IEC 61508 Functional Safety Assessment

Project:

KFD2-SR3-(Ex)2.2S
KFD2-SOT3-Ex*(.LB)(.IO)(-Y1)
KFD2-ST3-Ex*(.LB)

Customer:

Pepperl + Fuchs GmbH
Mannheim
Germany

Contract Number: Q14/08-047-C
Report No.: 1408-047-C R039
Version V1, Revision R1, May 2016

Peter Söderblom, Cornelius Riess

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

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the following products from Pepperl + Fuchs GmbH:

- KFD2-SR3-(Ex)2.2S
- KFD2-SOT3-Ex*(.LB)(.IO)(-Y1)
- KFD2-ST3-Ex*(.LB)

The functional safety assessment performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Pepperl + Fuchs GmbH through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* performed a review of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) reports of the devices documenting the hardware architecture and failure behavior.

The functional safety assessment was performed to the requirements of IEC 61508:2010, SIL 2. A full IEC 61508 Safety Case was prepared using the *exida* Safety Case tool as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also the user documentation (safety manual) was reviewed.

The results of the Functional Safety Assessment can be summarized as:

The audited development process as tailored and implemented by the Pepperl + Fuchs GmbH KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) development project, complies with the relevant safety management requirements of IEC 61508:2010 SIL2, SC 2 (SIL 2 Capable).

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) can be used in a low / high demand safety related system in a manor where the PFD_{avg} / PFH is within the allowed range for up to SIL2 (HFT = 0) according to table 3 of IEC 61508-1.

The assessment of the FMEDA also shows that the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) meet the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) are capable for use in SIL2 applications in Low / High DEMAND mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.

The manufacturer will be entitled to use the Functional Safety Logo.

CERTIFIED • IEC 61508 • SIL 2 CAPABLE • exida

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the following products from Pepperl + Fuchs GmbH:

Ø KFD2-SR3-(Ex)2.2S

Ø KFD2-SOT3-Ex*(.LB)(.IO)(-Y1)

Ø KFD2-ST3-Ex*(.LB)

by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508:2010.

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

The results of this provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with Pepperl + Fuchs GmbH.

All assessment steps were continuously documented by *exida* (see [R1] and [R2]).

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Pepperl + Fuchs GmbH	Manufacturer of the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB)
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment.

P+F contracted *exida* in November 2014 for the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards and literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508 (Parts 1 - 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Pepperl + Fuchs GmbH

[D1]	P02-03 Development	P+F P02 Product Life Cycle
[D2]	141126B: EAW 048 / DWI 048 B.0, 12.11.2009	Development working instruction to provide full traceability of the Safety functionality items during the whole development process.
[D3]	V&V Plan for KFD2-SOT3/ST3/SR3 2.2S fs0096ea-22d.pdf 24.03.2016	V&V plan (FSM / V&V plan)
[D4]	V&V Plan Review Minutes based on Checklist 14-1263A fs0096ea-23a.pdf, 26.03.2014	Review record V&V plan
[D5]	Technical Requirements (incl. SRS) rpd0011b.pdf, 07.09.2015	Requirements Profile
[D6]	Review Requirements Profile incl. Safety Req. Checklist 14-1260A fs0096ea-23.pdf, 04.04.2014	Review record Requirement Profile
[D7]	Design Specification dsd0011a.pdf 27.03.2015	Design Specification:

[D8]	Review Design Specification based on Checklist 14-1261A fs0096ea-23a4.pdf, 16.07.2014	Review record Design Specification:
[D9]	Derating Analysis and Fault Insertion Test V1R1 fs0096ea-26_8.pdf, 23.02.2015	De-rating analysis, Fault Insertion Tests
[D10]	TDOCT-5021_ENG, 03/2016 TDOCT-5022_ENG, 03/2016 TDOCT-0187T, 04/2014	Safety Manual: KFD2-SOT3, KFD2-ST3 KFD2-SR3-(Ex)2.2S System Description K-System
[D11]	FS-0096EA-33, 11.11.2015 FS-0096EA-33_2, 11.11. 2015 FS-0096EA-33_3, 03.12.2015 FS-0096EA-33_4, 11.11.2015 FS-0096EA-33_5, 11.11.2015	Data sheets: KFD2-SOT3-Ex1.LB KFD2-ST3-Ex2 KFD2-SR3-Ex2.2S KFD2-SOT3-Ex1.LB.IO KFD2-SOT3-Ex2.IO-Y1
[D12]	FS-0096EA-29, 16.06.2014 FS-0096EA-29_2, 16.06.2014 FS-0096EA-29_3, 16.06.2014	V&V Test Specifications: KFD2-SOT3-* KFD2-ST3-* KFD2-SR3-(Ex)2.2S
[D13]	FS-0096EA-30, 02.11.2015 FS-0096EA-30_2, 04.11.2015 FS-0096EA-30_3, 23.09.2015	V&V Test Results: KFD2-SOT3-* KFD2-ST3-* KFD2-SR3-(Ex)2.2S
[D14]	FS-0096EA-26, 09.02.2015 FS-0096EA-26_2, 09.02.2015 FS-0096EA-26_3, 09.02.2015 FS-0096EA-26_4, 09.02.2015 FS-0096EA-26A5, 24.03.2016	FMEDA : FMEDA KFD2-SOT3-*.IO Input1 to Output1 inverting mode FMEDA KFD2-SOT3-*.IO Input1 to Output1 non-inverting mode FMEDA KFD2-ST3-* Input1 to Output1 inverting mode FMEDA KFD2-SR3-(Ex)2.2S Input1 to Output1 inverting mode FMEDA version evaluation
[D15]	FS-0096EA-26_6, 23.01.2015 FS-0096EA-26_7, 23.01.2015 FS-0096EA-26_9, 28.01.2015 FS-0096EA-26_A, 30.01.2015 FS-0096EA-26_B, 02.02.2015	Schematic ST3 / SOT3 versions Schematic SR3-(Ex)2.2S versions BOM KFD2-SR3-EX2.2S #262112 BOM KFD2-ST3-EX1_LB #262110 BOM KFD2-SOT3-EX2 #262108
[D16]	PRDE-B9Y5A, 24.09.2015 PRDE-BAD7, 14.01.2015 PRDE-BBA5A, 15.10.2015 PRDE-BBE0, 15.04.2015	EMC test report SR3 Electromechanical test report SR3 EMC test report KFD2-ST3/SOT3* Electromechanical test report KFD2-ST3/SOT3*
[D17]	05-7185A, 22.06.2015 05-7133B, 10.06.2015	Layout KFD2-S(O)T3* as hardware revision Layout KFD2-SR3-(Ex)2.2S as hardware revision

[D18]	FS0096EAA, 16.03.2016	Functional safety document overview KFD2-SOT3/ST3/SR3 2.2S / Project DDE-2650

2.4.2 Documentation generated by *exida*

[R1]	P+F 1408-047-C R036 Assessment and Review comments V0R3.docx	Assessment and review comments DDE-2650
[R2]	P+F 1408-047-C R040 Safety case.xls	IEC 61508 SafetyCaseDB for DDE-2650
[R3]	P+F 1408-047-C R039 Assessment Report V1 R1	IEC 61508 Functional Safety Assessment, Pepperl + Fuchs GmbH DDE-2650 (this report)
[R4]	P+F 0905-35-R1-C R038 Assessment Report FSM Certificate V1 R1.docx	Results of the IEC 61508 Functional Safety Management Assessment

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed upon by 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
    - Tools
- Safety Requirement Specification
- Change and modification management
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
    - Fault insertion test strategy
- System / hardware validation
- Hardware-related operation, installation and maintenance requirements

3 Product Descriptions

The devices will serve as switch amplifiers that transfer digital signals from the field to a PLC via galvanic isolation. The ‘Ex‘ versions may be used as isolated barriers, bringing digital signals from the hazardous area to the non-hazardous area by means of intrinsic safety. The transferred signal may originate from either a NAMUR input signal or a mechanical contact.

The device variants will be distinguished by the number of inputs and the output characteristics. Depending on the variant, the device offers one or two inputs and two outputs. The input characteristics for all device variants are the same, not depending on the number of inputs. In detail the device output(s) have to be developed in the following variants:

- A variant with a dual “active transistor output”, called “*-ST3-*”. This means that the transistor used for output switching is supplied by the power supply of the device.
- A variant with a dual “isolated transistor output”, called “*-SOT3-*”. This means that the transistor used for output switching is supplied by an external supply.
- A variant with “2 x 2 relay contact outputs with ‘and’ logic”, called “*-SR3-*2.2S”. This means that the relays used for output switching can be used as signal splitter (1 input and 2 outputs).

