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:

KFD2-RCI-(EX)1

Customer:

Pepperl+Fuchs GmbH
Sulbiate
Italy

Contract No.: P+F 0905-35R1-C
Report No.: 0905-35R1-C R015

Version 1, Revision 0, August 2010

Audun Opem, Peter Söderblom

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 Pepperl+Fuchs GmbH, KFD2-RCI-(EX)1 development project, performed by *exida* Certification S.A. consisted of the following activities:

- *exida* Certification S.A. assessed the setup of the development process used by Pepperl+Fuchs GmbH for development projects against the relevant requirements of IEC 61508 parts 1 and 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 KFD2-RCI-(EX)1 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 Pepperl+Fuchs GmbH KFD2-RCI-(EX)1 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 Pepperl+Fuchs GmbH against the technical requirements of IEC 61508.

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

The audited development process as tailored and implemented by the Pepperl+Fuchs GmbH Type A KFD2-RCI-(EX)1 development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, which was performed according to IEC 61508, has shown that the KFD2-RCI-(EX)1 has a PFH and PFD$_{AVG}$ within the allowed range for SIL 3 (HFT = 0) according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of > 99%.

This means that the KFD2-RCI-(EX)1 with Hardware version 355-0257C is capable for use in SIL 3 applications in low or high demand mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor Audun Opem	Assessor Peter Söderblom	Review Dipl-Ing. (FH) Peter Müller

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 KFD2-RCI-(EX)1 with the technical IEC 61508-2 requirements for SIL 3 and the derived product safety property requirements

and

- the KFD2-RCI-(EX)1 development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1 and -2 requirements for SIL 3.

It was not the purpose to assess the fulfillment of the statement of conformance from Pepperl+Fuchs GmbH 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 Pepperl+Fuchs GmbH 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**.**

1.1 Tools and Methods used for the assessment.

This assessment was carried by using the *exida* Certification assessment documents, templates and checklists which are derived from the Safety Case DB tool. The expectations for a positive judgment of the assessor are documented within this tool.

The assessment was based on a set of document templates, e.g. for the document review & assessment comments and the assessment plan.

2 Project Description

2.1 Description of the Functional Safety Management System

The functional safety management system is implemented by the use of the functional safety management plan contained in the V&V plan [D1], the P+F Development process [D2] and the related planning documents, which describes the activities in detail. The V&V plan shows the implementation of a safety life cycle model which adopts the V-model as described in IEC 61508.

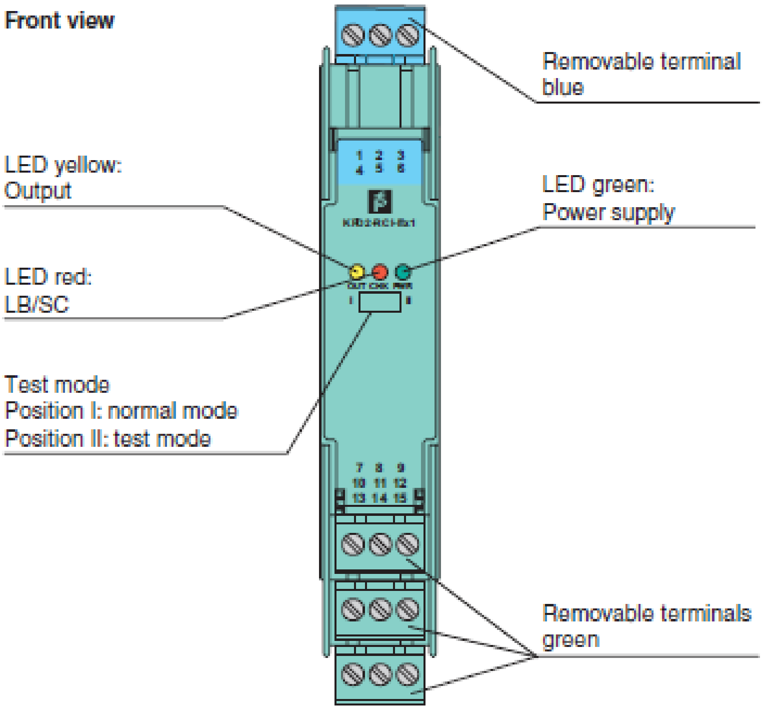
The related planning documents are mainly the configuration management plan, the test plan and a set of templates and guidelines.

Evidence for the fulfilment of the detailed requirements has been collected in a FSM Justification report section in the V&V plan[D1], which was subject to the assessment.

