PAC8000
SafetyNet System

Safety Manual

SM8000

Safety Manual

for the

PAC8000 SafetyNet System

Issue 4.2
20th July 2012

Contents

List of Figures

List of Tables

In the text, any wording which is in **bold** has specific meaning within IEC 61508. Further explanations and definitions of these terms can be found in Annex A of this Safety Manual or in IEC 61508 - 4: Definitions and abbreviations.

1 Introduction

This Safety Manual describes the actions that must be taken to use the PAC8000 SafetyNet System in **safety-related** applications.

The actions that are described can be either technical or procedural. For example, a procedural action would be the need to maintain password protection of configuration programs, so that non-approved staff cannot modify these.

This document is limited to those actions that are required to ensure compliance with the relevant safety certifications and standards. Other documents – Instruction Manuals and Datasheets – must be referred to for information outside the scope of this document. These documents may be found on the website www.ge-ip.com.

The Safety Manual is approved and certified by TÜV Rheinland as part of the overall SafetyNet System. Satisfying the requirements it describes is a necessary part of using the SafetyNet System in **safety-related** applications.

Failure to complete the actions described in this document would contravene the certification requirements.

Completing the actions described in this document will only satisfy some of the requirements defined by IEC 61508 for **safety-related** applications. It will be necessary to satisfy the full requirements of IEC 61508 and – for Process Industry applications - the requirements of IEC61511, in order to use the PAC8000 SafetyNet System in **safety-related** applications.

In all cases, it is the responsibility of the end user to ensure that all aspects of the safety-lifecycle are competently implemented.

1.1 Scope

The PAC8000 SafetyNet System is intended for use as part of a **programmable electronic system** as defined by IEC61508. It is suitable for **safety functions** up to **safety integrity level 2** (**SIL2**).

The SafetyNet System employs a "**1oo1D**" (i.e. **1 out of 1 with diagnostics**) architecture to achieve **SIL2**. SafetyNet Controllers may be used in redundant mode to increase system availability, but this is neither required by, nor relevant to, the **safety-related** performance of the system.

Configuring and programming the SafetyNet System must be via a GE Intelligent Platform software program known as the Workbench.

In addition to completing the actions specifically related to the SafetyNet System, it is necessary to satisfy the wider requirements of IEC 61508. This includes such elements within the framework of the **safety lifecycle**, such as **hazard and risk analysis** and defining the **safety requirements specification**. This work must be carried out through appropriate and competent Safety Management procedures and staff.

1.2 Document Structure

This Safety Manual describes the actions that must be taken to use the PAC8000 SafetyNet System in **safety-related** applications. The main sections are as follows:

Section 1 – **Introduction**

Section 2 – **Product Overview**, gives an overview of the PAC8000 product range in general and the PAC8000 SafetyNet products in particular.

Section 3 – **Maintenance Overrides**, describes the implementation of maintenance overrides.

Section 4 - **Peer to Peer Communications between SafetyNet Controllers**, describes the use of SafetyNet P2P, for safety functions distributed across different nodes.

Section 5 – **SafetyNet as Integrated Control and Safety System (ICSS)**, describes how SafetyNet nodes can be used to deliver both control and safety functions from a single node.

Section 6 - **Installation**.

Section 7 - **Suitable Applications**, describes the use of the PAC8000 SafetyNet System in some practical applications.

Section 8 - **Proof Testing**, describes the proof testing that is necessary.

A glossary of terms and abbreviations used within this Safety Manual is given in Appendix A.

A summary of the essential data for safety applications for the PAC8000 SafetyNet System is given in Appendix B.

2 Product Overview

2.1 PAC8000 SafetyNet System

The PAC8000 SafetyNet System uses the same basic structure, and many of the components of the PAC8000 Process Control System. The following components have been specifically developed for use in the SafetyNet System:

- SafetyNet Controller
- ELFD Controller Carrier (for applications that require earth leakage fault detection)
- SafetyNet IO Modules
- Workbench software specifically for use with the SafetyNet System

The data required to establish the suitability of the SafetyNet System for **safety-related** applications is given in the data sheets for each of the SafetyNet components and also in Appendix B of this Safety Manual.

SafetyNet System components and standard components can be used together in certain circumstances – see Section 5. A listing of which components can be used together, and under which circumstances, is maintained at the TÜV website: www.tuvasi.com.

2.2 PAC8000 SafetyNet System Normal and Safe States

Digital Outputs from a SafetyNet DI/DO Module can be configured to be either normally energised or normally de-energised. For both normally energised and normally de-energised, the safe state for outputs is de-energised.

Normally energised outputs are de-energised to their safe state on command or on detection of an internal fault.

Normally de-energised outputs are energised on command (for example to release an extinguishant by opening a normally closed solenoid valve). On detection of an internal fault, however, the outputs will be held in the safe state of de-energised.

2.2.1 PAC8000 SafetyNet System Component Overview

The figure below gives an overview of the role of each element of the PAC8000 SafetyNet System.

