Safety Manual

Honeywell

Touchpoint Pro Gas Detection System

REVISIONS

Revision History

Revision	Comment	Date
Issue 1	A04948	Jan 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

Microsoft, MS and Windows are registered trademarks of Microsoft Corp.

Other brand and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective holders.

Touchpoint is a registered trademark of Honeywell Analytics (HA).

Find out more at www.honeywellanalytics.com

LEGAL NOTICES

This page deliberately blank.

CONTENTS

Contents

1 Introduction 7

1.1 References 7

1.2 Abbreviations 8

1.3 Definitions 9

2 Touchpoint Pro Safety Parameters 10

2.1 Proof Test Interval 11

2.2 Special Conditions for Safety Compliance 12

2.2.1 General / System Conditions 12

2.2.2 Modification Conditions 12

2.2.3 System Input Conditions 12

2.2.4 Relay Output Conditions 13

3 Proof Tests 14

3.1 Controller Proof Tests 14

3.1.1 LED Panel Test 14

3.1.2 Panel Button Test 15

3.1.3 LCD Screen Test 15

3.2 CCB Proof Tests 16

3.2.1 System Relay Test 16

3.2.2 Configuration Settings Test 17

3.2.3 Cause and effect tests 18

3.3 AIM mA Proof Tests 19

3.4 AIM mV Proof Tests 20

3.5 DIM Proof Tests 21

3.6 ROM Proof Tests 22

4 Example Safety Chain Calculations 23

4.1 Example for System Fail or System Fault safety chain 24

4.2 Example for SIL 1 Applications 24

4.3 Example for SIL 2 Applications 25

CONTENTS

This page deliberately blank.

INTRODUCTION

1 Introduction

This Touchpoint Pro Safety Manual contains information, tables, examples and instructions to assist readers to install, commission and perform maintenance that ensure the ongoing safety of the Touchpoint Pro gas detection system.

This manual may be used to calculate the probability of Touchpoint Pro system or component failure (PFD/PFH) for use in risk assessments and other scenarios.

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.

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.

SAFETY PARAMETERS

2 Touchpoint Pro Safety Parameters

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. The “simple” entry shows the effect of the simple relay contact portion of the module. 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.

NOTE: Control Module figures appear twice in the table above. The “complex” entry indicates the common complex portion of the module. The “simple” entry shows the effect of the relay outputs for the System Fault and System Fail relays. 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).

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 also section 2.2.4 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	$1.50*10^{-04}$	$3.86*10^{-09}$	$1.46*10^{-04}$	$3.76*10^{-09}$

INTRODUCTION

2.1 Proof Test Interval

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.

Proof test variations will depend on the system, hardware architectures and applications, and should be reviewed annually.

Given that relay outputs could be complex to isolate and test, the user may determine that a longer proof test interval would be desirable. The table given in section 2 provides the different PFD & PFH values for these differing proof test intervals.

***Note**: The nominal proof test interval should not preclude more frequent maintenance of Touchpoint Pro in accordance with the Operating Instructions if site conditions or other factors require it.*

INTRODUCTION

2.2 Special Conditions for Safety Compliance

2.2.1 General / System Conditions

1. Specification of the Touchpoint Pro system must be carried out using the Honeywell provided power calculator (refer to your Honeywell service representative to obtain this tool). This is to ensure that temperature rise and power dissipation remains within expected and previously observed limits.
2. The notes in the Technical Handbook for installation, operation and maintenance have to be considered.
3. Power Supply Fluctuations are not to exceed DC 18 – 32 V Supply or ±10 % of nominal. A SELV / PELV power supply should be used.
4. All equipment in this manual is rated to 2000 m (6562 ft.) altitude maximum.
5. All rack-mounted enclosures are Equipment Class 1 (grounded) and Installation Category 2.
6. Touchpoint Pro may be the primary or only alarm system in use. Always ensure that risk is identified and alternative arrangements are put in place before carrying out any proof testing, bump testing, or sensor calibrations.
7. The TPPR product performs a full diagnostic self-check every 30 seconds. Hence, in the unlikely event that a fault occurs immediately after the diagnostic has just completed, the indication of this fault could be delayed by up to 30 seconds.
8. The end user must satisfy themselves that the Touchpoint Pro product meets the needs of the targeted safety application. Overall safety validation remains the responsibility of the end user.