2.2 Description of the System

The KFD2-RCI-(EX)1 is an isolated barrier to be used for intrinsic safety applications. It supplies power to a safety valve controller with HART capability. The barrier is controlled by means of a logic circuit which is loop powered and exist in both EX and Non-EX variants.

This KFD2-RCI-(EX)1 additionally provides non-safety-related HART pass-through for maintenance and diagnostic of the attached solenoid valve. The HART communication is available both in ON condition and in OFF condition of the attached solenoid.



Features of the KFD2-RCI-(EX)1 are:

- 1-channel isolated barrier
- 24V DC supply (Power rail)
- Output 20.4 mA at 13.5V DC
- 19V DC … 30V DC input
- Line fault detection
- Capable for installation in SIL 3 loops
- Available terminals for a measurement of the field loop current (2, 1+) with an intrinsically safe ampere meter

3 Project management

3.1 Assessment of the development process

The development audit was closely driven by subsets of the IEC 61508 requirements. 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 reports, (Design description [D4] - technical requirements and V&V Plan [D1] – process requirements) were subject to the assessment. This assessment of the justification reports was supplemented by the prior review of documents.

The assessment was planned by *exida* Certification S.A. [R3] and agreed with Pepperl+Fuchs GmbH.

The following IEC 61508 objectives were subject to detailed auditing at Pepperl+Fuchs GmbH:

- 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 development audit was performed in Sulbiate 11-12-May-2010

3.2 Roles of the parties involved

Pepperl+Fuchs GmbH

Represents the designers of the safety related KFD2-RCI-(EX)1 and the investigated organization. The following teams / roles were audited:

- Project Management
- System Architect
- Safety Manager
- Safety Coordinator

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 Audun Opem and Peter Söderblom who were 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 Pepperl+Fuchs GmbH for this development project against the objectives of IEC 61508 parts 1 and 2. The results of the pre-assessment are documented in [R1].
All objectives have been successfully considered in the Pepperl+Fuchs GmbH development processes for the KFD2-RCI-(EX)1 development.

exida Certification S.A. assessed the safety case prepared by Pepperl+Fuchs GmbH, including 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 and 2.

The detailed development audit (see [R2]) investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the Pepperl+Fuchs GmbH KFD2-RCI-(EX)1.

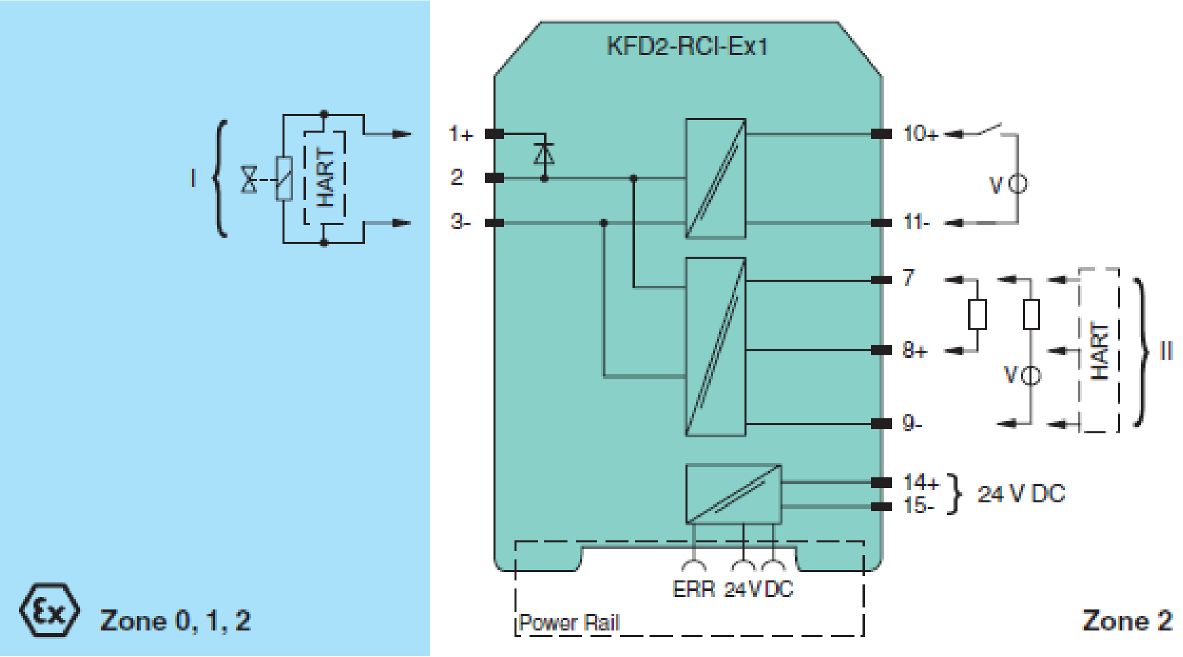
The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the KFD2-RCI-(EX)1 with Hardware version 355-0257C is capable for use in SIL 3 applications in low or high demand mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