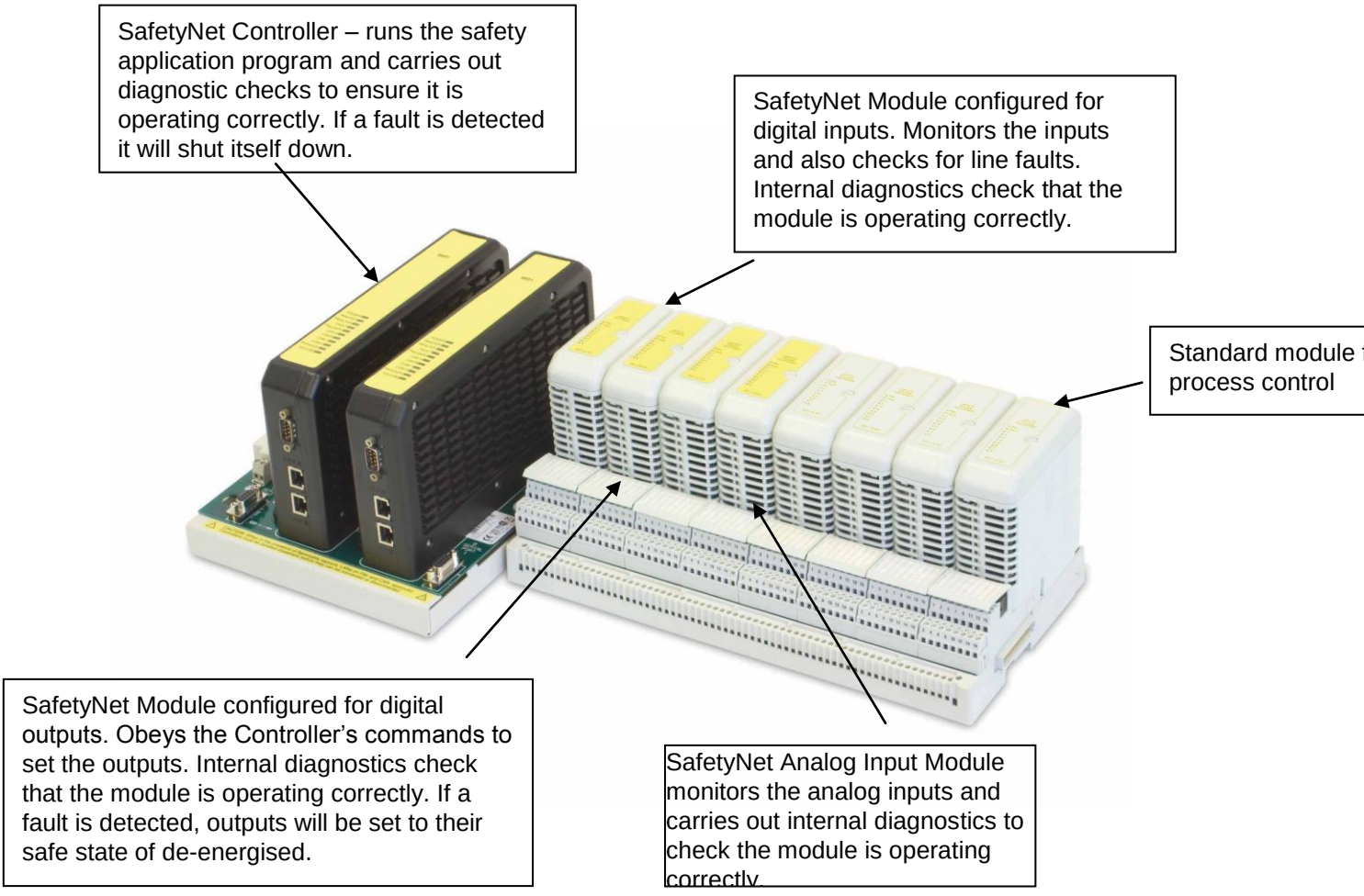


Figure 1 PAC8000 SafetyNet System Component Overview

2.3 PAC8000 SafetyNet Controllers

The 8851-LC-MT SafetyNet Controller shares the same hardware platform as a standard PAC8000 Controller. Safety compliance is assured by constraining the Controller so that it can only perform appropriate operations and adding additional diagnostic software that detects failures and takes appropriate action should errors be detected.

SafetyNet Controllers can be mounted on either the 8751-CA-NS or 8750-CA-NS Controller Carriers. The 8751-CA-NS provides earth-leakage fault detection capability.

If the SafetyNet Controller detects a **dangerous** fault (i.e. one that would prevent the SafetyNet System from carrying out its **safety function**) then it will initiate a controlled shutdown. A controlled shutdown has two objectives – firstly, to ensure that the SafetyNet System enters its failsafe mode (with outputs set to the safe state of de-energised); and secondly, to record sufficient data to allow the reason for the shutdown to be determined.

Only authorised users can change a SafetyNet Controller's configuration and application programmes, and then only under certain conditions. See Section 2.6.2 for further information.

2.3.1 Controlled Shutdown by SafetyNet Controllers

A controlled shutdown involves the following steps:

- All SafetyNet Controller activity that could affect IO Modules is suspended. This leads to the IO Modules entering failsafe mode (loss of communication between the SafetyNet Controller and a SafetyNet IO Module trips the failsafe timer in that module).
- The current System State is saved for subsequent analysis. An event journal and a "reason for failure" message are also saved. This contains details of the fault that triggered the shutdown and time stamp data.
- The Controller main processor is reset. This is done to ensure that – whenever possible – the SafetyNet Controller returns to a state from which fault diagnosis can be carried out.
- Following the processor reset, the configuration, program and cold start data is CRC checked and re-loaded.
- The SafetyNet Controller then enters its "Failed State". Communication with IO Modules is still suspended, as is running of control strategies. Communication over the LAN is limited to certain commands, such as reading the "reason for failure" message.
- A SafetyNet Controller in "Failed State" illuminates both red FAULT and FAILSAFE LED's.