The transfer function of the device (inverting or non-inverting) and the behavior of the outputs shall be user configurable.

As a special function the input shall provide a lead breakage and short circuit detection. Depending on the device configuration an error in the input circuit might be shown at the output or not.

Below, the block diagrams for the different versions are shown.

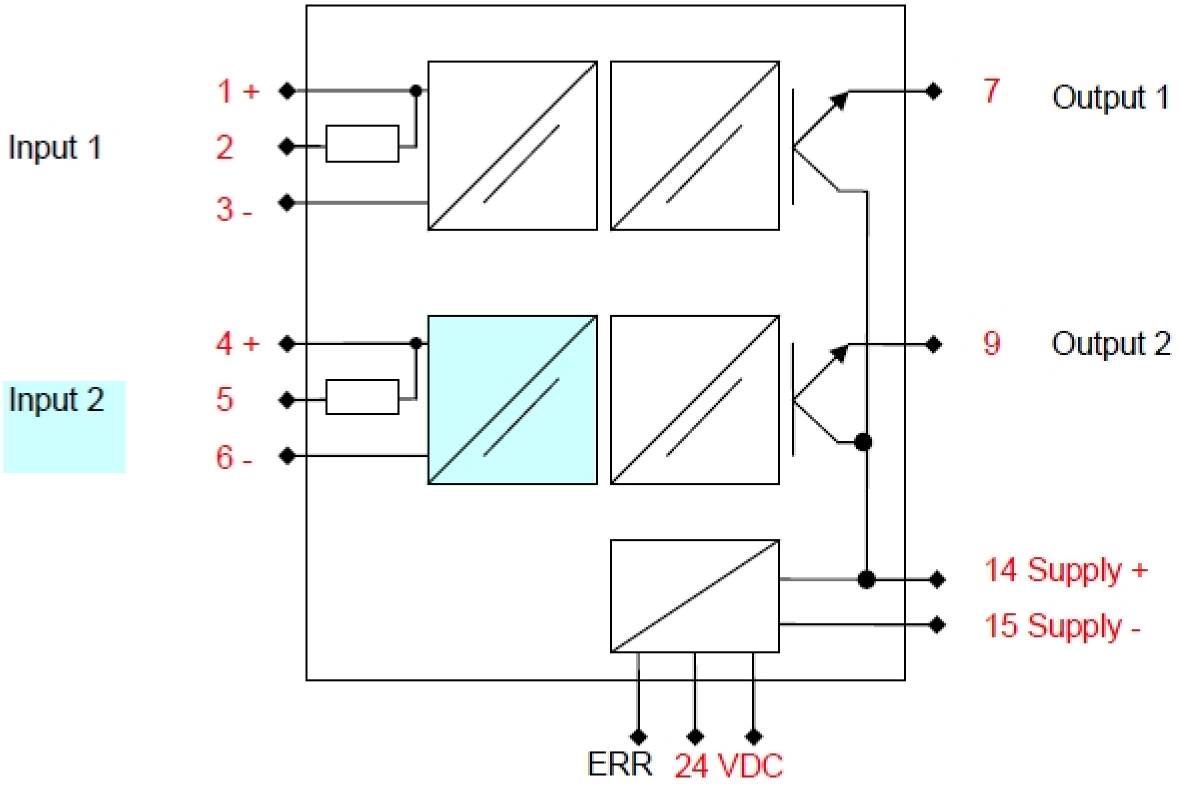

Figure 1: KFD2-ST3-*

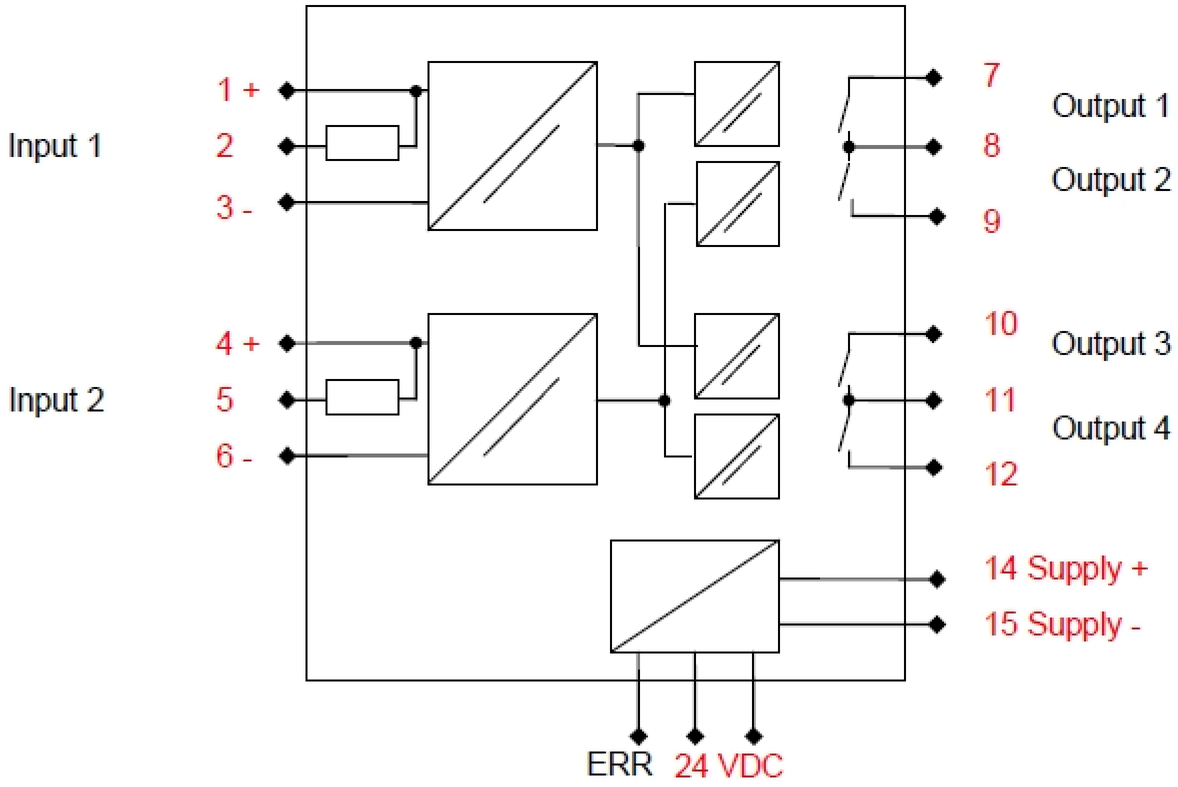