2.2.2 Modification Conditions

1. After any modification to the product configuration a verification shall be completed by testing the functionality (a sub-set of the relevant proof tests detailed in section 3.2 can be used to accomplish this)
2. After any firmware or software update to the product a verification shall be completed by testing the functionality and configuration (a sub-set of the relevant proof tests detailed in section 3.2 can be used to accomplish this)

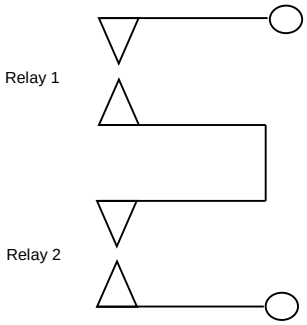
2.2.3 System Input Conditions

1. Any oxygen sensors connected to the product must have both a positive and negative alarm associated with them.
2. All digital inputs used for a safety function must be used in fully supervised mode.
3. Digital inputs used as inputs to a safety chain must be configured so that in normal (non-alarm) conditions the switch / input is closed.
4. Digital inputs used for interaction purposes (inhibit, reset) must be configured so that in normal conditions the switch / input is open.
5. Sensor cables must be protected from mechanical damage [e. g. by using armoured cable].

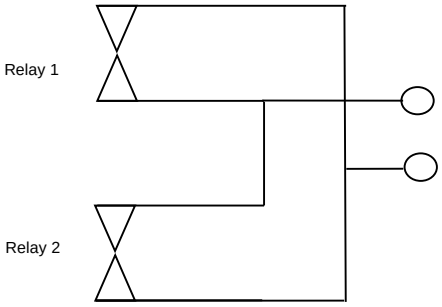
INTRODUCTION

2.2.4 Relay Output Conditions

1. Touchpoint Pro contains relays that may be used to perform executive actions when an alarm is triggered. Ensure that such systems are identified and inhibited / disconnected before carrying out any proof testing, bump testing, or sensor calibrations.
2. Users are expected to configure the cause and effect rules so that all outputs transition to the safe state when a fault is present on the associated inputs. For some specific outputs this may not be desirable hence it is possible to disable this option. In such cases the user is expected to pay close attention to the state of the entire system in the case that a system fault is indicated.
3. The System Fail and System Fault relay outputs are rated for SIL 2 operation.
4. The relay contacts must be protected with a fuse rated at a maximum of 3A. This applies both to the relay contacts from the control module (System Fail and System Fault relays), and the relay contacts from the Relay output modules when used in Configuration 1 as shown in the figure below.
5. The relay output module relays must be energised under normal conditions.
6. Use of one relay contact from a relay output module will allow a SIL 1 rated output to be realised.
7. To realise a SIL 2 rated output, it is mandatory to wire two relay contacts of a relay module together. One of the two configurations shown below can be used. Configuration 1 should be used when an “open contact” represents the activation of the safety function whereas Configuration 2 should be used when a “closed contact” represents the activation of the safety function. Configuration 1 requires the addition of a protective fuse rated at a maximum of 3A to protect the relay contacts from adverse events which may cause contact welding.



Normally Open Contacts
(as labelled on the module)
Configuration 1



Normally Closed Contacts
(as labelled on the module)
Configuration 2

3 Proof Tests

It is recommended that users carry out routine maintenance procedures before carrying out more specific proof tests.

It is recommended that the TPPR system or parts thereof be taken off-line to carry out proof testing in order to avoid false alarms or signalling. Always ensure that a risk assessment is carried out and alternative safety arrangements are put in place during testing.

Remote Units do not include a Controller but still require proof testing of all other components.