An uncontrolled shutdown is defined as one in which it is not possible to record the event journal and the "reason for failure" message. An uncontrolled shutdown will occur due to a hardware fault or when a hardware watchdog triggers a reset of the processor.

Should the power supply to the SafetyNet Controller fail and then be reinstated, the SafetyNet Controller will enter cold start mode. Cold start re-initialises all data, including IO Module data. (The warm start mode available in the standard Controller is disabled in this case, as a warm start in a state which is not pre-defined is unsuitable for a safety-related application).

The SafetyNet Controller cold start mode has two configurable options – Offline, in which manual intervention is required to bring the SafetyNet Controller online, and Automatic whereby the SafetyNet Controller will automatically come online once the power is restored.

2.3.2 SafetyNet Controller Diagnostic Checks

The SafetyNet Controller automatically carries out a number of diagnostic checks on a continuous basis. All checks are monitored and completed at least once every 5 seconds (i.e. the test is confirmed as being done at least once every 5 seconds). This period is called the **diagnostic test interval**.

The internal, automatic diagnostic tests carried out by the PAC8000 SafetyNet System are sufficient to meet the requirements for use in **SIL2 safety-related** applications, with the exceptions discussed in Sections 2.4.8.9 and 2.6.14. (Proof testing – which is always the responsibility of the user – is discussed in Section 8

2.3.3 Redundant SafetyNet Controllers

When a second Controller is added to introduce redundancy to a SafetyNet node, the new Controller will only operate as a standby once it has confirmed that it has exactly the same firmware (the software embedded in the Controller's microprocessor) and control strategy (the application programme stored in memory) as the master. If a new Controller does not have identical firmware and/or control strategy, then the new Controller will be automatically updated by the master.

When used in redundant mode, SafetyNet Controllers perform the same processing on the same data at the same time. A number of rendezvous points are defined in each cycle – at which the master and slave must arrive within a defined time period and cross check one another's data. Only the master writes to the outputs, but the standby Controller checks that it would have written the same data had it been master. (The exception to this is when the master allows the standby to write the agreed output to confirm that the standby is capable of writing successfully).

A standby Controller will take over from a master if the master fails to arrive at a rendezvous point, or if the master self diagnoses a fault. A standby Controller will report to the master that it is unable to act as a redundant back-up if it self-diagnoses a fault.

Using PAC8000 SafetyNet Controllers in redundant mode will increase their availability, but will have no effect on their ability to perform a **safety-related** function. A SafetyNet node is certified for use as part of a **SIL2** system, whether the Controllers are used in simplex or redundant mode.

When used in Redundant Mode, SafetyNet Controllers cross-check that one Controller is the master and the other is the standby (i.e. anything other than one Controller as master and one as standby is reported as an error, as the two Controllers have not adopted a proper master/standby relationship). If an error is detected, a Controlled Shutdown of both Controllers is initiated.

2.3.4 Downloading New Controller Firmware

When permitted and approved by local operating procedures, new firmware can be downloaded to SafetyNet Controllers from the Workbench.

On-line (i.e. without interrupting the operation of the safety function) download of new Controller firmware can only be carried out where a redundant SafetyNet Controller is available. The new firmware is first downloaded to the standby Controller, and then once it has been verified and the standby Controller has been reset – so as to initiate the new firmware - control can be passed to this Controller. The new firmware can then be downloaded and enabled in the remaining Controller.

To carry out such an on-line download, the SafetyNet Controller must first be in "Configuration Mode" (see Section 2.6.2).

2.3.5 Downloading New SafetyNet Applications

When permitted and approved by local operating procedures, new safety applications can be downloaded to SafetyNet Controllers from the Workbench.

On-line (i.e. without interrupting the operation of the safety function) download of new applications can be carried out with either simplex or redundant SafetyNet Controllers.

When downloading a new application to SafetyNet Controllers, the process takes place as a background task, to minimise the impact on the **response time** of the system. It is necessary to ensure that this does not contravene the limitations imposed by the **process safety time**. Once the new application has been downloaded and checked the Controller will automatically initiate the new application programme.

Downloading a new safety application to redundant SafetyNet Controllers is as for simplex Controllers. The new safety application is simultaneously downloaded to both master and standby Controllers to ensure that they remain in the same state at all times.

To carry out such an on-line download, the SafetyNet Controller must first be in "Configuration Mode" (see Section 2.6.2).

2.4 SafetyNet IO Modules

SafetyNet IO Modules share many of the same attributes as standard 8000 Process IO Modules. They have the same physical form and are connected to the Module Carriers and Field Terminals in the same manner.

They differ from the standard modules in that they perform additional software diagnostic checks and have hardware specifically designed for **safety-related** applications.

2.4.1 IO Module Configuration

SafetyNet IO Modules are configured using the IO Configurator within the Workbench.

When permitted and approved by local operating procedures, new IO Configuration can be downloaded to SafetyNet IO Modules, without interrupting the operation of other SafetyNet IO Modules mounted on the same node.

To carry out such an on-line download, the SafetyNet Controller must first be in “Configuration Mode” (see Section 2.6.2).

2.4.2 LED Indication

Each PAC8000 IO Module features a green LED marked “Pwr”, a red LED marked “Fault” and – typically - a yellow LED for each IO channel marked with the appropriate channel number.

LED's may be on, off, flashing or blinking. An LED is flashing is when it is turned on and off with an equal mark-space ratio. An LED is blinking is when it repeatedly alternates between being on for a short period and then on for a longer period (this is continuous transmission of the letter ‘a’ in Morse code: • —)

The status indication provided by the LED’s is described in Section 2.4.3 and its sub-sections.