Figure 2: KFD2-SR3-*2.2S

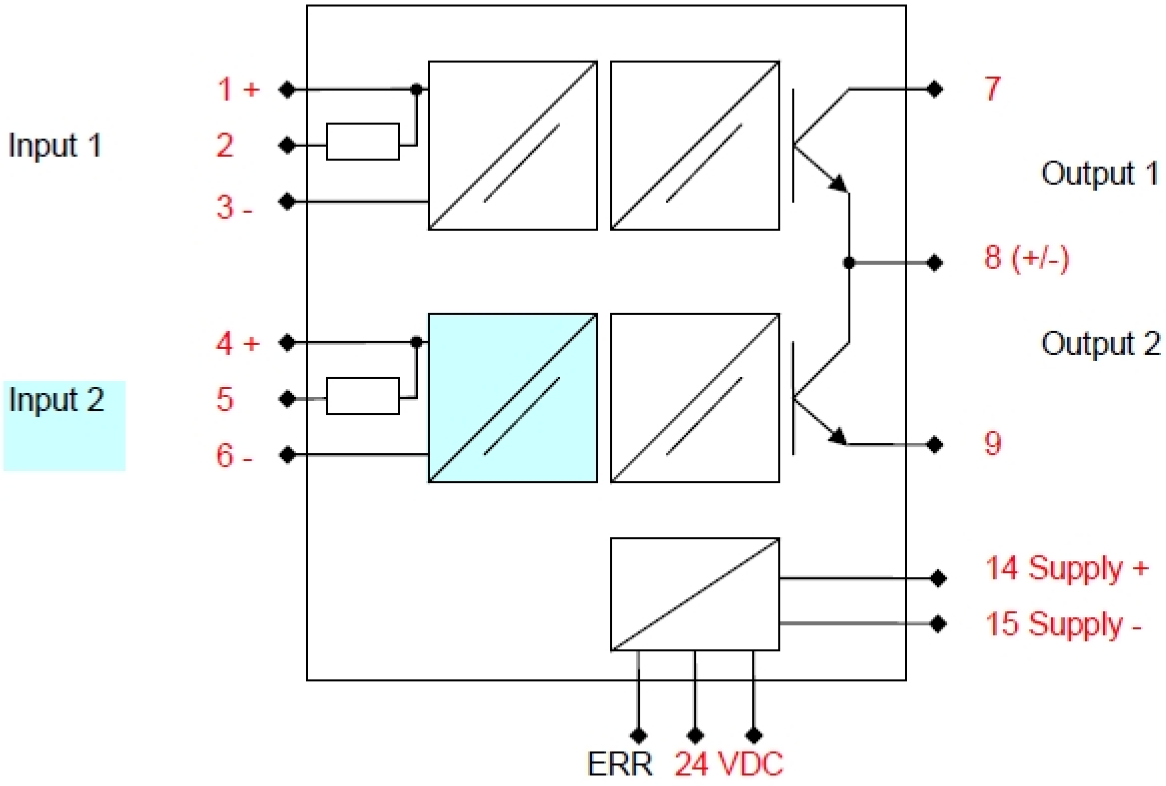

Figure 3: KFD2-SOT3-*

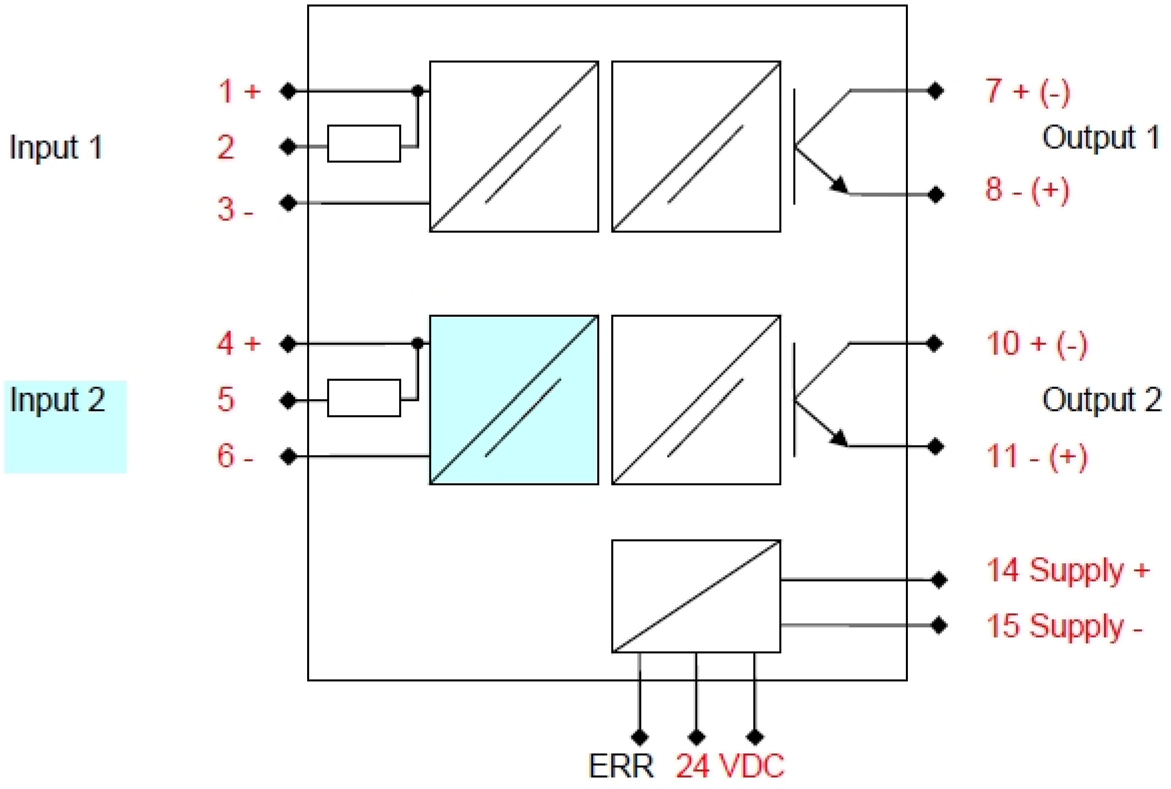

Figure 4: KFD2-SOT3-*.IO

3.1 Hardware Version Numbers

This assessment is applicable to the following hardware versions:

Model	HW version
KFD2-SR3-(Ex)2.2S	05-7133B
KFD2-SOT3-Ex*(.LB)(.IO)(-Y1)	05-7185A
KFD2-ST3-Ex*(.LB)	05-7185A

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Pepperl + Fuchs GmbH for this development project against the objectives of the *exida* certification scheme which includes subsets of IEC 61508 -1 and 2. The results of the assessment are documented in [R1] to [R3].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software. The assessment also includes a review of existing manufacturing quality procedures to ensure compliance to the quality requirements of IEC 61508.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
    - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
    - Specification process, techniques and documentation
    - Design process, techniques and documentation, including tools used
    - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
    - Verification activities and documentation
    - Modification process and documentation
    - Installation, operation, and maintenance requirements, including user documentation
- Product design
    - Hardware architecture and failure behavior, documented in four FMEDAs

The review of the development procedures is described in section 5. The review of the product design is described in section 5.2.

4.2 Assessment level

The KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) has been assessed per IEC 61508 to the following levels:

- SIL 2 capability

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 2 (SIL2) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Pepperl + Fuchs GmbH for these products against the objectives of IEC 61508 parts 1 - 7. The development process has already been assessed and certified as SIL 3 compliant in a separate assessment [R4]

The assessment was done in April 2016 and documented in the SafetyCase [R2].

5.1 Lifecycle Activities and Fault Avoidance Measures

Pepperl + Fuchs GmbH have a defined product lifecycle process in place. This is documented in the Quality Management System Manual [D1] and various Quality Procedures [D2]. A documented modification process is also covered in the Quality Manual. No software is part of the design and therefore any requirements specific from IEC 61508 to software and software development do not apply.

The assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for product design and development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 2 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited Pepperl + Fuchs GmbH design and development process complies with the relevant managerial requirements of IEC 61508 SIL 2.

5.1.1 Functional Safety Management

FSM Planning

Pepperl + Fuchs GmbH have a defined process in place for product design and development. Required activities are specified along with review and approval requirements. The different phases together with the corresponding work items and their required input and output is defined. It also contains references to other planning documents where the verification and validation activities and methods are defined. The roles and responsibilities are also defined herein.

Templates and sample documents have been reviewed and found to be sufficient. The modification process is covered by the V&V plan [D3]. This process and the procedures referenced therein fulfill the requirements of IEC 61508 with respect to functional safety management for a product with simple complexity and well defined safety functionality.

Version Control

The handling of configurations is described in P+F development process [D1]. This includes responsibilities for the activities, the items to be under version control and the defined tools / methods for this.

All safety related work products are part of document / version management system.

The HW modules can be identified by a naming / numbering convention as described in the P+F development process. The project documents are listed / defined in the Documentation plan [D18] together with their version and revision.

Which versions of a work product was part of which test run is documented in the respective test reports [D13] and [D16].

Training, Competency recording

The different training courses / seminars of each individual in the project are documented in addition to the official education in project specific contact lists. Also the applicable project experiences were, in some cases, used as reasoning behind the competence evaluation for the members of the projects. The corresponding competence records are included in the FSM / V&V plan [D3].

The FSM / V&V Plan have been specified, reviewed and approved by the responsible people for the specified activities of the project. The responsibilities for the documents are tracked in this plan.

5.1.2 Safety Requirements Specification and Architecture Design

The FSM / V&V plan requires the SRS to be developed before any other design and development activity as input for the architecture design of the product. For each product one SRS is existing covering all technical safety requirements with a clear identification of safety and non-safety related requirements.

