Functional Safety Whitepaper

Honeywell

Touchpoint Pro Gas Detection System

LEGAL NOTICES

Revision History Table			
Issue	**ECO No**	**Date**	**Comments**
01	A05003	July 2017	

LEGAL NOTICES

Disclaimer

In no event shall Honeywell be liable for any damages or injury of any nature or kind, no matter how caused, that arise from the use of the equipment referred to in this manual.

Strict compliance with the safety procedures set out and referred to in this manual, and extreme care in the use of the equipment, are essential to avoid or minimise the chance of personal injury or damage to the equipment.

The information, figures, illustrations, tables, specifications, and schematics contained in this manual are believed to be correct and accurate as at the date of publication or revision. However, no representation or warranty with respect to such correctness or accuracy is given or implied and Honeywell will not, under any circumstances, be liable to any person or corporation for any loss or damages incurred in connection with the use of this manual.

The information, figures, illustrations, tables, specifications, and schematics contained in this manual are subject to change without notice.

Unauthorised modifications to the gas detection system or its installation are not permitted, as these may give rise to unacceptable health and safety hazards.

Any software forming part of this equipment should be used only for the purposes for which Honeywell supplied it. The user shall undertake no changes, modifications, conversions, translations into another computer language, or copies (except for a necessary backup copy).

In no event shall Honeywell be liable for any equipment malfunction or damages whatsoever, including (without limitation) incidental, direct, indirect, special, and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss, resulting from any violation of the above prohibitions.

Warranty

Honeywell Analytics warrants the Touchpoint Pro system against defective parts and workmanship, and will repair or (at its discretion) replace any components that are or may become defective under proper usage within 12 months from the date of commissioning by a Honeywell Analytics approved representative* or 18 months from shipment from Honeywell Analytics, whichever is sooner.

This warranty does not cover consumables, batteries, fuses, normal wear and tear, or damage caused by accident, abuse, improper installation, unauthorized use, modification or repair, ambient environment, poisons, contaminants or abnormal operating conditions.

This warranty does not apply to sensors or components that are covered under separate warranties, or to any 3rd-party cables and components.

Any claim under the Honeywell Analytics Product Warranty must be made within the warranty period and as soon as reasonably practicable after a defect is discovered. Please contact your local Honeywell Analytics Service representative to register your claim.

This is a summary. For full warranty terms please refer to the Honeywell Analytics' General Statement of Limited Product Warranty, which is available on request.

* A Honeywell Analytics approved representative is a qualified person trained or employed by Honeywell Analytics, or a qualified person trained in accordance with this manual.

Copyright Notice

Find out more at www.honeywellanalytics.com

LEGAL NOTICES

This page deliberately blank.

CONTENTS

Contents

CONTENTS

This page deliberately blank.

INTRODUCTION

1 Introduction

This Touchpoint Pro Safety Whitepaper contains information, examples and instructions to assist readers to design and configure the functional safety case for their Touchpoint Pro gas detection system and associated equipment. Overall responsibility for such equipment lies with the end user.

1.1 References

IEC 61508: *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)*

IEC 61508 has seven parts:

- Parts 1-3 contain the requirements of the standard (normative)
- Parts 4-7 are guidelines and examples for development and are thus informative.

Central to the standard are the concepts of risk and safety function. Risk is a function of the likely frequency of the hazardous event and the likely consequence and severity of an event. The risk can be reduced to a tolerable level by applying safety functions that may consist of E/E/PES and/or other technologies. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PES are covered by the detailed requirements of *IEC 61508*.

2400M2501 *Touchpoint Pro Technical Handbook.*

This manual contains all of the TPPR specifications, approvals, certifications and core technical information. It is intended for use by authorised technical personnel and OEMs, and is available in Technical English only.

2400M2566 *Touchpoint Pro Operating Manual*.

This manual is an abridged and translated version of the TPPR Technical Handbook. It is intended for use by end users and operators.

2400M2568 *Touchpoint Pro Safety Manual*.

This manual outlines the constraints and design guidance that must be adhered to when creating a functional safety system including the Touchpoint Pro gas detection controller.