The proof tests detailed below use the inbuilt test facilities (test modes) provided by the TPPR controller.

When a test mode is active the **System Fault** relay will normally open and a **Test Mode Fault** will be shown as an **Active Event** on the User Interface, which cannot be reset. The exceptions are the LED Panel Test and LCD screen, which do not indicate a fault.

Once a test mode is active, the system will remain in test mode until the test is exited. The only exception is in the case of a power cycle of the TPPR, when it will restart in normal mode.

Note: After 20 minutes of inactivity the system will logout and return to the **System Status** screen. However it is still running in test mode and you will need to login to complete the tests.

All events generated while the system is in test mode will be logged in the event history.

3.1 Controller Proof Tests

Three main elements should be periodically tested as a part of the HMI controller (LED Panel, Panel Buttons, LCD Screen). The testing for these three elements are detailed in the sub-sections below:

3.1.1 LED Panel Test

Engineer access level is required.

The purpose of this test is to check that the LEDs on the panel are working correctly. This test does not indicate a Fault while in progress.

How to use the LED Panel Test mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select **LED Panel Test**.
6. The system will ask you to confirm, select **OK** to proceed.
7. The system will illuminate all LEDs and then cycle through the LEDs turning each one on in turn.
   Note: The green power LED will remain illuminated throughout if it is working correctly.
8. At the end of the test the system will ask you to confirm the LED test passed.

PROOF TESTING

3.1.2 Panel Button Test

Engineer access level is required.

The purpose of this test is to check that the buttons on the panel are working correctly.

How to use the Panel Button Test mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select **Panel Button Test**.
6. The system will ask you to confirm, select **Yes** to proceed.
7. The system will confirm you are in panel button test mode. Press **OK** to proceed.
8. Follow the on-screen prompts to test the panel buttons
9. At the end of the test the system will display the test results
10. Press **OK**.
11. Select the **Menu** icon:
12. Select Stop panel Button Test.
13. The system will show a confirmation message that it has returned to normal operation.

3.1.3 LCD Screen Test

Engineer access level is required.

The purpose of this test is to check that the LCD screen is working correctly. This test does not indicate a Fault while in progress.

How to use the LCD Screen Test mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select **LCD Screen Test**.
6. The system will display a series of coloured bars and a progress bar.
7. When the progress bar completes the system asks you to confirm the bars were visible
8. Then select **Yes** if the bars were visible and **No** if the screen appears abnormal.

PROOF TESTING

3.2 CCB Proof Tests

The purpose of the Control Centre Board tests are to ensure that the controller holds the correct configuration, executes the expected cause and effect rules and has a fully operational System Fault and System Fail relay output. Tests for each of these areas is detailed in the sub-sections below:

3.2.1 System Relay Test

Engineer access level is required.

The purpose of this test is to check that the System Failure and System Fault relays are working correctly. A multimeter or similar test instrument should be used to check the state of the contacts at various points through the proof test.

Note: It may be necessary to disconnect wiring to higher level systems from TB4 (System Failure) and TB5 (System Fault) on the TPPR controller. This test may cause higher level systems to activate if connected.

How to use the System Relay Test mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select **System Relay Test**.
6. The system will ask you to confirm, select **Yes** to proceed.
7. The system will confirm you are in relay test mode. Press **OK** to proceed.
8. The system will operate the System Fail relay and ask the user to confirm the monitoring applied by the engineer has indicated that the relay has been activated (contacts closed).
9. The system will operate the System Fail relay and ask the user to confirm the monitoring applied by the engineer has indicated that the relay has been deactivated (contacts permanently open with no state switching).

   Note: The System Fail relay will be toggling during this test to ensure that no contacts have welded
10. The system will operate the System Fault relay and ask the user to confirm the monitoring applied by the engineer has indicated that the relay has been activated (contacts closed).
11. The system will operate the System Fault relay and ask the user to confirm the monitoring applied by the engineer has indicated that the relay has been deactivated (contacts permanently open with no state switching).