Some areas of improvement were nevertheless identified. The recommended improvements given are generally required to formally show the compliance to IEC 61508. However, Pepperl+Fuchs GmbH was able to demonstrate with respect to the size of the project (limited number of people) and the specific complexity of the product that the objectives of the related areas have been successfully met. More details can be found in the chapter below.

4.1 Technical aspects of the KFD2-RCI-(EX)1

The KFD2-RCI-(EX)1 provides an interface between a SIL 3 compliant Digital Output from a safety PLC (terminal 10 and 11), and a SIL 3 compliant solenoid valve (terminal 1, 2 and 3).



The KFD2-RCI-(EX)1 is a single channel Type A (HFT=0) device with low complexity and with a systematic capability of SIL 3.

The ON / OFF functionality is provided by the Digital Output from a safety PLC where the control voltage is converted into a current of 16.2 mA which is added to the output current to the solenoid valve.

The safety concept is that the basic current, 4.2 mA, which is provided by the non-safety-related 24V DC supply circuitry, (terminals 14+ and 15-) to keep HART communication running, is prevented from exceeding the value of the defined safe state even in case of a fault, by redundant circuitry. The additional current for activating the solenoid valve can only be provided by the safety circuitry via the Digital Output from the safety PLC. The output of the KFD2-RCI-(EX)1 is defined to be in safe state when the output current is below 6 mA.

The current output will be approximately 4.2 mA in shutdown mode and 20.4 mA in energized mode.

No single faults in the decoupling mechanism can put the output in a dangerous state.

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.
- 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 as described in the V&V plan [D1] and in the P+F Development process [D2] is structured such that all relevant phases of the overall Safety Life Cycle are identified and that different phases are defined with the necessary activities, their inputs and outputs.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH functional safety management system.

4.2.2 FSM planning

The V&V plan [D1] and the P+F Development process [D2] defines the different development phases together with the corresponding input and output documents, related templates and guidelines. All major activities related to specification, design, implementation, verification and validation are defined and planned in these process documents.

The different roles and responsibilities of the project members are defined. Furthermore the V&V plan [D1] is also used for tracking of the safety activities in the project.

The modification procedures for both the development project and after product release are also described in the V&V plan [D1] and referred by the P+F development process [D2].

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH functional safety management system.

4.2.3 Documentation

A set of templates and guidelines which controls the common layout of documents together with basic properties as document name or number, revision and approval identification exists and is part of the normal quality system of Pepperl+Fuchs GmbH.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH functional safety management system.

4.2.4 Training and competence recording

The competence tracking for the project members is contained within the V&V plan [D1]. In addition to the extensive experience in safety and non-safety HW development, the safety competence within the project is also ensured by a separate safety support group including external safety experts which were available throughout the project.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH functional safety management system.

4.2.5 Configuration Management

The handling of configurations is described in the V&V plan [D1]. This includes responsibilities for the activities, the items to be under version control and the defined tools and methods for this.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH 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 objective of the SRS is covered by the Requirements Profile [D3] and supported by the Design Specification [D4]. The requirements Profile contains a background for the project together with a description of the intended use and targeted application areas. Each requirement has an allocation to the responsible person, an identity which both identifies the type of requirement and the safety relevance. The used requirement identity supports requirements traceability both to the Design Specification [D4] and to the V&V Test Specification [D11] (validation test specification).

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH requirements 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

A modification procedure is defined in the V&V plan [D1]. This is implemented for product changes and is used for changes performed from start of formal validation tests as there is no integration test planned for this type of product. The defined modification procedure, containing a procedure for Impact Analysis including checklists, in combination with the generic development model fulfils the objectives of IEC 61508.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH 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

The HW architecture is described by the Design Specification [D4]. The hardware design follows the rules of modularization, the use of well known components and de-rating.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH HW design process.