INTRODUCTION

1.2 Abbreviations

The following abbreviations have been used in this manual:

- AC Alternating Current
- AIM Analogue Input Module
- β Beta Factor – Common Cause Failure Factor for Undetected Dangerous Failures
- β_D Beta Factor – Common Cause Failure Factor for Detected Dangerous Failures
- CCB Control Centre Board (Touchpoint Pro)
- COB Communications Board (Touchpoint Pro)
- DC Direct Current
- D_D Detected Dangerous Failures
- DIM Digital Input Module
- D_u Undetected Dangerous Failures
- I/O Input/Output
- LED Light Emitting Diode
- mA Milliamp
- mV Millivolt
- NC Normally Closed (circuit)
- NO Normally Open (circuit)
- PFD Probability of failure to perform its design function on demand
- PFD_{avg} Probability of failure to perform its design function on demand (Averaged)
- PFH Probability of a dangerous failure per hour
- POST Power On Self-Test
- PSU Power Supply Unit
- ROM Relay Output Module
- SD Secure Digital (memory card)
- SFF Safe Failure Fraction; a percentage of safe failures as compared to all failures
- SIL Safety Integrity Level
- SIS Safety Instrumented Systems
- SPCO Single Pole Change Over (Switch or Relay)
- TPPR Touchpoint Pro Gas Detection System
- UI User Interface
- UPS Uninterruptible Power Supply
- USB Universal Serial Bus

INTRODUCTION

1.3 Definitions

Mean Time to Restoration	The average time for failures of the device to be repaired or otherwise fixed.
Proof Test	A test procedure undertaken to ascertain that the product is operating in an “as new” condition.
Proof Test Interval	The maximum interval allowed between proof tests. A shorter proof test interval will decrease the PFD figure.

EXAMPLES

2 Touchpoint Pro Safety Parameters

The tables below are reproduced from the Touchpoint Pro safety manual but shown here for ease of reference.

Module	PFD Value	PFH Value	SFF	Diagnostic Coverage	β	β_D	D_D	D_U	Safe
4-20mA Input Module	$1.91*10^{-04}$	$4.10*10^{-08}$	97%	96%	2%	1%	1427.11	40.98	460.08
mV Input Module	$1.621*10^{-04}$	$3.41*10^{-08}$	98%	97%	2%	1%	1800.34	34.12	236.54
Digital Input Module	$2.20*10^{-04}$	$4.78*10^{-08}$	95%	94%	2%	1%	1446.12	47.78	196.52
Relay Output Module (Complex)	$1.48*10^{-04}$	$3.20*10^{-08}$	97%	94%	2%	1%	1045.18	31.96	315.13
Relay Output Module (Simple)	$5.53*10^{-04}$	$1.26*10^{-07}$	54%	11%	2%	1%	15.40	126.05	134.98
Control Module (Complex)	$3.08*10^{-04}$	$6.58*10^{-08}$	98%	91%	2%	1%	2256.51	64.66	1144.59
Control Module (Simple)	$1.13*10^{-05}$	$2.64*10^{-09}$	55%	18%	2%	1%	54.20	242.82	241.65

NOTE: Relay Module figures appear twice in the table above. The “complex” entry indicates the common complex portion of the module (assessed as a complex or Type B component in terms of IEC61508). The “simple” entry shows the effect of the simple relay contact portion of the module (assessed as a simple or Type A component in terms of IEC61508). This approach allows the user to determine the effect of using multiple relay contacts (which is required to attain a SIL 2 level for a safety chain). Using only one relay contact will allow the user to construct a SIL 1 safety chain, this meets the needs laid out in IEC61508-2 (see Table 2) that allows a simple or Type A component with a hardware fault tolerance of 0 to achieve SIL 1 with any safe failure fraction. However, two relay contacts must be used in order to reach SIL 2 as this forces a redundant structure (1oo2) that raises the hardware fault tolerance to 1. The same table again shows that in this case SIL 2 can be achieved.

NOTE: Control Module figures appear twice in the table above. The “complex” entry indicates the common complex portion of the module (assessed as a complex or Type B component in terms of IEC61508). The “simple” entry shows the effect of the relay outputs for the System Fault and System Fail relays module (assessed as a simple or Type A component in terms of IEC61508). The “simple” entry values only need to be added to evaluate any safety chain that contains the control module relay outputs (System Fail or System Fault Relay contacts). As the control module internally has a hardware fault tolerance of 1, SIL 2 can be achieved with no further limitations.