    Note: The System Fault relay will be toggling during this test to ensure that no contacts have welded.
12. At the end of the test the system will display the test results.
13. Press **OK**.
14. Select the **Menu** icon:
15. Select Stop System Relay Test.
16. The system will show a confirmation message that it has returned to normal operation.
17. Reconnect TB4 and TB5 if necessary.

PROOF TESTING

3.2.2 Configuration Settings Test

This proof test should be run following initial commissioning, after the required periodic interval as well as after any modification to the configured rules (where all affected rulesets should be verified) or after upgrading the firmware of the CCB.

Engineer access level is required.

During this test, all field device inputs will be ignored by the TPPR. The **Cause and Effect** matrix will not be evaluated. No outputs will be generated.

The purpose of this test is to check that input channels are configured correctly, including alarm, warning, fault thresholds etc. The gas concentration and alarm states raised by forcing the input value can be viewed on the TPPR UI or the PC GUI. All configured rules should be tested to ensure the logic in the controller is correct. The system fault relay will be open.

How to use the Configuration Settings Test Mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select Configuration Settings Test.
6. The system will ask you to confirm; select **Yes** to proceed.
7. The system will display a confirmation message, click on **OK** and you will be automatically navigated to the **Inputs** screen.
8. Select the channel to be tested and select **Input Details** from the popup menu.
9. From the **Input Details** screen, select the **Menu** icon:
10. Select Force Value.
11. Enter the gas concentration that you want to simulate. This can include over and under range values.
12. The system will return to the **Input Details** screen, where it will show the simulated gas value as well as any corresponding active events (e.g. Alarm 1).
13. When ready, select the **Menu** icon:
14. Select Clear Force.
15. Repeat steps 9 – 14 as required, completing the channel tests.
16. Return to the **Inputs** screen and repeat steps 8 – 14 for the next channel.
17. When the test is complete, go to the **System Status** screen and select the **Tool Box** icon:
18. Select Diagnostics.
19. Select the **Menu** icon:
20. Select Stop Configuration Settings Test.
21. The system will show a confirmation message that it has returned to normal operation.

WARNING

Check and ensure that the system is restored to normal operation once all testing is finished.

3.2.3 Cause and effect tests

This proof test should be run following initial commissioning, after the required periodic interval as well as after any modification to the configured rules (where all affected rulesets should be verified) or after upgrading the CCB firmware.

Engineer access level is required.

During this test, all field device inputs will be ignored by the TPPR system. The **Cause and Effect** matrix will be evaluated based on simulated input states and outputs will be generated. The system fault relay will be open.

WARNING

During the Cause and Effect Test, **outputs will be generated and relays will be activated**. To avoid any unwanted activation of output devices (e.g. emergency flooding) always inhibit or disable relay activated outputs before starting and remember to enable them when testing is finished.

This test has two purposes:

1. To verify that Cause and Effect matrix configuration is correct by forcing the state of the input channels to various combinations. The activated/de-activated output channels corresponding to the forced state of input channels can be viewed on the TPPR UI or Webserver (if enabled).
2. To check that the output channels are configured correctly, including delay on/off times etc. By forcing the state of the output channel to change the corresponding change in the output device state can be viewed on the TPPR UI or Webserver (if enabled).

When performing this proof test due to modifications made to the system only the modified portions must be re-tested.

This may be limited to test purpose 1 or 2 in this scenario depending on the modifications made.

