IEC 61508 Functional Safety Assessment

Project:

HiC2027**
KCD2-STC-1.20
KCD2-STC-Ex1.20**

Customer:

Pepperl + Fuchs GmbH
Oldham
United Kingdom

Contract Number: Q09/05-035-C
Report No.: 0905-035-C R044
Version V1, Revision R1, November 2017

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

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

- HiC2027**
- KCD2-STC-1.20
- KCD2-STC-Ex1.20**

Hereafter they are commonly referred to as HiC2027 / KCD2-STC-(Ex)1* in this report.

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 3. 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 HiC2027 / KCD2-STC-(Ex)1* development project, complies with the relevant safety management requirements of IEC 61508:2010 SIL3, SC 3 (SIL 3 Capable).

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the HiC2027 / KCD2-STC-(Ex)1* can be used in a low / high demand safety related system in a manner where the PFD_{avg} / PFH is within the allowed range for up to SIL 2 (HFT = 0) and the ES versions up to SIL 3 (HFT = 0) according to table 3 of IEC 61508-1.

The assessment of the FMEDA also shows that the HiC2027 / KCD2-STC-(Ex)1* 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). The ES versions can be used to implement a SIL 3 safety function with HFT=0.

This means that the HiC2027 / KCD2-STC-(Ex)1* are capable for use in SIL 3 applications in Low / High demand mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

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

CERTIFIED
IEC 61508
SIL 3 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:

- HiC2027**
- KCD2-STC-1.20
- KCD2-STC-Ex1.20**

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 400 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 based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

Pepperl + Fuchs GmbH	Manufacturer of the
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment.

P+F contracted *exida* in September 2010 for the IEC 61508 Functional Safety Assessment of the first version of the HiC2027 / KCD2-STC-(Ex)1*. After a redesign, the assessment restarted March 2017.

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]	Verification and Validation Plan For KCD2-STC-Ex1.2O & HiC2027 fs0036ea-22d.pdf 27.03.2017	V&V plan (FSM / V&V plan)
[D4]	Requirements Profile Technical Part for HiC2027, KCD2-STC-EX1.2O dde1281j2.pdf, 14.11.2016	Requirements Profile

[D5]	Review Minutes for the Requirement Profile SMART Transmitter Power Supply with analog output HiC2027, KCD2-STC-Ex1.2O Fs0036ea-23b2.pdf, 23.11.2016	Review record for Requirements Profile
[D6]	Design Specification for KCD2-STC-Ex1.2O and HiC2027 dde1281j3.pdf, 14.11.2016	Design Specification
[D7]	Review Minutes for the Design Specification SMART Transmitter Power Supply with analog output HiC2027, KCD2-STC-Ex1.2O Fs0036ea-23b3.pdf, 23.11.2016	Review record for Design Specification
[D8]	Derating Analysis KCD2-STC-Ex1.2O / HiC2027 fs0036ea-26e5.pdf, 28.02.2017	De-rating analysis
[D9]	FMEDA – Report Failure Modes, Effects and Diagnostic Analysis KCD2-STC-(Ex)1.2O(.DE)(.ES)(-AB) / HiC2027(DE)(ES) fs0036ea-20d.pdf, 01.03.2017	FMEDA Report
[D10]	FMEDA Review Minutes For KCD2-STC-(Ex)1.2O* / HiC2027* fs0036ea-23b5.pdf, 15.12.2016	FMEDA Review
[D11]	Impact analysis for changes in devices with functional safety according to IEC61508 Fs-0036ea-25c.pdf, 11.09.2015	Impact analysis KFD2-STC-1.20 – Introduction of non-Ex version into Signal Conditioner range of devices
[D12]	Fault Insertion Test KCD2-STC-Ex1.2O / HiC2027 fs0036ea-26d4.pdf, 20.09.2016	Fault Insertion Test
[D13]	tdoct5513_eng.pdf , 03/2017	Safety Manual Functional Safety SMART Transmitter Power Supply HiC2027**, KCD2-STC-(Ex)1.2O.**
[D14]	V&V Test Specification For DDE-1281J KCD2-STC-Ex1.2O & HiC2027 Fs0036ea-29c.pdf, 24.11.2016	V&V Test Specification
[D15]	Review minutes to the V&V Test Specification for SMART Transmitter Power Supply with analog output HiC2027, KCD2-STC-Ex1.2O Fs0036ea-23b4.pdf, 24.11.2016	V&V Test Specification

[D16]	V&V Test Results For DDE-1281J KCD2-STC-Ex1.2O & HiC2027 Fs0036ea-30b.pdf, 21.03.2017	V&V Test Results
[D17]	Review minutes to the V&V Test Results Prototype for KCD2-STC-EX1.2O, HiC2027 Fs0036ea-23b.pdf, 30.08.2016	Review V&V Test Results
[D18]	fs0036ea-26e.pdf, 01.03.2017 fs0036ea-26e2.pdf, 01.03.2017 fs0036ea-26e3.pdf, 01.03.2017	FMEDA : FMEDA for SIL 2 devices - both channels V1.1 FMEDA for SIL 3 devices – channel 1 V1.1 FMEDA for SIL 2 devices – channel 2 V1.1
[D19]	fs0036ea-33b.pdf, 31.01.2017 fs0036ea-33b2.pdf, 31.01.2017 fs0036ea-33b3.pdf, 31.01.2017 fs0036ea-33b4.pdf, 31.01.2017 fs0036ea-33b5.pdf, 31.01.2017 fs0036ea-33b6.pdf, 31.01.2017 fs0036ea-33b7.pdf, 01.02.2017	Data sheet: HiC2027 HiC2027DE HiC2027ES KCD2-STC-Ex1.2O.DE KCD2-STC-Ex1.2O.ES KCD2-STC-Ex1.2O KCD2-STC-1.2O
[D20]	2515230b.pdf, 25.10.2015 2515231a.pdf, 29.10.2015 2515452.pdf, 14.11.2016	Circuit diagram: KCD2-STC-Ex1.2O(.DE)(.ES) HiC2027(DE)(ES) without ID resistor HiC2027(DE)(ES) with ID resistor
[D21]	2555095b.pdf, 28.10.2015 2555096.pdf, 29.10.2015 2555106.pdf, 15.11.2015	PCB Layout : KCD2-STC-Ex1.2O(.DE)(.ES) HiC2027(DE)(ES) without ID resistor HiC2027(DE)(ES) with ID resistor
[D22]	2645020.pdf, 28.07.2016 2645021.pdf, 12.10.2016	Circuit Description: HiC2027DE KCD2-STC-Ex1.2O.DE
[D23]	prgb5238a.pdf, 10.08.2016 prgb5239a.pdf 10.08.2016	Test selection: HiC devices KCD devices
[D24]	prdebjk8b.pdf, 09.09.2016 prdebjm6b.pdf, 09.09.2016	EMC test report: HiC devices KCD devices
[D25]	prgb5255.pdf, 22.11.2016 prgb5254.pdf, 17.01.2017	Environmental test report: HiC devices KCD devices
[D26]	Fs0036eab, 28.09.2017	Functional safety document overview Project DDE-1281 KCD2-STC-(Ex)1.2O(.DE)(.ES) / HiC2027(DE)(ES)

2.4.2 Documentation generated by *exida*

[R1]	Assessment & Document Review comments R021 V0R11 P+F 0905-035-C	Assessment and review comments HiC2027
[R2]	P+F 0905-035-C R043 Safety case.xls	IEC 61508 SafetyCaseDB for HiC2027
[R3]	P+F 0905-035-R1-C R044 Assessment Report HiC2027 V1 R1.docx	IEC 61508 Functional Safety Assessment, Pepperl + Fuchs GmbH HiC2027 (this report)
[R4]	P+F 0905-35-R1-C R038 Assessment Report FSM Certificate V2 R0.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

These SMART Transmitter power supplies supply 2-wire transmitters in the hazardous area, and can also be used with current sources. They transfer the analog input signal to the safe area as two isolated output signals. Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data. The output is selected as a current source, current sink, or voltage source via switches.

HiC2027(DE)(ES)

These isolated barriers are used for intrinsic safety applications. They mount on a HiC Termination Board. The DE version can drive higher loads, the ES version has additional diagnostics to be suitable for SIL3 applications.

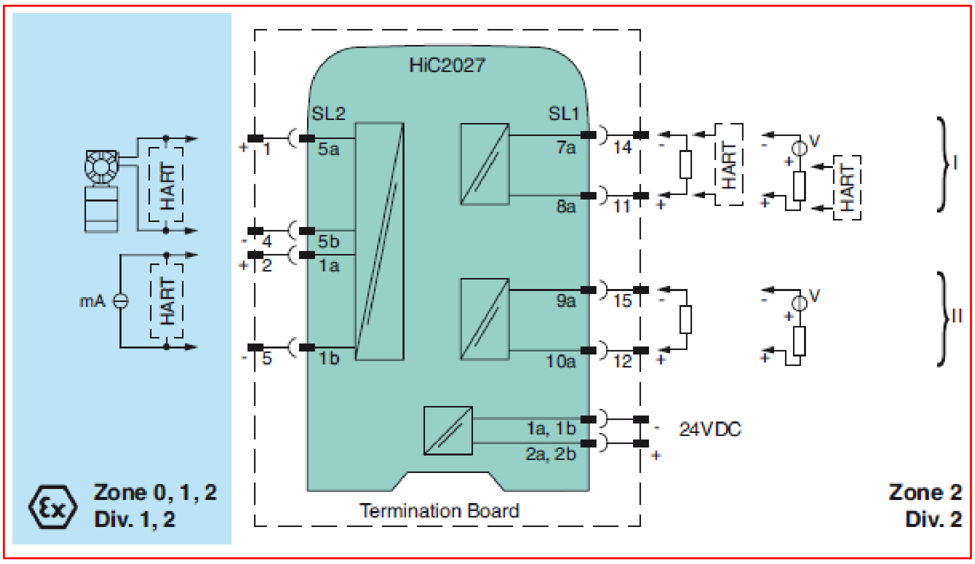

Figure 1: HiC2027

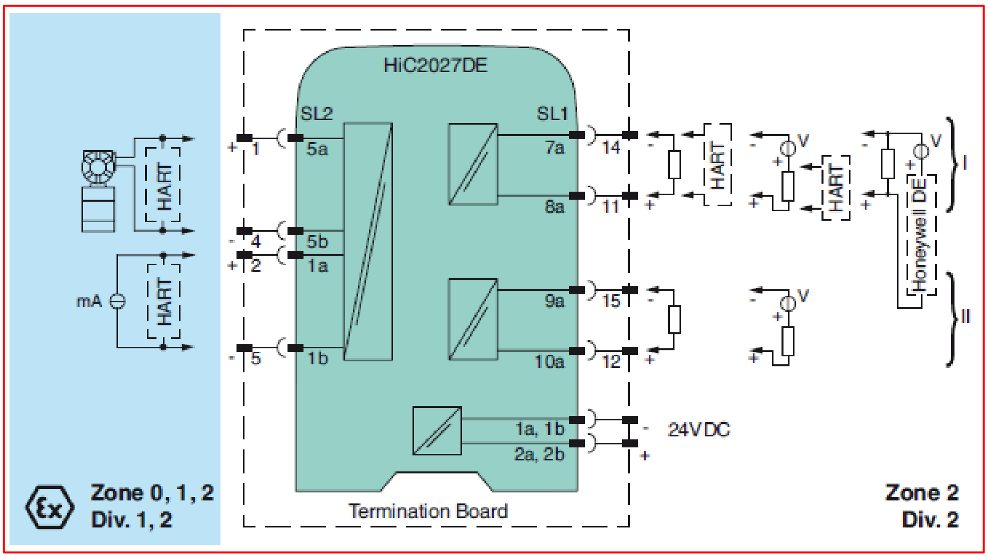

Figure 2: HiC2027DE

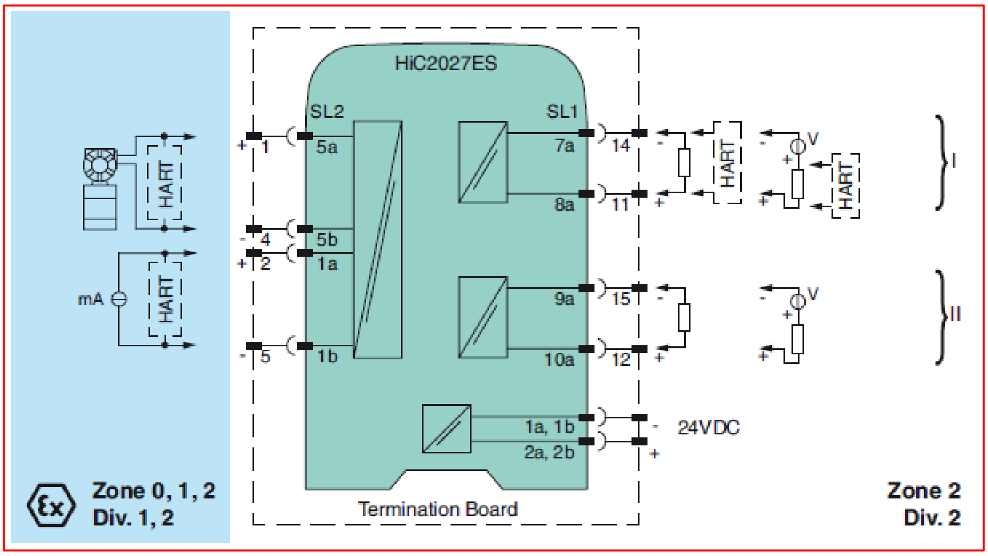

Figure 3: HiC2027ES

KCD2-STC-Ex1.2O(.DE)(.ES)

These isolated barriers are used for intrinsic safety applications. They mount on DIN rail. Terminals contain test sockets. The .DE version can drive higher loads, the .ES version has additional diagnostics to be suitable for SIL3 applications.

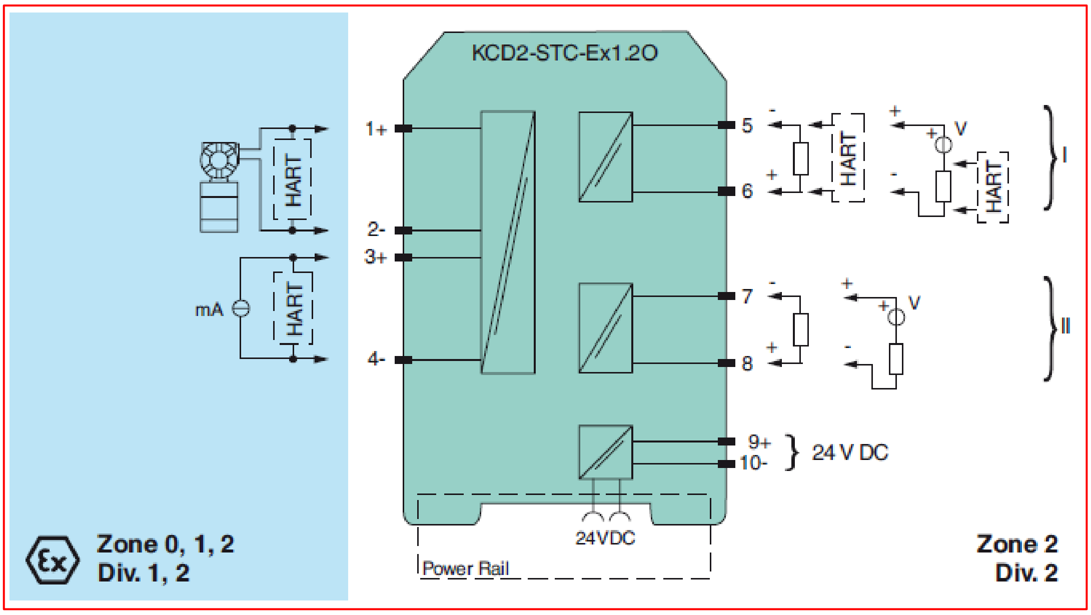

Figure 4: KCD2-STC-Ex1.2O

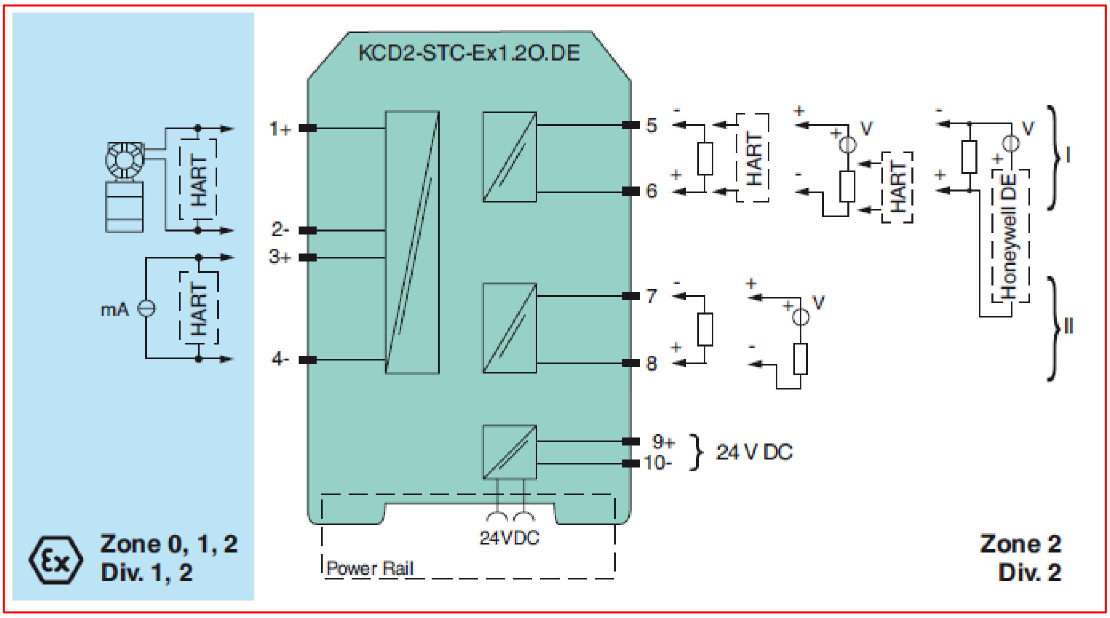

Figure 5: KCD2-STC-Ex1.2O.DE

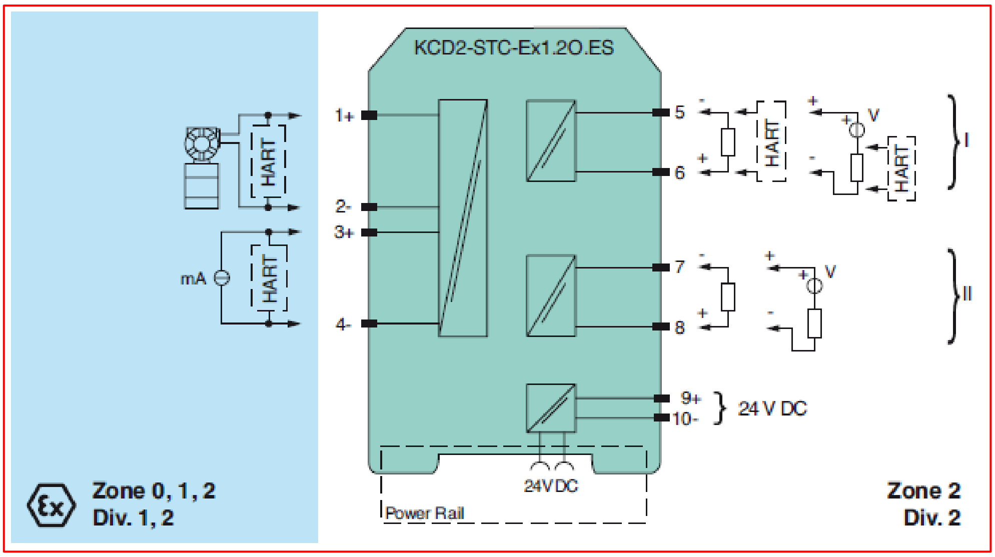

Figure 6: KCD2-STC-Ex1.2O.ES

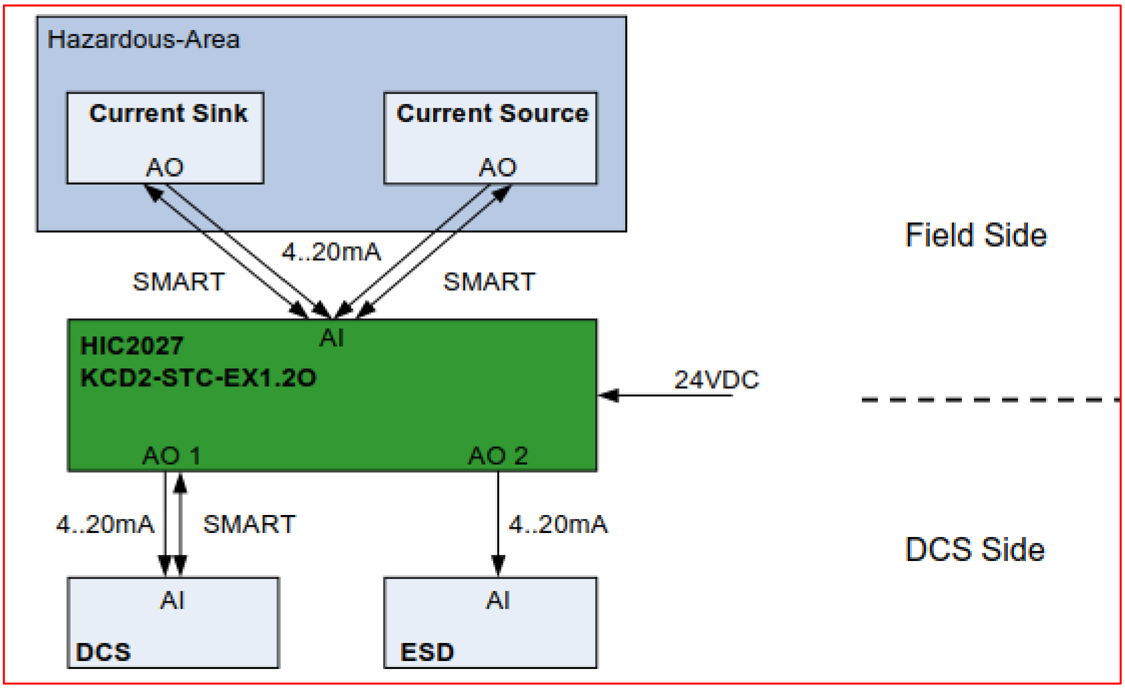

Figure 7: Typical SIL2 configuration

3.1 Hardware Version Numbers

The following Hardware versions were subject to the assessment:

Product	Hardware Version Number
KCD2-STC-Ex1.2O(.DE)(.ES)	255-5095B
HiC2027(DE)(ES) without ID resistor	255-5096
HiC2027(DE)(ES) with ID resistor	255-5106

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 HiC2027 / KCD2-STC-(Ex)1* has been assessed per IEC 61508 to the following levels:

- SIL 3 capability

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL3) 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]

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 and various Quality Procedures. 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 3 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 3.

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. 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. 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 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.

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.

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 and supported by the Design Specification. 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).

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 3.

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 3.

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 3.

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 3.

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 3.

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 (HiC2027 / KCD2-STC-(Ex)1* perform well-defined actions)

This meets SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the HiC2027 / KCD2-STC-(Ex)1*, a Failure Modes, Effects, and Diagnostic Analysis’s were performed by P+F.

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. The FMEDAs list failure rates for the HiC2027 / KCD2-STC-(Ex)1*. 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.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

Note, as the HiC2027 / KCD2-STC-(Ex)1* 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 HiC2027 / KCD2-STC-(Ex)1* can meet the hardware requirements of IEC 61508 SIL 3 depending on the complete 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:

	λ_{Safe}	λ_{DU}	λ_{DD}
KCD2-STC-(Ex)1.2O(.DE)(-AB) or HiC2027(DE) 1oo1 structure	0	55	222
KCD2-STC-(Ex)1.2O.ES or HiC2027ES 1oo1 structure, channel 1	0	7	229
KCD2-STC-(Ex)1.2O.ES or HiC2027ES 1oo1 structure, channel 2	0	8.4	243

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

Contract Number	Report Number	Revision Notes
Q09/05-035-C	0905-035-C R044 V1, R1	Minor typos corrected, November 6th 2017
Q09/05-035-C	0905-035-C R044 V1, R0	Updated by certifying assessor, November 1st 2017
Q09/05-035-C	0905-035-C R044 V0, R3	Updated with P+F comments October26th, 2017
Q09/05-035-C	0905-035-C R044 V0, R2	Updated with P+F comments October13th, 2017
Q09/05-035-C	0905-035-C R044 V0, R1	Initial version September 27th, 2017

Authors: Peter Söderblom

Reviewer: Steven Close

Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Peter Söderblom, Senior Safety Engineer

Steven Close, Senior Safety Engineer