The PFD figures quoted above assume a nominal one-year proof test interval and 8-hours mean time to restoration.

Common cause analysis has been undertaken for the Relay contacts (shown above in the “Relay Output Module (Simple)” row). This allows us to give PFD and PFH figures for the use of two relay contacts wired together (see the document 2400M2568 TPPR safety manual for further information) for differing proof test intervals (as it is seen to be a complex procedure for the user to test his output contacts). A similar calculation has been undertaken for the system fail and system fault relays on the control module (although in this case the two relays are wired together internally).

Proof Test Interval	Relay Output Module		Control Module Relays	
	PFD Value	PFH Value	PFD Value	PFH Value
6 Months	$5.64*10^{-06}$	$2.59*10^{-09}$	$5.59*10^{-06}$	$2.58*10^{-09}$
1 Year	$1.15*10^{-05}$	$2.66*10^{-09}$	$1.13*10^{-05}$	$2.64*10^{-09}$
2 Years	$2.37*10^{-05}$	$2.79*10^{-09}$	$2.34*10^{-05}$	$2.77*10^{-09}$
3 Years	$3.67*10^{-05}$	$2.92*10^{-09}$	$3.62*10^{-05}$	$2.89*10^{-09}$
4 Years	$5.05*10^{-05}$	$3.06*10^{-09}$	$5*10^{-05}$	$3*10^{-09}$
5 Years	$6.50*10^{-05}$	$3.19*10^{-09}$	$6.4*10^{-05}$	$3.14*10^{-09}$
7 Years	$9.65*10^{-05}$	$3.46*10^{-09}$	$9.45*10^{-05}$	$3.4*10^{-09}$
10 Years	$1.50*10^{-04}$	$3.86*10^{-09}$	$1.46*10^{-04}$	$3.76*10^{-09}$

EXAMPLES

2.1 Proof Test Interval Effect

The purpose of a proof test is to return the unit to an 'as new' condition in terms of its safety parameters.

The nominal proof test interval is 12 calendar months but, as stated in IEC 61508 and always dependent on local conditions, users may vary the proof test interval to meet their system needs. Honeywell allows such variations provided that the proper calculation method for calculating a proof test interval –as defined in IEC 61508 – is used to attain the required SIL level.

The proof test interval can be altered to fit in with attached equipment or other site considerations. Altering the proof test interval has an effect on the PFD values for the components. The effect of proof test interval on the Relay output module contacts and Control module contacts can be clearly seen in the previous section.

The effect on the PFD for other components can be calculated using the formula below in conjunction with the component information given in the preceding table (and safety manual).

The formulae stated can be found in IEC 61508-6 section B.3.2.2.1

Firstly the channels equivalent mean down time (t_{CE}) must be calculated:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}\,MTTR$$

Once this is known, then the overall PFD can be calculated:

$$PFD_{Overall} = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

For all modules, the MRT and MTTR are fixed at 8 hours. The parameter T_1 is the desired proof test interval. The other parameters can be found in the table from the preceding section. For ease, the PFD values for differing proof test intervals are shown in the table below for all modules:

Proof Test Interval	4-20mA Input Module	mV Input Module	Digital Input Module	Relay Output Module (Complex)	Relay Output Module (Simple)	Control Module (Complex)	Control Module (Simple)
6 Months	$1.00*10^{-04}$	$8.70*10^{-05}$	$1.16*10^{-04}$	$7.84*10^{-05}$	$2.77*10^{-04}$	$1.64*10^{-04}$	$5.59*10^{-06}$
1 Year	$1.91*10^{-04}$	$1.62*10^{-04}$	$2.20*10^{-04}$	$1.48*10^{-04}$	$5.53*10^{-04}$	$3.08*10^{-04}$	$1.13*10^{-05}$
2 Years	$3.70*10^{-04}$	$3.11*10^{-04}$	$4.29*10^{-04}$	$2.88*10^{-04}$	$1.11*10^{-03}$	$5.96*10^{-04}$	$2.34*10^{-05}$
3 Years	$5.50*10^{-04}$	$4.61*10^{-04}$	$6.39*10^{-04}$	$4.28*10^{-04}$	$1.66*10^{-03}$	$8.85*10^{-04}$	$3.62*10^{-05}$
4 Years	$7.30*10^{-04}$	$6.10*10^{-04}$	$8.48*10^{-04}$	$5.68*10^{-04}$	$2.21*10^{-03}$	$1.17*10^{-03}$	$5.00*10^{-05}$
5 Years	$9.09*10^{-04}$	$7.60*10^{-04}$	$1.06*10^{-03}$	$7.08*10^{-04}$	$2.76*10^{-03}$	$1.46*10^{-03}$	$6.40*10^{-05}$
6 Years	$1.09*10^{-03}$	$9.09*10^{-04}$	$1.27*10^{-03}$	$8.48*10^{-04}$	$3.31*10^{-03}$	$1.75*10^{-03}$	$7.88*10^{-05}$
7 Years	$1.27*10^{-03}$	$1.06*10^{-03}$	$1.47*10^{-03}$	$9.88*10^{-04}$	$3.87*10^{-03}$	$2.04*10^{-03}$	$9.45*10^{-05}$
10 Years	$1.81*10^{-03}$	$1.51*10^{-03}$	$2.10*10^{-03}$	$1.41*10^{-03}$	$5.52*10^{-03}$	$2.90*10^{-03}$	$1.46*10^{-04}$