2.4.3 Module States

SafetyNet IO Modules can be in one of four “stable” states:

- Running State – the IO module is working normally and reading inputs or writing outputs as required. The module carries out diagnostic tests to ensure that it continues to operate correctly and that it is capable of carrying out the required **safety function**. All valid Railbus commands are accepted.
- Failsafe State – the IO module has been running normally but has either been instructed to enter Failsafe State by the Controller, or the module itself has detected that the Failsafe Timeout has expired. If the module enters the Failsafe State, it will remain there until either the Controller instructs it to return to the Running State, or it is subject to a power cycle.
- Fault State – the IO module has been through a Controlled Shutdown, either because a watchdog timer has expired or because a module hardware fault has been detected.
- Halt State – the IO module has failed to learn its address from the Controller via the Railbus. The IO module is inactive – it does not read or write to the Railbus, it does not read or write to the IO channels and it sets them to their default configuration (which is all channels inactive).

In addition to the states above, the IO Module can be in one of three “transition” states:

- Power Up
- Cold Start
- Controlled Shutdown

IO Module states are described in more detail in the following Sections.

The diagram below shows the transitions between the various IO Module States:

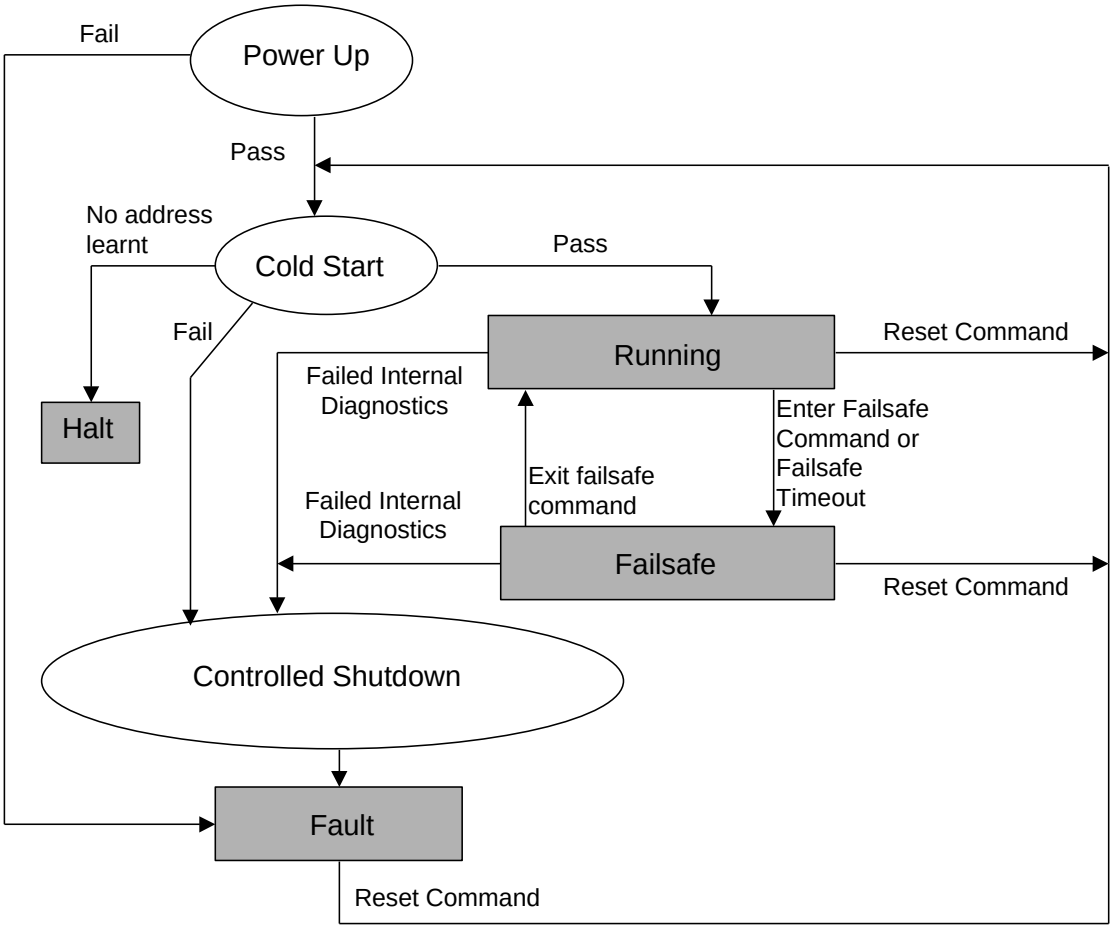


Figure 2 SafetyNet IO Module States and Transitions

The individual steps and states shown in the above diagram are explained in more detail in the following sections.

2.4.3.1 Power Up

Power cycling (removing and re-applying power) the Bussed Field Power supply to a SafetyNet IO Module will cause it to enter 'Power-Up' and subsequent processes, irrespective of the module's state prior to the removal of the power. (For simplicity, these transitions are not shown on the above diagram). Removing power will cause all data stored within the module – IO data, diagnostic, status and any event logs not yet transmitted to the Controller – to be lost.

If a SafetyNet IO Module fails Power Up diagnostic testing, it will enter the Fault State; if it passes it will carry out a Cold Start.