How to use the Cause and Effect Test Mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select Cause and Effect Test.
6. The system will ask you to confirm, select **Yes** to proceed.
7. The system will display a confirmation message, click on **OK** and you will be automatically navigated to the **Outputs** screen.
8. Select the channel to be tested and select **Output Details** from the popup menu.
9. Select the **Menu** icon:
10. Select **Force Input States** to do a full test of the **Cause and Effect** matrix (test purpose1 described above).
11. The system will display a matrix of all the input channels that are linked to the output channel being tested.
12. Select the input channel states that you want to simulate, and click on **Force**. The cells corresponding to the forced states will be coloured.
13. The system will return to the **Outputs** screen where the results of the forced input states can be viewed.
14. When ready, return to the **Output Details** screen and select the **Menu** icon:
15. Select Clear Force.
16. Repeat steps 8 – 15 for the next channel.
17. To force the output relays (test purpose 2, described above) select the channel to be tested and select **Output Details** from the popup menu.
18. Select the **Menu** icon and select **Force** from the popup menu. The output will now be activated and the result can be verified.
19. When ready, select the channel again, and select **Clear Force**.
20. Repeat steps 17 – 19 for the next channel.
21. When the test is complete. go to the **System Status** screen and select the **Tool Box** icon then **Diagnostics**.
22. Select the **Menu** icon:
23. Select Stop Cause and Effect Test.
24. The system will show a confirmation message that it has returned to normal operation.

WARNING

Check and ensure that the system is restored to normal operation once all testing is finished.

PROOF TESTING

3.3 AIM mA Proof Tests

Engineer access level is required.

During this test, all field device inputs will be displayed, but the **Cause and Effect** matrix will not be evaluated. No outputs will be generated.

The purpose of this test is to check that the input module correctly reports the expected input value. Typically, this can be done either by applying a test gas to the sensor in the field or by forcing the mA output of the sensor to a given value (if the sensor provides such a functionality). The gas concentration and alarm states raised for the channel can then be viewed on the Touchscreen UI or PC GUI. The system fault relay will be open.

The proof test should check that the input reads accurately (+/-10% of full scale value) for a given input value. A minimum of two points throughout the measurement range must be checked per input sensor (for instance, 4mA equating to 0% gas range and 12mA equating to 50% gas range).

How to use the Field Inputs Test mode:

1. Login as an **Engineer**.
2. From the **System Status** screen select the **Tool Box** icon:
3. Select Diagnostics.
4. Select the **Menu** icon:
5. Select Field Inputs Test.
6. The system will ask you to confirm, select **Yes** to proceed.
7. The system will display a confirmation message, click on OK and you will be automatically navigated to the Active Events screen.
8. Proceed with the test of the field devices. To see more detailed information at any time, select the channel of interest and select Input Details from the popup menu.

Note: If the test is done from the **Active Events** screen, the channel of interest will be shown as soon as its state changes, i.e. a threshold alarm is generated. Alternatively, you may wish to work from the Inputs screen (return to System Status screen and select Inputs) by scrolling down to the channel you want.

9. When the test is complete, return to the **System Status** screen and select the **Tool Box** icon:
10. Select Diagnostics.
11. Select the **Menu** icon:
12. Select Stop Field Inputs Test.
13. The system will show a confirmation message that it has returned to normal operation.

WARNING

Check and ensure that the system is restored to normal operation once all testing is finished.

PROOF TESTING

3.4 AIM mV Proof Tests

Engineer access level is required.

During this test, all field device inputs will be displayed, but the **Cause and Effect** matrix will not be evaluated. No outputs will be generated.

The purpose of this test is to check that the input module correctly reports the expected input value. Typically, this can be done either by applying a test gas to the sensor in the field or by forcing the output of the sensor to a given value (if the sensor provides such a functionality). The gas concentration and alarm states raised for the channel can then be viewed on the Touchscreen UI or PC GUI. The system fault relay will be open.

The proof test should check that the input reads accurately (+/-10% of full scale value) for a given input value. A minimum of two points throughout the measurement range must be checked per input sensor (for instance, 0% gas range and 50% gas range).

How to use the Field Inputs Test mode:

14. Login as an **Engineer**.
15. From the **System Status** screen select the **Tool Box** icon:
16. Select Diagnostics.
17. Select the **Menu** icon:
18. Select Field Inputs Test.
19. The system will ask you to confirm, select **Yes** to proceed.
20. The system will display a confirmation message, click on OK and you will be automatically navigated to the Active Events screen.
21. Proceed with the test of the field devices. To see more detailed information at any time, select the channel of interest and select Input Details from the popup menu.