3 Example Safety Chain Calculations

This chapter shows examples of how to calculate the PFD and PFH figures for a given safety chain. It provides guidance to the end user in correctly specifying the safety chains given the different configurations of the TPPR system. This section gives information only on some of the configurations that are possible, but the approach used can be extended to apply to the more complex configurations (1oo3 sensor voting etc) that are realisable with the TPPR system.

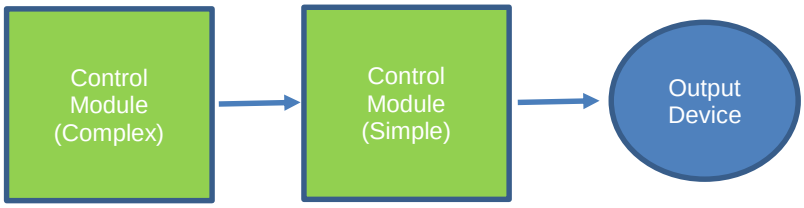
The figures quoted come from the table shown in section 2 of this document as well as excerpted tabular information from *IEC 61508-6*.

These figures represent the PFD and PFH for the Touchpoint Pro controller only. PFD and PFH values for the sensor and output device have to be added to complete the chain.The table below shows how Safety Integrity Level (SIL) is related to the likely frequency of occurrence over a nominal period, and gives probability figures for both low risk (PFD) and high risk (PFH) failures. This table repeats information given in IEC 61508-2.

Safety Integrity Level (SIL)	Low Demand (PFD)	High Demand (PFH)
4	$>10^{-5}$ to $<10^{-4}$	$>10^{-9}$ to $<10^{-8}$
3	$>10^{-4}$ to $<10^{-3}$	$>10^{-8}$ to $<10^{-7}$
2	$>10^{-3}$ to $<10^{-2}$	$>10^{-7}$ to $<10^{-6}$
1	$>10^{-2}$ to $<10^{-1}$	$>10^{-6}$ to $<10^{-5}$

EXAMPLES

3.1 Example for System Fail or System Fault safety chain



The figure above shows the connection of the System Fail or System Fault relay output to a higher level system to inform that system of partial or full impairment of operation. The assumed application is a low demand (PFD) SIL 2 application with a proof test interval of one year for the Control Module and ten years for the relay output.

The elements of the chain can simply be added together (refer to the table in section 2 for numbers used):

Chain elements = Control Module (Complex) + Control Module (Simple)

PFD = $3.08*10^{-4} + 1.46*10^{-04} = 4.54*10^{-4}$

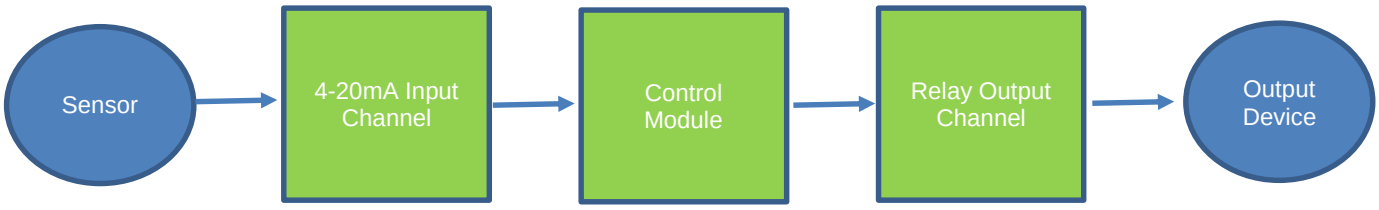
PFD = $4.54*10^{-4}$, which = 4.5% of the SIL 2 Budget