If the SafetyNet IO Modules are mounted in a safe area, they can be power cycled most easily by un-plugging and replacing them. If mounted in a zone 2 hazardous area, their Bussed Field Power supply would anyway need to be isolated before removing the modules.

2.4.3.2 Cold Start

During a Cold Start, the SafetyNet IO Module performs a number of tests and learns its address, before moving on to the Running State. If it fails any of the tests it will move to a Controlled Shutdown. If it fails to learn its address it will enter the Halt State. During the Cold Start the red Fault LED will flash.

2.4.3.3 Halt State

This state is entered if a module has failed to learn its address during a Cold Start. In this state:

- The Red Fault LED blinks (• —)
- The module is inactive; all Railbus commands are ignored, inputs are not scanned, outputs are de-energised and diagnostic tests are suspended.

A module can only exit the Halt State by going through a power cycle (as the module has failed to learn its address, it cannot be addressed and cannot therefore receive commands).

2.4.3.4 Running State

This state is the normal operating state for the module. In this state:

- Input channels are scanned and output channels are written to.
- Railbus is fully active, accepting all valid commands.
- Background diagnostics are running and if a failure is detected, then the module may enter Controlled Shutdown (depending on the type of failure and the way in which the IO Module is programmed to respond to that failure type).
- The yellow LED's indicate the channel status.

2.4.3.5 Failsafe State

This module state will be entered from the Running State either due to loss of communications with the Controller or because the module has received an instruction from the Controller to enter the Failsafe State. In this state:

- The Red Fault LED is lit.
- The Failsafe flag is set.
- All Railbus Write requests are rejected, except instructions to Reset or to exit the Failsafe State.
- Scanning of inputs and HART data is performed.
- Digital outputs are de-energised.
- Background diagnostics are running and if a failure is detected, then the module will enter Controlled Shutdown.

2.4.3.6 Controlled Shutdown

A Controlled Shutdown has two objectives – to take the IO Module to a state from which it can be re-started and to try to store the reason for its failure. Controlled shutdown involves the following steps:

- The Event Log and the Diagnostic Status Register record the reason for the failure.
- The Railbus is enabled to allow the module to re-learn its slot address by communicating with the Master Controller.
- Module training is completed to allow the Controller to communicate with the module.

Following a Controlled Shutdown the IO Module will enter the Fault State.

2.4.3.7 Fault State

The module will enter the Fault State after a Controlled Shutdown. In this state:

- The red Fault LED blinks (• —).
- All Railbus Write requests are rejected (including the instruction to exit Failsafe State), except for instructions to Reset or to receive new firmware.
- All channels are set to inactive (no scanning of inputs is performed, outputs are de-energised)
- Fault State is indicated in the Diagnostic Status Register.

The module can only exit the Fault State by a power cycle or by receiving a Reset command (or firmware download – see Section 2.4.6). The module will enter a cold start when re-starting from the Fault State.

2.4.4 SafetyNet IO Module Failsafe Timeout

SafetyNet IO Modules must be configured to have a suitable failsafe timeout. This can be configured to be between 400ms and 5s. If communication with the master SafetyNet Controller does not take place within the failsafe timeout, then the Module will enter a controlled shutdown.

2.4.5 SafetyNet IO Module Diagnostics

The SafetyNet IO Modules automatically carry out a number of diagnostic checks on a continuous basis. All checks are monitored and completed at least once every 5 seconds (i.e. the test is confirmed as being done as well as being passed at least once every 5 seconds). This period is called the **diagnostic test interval**.

The internal diagnostic tests carried out by SafetyNet IO Modules are sufficient to meet the requirements for use in a SIL 2 safety function. Proof testing – which is the responsibility of the user – is discussed in Section 8

2.4.6 Downloading new IO Module Firmware

When permitted and approved by local operating procedures, new firmware can be downloaded to SafetyNet IO Modules from the Workbench.

During the download of new IO Module firmware, the SafetyNet IO Module will enter failsafe. It is therefore not possible for the SafetyNet System to continue to operate while the download is taking place.

2.4.7 SafetyNet Analogue Input Module

The 8810-HI-TX SafetyNet Analogue Input Module is an 8 channel module for use with 2-, 3- or 4-wire transmitters – which may, or may not, be HART devices. (Note that 3-wire transmitters may only be used which have a specified return current of no more than 25mA). The inputs are suitable for use in **SIL2** applications, using a "**1oo1D**" architecture to meet the requirements for use in **a safety-related** system.

Apart from the diagnostic checks that are carried out in order to meet the safety requirements, the module appears identical in operation to a standard Analogue Input Module with HART.

Detailed information regarding the use of the SafetyNet Analogue Input Module is given in the appropriate data sheets and user documentation. The information given here only relates to the **safety-related** aspects of the module.

2.4.7.1 HART Data

The HART data retrieved by the SafetyNet Analogue Input is defined as "**non-interfering**". That is, it is not data that can be used in the safety application, but its retrieval and transmission (perhaps to a host running an asset management package) by the SafetyNet System does not "interfere" with the required **safety function**.

When HART field instruments are used in a **safety-related** application, particular care must be exercised to ensure that these instruments may not be re-configured by unauthorised or unqualified personnel. Use of the HART instrument's internal hardware and software protection mechanisms and the design of local practices and procedures (for example in the use of hand held configurators) should be given careful consideration.

