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

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

Results of the
IEC 61508
Functional Safety Assessment

Project:

KCD2-ST-*
KCD2-SOT-*
KCD2-SON-*

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: 1005-041-C
Report No.: 1005-041-C R032

Version 1, Revision 0, September 2013

Peter Söderblom

Management summary

The Functional Safety Assessment of the Pepperl+Fuchs GmbH, 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 61508:2010 (hereafter referred as 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 KCD2-ST/SOT/SON 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 KCD2-ST/SOT/SON 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 development project for KCD2-ST/SOT/SON, complies with the relevant safety management requirements of IEC 61508 SIL 2.

The assessment of the FMEDA, which was performed according to IEC 61508, has shown that the KCD2-ST/SOT/SON have a PFD_{AVG} within the allowed range for SIL 2 (HFT = 0) according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of > 78%.

This means that the KCD2-S(O)T-(Ex)*(.LB)(.SP) with hardware version 05-5912A and KCD2-SON-(Ex)*(.R1)(.SP) with hardware version 05-6666A are capable for use in SIL 2 applications in low or high demand mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor Peter Söderblom	Certifying assessor Dr. Cornelius Rieß

Content

1 Purpose and Scope

This document describes the results of the

Full Functional Safety Assessment according to IEC 61508:2010

of the product development processes according to the safety lifecycle phases 9 and 10 of IEC 61508-1. The purpose of the assessment was to investigate the compliance of:

- the KCD2-ST/SOT/SON with the technical IEC 61508-2 requirements for SIL 2 and the derived product safety property requirements

and

- the KCD2-ST/SOT/SON development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1 and -2 requirements for SIL 2.

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
- 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 the quality management system of Pepperl+Fuchs GmbH 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 out 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 and addendums [D1], the P+F Development process [D2] and the related planning documents, which describe 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 section in the V&V plan [D1], which was subject to the assessment.

2.2 Description of the System

The KCD2-ST/SOT-(Ex)1.LB(.SP) devices are isolated switch amplifiers which provide the power for NAMUR sensors and convert the sensors supply current into a digital output signal (transistor output). The input of the KCD2-ST/SOT-(Ex)1.LB(.SP) controls two transistor outputs (ST: active outputs / SOT: passive outputs). With DIP switch S1 the output mode can be inverted. With DIP switch S2 the second output can either be configured to follow Output 1 or as a diagnostic output which indicates when a Short Circuit / Open Circuit is present in the loop.

The KCD2-ST/SOT-(Ex)2(.SP) devices are isolated switch amplifiers which provide the power for NAMUR sensors and convert the sensors supply current into a digital output signal (transistor output). Each input of the KCD2-ST/SOT-(Ex)2(.SP) controls one transistor output (ST: active output / SOT: passive output). With DIP switch S1 and S2 the output mode can be inverted.

The KCD2-SON-Ex1(.SP), KCD2-SON-Ex2(.SP), KCD2-SON-Ex1.R1 and KCD2-SON-Ex2.R1 devices are isolated switch amplifiers which provide the power for NAMUR sensors in the hazardous area and convert the sensors supply current into a line fault transparent (LFT) output signal. The input of the KCD2-SON-Ex1* controls two passive transistor outputs while each input of the KCD2-SON-Ex2* controls one passive transistor output with resistive output characteristic. With DIP switch S1 and S2 the output mode can be inverted. This means that the customer can decide whether a low or a high input current leads to a low impedance respectively high impedance output.

The device variants KCD2-SON-Ex1.R1 and KCD2-SON-Ex2.R1 have output impedances which are modified for compatibility with the Yokogawa ProSafe digital input card SDV144. The modification is a minor change of the output circuitry where the safety relevant behaviour is unchanged.

All devices with .SP use removable spring terminals instead of removable screw terminals.