The same chain could also be assessed for high or continuous demand (uses the PFH figure). For that case the PFH figures for each element of the chain are added together (refer to the table in section 2 for numbers used):

PFH = $6.58*10^{-8} + 3.76*10^{-09} = 6.96*10^{-8}$

PFH = $6.96*10^{-8}$, which = 7% of the SIL 2 Budget

3.2 Example for SIL 1 Applications



The figure above shows the use of one input and one output channel all in a 1oo1 configuration. The assumed application is a low demand (PFD) SIL 1 application with a proof test interval of one year.

It is assumed that the Sensor complies to use in a SIL 1 application, and consumes no more than 35% of the SIL 1 budget. Likewise, the Output Device is assumed to consume no more than 50% of the SIL 1 budget.

The elements of the chain can simply be added together (refer to the table in section 2 for numbers used):

Chain elements = 4-20mA Input Module + Control Module (Complex) + Relay Module (Complex) + Relay Module (Simple)

PFD = $1.91*10^{-4} + 3.08*10^{-4} + 1.48*10^{-4} + 5.53*10^{-4} = 1.2*10^{-3}$

PFD = $1.2*10^{-3}$, which = 1.2% of the SIL 1 Budget

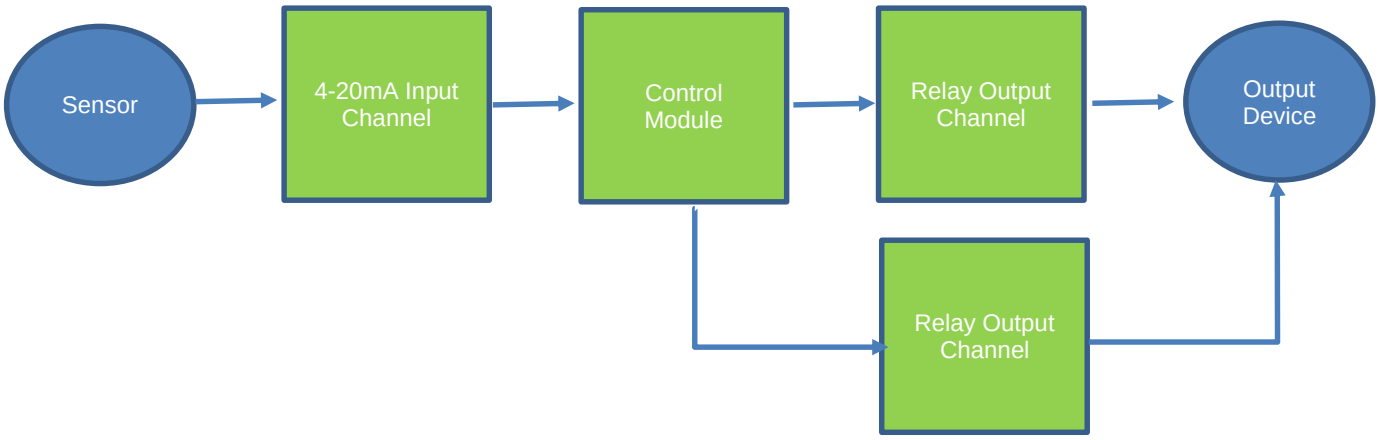
The same chain could also be assessed for high or continuous demand (uses the PFH figure). For that case the PFH figures for each element of the chain are added together (refer to the table in section 2 for numbers used):

PFH = $4.10*10^{-8} + 6.58*10^{-8} + 3.2*10^{-8} + 1.26*10^{-7} = 2.65*10^{-7}$

PFH = $2.65*10^{-7}$, which = 2.7% of the SIL 1 Budget

EXAMPLES

3.3 Example for SIL 2 Applications



The figure above shows the use of one input (in a 1oo1 configuration) and two output channels in a 1oo2 configuration. The assumed application is a low demand (PFD) SIL 2 application with a proof test interval of one year. It is also assumed that the output channels come from the same I/O Module (taking the output channels from two independent I/O modules would reduce the PFD figures further).