2.4.7.2 Configuration

Each channel of the module can be configured to:

- be active or inactive
- poll a HART device using HART command 3 to obtain status and process variable data
- apply a number of different filter times
- apply a specified dead zone – beyond which an input value must change before it is reported as new data
- provide high-high, high, low and low-low alarm points and a dead band that must be exceeded before an alarm is cleared

On power up, all Analogue Input Module channels will be inactive and the failsafe timeout will be set to 5s.

When an input channel is configured to be *active*, analogue current values in the range 0 to 25mA are converted to 16-bit digital data every 25ms. The digital data is filtered according to the selected filter time constant and stored ready to be communicated over the Railbus to the Controller. If the value stored differs from the previous value communicated by more than the configured dead zone, then the module's new data flag is set.

When a channel is configured to be *inactive*, the channel's input value is set to zero and all alarms are cleared. If the channel is inactive and configured for HART communication, the HART variables are set to "NaN" and all further HART processing on that channel is disabled.

2.4.7.3 Alarms

If the unfiltered input value exceeds an alarm point, then the appropriate alarm flag is set. When the unfiltered value falls back below the alarm point by the configured dead band, the alarm flag is removed. Setting the low alarms to 0mA and the high alarms to 25mA will disable them. A configurable dead band can be set to prevent alarms being cleared by process noise.

If the high-high and low-low alarms are set to be above 21.0mA and below 3.6mA, then these alarms will operate as specified by NAMUR NE43. The dead band will be ignored and alarms will only be set if the unfiltered input value exceeds the alarm value for more than 4 seconds. The alarms are cleared when the unfiltered input value falls below the alarm point.

Figure 3 shows the operation of alarms with the unfiltered input value.

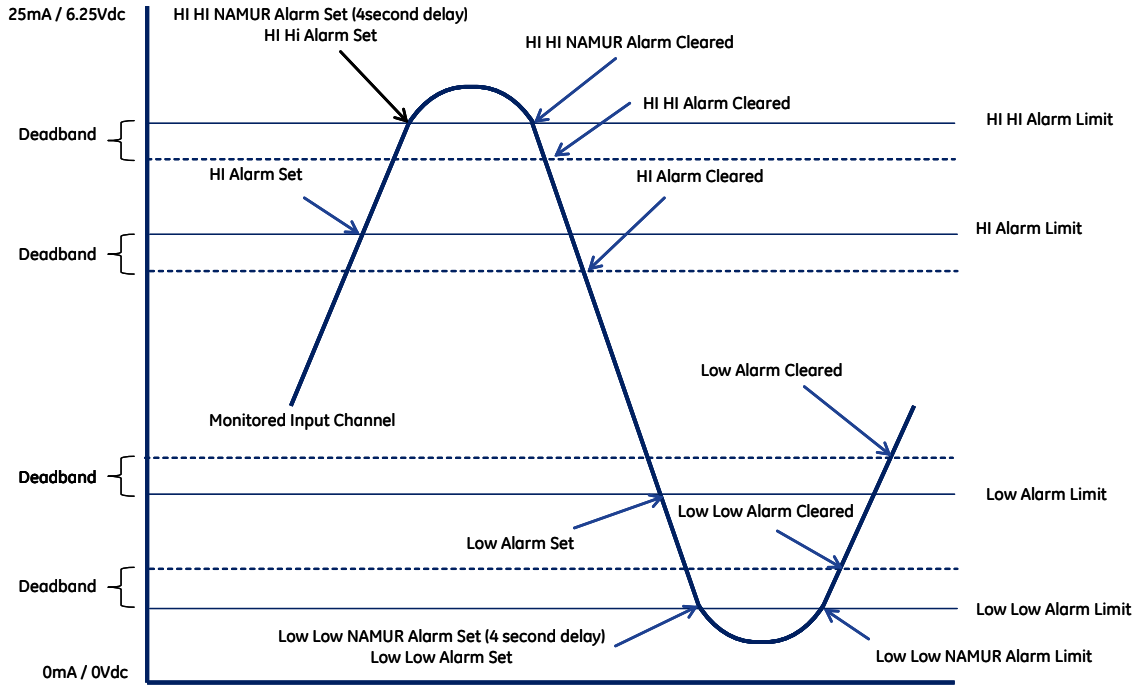


Figure 3 The operation of alarms for the 8810-HI-TX SafetyNet Analogue Input Module

2.4.7.4 Analogue Input Diagnostics

The SafetyNet Analogue Input Module carries out a diagnostic check to confirm the accuracy of the analogue input measurement.

In addition to the primary measurement of the input value, a second diagnostic measurement is made using different internal circuitry. The accuracy of the primary measurement is confirmed by comparing it with the value measured by the diagnostic measurement. The primary measurement is reported as faulty if it differs from the diagnostic measurement value by more than 2%.

The primary measurement circuitry is routinely switched to measure a number of known internal references. The channel is reported as faulty if it reports a value that differs from the internal reference by more than 2%.

If a channel fails either test, it is flagged as faulty and made inactive. It can be made active by a Reset Command or by cycling its power supply. (Note – the module and its other channels will carry on operating normally).

2.4.7.5 Intrinsically Safe Analogue Inputs

If an intrinsically safe field connection is required, an external galvanic isolator (that meets both the hazardous area and functional safety requirements) should be used. Note: IS zener barriers would not normally be suitable for use with 8810 modules as their internal leakage currents could cause measurement errors or earth leakage problems.

2.4.8 SafetyNet Digital Input/Output Module

The 8811-IO-DC SafetyNet Digital IO Module is an 8-channel module, with each channel configurable either as an input, a pulsed output (single or continuous) or as a discrete output. Channels can be further configured to provide a number of modes of operation and fault detection appropriate to the input device or load connected to that channel.

