Converter with the technical IEC 61508-2 and -3 requirements for SIL2 and the derived product safety property requirements

and

- the 9116 Universal Converter 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 describe 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 9116 Universal Converter shall provide the following Type-B safety functions:

> The 9116 Universal Converter shall convert various sensor input signals from hazardous areas to a 4..20 mA current output signal. An additional safety related output relay shall be available.

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 [R3].

The assessment was based on the existing certification of the Functional Safety Management System [R5] of PR electronics and the certification of the 9113 Temperature / mA Converter [R6] which is a technically nearly identical product (they are different in their inputs and outputs).

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

  - o 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
  - o 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 in March 2010.
The audit was performed in Rønde, Denmark at 2009.09.08 – 09.

3.2 Roles of the parties involved

PR electronics

Represents the designer of the safety related 9116 Universal Converter and the investigated organization. The following teams / responsible persons were audited:

• Project & Safety Management	Hans Jørgen Eriksen
• Hardware development	Mikal Nielsen
• Hardware Test	Kaj Harbo
• Software development	Flemming Svanholm Sørensen
• Software Test	Tommie Skriver Nielsen

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 [R5].
All objectives have been successfully considered in the PR electronics development processes for the 9116 Universal Converter 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 [R5]) investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the PR electronics 9116 Universal Converter.

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 9116 Universal Converter 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 9116 Universal Converter 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 >90%.

The assessment has shown that the Software developed for the 9116 Universal Converter, complies with the relevant safety requirements for design, implementation and verification for IEC 61508 SIL2.

This means that the 9116 Universal Converter with version 9116-001 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 next chapters.

4.1 Technical aspects of the 9116 Universal Converter

The following figure shows the principle product architecture of the 9116 Universal Converter.

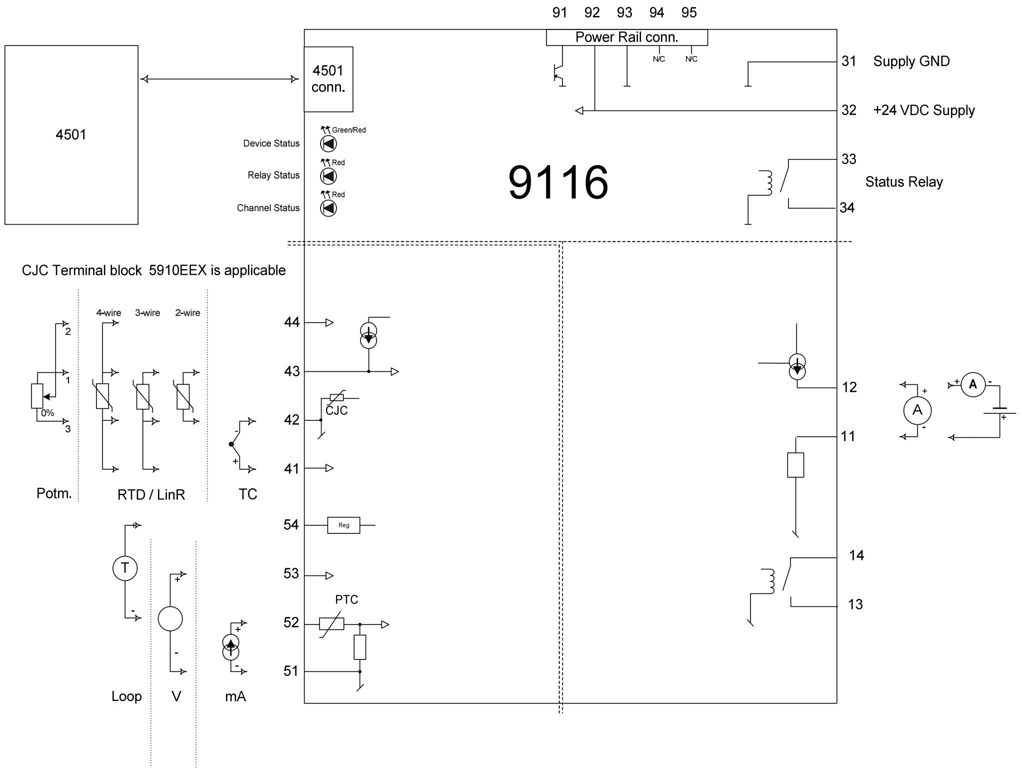

Figure 1 Product architecture of the 9116 Universal Converter

The safety architecture of the device makes use of two microprocessors and a separate HW supervision circuitry that realizes a second independent shutdown path, which is not shown in this diagram.