It is assumed that the Sensor complies with use in a SIL 2 application, and consumes no more than 35% of the SIL 2 budget. Likewise, the Output Device is assumed to consume no more than 35% of the SIL 2 budget.

The contribution of the 1oo2 architecture of the relay output modules can be estimated using the tables in *IEC 61508-6* (see *Tables B.3 & B.4*).

From the table given in section 2 an appropriate figure can be determined for the use of the two relay contacts. For this example, we are assuming a proof test interval of 10 years, giving a PFD figure of $1.50*10^{-04}$

The elements of the chain can now be added together (refer to the table in section 2 for numbers used):

Chain elements = 4-20mA Input Module + Control Module (Complex) + Relay Module (Complex) + 1oo2 redundant Relay Module (Simple)

PFD = $1.91*10^{-4} + 3.08*10^{-4} + 1.48*10^{-4} + 1.50*10^{-4} = 7.97*10^{-4}$

PFD = $7.97*10^{-4}$, which = 8% of the SIL 2 Budget

The same chain could also be assessed for high or continuous demand (using the PFH figure). For that case the PFH figures for the 1oo2 architecture of the relay output modules needs to be applied. These figures can be seen listed for various proof test intervals in the second table seen in section 2. For this example, we are assuming a proof test interval of 10 years, giving a PFH figure of $3.86*10^{-09}$

The elements of the chain can now be added together (refer to the table in section 2 for numbers used):

PFH = $4.1*10^{-8} + 6.58*10^{-8} + 3.2*10^{-8} + 3.86*10^{-9} = 1.42*10^{-7}$

PFH = $1.42*10^{-7}$, which = 14% of the SIL 2 Budget

Note that this final example assumes that the two relay contacts reside on the same relay module. If two relay channels from different relay modules were used the redundancy effect of using two separate relay modules would reduce the PFH figure accordingly (the effect of this redundancy can be calculated by using the data in the first table in section 2 for the Relay Output Module (Complex) along with the relevant calculations from IEC 61508:2010).

These overall figures could be improved by reducing the proof test interval of the relay contacts which has the effect of decreasing the probability of failure.

EXAMPLES

3.4 Example for Voted SIL 2 Applications

The example below shows two inputs being used in a 1oo2 voting group:

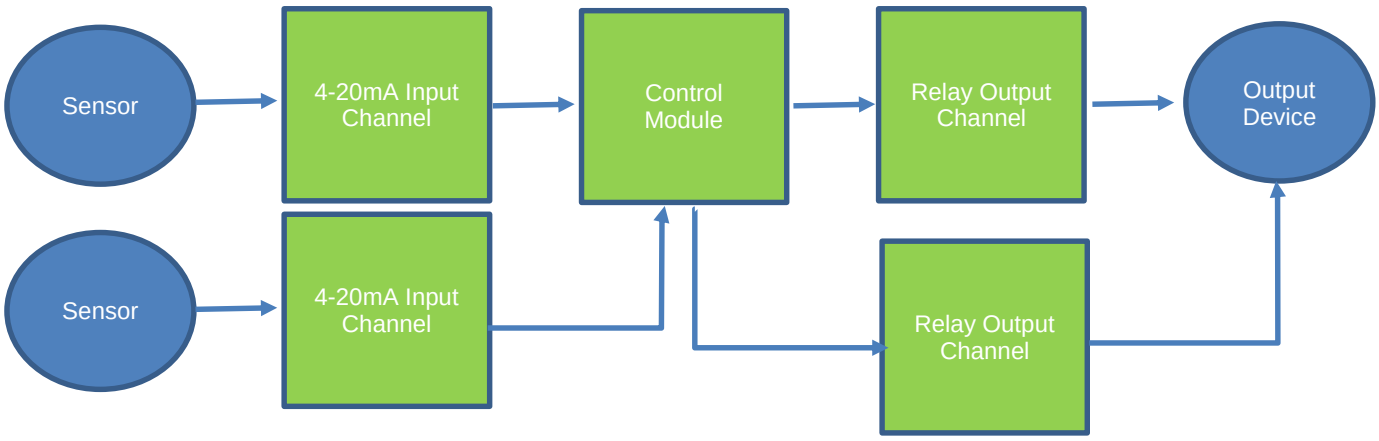


Figure 1. Example 1oo2 – 1oo2 Voting System Configuration for SIL 2

The assumed application is a low demand (PFD) SIL 2 application with a proof test interval of one year.

