



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:
9107 HART transparent driver

Customer:
PR electronics
Rønde,
Denmark

Contract No.: 0709-02C
Report No.: 0709-02C R017
Version 1, Revision 0, March 2012

Peter Müller

Management summary

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


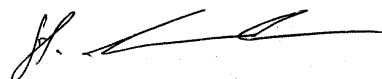
- *exida* Certification S.A. assessed the setup of the development process used by PR electronics for hardware development projects against the relevant requirements of IEC 61508 parts 1 to 2.
Subject to this assessment were the Functional Safety Planning activities, the tailoring of the Verification and Validation activities and the realization of the technical safety aspects using the 9107 HART transparent 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 9107 HART transparent 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 9107 HART transparent driver 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 Type A 9107 HART transparent 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 >60%.

This means that the 9107 HART transparent driver with version 9107-002 is qualified 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 Dipl.-Ing. (TU) Stephan Aschenbrenner

Content

Management summary.....	2
1 Purpose and Scope.....	4
2 Project Description.....	5
2.1 Description of the Functional Safety Management System.....	5
2.2 Description of the System.....	5
3 Project management.....	5
3.1 Assessment of the development process.....	5
3.2 Roles of the parties involved.....	6
4 Results of the Functional Safety Assessment.....	7
4.1 Technical aspects of the 9107 HART transparent driver.....	8
4.2 Functional Safety Management.....	9
4.2.1 Safety Life Cycle.....	9
4.2.2 FSM planning.....	9
4.2.3 Documentation.....	10
4.2.4 Training and competence recording.....	10
4.2.5 Configuration Management.....	10
4.3 Safety Requirement Specification.....	11
4.3.1 Safety Requirement Specification and traceability into design.....	11
4.4 Change and modification management.....	11
4.4.1 Change and modification procedure.....	11
4.5 Hardware Design.....	12
4.5.1 Hardware architecture design.....	12
4.5.2 Hardware Design / Probabilistic properties.....	13
4.6 Verification & Validation.....	13
4.6.1 HW related V&V activities.....	14
4.7 Safety Manual.....	14
4.7.1 Operation, installation and maintenance requirements.....	14
5 Agreement for future assessment.....	15
6 Reference documents.....	16
7 Status of the document.....	17
7.1 Releases.....	17

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 9107 HART transparent driver with the technical IEC 61508-2 requirements for SIL2 and the derived product safety property requirements

and

- the 9107 HART transparent driver development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1 -and 2 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 9107 HART transparent driver shall provide the following Type-A safety functions:

The 9107 HART transparent driver isolates 4-20 mA process signals and realizes a ground loop elimination.

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.

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
- Safety Requirement Specification
- Change and modification management

- 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
- System 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 June - August 2010 and January – February 2012.

The audit was performed in Rønne, Denmark at May 31 – June 02 2010.

3.2 Roles of the parties involved

PR electronics

Represents the designer of the safety related 9107 HART transparent driver and the investigated organization. The following teams / responsible persons were audited:

- | | |
|-------------------------------|----------------|
| • Project & Safety Management | Nikolaj Wehner |
| • Hardware development | Mikal Nielsen |
| • Hardware Test | 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 2. The results of the pre-assessment are documented in [R5].

All objectives have been successfully considered in the PR electronics development processes for the 9107 HART transparent 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 2.

The detailed development audit (see [R5]) investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the PR electronics 9107 HART transparent 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 PR electronics development process, tailored and implemented by the 9107 HART transparent driver 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 Type A 9107 HART transparent 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 >60%.

This means that the 9107 HART transparent driver with version 9107-002 is qualified for use in SIL2 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

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 9107 HART transparent driver

The following figure shows the principle product architecture of the 9107 HART transparent driver.

The figure shows the principle product architecture of the 9106. The principle in 9107 is the same except EX protection applies to the outputs.