When configured as an input, the channel is suitable for use in **SIL2 safety functions**. The architecture is "**1oo1D**". Line fault detection should normally be enabled*.

When configured as an output, the channel is suitable for use in **SIL2 safety functions**. The architecture is "**1oo1D**", although internally the output stage employs two switches, arranged in series with the load. This provides a level of redundancy (a single switch failure does not prevent the output from de-energising a normally energised load). Line fault detection should normally be enabled for normally de-energised loads*.

*Note: if line fault detection is not enabled, then the installer must establish that the reduction in **diagnostic coverage** is acceptable in the given application.

Detailed information regarding the use of the SafetyNet Digital IO Module is given in the appropriate data sheets and user documentation. The information given here only refers to the **safety-related** aspects of the module.

2.4.8.1 Inactive Digital IO Channels

IO channels can be configured to be "Inactive". When in this state:

- If the channel is configured to be an input, then the input state is set to zero.
- If the channel is configured to be an output, then it is de-energised and the stored Output state (the value returned to the Controller) is set to zero.
- All signal processing for the channel is discontinued, including line fault detection.
- The appropriate channel health flag in the Controller is set to indicate an unhealthy channel – though the channel could well be healthy if it was made active.

2.4.8.2 Digital Input Channel Configuration

A SafetyNet Digital Input channel can be configured as a discrete or latching input. In both of these modes the channel may also be configured to be a pulse counter.

SafetyNet Digital Input channels may also be configured to monitor for earth-leakage faults. A single channel per node is required to implement this, wired to the appropriate terminals of the 8751-CA-NS Controller Carrier. Further information can be found in the relevant Installation Manuals.

A change in the input state only occurs if the states observed at the start and end of the filter time interval are the same. If they are different, the previous state is maintained.

The filter time interval can be configured between 0 and 8 seconds, in 1ms intervals.

Inputs can be configured to "latch" a particular (filtered) input transition – either transitions from 0 to 1, or transitions 1 to 0. The "latch" is cleared by a reset signal from the SafetyNet application program.

Inputs can be configured to count (filtered) input transitions. The counter "wraps round" from 65,535 to 0 without warning. Input transitions are counted even if the channel is configured to latch the input. The counter could be used – for example – to measure that a minimum amount of a particular substance has been added to a chemical reaction, when the reaction would be potentially hazardous without the addition of this minimum amount.

Inputs can be configured to be unsupervised (i.e. with no line-fault-detection enabled), with open-circuit line-fault-detection or open-circuit line-fault-detection *and* short-circuit detection. If line-fault-detection is enabled, the line will be tested at least once every 5s.

2.4.8.3 Digital Input Channel Diagnostics

A number of internal diagnostic tests are carried out on individual channels. If a channel fails any of the tests, it will be flagged as faulty and made inactive. (Note – the module and its other channels will carry on operating normally). The channel can be made active by a Reset Command or by cycling the power supply to the entire module.

2.4.8.4 Digital Input Line Fault Detection

Wherever possible, input channels should be configured for line fault detection –with both open circuit detection and short circuit detection.

For open circuit detection it is necessary to incorporate an end of line (parallel) resistance in to the field wiring, close to the switch. For open and short circuit detection, it is also necessary to incorporate a series resistance in to the field wiring, close to the switch. The diagram below describes this and gives the values for the resistances.

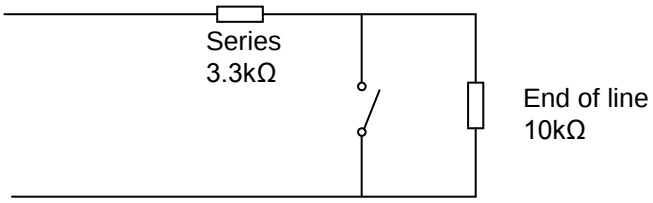


Figure 4 Resistor Values for Line Fault Detection

The table below gives the measured values that are used for reporting open and circuit line faults according to NFPA 72:

Input mode	Unsupervised	Open circuit detect	Open & short circuit detect
NFPA 72 class	Unsupervised	Class B, style B	Class B, style C
Open line (measured as)	-	>45kΩ	>45kΩ
Open contact (measured as)	>8kΩ	8-14kΩ	<14kΩ
Closed contact (measured as)	<5kΩ	<5kΩ	2.5kΩ-5kΩ
Shorted line (measured as)	-	-	<1.4kΩ
End of line resistor	-	10kΩ	10kΩ
Series resistor	-	-	3.3kΩ

Table 1 Measured and Resistor Values for Line Fault Detection with SafetyNet Digital Input channels

2.4.8.5 Digital Output Channel – Single Pulsed Mode Configuration

When configured as a single pulsed mode output, a channel is suitable for use - for example - with agent release solenoids that latch once they have been pulsed. The channel can only be pulsed ON.

The ON time can be configured to be ON for up to 60 seconds in 1ms intervals. Once turned ON, a pulsed mode output may be turned OFF before the configured time by instructing it to turn OFF or by changing the ON time to be shorter.

Outputs can be configured to be unsupervised (i.e. with all fault detection disabled) or to test the channel's output switches and/or to detect line faults.

The option for detecting line faults can be further configured to test for open and/or short circuits, with the short circuit test by either a forward or reverse test current. The correct test configuration depends on the characteristics of the load. The line fault tests are only performed when the channel is OFF.