It is assumed that the two Sensors are identical and comply with use in a SIL 2 application. Likewise, the Output Device is assumed to consume no more than 50% of the SIL 2 budget. It is also assumed that the input and output channels come from the same I/O Module (taking the input or output channels from independent I/O modules would reduce the PFD figures further).

The output stage can be calculated as per the previous example, giving a PFD for the output stage of $1.5*10^{-4}$.

For the input stage, we can see from the table in section 2 that one channel of the mA input has a failure rate per hour (PFH) of $4.10*10^{-8}$ and a diagnostic coverage of 96%. The closest assumption from *Tables B.3* assumes a failure rate per hour of $5*10^{-7}$ or lower. Given this and taking into account the common cause β value, the PFD for the input stage can be seen to be $4.4*10^{-4}$

The elements of the chain can now be added together (refer to the table in section 2 for numbers used):

PFD = $4.4*10^{-4} + 7.5*10^{-4} + 1.5*10^{-4} = 1.34*10^{-3}$

PFD = $1.34*10^{-3}$, which = 13.4% of the SIL 2 Budget

The same chain could also be assessed for high or continuous demand (using the PFH figure). For that case the PFH figures for the 1oo2 architecture of the input modules can be estimated using the tables in *IEC 61508-6:2010* (see *Tables B.13* with the assumption that a proof test of one year is applied).

One channel of the mA input has a failure rate per hour of $4.1*10^{-8}$ and a diagnostic coverage of 96%. The closest assumption from Tables B.13 assumes a failure rate per hour of $2.5*10^{-7}$ or lower. Given this and taking into account the common cause β value, the PFH for the input stage can be seen to be $5.0*10^{-9}$

The output stage can be calculated as per the previous example, giving a PFH for the output stage of $3.86*10^{-9}$ if we assume a proof test interval of 10 years.

The elements of the chain can now be added together (refer to the table in section 2 for numbers used):

PFH = $5.0*10^{-9} + 7.5*10^{-8} + 3.86*10^{-9} = 8.39*10^{-8}$

PFH = $8.39*10^{-8}$, which = 8.4% of the SIL 2 Budget

EXAMPLES

3.5 Examples for a Full Safety Chain

This chapter provides guidance in selecting suitable devices to create a full safety chain.

3.5.1 Example for a Low Demand SIL 2 Application

Given these figures, the remaining SIL budget for a low and high demand SIL 2 application is $9.0*10^{-3}$ / $8.8*10^{-7}$. Assuming that the output device consumes 50% of the SIL 2 budget ($5*10^{-4}$ low demand / $5*10^{-7}$ high demand) and assuming the use of identical input sensors with a proof test interval of one year a maximum PFD value of $8.5*10^{-3}$ can be consumed by the sensors.

The following table excerpt from *IEC 61508-6* can be followed to provide a SIL 2 compliant safety chain:

Individual Sensor PFH	%DC	%β	Achieved PFD
$2.5*10^{-5}$	90	20	$2.3*10^{-3}$
$2.5*10^{-5}$	60	10	$6.6*10^{-3}$
$5*10^{-6}$	0	20	$4.8*10^{-3}$
$5*10^{-6}$	0	2	$1.1*10^{-3}$
$5*10^{-7}$	0	20	$4.4*10^{-4}$
$5*10^{-7}$ or lower	Any	Any	≤ $4.4*10^{-4}$

Table 1. IEC 61508-6:2010 Table B.3

Assume an individual sensor is chosen with a PFH of $2.5*10^{-5}$, a diagnostic coverage of 60% and a β of 10%.

Assume also that an output device with a PFD of 50% of the SIL 2 application is used ($5*10^{-4}$).

The input sensor 1oo2 chain would then be assigned a PFD of $6.6*10^{-3}$ from the table above.