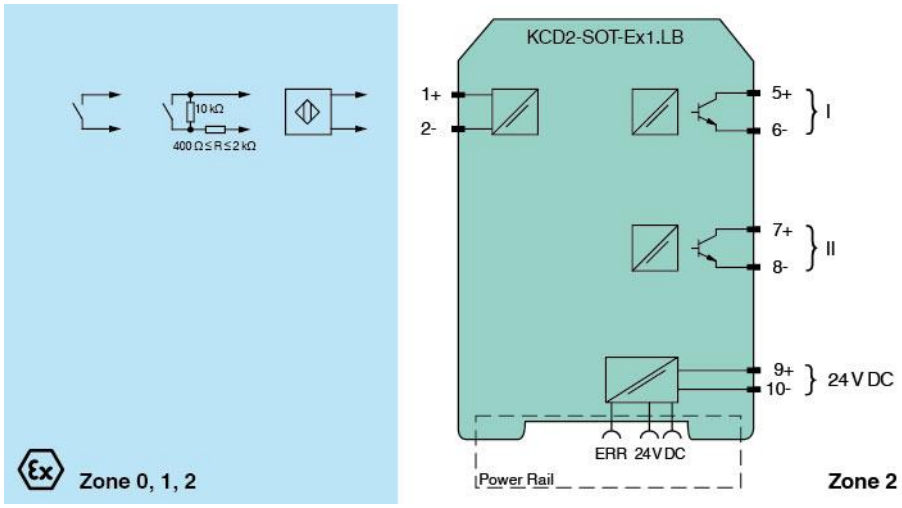

Figure 1 KCD2-SOT-Ex1.LB, KCD2-SOT-Ex1.LB.SP, KCD2-SOT-1.LB and KCD2-SOT-1.LB.SP

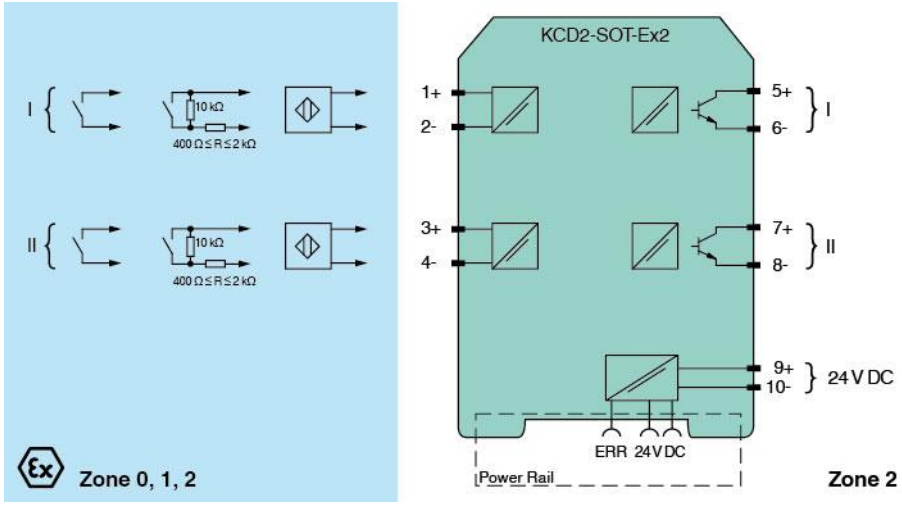

Figure 2 KCD2-SOT-Ex2, KCD2-SOT-Ex2.SP, KCD2-SOT-2 and KCD2-SOT-2.SP

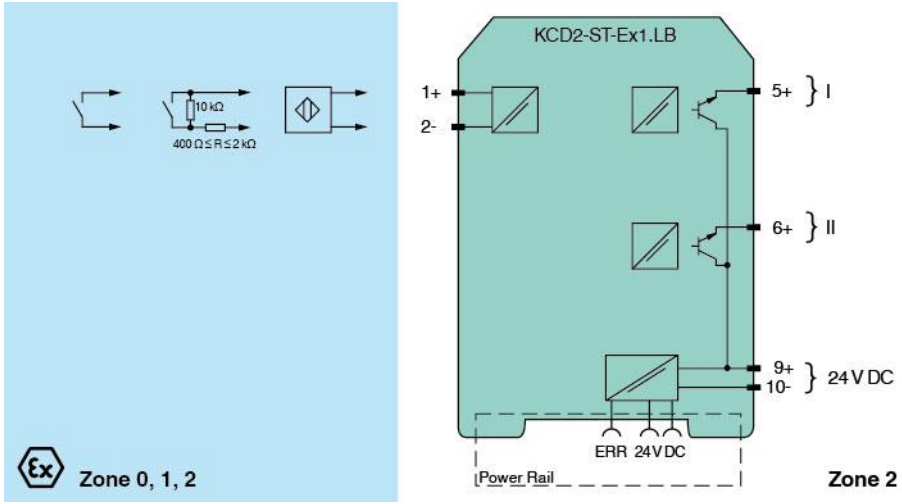

Figure 3 KCD2-ST-Ex1.LB, KCD2-ST-Ex1.LB.SP, KCD2-ST-1.LB and KCD2-ST-1.LB.SP

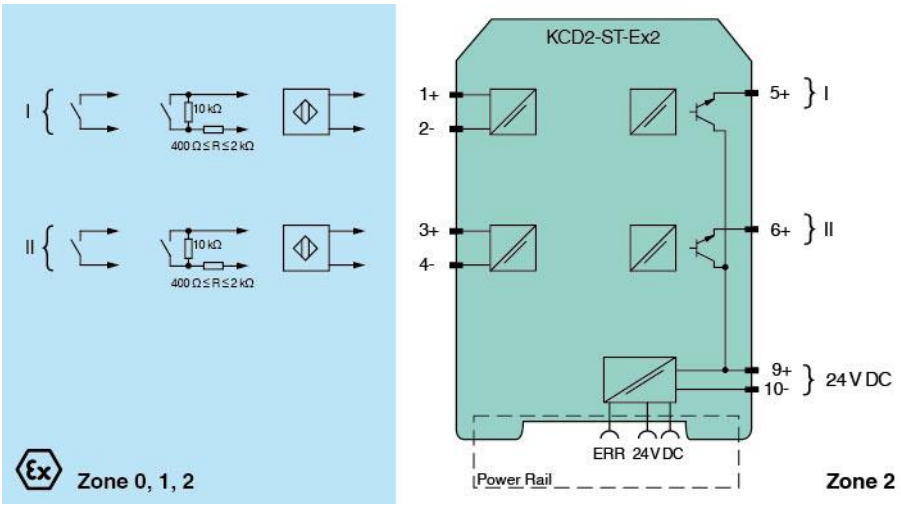

Figure 4 KCD2-ST-Ex2, KCD2-ST-Ex2.SP, KCD2-ST-2 and KCD2-ST-2.SP

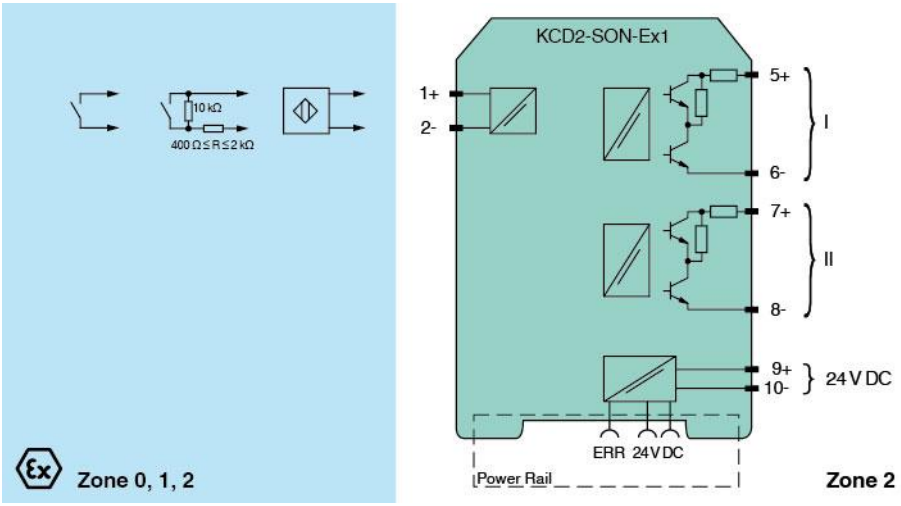

Figure 5 KCD2-SON-Ex1 and KCD2-SON-Ex1.SP

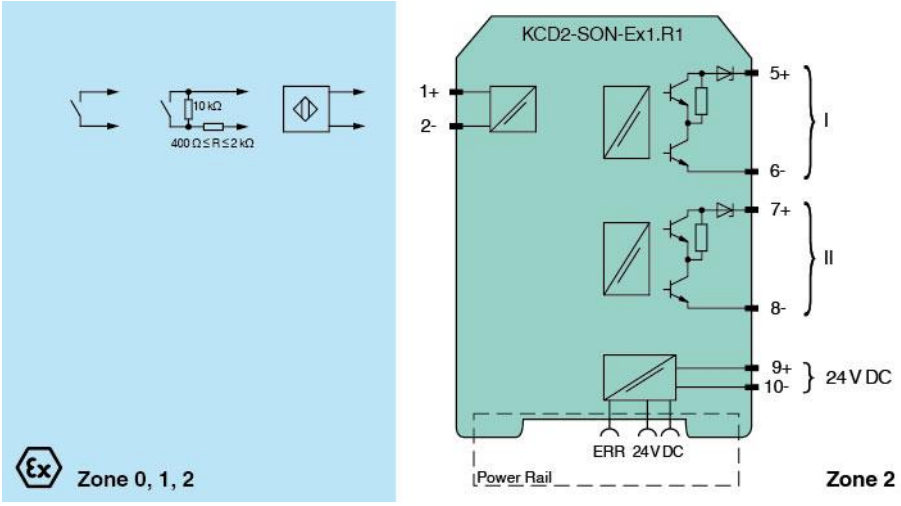

Figure 6 KCD2-SON-Ex1.R1

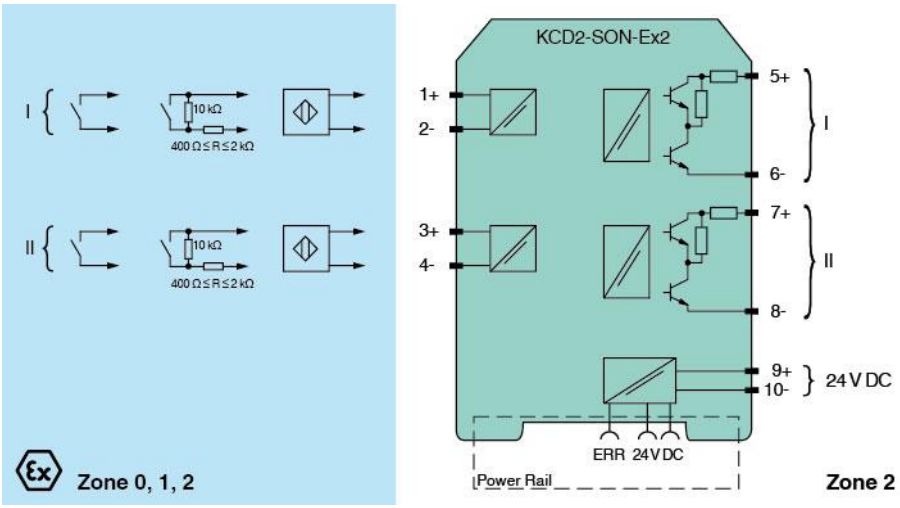

Figure 7 KCD2-SON-Ex2 and KCD2-SON-Ex2.SP

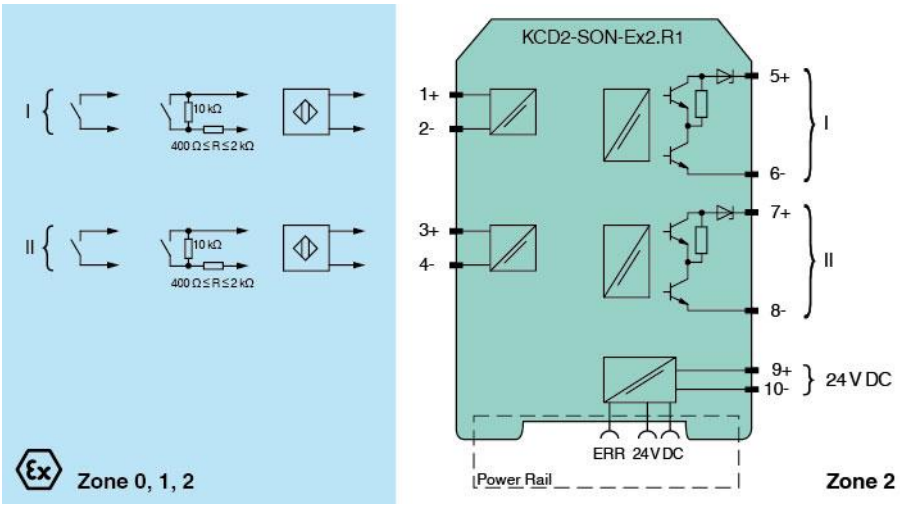

Figure 8 KCD2-SON-Ex2.R1