The SRS is covered by the Requirements Profile [D5] and supported by the Design Specification [D7]. 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 and to the V&V Test Specification (validation test specification) [D12].

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

5.1.3 Hardware Design

The design process is documented in the P+F Development process. Items from IEC 61508-2, Table B.2 include observance of guidelines and standards, (ATEX) project management, documentation (design outputs are documented per quality procedures), structured design, modularization, use of well-tried components computer-aided design tools. This meets SIL 2.

5.1.4 Validation

All specified safety requirements were tracked and successfully validated. The test specifications contain 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.

Items from IEC 61508-2, Table B.3 include functional testing, project management, documentation, and black-box testing (for the considered devices this is similar to functional testing). Field experience and statistical testing via regression testing are not applicable. This meets SIL 2.

Items from IEC 61508-2, Table B.5 included functional testing and functional testing under environmental conditions, project management, documentation, failure analysis (analysis on products that failed), expanded functional testing, black-box testing, and fault insertion testing. This meets SIL 2.

5.1.5 Verification

The development and verification activities are defined in the FSM / V&V plan. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 2.

5.1.6 Modifications

A modification procedure is defined in the FSM / V&V plan. 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.

As part of the *exida* scheme a surveillance audit is conducted every 3 years. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which shall indicate with respect to the modification:
  - The initiating problem (e.g. results of root cause analysis)
  - The effect on the product / system
  - The elements/components that are subject to the modification
  - The extent of any re-testing
- List of modified documentation
- Regression test plans

This meets SIL 2.

5.1.7 User documentation

Pepperl + Fuchs GmbH create the following user documentation: product catalogs and a Safety Manual. The Safety Manual was found to contain all of the required information given the simplicity of the products. The Safety Manual references the FMEDA reports which are available and contain the required failure rates, failure modes, useful life, and suggested proof test information.

Items from IEC 61508-2, Table B.4 include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation and limited operation possibilities (KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) perform well-defined actions)

This meets SIL 2.

5.2 Hardware Assessment

To evaluate the hardware design of the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) Failure Modes, Effects, and Diagnostic Analysis's were performed by P+F. These are documented in four FMEDAs [D14].

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA, failure rates are derived for each important failure category. All failure rate analysis results and useful life limitations are listed in the FMEDAs and related documents [D14]. The FMEDAs list failure rates for the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB). The failure rates listed are valid for the useful life of the devices.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

Note, as the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) are only one part of a (sub)system, the SFF should be calculated for the entire final element combination.

These results must be considered in combination with PFD_{avg} / PFH values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The architectural constraints requirements of IEC 61508-2, Table 2 also need to be evaluated for each final element application. It is the end-users responsibility to confirm this for each particular application and to include all components of the final element in the calculations.

The analysis shows that the design of the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) can meet the hardware requirements of IEC 61508, SIL 2 for the KFD2-SR3-(Ex)2.2S, KFD2-SOT3-Ex*(.LB)(.IO)(-Y1) and KFD2-ST3-Ex*(.LB) depending on the complete final element design. The Hardware Fault Tolerance and PFD_{avg} / PFH requirements of IEC 61508 must be verified for each specific design.

5.2.1 Failure rates

The table below lists the failure rates in FIT (failures / 10^9 hours) for the assessed products:

	l_{Safe}	l_{DU}	l_{DD}
KFD2-SR3-(Ex)2.2S	145	73	4.1
KFD2-SOT3-Ex*(.LB)(.IO)(-Y1)	113	30.4	3.3
KFD2-ST3-Ex*(.LB)	97	25.2	3.3

6 Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
Random Capability	The SIL limit imposed by the PFD_{avg} for each element.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares reports based on methods advocated in International standards. *exida* accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version: V1
Revision: R2

Version History: V0, R1: Draft; 18.04.2016
V0, R2: Updated after first review by P+F 25.04.2016
V0, R2: Updated after second review by P+F 28.04.2016
V1, R0: Released version 13.05.2016
V1, R1: Typos corrected 24.05.2016

Authors: Peter Söderblom, Cornelius Riess

Review: V0, R1: P+F
V0, R2: P+F, Certifying assessor

Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Peter Söderblom, Senior Safety Engineer

Dr. Cornelius Rieß, Senior Safety Engineer

Steven Close, Senior Safety Engineer