The calculation can then be used as per the previous example:

Sensor 1oo2 Chain + Input module 1oo2 Chain + Logic + Output Module 1oo2 Chain + Output Device.

Or numerically:

System PFD = $6.6*10^{-3}$ + $4.4*10^{-4}$ + $7.5*10^{-4}$ + $1.5*10^{-4}$ + $5*10^{-4}$ = $8.44*10^{-3}$, which = 84% of the SIL 2 Budget.

EXAMPLES

3.5.2 Example for a High Demand SIL 2 Application

The same calculation can be performed for a high demand application. From the calculation given in *Ch.0*, the remaining SIL budget for the high demand application is $8.8*10^{-7}$.

Assuming that the output device consumes 50% of the SIL 2 budget ($5*10^{-7}$), this leaves a budget of $3.8*10^{-7}$ for the combination of input sensors.

The following table excerpt from *IEC 61508-6* can be followed to provide a SIL 2 compliant safety chain:

Individual Sensor PFH	%DC	%β	Achieved PFH
$2.5*10^{-5}$	99	20	$5.0*10^{-8}$
$2.5*10^{-5}$	90	10	$3.0*10^{-7}$
$2.5*10^{-5}$	90	2	$1.0*10^{-7}$
$5*10^{-6}$	60	20	$4.2*10^{-7}$
$5*10^{-6}$	60	10	$2.3*10^{-7}$
$5*10^{-6}$	0	2	$3.1*10^{-7}$
$2.5*10^{-6}$	60	20	$2.1*10^{-7}$
$2.5*10^{-6}$	0	10	$2.9*10^{-7}$
$2.5*10^{-6}$	0	2	$1.0*10^{-7}$
$5*10^{-7}$	60	20	$4.0*10^{-8}$
$5*10^{-7}$	90	20	$1.0*10^{-8}$
$5*10^{-7}$	90	10	$5.0*10^{-9}$
$2.5*10^{-7}$ or lower	Any	Any	$\leq 5.0*10^{-9}$

Table 2. IEC 61508-6:2010 Table B.13

Assume an individual sensor is chosen with a PFH of $2.5*10^{-5}$, a diagnostic coverage of 90% and a β of 10%.

Also assume that an output device with a PFD of 50% of the SIL 2 application is used ($5*10^{-7}$).

The input sensor 1oo2 chain would then be assigned a PFD of $3.0*10^{-7}$ from the table above.

The calculation can then be used as per the previous example:

Sensor 1oo2 Chain + Input module 1oo2 Chain + Logic + Output Module 1oo2 Chain + Output Device

Or numerically:

System PFD = $3.0*10^{-7} + 5.0*10^{-9} + 7.5*10^{-8} + 3.86*10^{-9} + 5*10^{-7} = 8.8*10^{-7}$, which = 88% of the SIL 2 Budget

EXAMPLES

This page deliberately blank.

Find out more at

www.honeywellanalytics.com

Contact Honeywell Analytics:

Europe, Middle East, Africa

Life Safety Distribution GmbH

Javastrasse 2

8604 Hegnau

Switzerland

Tel: +41 (0)44 943 4300

Fax: +41 (0)44 943 4398

gasdetection@honeywell.com

Customer Service

Tel: 00800 333 222 44 (Freephone number)

Tel: +41 44 943 4380 (Alternative number)

Fax: 00800 333 222 55

Middle East Tel: +971 4 450 5800 (Fixed Gas Detection)

Middle East Tel: +971 4 450 5852 (Portable Gas Detection)

Americas

Honeywell Analytics Inc.

405 Barclay Blvd.

Lincolnshire, IL 60069

USA

Tel: +1 847 955 8200

Toll free: +1 800 538 0363

Fax: +1 847 955 8210

detectgas@honeywell.com

Asia Pacific

Honeywell Analytics Asia Pacific

7F SangAm IT Tower,

434 Worldcup Buk-ro, Mapo-gu,

Seoul 03922,

Korea

Tel: +82 (0)2 6909 0300

Fax: +82 (0)2 2025 0328

India Tel: +91 124 4752700

analytics.ap@honeywell.com

Technical Services

EMEA: HAexpert@honeywell.com

US: ha.us.service@honeywell.com

AP: ha.ap.service@honeywell.com

www.honeywell.com

Issue a1_07/2017

2400M2559 A05003