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 Requirements 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 of the KCD2-ST/SOT/SON project was performed in Mannheim 17 – 19 Apr 2013.

3.2 Roles of the parties involved

Pepperl+Fuchs GmbH

Represents the designer of the safety related KCD2-ST/SOT/SON and the investigated organization. The following teams / responsible persons 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 Peter Söderblom 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 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 KCD2-ST/SOT/SON 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 KCD2-ST/SOT/SON development project.

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 KCD2-S(O)T-(Ex)*(.LB)(.SP) with hardware version 05-5912A and KCD2-SON-(Ex)*(.R1)(.SP) with hardware version 05-6666A are capable for use in SIL 2 applications, 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 KCD2-ST/SOT/SON

The device KCD2-ST/SOT-(Ex)* can be used as interface between Namur sensors in the field and digital inputs e.g. of a PLC in the control area. The current input signal is compared with a fixed limit value and the output is controlled accordingly. Also the signal LED is indicating the output state. The line fault detection can be configured by the DIP switch S3 (KCD2-ST/SOT-(Ex)2 – S3 / S4) to block the output in non-conducting state. With DIP switch S1 (KCD2-ST/SOT-(Ex)2 – S1 / S2) the output mode can be inverted. This means the End-user can decide whether a low or a high input current leads to a conducting respectively non-conducting output. The safe state is a de-energized / non-conducting output. This is a single channel Type A (HFT=0) system with low complexity and with built-in Short Circuit and Open Loop detection in HW. The line fault detection (DIP switch S3 / S4) is mandatory for KCD2-ST/SOT-(Ex)* when used as a part of a safety instrumented function. There is also an under-voltage detection included but this is considered as a part of the safety function. The two channels of KCD2-ST/SOT-(Ex)2 are not intended to be used in a single safety instrumented function, e.g. to increase the hardware fault tolerance. The two channels can be used in two separate and independent safety instrumented functions.

For KCD2-ST/SOT-(Ex)1.LB(.SP) only:
The DIP switch S2 can be used to configure Output 2 to follow Output 1 and thus being suitable as a second safety related output or indicate if a loop fault is present and thus NOT being suitable for safety related functions.