The possibility to use the device with a single Relay output, where the Relay has been subject to endurance testing [D19] and external over current protection is required by the Safety Manual [D63], is seen to be compliant to IEC 61508.

The status relay is not part of the safety function.

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 the required input documents, guidelines and templates for the different work items. 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 has 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 obtainedfrom 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 were 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 System 9000 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 exists 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 objective of the review is to detect inconsistencies and incompatibilities of the requirements.

The safety concept contains references to the requirements in the SRS. This allows for a verification of the architecture to ensure it adresses 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) The initiation of a 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) An impact analysis to determine the appropriate re-entry point to the safety life cycle;
(5) Implementation of 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 9116-001 it was demonstrated that the change procedure has been followed. The change request with an embedded impact analysis was assessed. The changes are documented in the HW and SW design documents and the relevant 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 are carried out for the safety related products, as planned by the 9000 FSM plan.

The FMEDA confirms that the Type B Safety Function fulfills the requirements. The fault injection testing performed supports the claim of SFF > 90%.

For the relay output an investigation on the quality of the single relay output has been carried out to support the SIL capability.

[D19] shows the test results, verifying that 250.000 electrical cycles and 3.000.000 mechanical cycles can be performed without damage of the device. The test specification was chosen in accordance to EN 50156-1:2003.

Table 1 Configuration overview of the 9116 Universal Converter

ID	Name	Description
[C1]	3w Pt100 Aout	Resistance / RTD temperature / TC temperature inputs, Current output
[C2]	3w Pt100 Relay	Resistance / RTD temperature / TC temperature inputs, Relay output
[C3]	Current Aout	Current input, Current output
[C4]	Current Relay	Current input, Relay output
[C5]	Voltage Aout	Voltage input, Current output
[C6]	Voltage Relay	Voltage input, Relay output

Table 2 Failure rates according to IEC 61508

ID	l_{s}[1]	l_{dd}	l_{du}	SFF	DC_D
[C1]	278 FIT	352 FIT	43 FIT	93 %	89 %
[C2]	359 FIT	230 FIT	62 FIT	90 %	79 %
[C3]	444 FIT	554 FIT	42 FIT	95 %	93 %
[C4]	636 FIT	320 FIT	62 FIT	93 %	83 %
[C5]	395 FIT	479 FIT	56 FIT	93 %	89 %
[C6]	480 FIT	353 FIT	76 FIT	91 %	82 %

Table 3 PFD_{AVG} values

ID	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	
[C1]	PFD_{AVG} = 2,82E-04	PFD_{AVG} = 4,63E-04	PFD_{AVG} = 1,00E-03	PFH = 4,33E-08 1/h
[C2]	PFD_{AVG} = 4,03E-04	PFD_{AVG} = 6,63E-04	PFD_{AVG} = 1,44E-03	PFH = 6,24E-08 1/h
[C3]	PFD_{AVG} = 2,77E-04	PFD_{AVG} = 4,52E-04	PFD_{AVG} = 9,76E-04	PFH = 4,20E-08 1/h
[C4]	PFD_{AVG} = 4,00E-04	PFD_{AVG} = 6,56E-04	PFD_{AVG} = 1,42E-03	PFH = 6,16E-08 1/h
[C5]	PFD_{AVG} = 3,66E-04	PFD_{AVG} = 5,99E-04	PFD_{AVG} = 1,30E-03	PFH = 5,60E-08 1/h
[C6]	PFD_{AVG} = 4,89E-04	PFD_{AVG} = 8,04E-04	PFD_{AVG} = 1,75E-03	PFH = 7,57E-08 1/h

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

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.

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

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-tests 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 allows for traceability between safety requirements, validation tests and design. The target is 100% coverage of the safety 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.

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 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(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 de-commissioning 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 assessment delivered by *exida* Certification S.A. and documented by [R5], [R6] and [R2] were performed based on the assessment of the following documents.