4.5.2 Hardware Design / Probabilistic properties

The detailed HW design is partly described by the Design Specification [D4] and by the circuit diagram / Bill of Material [D6]. An FMEDA Report [D5] is documenting the probabilistic calculations for the applicable configurations of the device. The assumptions of the FMEDA are confirmed by a documented Fault Insertion Test [D7].

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH HW design.

4.5.2.1 FMEDA - KFD2-RCI-(EX)1:

The Safe Failure Fraction was confirmed additionally by the Fault insertion tests. The PFH and PFD_{AVG} listed below shows SIL 3 capability.

Table 1 Failure rates according to IEC 61508

λ_s [1]	λ_{dd}	λ_{du}	SFF
204 FIT	0 FIT	1 FIT	99.5%

Table 2 PFH and PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 year
PFH = 1.0E-09	PFD_{AVG} = 4.77E-06	PFD_{AVG} = 9.11E-06	PFD_{AVG} = 2.21E-05

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.

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

- 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.

4.6.1 HW related V&V activities

The V&V plan [D1] defines the required verification activities related to hardware and system including documentation, verification planning, test strategy and requirements tracking to validation test.

All applicable analysis steps as e.g. FMEDA [D5] and de-rating analysis [part of D4] were planned and verified to be successful. All relevant practical tests as e.g. fault insertion test [D13], EMC/Mechanical/Environmental tests [D14] and validation tests [D11] were planned and, successfully executed [D7], [D14] and [D12].

All specified safety requirements were tracked and successfully validated [D12]. The Validation Test specification [D11] contains the required description of the test, acceptance criteria and the documented result. Other applicable aspects as the used configuration and version are documented in order to enable a re-test of the product at a later stage.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH 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 responsibility of P+F is to provide the end-users with a Safety Manual [D8], with all necessary product information in order to enable a correct and safe engineering of the product in a safety instrumented function. Additionally, the provided information enables the end-user to perform the required verification analysis steps of a safety instrumented function, e.g. SFF, PFD/PFH, proof test interval and procedure, etc. The Safety Manual also refers the data sheets which are available of the official web-site for details regarding environmental conditions and other approvals of the product.

Conclusion: The objectives of the standard are fulfilled by the Pepperl+Fuchs GmbH Safety Manual.

5 Agreement for future assessment

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

Recommendations have been given by *exida* Certification S.A. to Pepperl+Fuchs GmbH as confidential information for the following lifecycle phases / sub-phases:

- Change and modification management
- HW related V&V activities

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. was performed based on the audit of the following documents as provided by Pepperl+Fuchs GmbH.

D1	V&V plan	FS-0035EA-22A, 18-Jan-2010
D2	P+F P02 Product Life Cycle	P02-03 Development
D3	Requirements Profile	DDE-1460E 14-Apr-2010
D4	Design Specification – KFD2-RCI-(Ex)1	DDE-1460E3, 07-May-2010
D5	FMEDA – Report KFD2-RCI-(Ex)1	FS-0035EA-20A2, 07-May-2010
D6	Circuit Diagram / Bill of Material	351-0592C, 22-May-2009
D7	Fault Insertion Test results	FS0035EA-26_3, 03-Jun-2009
D8	Safety Manual	FS0035EA-34A 223033/DOCT-1940 06/2010
D9	Data sheet(s)	FS-0035EA-33, 25-Nov-2009 216568_ENG
D10	Development Process	-
D11	V&V Test Specification	FS-0035EA-29B, 18-Nov-2009
D12	V&V Test Results	FS-0035EA-30B, 18-Nov-2009
D13	FMEDA / Fault Insertion Test (specification)	FS-0035EA-26_2, 31-Mar-2009
D14	Test report – Elektromechanical and Environmental	PRDE-A6P1, 07-Jul-2010

The supporting services delivered by *exida* Certification S.A. were documented by the following documents / databases.

R1 Assessment & Document Review comments R006 V0R9 P+F 0905-35R1C

R2 P+F 0905-35R1-C R015 Assessment report KFD2-RCI-(EX)1 V1R0 (this document)

R3 P+F 0905-35C R009 Assessment plan - DDE-1460, V1R0 September 2009

R4 P+F 0905-35R1-C R004 Assessment Recommendations V5R0

7 Status of the document

7.1 Releases

Version History:	V0R1	Initial Report 05-Aug-2010
	V0R2	Updated after customer review
	V1R0	Updated after review by exida 20-Aug-2010
Author:	Audun Opem, Peter Söderblom	
Review:	V0R1	Customer.
	V0R2	Peter Müller
Release status:	Released to customer	