The device KCD2-SON-Ex* can be used as interface between Namur sensors located in hazardous areas and digital inputs e.g. a PLC outside the hazardous area. The current input signal is compared with a fixed limit value and the output is controlled accordingly. Also the signal LED is indicating the output state. The line fault detection can be configured by the DIP switch S3 (KCD2-SON-Ex2 – S3 / S4) to block the output in high impedance state. With DIP switch S1 (KCD2-SON-Ex2 – S1 / S2) the output mode can be inverted. This means the End-user can decide whether a low or a high input current leads to a low impedance respectively high impedance output. The safe state is a de-energized / high impedance output. This is a single channel Type A (HFT=0) system with low complexity and with built-in Short Circuit and Open Loop detection in HW. The line fault detection (DIP switch S3 / S4) is mandatory for KCD2-SON-Ex* when used as a part of a safety instrumented function. There is also an under-voltage detection included but this is considered as a part of the safety function. The two channels of KCD2-SON-Ex2 are not intended to be used in a single safety instrumented function, e.g. to increase the hardware fault tolerance. The two channels can be used in two separate and independent safety instrumented functions.

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, 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] define 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 Requirements Specification

Objectives of the Safety Requirements 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 responsibility 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 and an identity. The identity both identifies the type of requirement and its 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 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

A modification procedure is defined in the V&V plan [D1]. This is implemented for product changes starting with formal validation tests as there is no integration test planned for this Type A 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.

The handling of the R1 variant of the project, also shows that the modification process as described in the V&V plan [D1] is implemented and followed according the process description. The key document Impact analysis [D13], is used to both describe the change as well as defining the relevant activities and tracking them in the project.

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 functional safety management system.

4.5.2 Hardware Design / Probabilistic properties

The detailed HW design is partly described by the Design Specification [D4] and by the circuit diagram [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 functional safety management system.

4.5.2.1 FMEDA – KCD2-S(O)T-(Ex)* – Inverting mode

The Safe Failure Fraction was confirmed additionally by the Fault insertion tests. The PFH and PFD_{AVG} listed below shows SIL 2 capability.

Table 1 Failure rates according to IEC 61508

λ_s [1]	λ_{dd}	λ_{du}	SFF
106 FIT	3.3 FIT	29.1 FIT	78%

Table 2 PFD_{AVG} values

	T[Proof] = 1 year
PFH = 29,1E-09	PFD_{AVG} = 1,27E-04

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

4.5.2.2 FMEDA – KCD2-S(O)T-(Ex)* – Non-inverting mode

The Safe Failure Fraction was confirmed additionally by the Fault insertion tests. The PFH and PFD_{AVG} listed below shows SIL 2 capability.

Table 3 Failure rates according to IEC 61508

λ_s [2]	λ_{dd}	λ_{du}	SFF
107 FIT	3.3 FIT	27.4 FIT	80%

Table 4 PFD_{AVG} values

	T[Proof] = 1 year
PFH = 27,4E-09	**PFD_{AVG} = 1,20E-04**

4.5.2.3 FMEDA – KCD2-SON-(Ex)* – Inverting mode

The Safe Failure Fraction was confirmed additionally by the Fault insertion tests. The PFH and PFD_{AVG} listed below shows SIL 2 capability.

Table 5 Failure rates according to IEC 61508

λ_s [2]	λ_{dd}	λ_{du}	SFF
108 FIT	3.3 FIT	26.0 FIT	81%

Table 6 PFD_{AVG} values

	T[Proof] = 1 year
PFH = 26,0E-09	**PFD_{AVG} = 1,14E-04**

4.5.2.4 FMEDA – KCD2-SON-(Ex)* – Non-inverting mode

The Safe Failure Fraction was confirmed additionally by the Fault insertion tests. The PFH and PFD_{AVG} listed below shows SIL 2 capability.

Table 7 Failure rates according to IEC 61508

λ_s [2]	λ_{dd}	λ_{du}	SFF
109 FIT	3.3 FIT	24.2 FIT	82%

Table 8 PFD_{AVG} values

	T[Proof] = 1 year
PFH = 24,2E-09	**PFD_{AVG} = 1,12E-04**

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

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.

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 [D7] were planned and verified to be successful. All relevant practical tests as e.g. fault insertion test [D7] and validation tests [D11] were planned and successfully executed [D12].

All specified safety requirements were tracked and successfully validated [D12]. The 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 partly 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 functional safety management system.