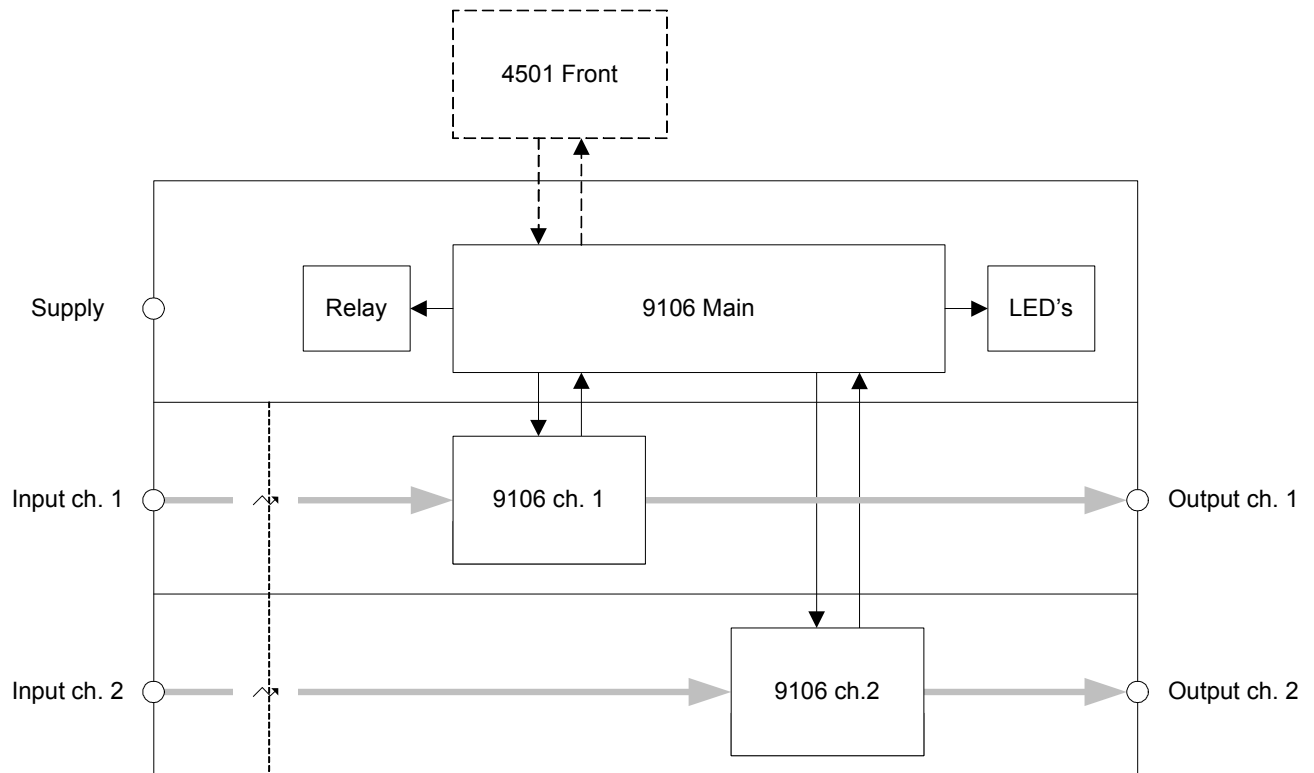


Figure 1 Product architecture of the 9106 / 9107 HART transparent driver

The safety architecture of the device makes no use of any microprocessor. A separate HW supervision circuitry ensures the independence of the safety function and the microprocessors accuracy adjustments.

The status relay is not part of the safety function.

Dangerous detected (DD) failures (see chapter 4.5.2) can only be detected by an external logic solver, which is assumed to be connected to the 9107 Transparent Driver.

Internally the 9107 Transparent Driver doesn't have any diagnostic 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 obtained from 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.

4.3 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 addresses 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 other products of the System 9000 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 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.

4.5.1 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.

4.5.2 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 A Safety Function fulfills the requirements under the assumptions described in chapter 4.1. The fault injection testing performed supports the claim of SFF > 60% (HFT=0).

The following numbers are valid for the configuration: single, active input and active output.

Table 1 Failure rates according to IEC 61508

ID	λ_s^1	λ_{dd}	λ_{du}	SFF	DC _D
SIL2	164 FIT	127 FIT	48 FIT	85 %	72 %

Table 2 PFD_{AVG} values

ID	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	
SIL2	PFD _{AVG} = 2,29E-4	PFD _{AVG} = 4,37E-4	PFD _{AVG} = 1,06E-3	PFH = 4,8E-8 /h

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

4.6 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

4.6.1 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 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.

4.7.1 Operation, installation and maintenance requirements

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;
 - $\Lambda(du)$, $\Lambda(dd)$, $\Lambda(su)$, $\Lambda(sd)$
 - safe failure fraction (SFF);
- All safety-related interfaces (I/O, communication) 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
- 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

The assessment delivered by *exida* Certification S.A. and documented by [R5] and [R2] were performed based on the assessment of the following documents.

- D1 9000 Functional Safety Management Plan V5R0
- D2 9000 Configuration Management Plan V3R0
- D3 9000 Verification & Validation Plan V2R0
- D4 Requirements Specification V5R0
- D5 9106 Safety Requirements Specification V3R0
- D6 9106 Safety Concept V3R0
- D7 System FMEA / Safety Criticality Analysis V2R0
- D8 9106 / 9107 FMEDA Report V1R0
- D9 Schematics 9107-1 V1R1
- D10 9107 De-rating Analysis V0R3
- D11 9107 Circuit Description V1R0
- D12 9107 Hardware Fault Insertion Test Specification V1R0
- D13 9107 Hardware Fault Insertion Test Report V2R0
- D14 9107 Hardware Design Specification V2R0
- D15 9107 Hardware Module Test Specification V2R0
- D16 9107 Hardware Module Test Report V3R0
- D17 9107 Integration Test Specification V1R0
- D18 9107 Integration Test Report V2R0
- D19 9107 Analytic Validation Report V1R0
- D20 9107 Acceptance Test Report V3R0
- D21 Technical Justification Report in 9106 / 9107 SafetyCaseDB – Requirements & Solutions V0R16
- D22 Technical Justification Report in 9106 / 9107 SafetyCaseDB – Validation Objectives V0R16
- D23 9107 Safety Manual V1R0
- D24 9107 Routine Test Specification V2R0

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

- R1 Document Review & Assessment Comments,
Version 1, Revision 5, February 2012. Report No. 0709-02C R015
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

7 Status of the document

7.1 Releases

Version History:	V0, R1	Initial draft Report February 2012
	V0, R2	updated list of documents
	V1, R0	updated according to the review comments

Author: Peter Müller

Review: V0, R2 Stephan Aschenbrenner

Release status: released