SAFETY MANUAL SIL

Switch Amplifier
HiC2851

SIL
IEC 61508/61511

ISO9001

CE

SIL3

Ex

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

With regard to the supply of products, the current issue of the following document is applicable: The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship"

0 2014-11

1 Introduction

1.1 General Information

This manual contains information for application of the device in functional safety related loops.

The corresponding data sheets, the operating instructions, the system description, the Declaration of Conformity, the EC-Type-Examination Certificate, the Functional Safety Assessment and applicable Certificates (see data sheet) are integral parts of this document.

The documents mentioned are available from **www.pepperl-fuchs.com** or by contacting your local Pepperl+Fuchs representative.

Mounting, installation, commissioning, operation, maintenance and disassembly of the device may only be carried out by trained, qualified personnel. The instruction manual must be read and understood.

When a fault is detected within the device, it must be taken out of service and action taken to protect against accidental use. Devices shall only be repaired directly by the manufacturer. De-activating or bypassing safety functions or failure to follow the advice given in this manual (causing disturbances or impairment of safety functions) may cause damage to property, environment or persons for which Pepperl+Fuchs GmbH will not be liable.

The devices are developed, manufactured and tested according to the relevant safety standards. They must only be used for the applications described in the instructions and with specified environmental conditions, and only in connection with approved external devices.

1.2 Intended Use

This isolated barrier is used for intrinsic safety applications. It transfers digital signals (SN/S1N proximity sensors and approved mechanical contacts) from a hazardous area to a safe area. It has additional protective circuitry to maintain a reliable safety function.

The proximity sensor or switch controls one 24 V DC voltage source safety output, one passive NAMUR compatible signal output, and a separate collective error message. Lead breakage (LB) and short circuit (SC) conditions are continuously monitored.

This barrier is a plug-in device to be inserted into a specific Termination Board.

0 2014-11

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

HiC2851

Up to SIL3

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 – 7, edition 2000:
  Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)
- Electromagnetic compatibility:
  - EN 61326-1:2006
  - NE 21:2006

System specific standards and directives

- Functional safety IEC 61511 part 1 – 3, edition 2003:
  Standard of functional safety: safety instrumented systems for the process industry sector (user)

2 Planning

2.1 System Structure

2.1.1 Low Demand Mode of Operation

If there are two loops, one for the standard operation and another one for the functional safety, then usually the demand rate for the safety loop is assumed to be less than once per year.

The relevant safety parameters to be verified are:

- the PFD_{avg} value (average **P**robability of **F**ailure on **D**emand) and the T_{proof} value (proof test interval that has a direct impact on the PFD_{avg})
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

2.1.2 High Demand or Continuous Mode of Operation

If there is only one loop, which combines the standard operation and safety related operation, then usually the demand rate for this loop is assumed to be higher than once per year.

The relevant safety parameters to be verified are:

- the PFH value (**P**robability of dangerous **F**ailure per **H**our)
- Fault reaction time of the safety system
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance architecture)

2.1.3 Safe Failure Fraction

The safe failure fraction describes the ratio of all safe failures and dangerous detected failures to the total failure rate.

$SFF = (\lambda_s + \lambda_{dd}) / (\lambda_s + \lambda_{dd} + \lambda_{du})$

A safe failure fraction as defined in EN 61508 is only relevant for elements or (sub)systems in a complete safety loop. The device under consideration is always part of a safety loop but is not regarded as a complete element or subsystem.

For calculating the SIL of a safety loop it is necessary to evaluate the safe failure fraction of elements, subsystems and the complete system, but not of a single device.

Nevertheless the SFF of the device is given in this document for reference.

0 2014-11

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- The device shall claim less than 10 % of the total failure budget for a SIL3 safety loop.
- For a SIL3 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (**S**afety **I**nstrumented **F**unction) should be smaller than 10^{-3}, hence the maximum allowable PFD_{avg} value would then be 10^{-4}.
- For a SIL3 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-7} per hour, hence the maximum allowable PFH value would then be 10^{-8} per hour.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HDBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 ºC. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 ºC, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- The safety-related device is considered to be of type **A** components with a Hardware Fault Tolerance of **0**.
- Since the loop has a Hardware Fault Tolerance of **0** and it is a type **A** component, the SFF must be > 90 % according to table 2 of IEC 61508-2 for a SIL3 (sub)system.
- Failure rate based on the Siemens SN29500 data base.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours (e. g. remove sensor fault).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (e. g. substitution by an equivalent device).
- The indication of a dangerous fault (via fault bus) is detected within 1 hour by the programmable logic controller (PLC).
- Since the two outputs of the device use common components, these outputs must not be used in the same safety function.

0 2014-11

2.3 Safety Function and Safe State

Safety Function

The safe state is initiated by an input low condition. The mode of operation can not be changed, which is part of the safety concept of the devices.

Safe State

The safe state of the active voltage output (output I) is the 0-signal/error state (0 V). The safe state of the passive transistor output (output II) is the 0-signal (= 14 kΩ) or the error state (> 100 kΩ).

Reaction Time

The reaction time for all safety functions is < 20 ms. For the voltage output the safety reaction time is reached with a load of 4.7 kΩ or lower impedance.

0 2014-11

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables	
Assessment type and documentation	Full assessment	
Device type	A	
Demand mode	Low Demand Mode or High Demand Mode	
Safety function	Electronic output	Resistive output
HFT	0	0
SIL (hardware)	3	3
λ_s	186 FIT	145 FIT
λ_{dd}	0 FIT	0 FIT
λ_{du}	1.91 FIT	2.99 FIT
$\lambda_{no\ effect}$	146 FIT	190 FIT
$\lambda_{total\ (safety\ function)}$	334 FIT	337 FIT
λ_{total}	437 FIT	
SFF	99.4 %	99.11 %
MTBF [1]	261 years	
PFH	1.91×10^{-9} 1/h	2.99×10^{-9} 1/h
PFD_{avg} for T_1 = 1 year	8.37×10^{-6}	1.31×10^{-5}
T_{proof} max.	5 years	
Fault reaction time [2]	≤ 20 ms	
Reaction time [3]	< 1 s	

[1] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.

[2] Time between fault detection and fault reaction

[3] Step response time

Table 2.1

The characteristic safety values like PFD, PFH, SFF, HFT and T_{proof} are taken from the SIL report/FMEDA report. Please note, PFD and T_{proof} are related to each other.

The function of the devices has to be checked within the proof test interval (T_{proof}).

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces. For corresponding terminals see data sheet.

- Safety relevant interfaces: input, output I, output II
- Non-safety relevant interfaces: output FAULT

3.2 Configuration

A configuration of the device is not necessary and not possible.

3.3 Useful Life Time

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful life time of components is not exceeded. Beyond this useful life time, the result of the probabilistic calculation is meaningless as the probability of failure significantly increases with time. The useful life time is highly dependent on the component itself and its operating conditions – temperature in particular (for example, the electrolytic capacitors can be very sensitive to the working temperature).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful life time of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful life time is valid.

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 years.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.

Our experience has shown that the useful life time of a Pepperl+Fuchs product can be higher

- if there are no components with reduced life time in the safety path (like electrolytic capacitors, relays, flash memory, opto coupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful life time refers to the (constant) failure rate of the device.

0 2014-11

3.4 Installation and Commissioning

During installation all aspects regarding the SIL level of the loop must be considered. The safety function must be tested to ensure the expected outputs are given. When replacing a device, the loop must be shut down. In all cases, devices must be replaced by the same type.

0 2014-11

4 Proof Test

4.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous fails that are otherwise not detected by diagnostic test.

The functionality of the subsystem must be verified at periodic intervals depending on the applied PFD_{avg} in accordance with the data provided in this manual. See chapter 2.4.

It is under the responsibility of the operator to define the type of proof test and the interval time period.

The ancillary equipment required:

- Digital multimeter with an accuracy better than 0.1 %
  For the proof test of the intrinsic safety side of the devices, a special digital multimeter for intrinsically safe circuits must be used.

  Intrinsically safe circuits that were operated with non-intrinsically safe circuits may not be used as intrinsically safe circuits afterwards.
- Power supply set at nominal voltage of 24 V DC

Procedure:

Sensor state must be simulated by a potentiometer of 4.7 kΩ (threshold for normal operation), by a resistor of 220 Ω (short circuit detection) and by a resistor of 150 kΩ (lead breakage detection).

The voltage output needs to be loaded with 1.3 kΩ and observed with a Digital Volt Meter. The NAMUR output needs to be tested with an impedance meter. The input threshold must be between 2.1 mA and 2.8 mA, the hysteresis must be between 170 µA and 250 µA (by means of input current meter and potentiometer).

If the input current is above the threshold

- the output must be activated, voltage level higher than 20 V DC,
- the NAMUR output must be low impedant (1.8 kΩ ± 10 % at 8.3 V supply voltage),
- the yellow LED must be on.

If the resistor R_{SC} (220 Ω) or the resistor R_{LB} (150 kΩ) is connected to the input, the unit must detect an external error. The red LED shall be flashing, the voltage output is off, the NAMUR output is high impedant (> 100 kΩ).

For the philosophy of Functional Safety it is important to test, that the voltage output is **definitely off** (less than 1 V DC) and the NAMUR output is **definitely high impedant** (14 kΩ ± 10 %), if the input is below the lower threshold (typ. 2.5 mA) or above the higher threshold (typ. 6 mA).

As the unit does not have any switches or settings, no special actions have to be taken in terms of different configurations. The mode of operation is only interchangeable by the use of a different sensor (S1N instead of SN type)

0 2014-11

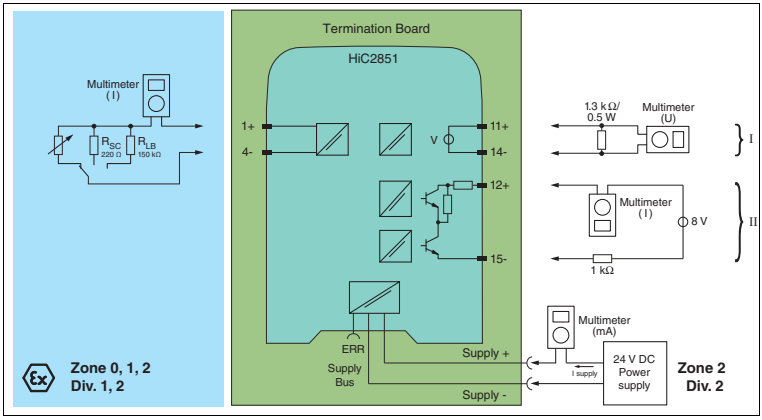

Figure 4.1 Proof test set-up for HiC2851

Tip

Normally the easiest way to test H-System modules is by using a stand-alone HiCTB08-UNI-SC-SC Termination Board. The tester then has no need to disconnect wires in the existing application, so subsequent miswiring of the module is prevented.

5 Abbreviations

DCS	**D**istributed **C**ontrol **S**ystem
ESD	**E**mergency **S**hut**d**own
FIT	**F**ailure **I**n **T**ime in 10^{-9} 1/h
FMEDA	**F**ailure **M**ode, **E**ffects and **D**iagnostics **A**nalysis
λ_{s}	Probability of safe failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{no\ effect}$	Probability of failures of components in the safety path that have no effect on the safety function
$\lambda_{not\ part}$	Probability of failure of components that are not in the safety path
$\lambda_{total\ (safety\ function)}$	Safety function
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
MTTR	**M**ean **T**ime **T**o **R**epair
PFD_{avg}	Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
PTC	**P**roof **T**est **C**overage
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIS	**S**afety **I**nstrumented **S**ystem
T_{proof}	Proof Test Interval
ERR	Error
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

0 2014-11

2014-11

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

For the Pepperl+Fuchs representative
closest to you check www.pepperl-fuchs.com/contact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

DOCT-1594D
11/2014