Note: If the test is done from the **Active Events** screen, the channel of interest will be shown as soon as its state changes, i.e. a threshold alarm is generated. Alternatively, you may wish to work from the Inputs screen (return to System Status screen and select Inputs) by scrolling down to the channel you want.

22. When the test is complete, return to the **System Status** screen and select the **Tool Box** icon:
23. Select Diagnostics.
24. Select the **Menu** icon:
25. Select Stop Field Inputs Test.
26. The system will show a confirmation message that it has returned to normal operation.

WARNING

Check and ensure that the system is restored to normal operation once all testing is finished.

PROOF TESTING

3.5 DIM Proof Tests

Engineer access level is required.

During this test, all field device inputs will be displayed, but the **Cause and Effect** matrix will not be evaluated. No outputs will be generated.

The purpose of this test is to check that the input module correctly reports the expected input value. Typically, this can be done either by applying a test gas to the sensor in the field or by forcing the output of the sensor to a given state. Both input open and input closed states should be checked. For digital inputs used for interaction signalling, the input switch can be used to indicate the two states.

How to use the Field Inputs Test mode:

27. Login as an **Engineer**.
28. From the **System Status** screen select the **Tool Box** icon:
29. Select Diagnostics.
30. Select the **Menu** icon:
31. Select Field Inputs Test.
32. The system will ask you to confirm, select **Yes** to proceed.
33. The system will display a confirmation message, click on OK and you will be automatically navigated to the Active Events screen.
34. Proceed with the test of the field devices. To see more detailed information at any time, select the channel of interest and select Input Details from the popup menu.

Note: If the test is done from the **Active Events** screen, the channel of interest will be shown as soon as its state changes, i.e. a threshold alarm is generated. Alternatively, you may wish to work from the Inputs screen (return to System Status screen and select Inputs) by scrolling down to the channel you want.

35. When the test is complete, return to the **System Status** screen and select the **Tool Box** icon:
36. Select Diagnostics.
37. Select the **Menu** icon:
38. Select Stop Field Inputs Test.
39. The system will show a confirmation message that it has returned to normal operation.

WARNING

Check and ensure that the system is restored to normal operation once all testing is finished.

PROOF TESTING

3.6 ROM Proof Tests

Visual inspection of the relay contact wiring should be undertaken to verify that the wiring conforms to the configurations detailed in section 2.2.4 of this document for relay outputs designed to be compliant to SIL 2. This should include inspection to verify that a suitable fuse is present to protect the relay contacts.

The below test method should be repeated for each relay contact. A multimeter or similar test instrument should be used to physically check the state of the contacts at various points through the proof test.

To test the Relay output channels by forcing the relays to a specific state:

1. Login as an **Engineer**. Navigate to the Outputs screen:
   a) From the **System Status** screen select the **Inputs** icon:
   b) Toggle the Inputs Icon to select the **Outputs** icon:
2. Select the channel to be tested, and then select **Force** or **Force Deactivate**, as required. The channel will indicate a Fault until the action is cancelled.
3. When ready, select the channel again, and select **Clear Force** from the popup menu.
4. Repeat steps 4 and 5 for all relay output channels.

Note: The system will indicate a fault and the System Fault relay will open while a Force condition is present.

WARNING

Check and ensure that the system is restored to normal operation once all testing is finished.

EXAMPLES

4 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.

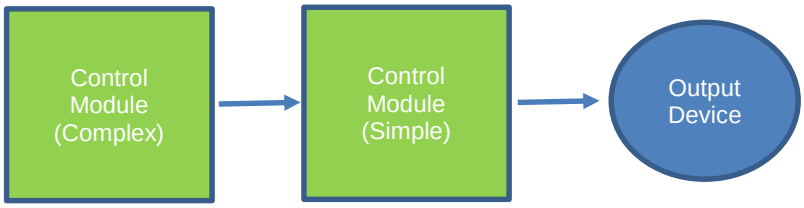
The figures quoted come from the table shown in section 2 of this document as well as excerpted tabular information from *IEC 61508-6*.