If any of the fault detection functions are enabled, they will be tested at least once every 5s.

2.4.8.6 Digital Output Channel – Continuous Pulsed Mode Configuration

When configured as a continuous pulsed mode output, a channel is suitable for use - for example - to sound alarms. As different ON-OFF patterns can be generated, the same alarm can be used to indicate different events.

Outputs can be configured to be unsupervised (i.e. with all fault detection disabled) or to test the module's output switches or to detect line faults.

The option for detecting line faults can be further configured to test for open and/or short circuits, with the short circuit test by either a forward or reverse test current, according to the type of load. The line fault tests are only performed when the channel is OFF.

If any of the fault detection functions are enabled, they will be tested at least once every 5s.

2.4.8.7 Digital Output Channel – Discrete Mode Configuration

When configured as a discrete mode output, a channel is suitable for use - for example - with a solenoid valve.

The state of the hardware of an output channel is read back. The result obtained is known as the read-back state and is used to set the stored state. If the read-back state is not the same as the desired output state then the channel fault flag is set.

Outputs can be configured to be unsupervised (i.e. with all fault detection disabled) or to test the module's output switches or to detect line faults.

The option for detecting line faults can be further configured to test for open and/or short circuits, with the short circuit test by either a forward or reverse test current, according to the type of load. The line fault tests are only performed when the channel is OFF.

The output is comprised of two switches arranged in series with the load, such that a single point of failure does not prevent an energised channel from being de-energised. See Section 2.4.8.8 for a more comprehensive discussion of the actions that must be taken in the event of an output switch failure.

2.4.8.8 Output Switch Health Testing

When a channel is configured for switch health testing, a test is performed that detects if either of the pair of switches is stuck open or closed.

The test is carried out by briefly opening or closing each switch and then returning it to its required state. Care must be taken to ensure that the load does not respond to the test switching, which is typically of less than 5ms duration.

If a single switch is stuck, the channel reports this and the application can determine the appropriate action to take. The correct action to take will depend on the nature of the fault and the requirements of the safety function. The table below shows the situations that arise in the event of various switch failure scenarios.

Switch failure mode	**Output Normally**	
	Energised (both switches normally closed)	**De-energised (both switches normally open)**
1 switch stuck open	Output de-energised to safe state by fault	Output cannot be energised
1 switch stuck closed	"Partfail" - output can still be de-energised	"Partfail" - output can still be energised
Both stuck open	Output de-energised to safe state by fault	Output cannot be energised
Both stuck closed	Unsafe – output cannot be de-energised	Output will be energised (but this is not the safe state)

The action that should be taken in each of the scenarios will depend on the particular requirements of the application. The Digital IO Module will report single or dual switch failures and the SafetyNet Logic Application program must be written so as to take the appropriate action – both in terms of operating the safety function (or not) and informing the Operator of the status of the output channel.

2.4.8.9 Digital Output state confirmation

Each output channel has tags allocated to it called "DO Desired" and "DO Echo". The value of "DO Desired" is the state that the SafetyNet Controller has requested. The "DO Echo" value is the state that the SafetyNet IO Module measures on the actual output (the read back value).

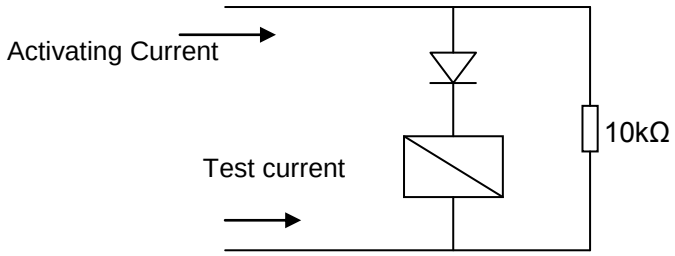
In certain circumstances, the internal diagnostics of the SafetyNet system will fail to detect that the desired value has not been set. (When the diagnostics do detect this, the channel will be set to failsafe). The user must therefore incorporate in to the safety application, a function that compares the requested and actual values of each output channel. If these two values do not agree after a given length of time (significantly longer than the response time of the system, but less than 5 seconds), and the channel has not been set to failsafe, then this indicates a fault with the IO module concerned. The application programme must then take appropriate action.

2.4.8.10 Digital Output Channel Line Fault Detection

Normally de-energised output channels should employ line fault detection – with both open circuit and short circuit detection.

For normally energised outputs open or short circuit line faults will de-energise the load, taking it in to the safe state. Short circuiting a normally energised output will cause the output to cycle OFF and ON as the internal thermal protection is triggered. While ON, several amperes of current may flow through the channel. If the channel remains short circuited, this will be detected by the module and the channel will be disabled and the status reported to the Controller.

For normally de-energised outputs, where the load incorporates a diode to allow for line fault detection using a “reverse” test current, a 10kΩ resistor needs to be wired in parallel with the load, as shown below:



The reverse test current is given by the equation (BFP Voltage) / (20kΩ + R_{FIELD}), where BFP Voltage is the voltage applied to the Bussed Field Power terminals of the IO Module Carrier and R_{FIELD} is the total resistance of the field wiring and instrumentation. The reverse test current is never greater that 1.5mA and is continuous (not pulsed) and always present, even if open- and short-circuit detection is disabled.

The table below gives the measured values that are used for reporting open and short circuit line faults with “reverse” test currents:

Output mode	Open circuit detect	Short circuit detect
Open line (measured as)	>45kΩ	-
Shorted line (measured as)	-	<1.4kΩ
End of line resistor	10kