PROCESS AUTOMATION

SAFETY MANUAL SIL

Switch Amplifier

HiC2853(R2)

SIL

IEC 61508/61511

ISO9001

SIL 3

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"

1 Introduction

1.1 General Information

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

The corresponding datasheets, instruction manuals, EU declarations of conformity, EC-type-examination certificates, certificates, control drawings, and the functional safety assessment if applicable supplement this document. You can find this information under www.pepperl-fuchs.com.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismounting of the device. The personnel must have read and understood the instruction manual.

The device is only approved for appropriate and intended use. Ignoring these instructions will void any warranty and absolve the manufacturer from any liability.

Use the device only with the approved external devices.

In the case of a device fault, proceed as follows:

- Take the device out of operation.
- Secure the device against accidental restart.
- If there is a defect, the device must be repaired by the manufacturer.

If the safety control loop is interrupted, the safety function is no longer guaranteed. This interruption can cause personal injury or property damage.

- Do not de-activate the device.
- Do not bypass the safety function.
- Do not repair, change or maipulate the device.

For more information about functional safety products from Pepperl+Fuchs see www.pepperl-fuchs.com/sil.

1.2 Intended Use

General

This isolated barrier is used for intrinsic safety applications.

The device transfers digital signals (SN/S1N proximity sensors or approved dry contacts) from a hazardous area to a safe area.

Lead breakage (LB) and short circuit (SC) conditions of the control circuit are continuously monitored.

Unlike a SN/S1N series safety sensor, an approved dry contact requires a 10 kΩ resistor to be placed across the contact in addition to a 1.5 kΩ resistor in series.

This device mounts on a HiC Termination Board.

HiC2853

The input controls one 24 V DC active voltage output and one passive transistor output with a resistive output characteristic (acc. to EN 60947-5-6).

The passive transistor output has three defined states: 1-Signal = 1.8 kΩ, 0-Signal = 14 kΩ and fault > 100 kΩ.

HiC2853R2

The input controls one 24 V DC active voltage output and one passive transistor output with a resistive output characteristic.

The passive transistor output has three defined states: 1-Signal = 5 kΩ, 0-Signal = 15 kΩ and fault > 100 kΩ.

1.3 Marking

Pepperl+Fuchs GmbH Lilienthalstraße 200, 68307 Mannheim, Germany

HiC2853
HiC2853R2

Up to SIL3

1.4 Relevant Standards and Directives

Device-specific standards and directives

EMC Directive 2004/108/EC	EN 61326-1:2006, NE 21:2006
Functional safety	IEC 61508 part 1 – 7, edition 2000: Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)

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 dangerous **F**ailure on **D**emand) and the T_1 value (proof test interval that has a direct impact on the PFD_{avg} value)
- 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)

2.2 Assumptions

The following assumptions have been made during the FMEDA:

- The device shall claim less than 10 % of the total failure rate for a SIL 3 safety control loop.
- For a SIL 3 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 SIL 3 application operating in high demand mode 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 device will be used under average industrial ambient conditions, which are comparable with the classification "stationary mounted" in MIL-HDBK-217F. Alternatively, the following ambient conditions are assumed:
  - IEC 60654-1 Class C (sheltered location) with temperature limits in the range of the manufacturer's specifications and an average temperature of 40 ºC over a long period. The humidity level is within manufacturer's rating. For a higher average temperature of 60 ºC, the failure rates must be multiplied by a factor of 2.5 based on experience. A similar factor must be used if frequent temperature fluctuations are expected.
- The safety-related device is considered to be of type **A** element with a hardware fault tolerance of **0**.
- Since the control loop has a hardware fault tolerance of **0** and it is a type **A** element, the SFF must be > 90 % according to table 2 of IEC 61508-2 for a SIL 3 (sub) system.
- Failure rate based on the Siemens standard SN29500.
- Any safe failures that occur (e. g. output in safe state) will be corrected within 8 hours (e. g. remove sensor fault).
- While the device is being repaired, measures must be taken to maintain the safety function (e. g. substitution by a replacement device).
- The indication of a dangerous faulure (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.

2.3 Safety Function and Safe State

Safety Function

The safe state is initiated when the sensor input goes to low current state (I < 2.1 mA) or failure state (I > 5.9 mA).

Safe State

The safe state for the resistive transistor output (output I) is high impedant. The safe state for the electronic output (output II) is de-energized. The safe state will also be achieved if the HiC2853(R2) is not powered. The output II safe state initiated by an input low condition will be reached within 20 ms at 4.7 kΩ load impedance. This mode of operation (output safe state when input low) cannot be changed. This is part of the safety concept of the HiC2853(R2).

Reaction Time

The reaction time for all safety functions is < 20 ms.

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
$\lambda_{\text{no effect}}$	146 FIT	190 FIT
$\lambda_{\text{total (safety function)}}$	334 FIT	337 FIT
λ_{total}	437 FIT	
SFF	99.4 %	99.11 %
MTBF [1]	261 years	
PFH	1.91 x 10^{-9} 1/h	2.99 x 10^{-9} 1/h
PFD_{avg} for T_1 = 1 year	8.37 x 10^{-6}	1.31 x 10^{-5}
T_1 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_1 are taken from the FMEDA report. Observe that PFD and T_1 are related to each other.

The function of the devices has to be checked within the proof test interval (T_1).

3 Safety Instructions

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 lifetime of elements is not exceeded. Beyond this useful lifetime, the result of the probabilistic estimation is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the element itself and its operating conditions – temperature in particular. For example, the electrolytic capacitors can be very sensitive to the operating temperature.

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

Therefore it is obvious that failure calculation is only valid for elements that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each element.

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

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

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

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

- if there are no elements with reduced life time in the safety path (for example electrolytic capacitors, relays, flash memories, optocoupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

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

3.4 Installation and Commissioning

When installing observe the requirements for the safety loop.

Check the safety function to ensure the expected outputs.

When replacing a device, the safety loop must be shut down.

Replace a defective device only by a device of the same type.

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 stated in the "Characteristic Safety Values" (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 resistive transistor 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 voltage output must be activated, voltage level higher than 20 V DC,
- the HiC2853 resistive transistor output must be low impedant (1.8 kΩ ± 10 % at 8.3 V supply voltage),
- the HiC2853R2 resistive transistor output must be low impedant (5 kΩ ± 10 % at 24 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 resistive transistor 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 resistive transistor output is **definitely high impedant** (HiC2853: 14 kΩ ± 10 %/HiC2853R2: 15 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)

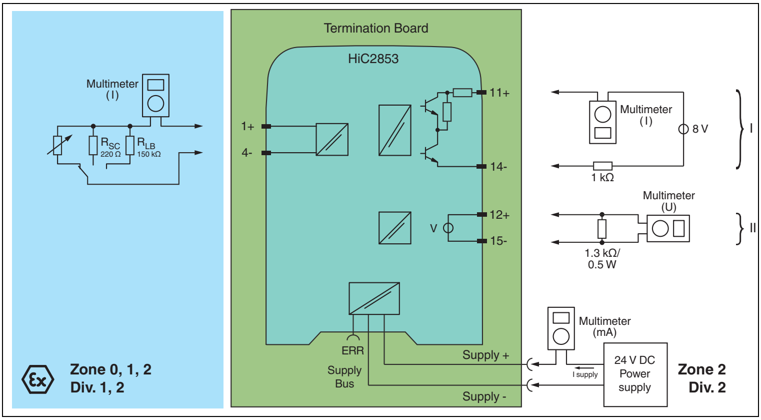

Figure 4.1 Proof test set-up for HiC2853

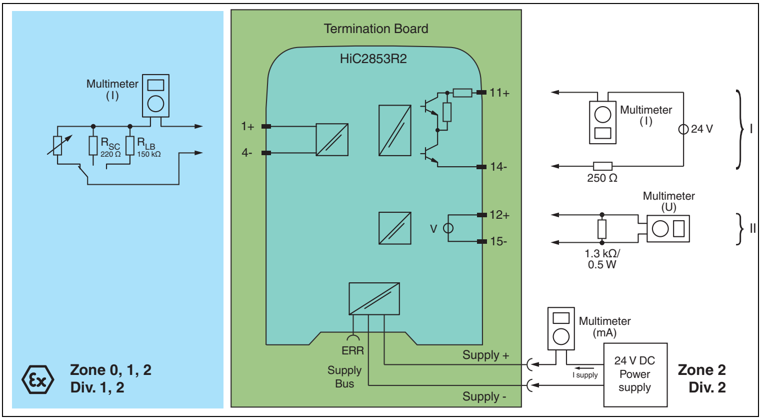

Figure 4.2 Proof test set-up for HiC2853R2

Tip

Normally the easiest way to test HiC modules is by using a stand-alone HiCTB**-SCT-***-**-** termination board. The tester then has no need to disconnect wires in the existing application, so subsequent miswiring of the module is prevented.

5 List of Abbreviations

PCS	**P**rocess **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_{sd}	Probability of safe detected failure
λ_{su}	Probability of safe undetected failure
λ_{d}	Probability of dangerous failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{\text{no effect}}$	Probability of failures of elements in the safety control loop that have no effect on the safety function. The no effect failure is not used for calculation of SFF.
$\lambda_{\text{not part}}$	Probability of failure of elements that are not in the safety control loop
$\lambda_{\text{total (safety function)}}$	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**estoration
PFD$_{avg}$	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
PTC	**P**roof **T**est **C**overage
SC	**S**ystematic **C**apability
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$_1$	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

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

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

DOCT-2418A
11/2015