D1	9000 Functional Safety Management Plan V5R0
D2	9000 Configuration Management Plan V2R1
D3	9000 Verification & Validation Plan V2R0
D4	Quality Handbook - Kvalitets og miljø handbog
D5	Quality Procedure: Calibration
D6	9000 RACI Chart V0R233
D7	9000 Competence of People
D8	9000 SRS Review Record
D9	9000 Safety Concept Design using UML V1R0
D10	9000 Style Guide for Firmware Coding V1R0
D11	9000 Code Review Template
D12	9000 Integration Test Report Template
D13	9000 Firmware Design Specification Review Template
D14	9000 Change Request Template
D15	9000 LED and Error Indications V1R0
D16	9000 Product History V1R73
D17	9000 Baseline Log V0R70
D18	9000 Confidence From-Use of Software Tools V4R0
D19	9000 Relay Endurance Test V0R3
D20	9000 MPASM Assembler Faults Circumventions V1R0
D21	9000 MPLAB C18 Compiler Faults Circumventions V3R0
D22	9000 IAR MSP430 C Compiler Faults Circumventions V1R0
D23	9000 Hardware Design Guide V1R0
D24	9000 Circuit Description Guide V1R0
D25	9000 Default Configurations V1R0

D26	Acceptance Test Report Review Template
D27	Requirements Traceability Matrix Review Template
D28	Supplier Statements Regarding ANSII Compliance (ZIP file)
D29	9113 Safety Requirements Specification V6R0
D30	9113 Safety Concept V4R0
D31	System FMEA / Safety Criticality Analysis 9113 / 9116 V2R0
D32	9116 FMEDA Report V1R0
D33	9116 FMEDA 3w Pt100 Aout V0R8
D34	9116 FMEDA 3W Pt100 Relay V0R8
D35	9116 FMEDA Current Aout V0R8
D36	9116 FMEDA Current Relay V0R8
D37	9116 FMEDA Voltage Aout V0R8
D38	9116 FMEDA Voltage Relay V0R8
D39	9116 CPU failure distribution estimation V0R1
D40	Schematics 9116-1 V3R0
D41	9116 Derating Analysis V0R5
D42	9116 Circuit Description V2R0
D43	9116 Software Fault Insertion Test Report V2R0
D44	9116 Hardware Fault Insertion Test Report V2R0
D45	91136xxx Firmware design Specification V0R49
D46	911360xx Firmware Design Specification V10R0
D47	911361xx Firmware Design Specification V3R0
D48	911362xx Firmware Design Specification V17R0
D49	911363xx Firmware Design Specification V6R0
D50	911364xx Firmware Design Specification V1R0
D51	911360xx Software Module test Report V5R0
D52	911361xx Software Module test Report V5R0
D53	911362xx Software Module test Report V10R0
D54	911363xx Software Module test Report V6R0
D55	9116 Hardware Design Specification V4R0
D56	9116 Hardware Module Test Report V6R0
D57	9116 Integration Test Report V7R0
D58	9116 Analytic Validation Report V0R1
D59	9116 Acceptance Test Report V5R0

D60 Technical Justification Report in 9113 SafetyCaseDB – Requirements & Solutions V0R26

D61 Technical Justification Report in 9113 SafetyCaseDB – Validation Objectives V0R26

D62 Functional Safety Management Justification Report in System 9000 IEC61508 FSM SafetyCaseDB

D63 9116 Safety Manual V1R0

D64 9116 Routine Test Specification V4R0

D65 Change Requests 9116SCR01 – 9116SCR14

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

R1 Document Review & Assessment Comments,
Version 1, Revision 8, July 2010. Report No. 0709-02C R010
Confidential Report

R2 Results of the IEC 61508 Functional Safety Assessment (this document).

R3 Assessment Plan, Version 0, Revision 2, July 2009

R4 Recommendations caused by the IEC 61508 Functional Safety Assessment V1R3,
February 2010. Report No.: 0709-02C R005
Confidential Report

R5 Results of the IEC 61508 Functional Safety Management Assessment,
Version 1, Revision 1, November 2008. Report No. 0709-02C R004

R6 Results of the IEC 61508 Functional Safety Assessment (9113-002)
Version 1, Revision 1, February 2010. Report No. 0709-02C R012

7 Status of the document

7.1 Releases

Version History:	V0, R1	Initial draft Report March 2010
	V0, R2	updated documents list April 2010
	V1, R0	updated according to the review comments

Author: Peter Müller

Review: V0, R2 Rachel van Beurden-Amkreutz, June 2010

Release status: released