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:

- Documentation
- Safety requirement specification

6 Reference documents

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

N1	IEC 61508-1:2010	Functional Safety of E/E/PES; General requirements
N2	IEC 61508-2:2010	Functional Safety of E/E/PES; Hardware 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	FS0021EA-22B	02-Jun-2012
	KCD2-ST addendum	FS-0021EA-22C2	04-Jun-2013
	KCD2-SOT addendum	FS-0021EA-22C3	04-Jun-2013
	KCD2-SON addendum	FS-0021EA-22C4	04-Jun-2013
D2	P+F P02 Product Life Cycle	P02-03 Development	
D3	Requirements Profile: KCD2-ST/SOT/SON	DDE-1526C,	23-May-2012
D4	Design Specification: KCD2-ST/SOT/SON	DDE-1526C2,	06-Jun-2012
D5	FMEDA Report	FS-0021EA-20	09-Jan-2012
D6	Circuit Diagram		
	KCD2-ST-Ex2	FS-0021EA-26_7	24-Oct-2011
	KCD2-SOT-Ex2	FS-0021EA-26_8	24-Oct-2011
	KCD-SON-Ex2	FS-0021EA-26_9	09-Nov-2011
D7	De-rating analysis, Fault Insertion Tests	FS0021EA-26_6,	09-Dec-2011
D8	Safety Manual		
	KCD2-SOT-(Ex)*(.LB)(.SP), KCD2-ST-(Ex)*(.LB)(.SP)	TDOCT-3051_ENG,	06/2013
	KCD2-SON-(Ex)*(.R1)(.SP)	TDOCT-3087_ENG,	06/2013
D9	Data sheets:		
	KCD2-SOT-Ex2	FS-0021EA-33,	04-Mar-2013
	KCD2-SOT-1.LB.SP	FS-0021EA-33_2,	04-Mar-2013
	KCD2-ST-Ex2.SP	FS-0021EA-33_3,	04-Mar-2013
	KCD2-ST-1.LB	FS-0021EA-33_4,	04-Mar-2013
	KCD2-SON-Ex1	FS-0021EA-33_5	04-Mar-2013
	KCD2-SON-Ex2.SP	FS-0021EA-33_6,	04-Mar-2013
	KCD2-SON-Ex2.R1	FS-0021EA-33_7,	04-Mar-2013
D10	Development Process	P02-03 Development	
D11	V&V Test Specifications:		
	KCD2-ST-(Ex)*(.LB),	FS-0021EA-29A,	06-Jun-2012
	KCD2-SOT-(Ex)*(.LB),	FS-0021EA-29A2,	06-Jun-2012
	KCD2-SON-(Ex)*	FS-0021EA-29A3,	06-Jun-2012

D12 V&V Test Results:

KCD2-ST-(Ex)*(.LB),	FS-0021EA-30,	11-Jan-2013
KCD2-SOT-(Ex)*(.LB),	FS-0021EA-30_2,	11-Jan-2013
KCD2-SON-(Ex)*	FS-0021EA-30_3,	11-Jan-2013
KCD2-SON-(Ex)*.R1	13-3747	23-Jan-2013

D13 Impact analysis:

KCD2-SON-(Ex)*.R1	FS-0021EA-25	28-Jan-2013

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

R1 Assessment & Document Review comments R024 V0R3 P+F 1005-041-C

R2 P+F 1005-041-C R032 Assessment Report, KCD2-ST/SOT/SON (this document)

R3 P+F 1005-041-C R018 Assessment Plan – HiC283*, V0,R1 August 2010

R4 P+F 0905-35R1-C R004 Assessment Recommendations V7R0

7 Status of the document

7.1 Releases

Version History:	V0R1	Initial version 24-Sep-2013
	V0R2	Updated after review 26-Sep-2013
	V1R0	Updated after customer review 27-Sep-2013
Author:	Peter Söderblom	
Review:	V0R1	Certifying assessor Dr Cornelius Rieß
	V0R2	P+F
Release status:	Released	