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

4.1 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 = $3.08*10^{-4} + 1.46*10^{-04} = 1.46*10^{-4}$

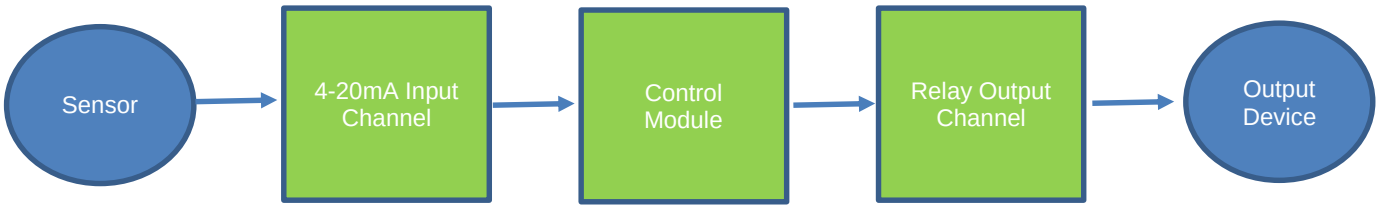
PFD = $1.46*10^{-4}$, which = 1.5% of the SIL 2 Budget

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

4.2 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

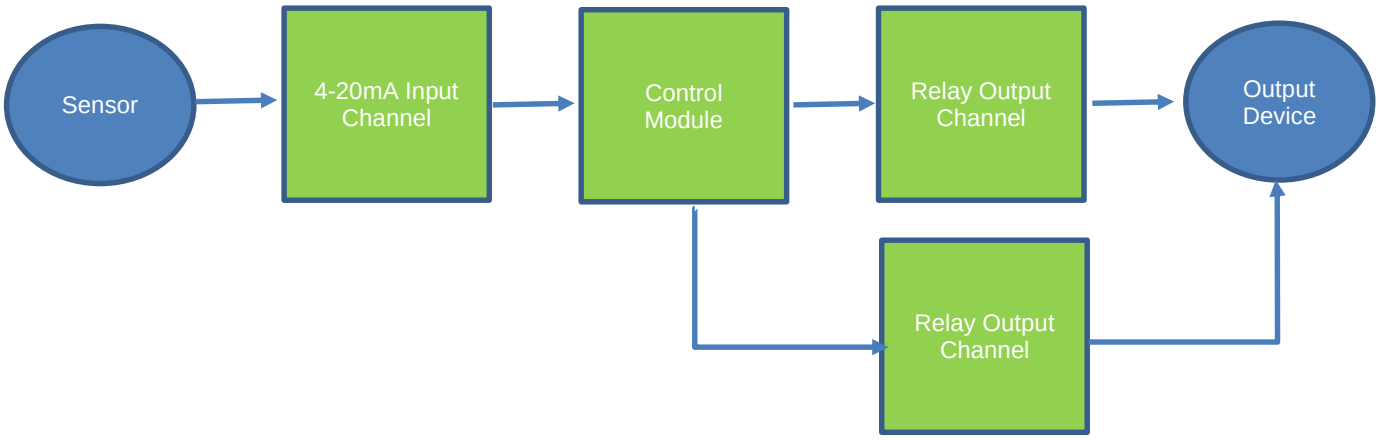
The same chain could also be assessed for high or continuous demand (uses the PFH figure). For that case the PFH figures for each element of the chain are added together (refer to the table in section 2 for numbers used):

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

4.3 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

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

Please Note:

While every effort has been made to ensure accuracy in this publication, no responsibility can be accepted for errors or omissions. Data may change as well as legislation and you are strongly advised to obtain copies of the most recently issued regulations, standards and guidelines. This publication is not intended to form the basis of a contract.

Issue 1_1/2017

2400M2568 A04948

© 2017 Honeywell Analytics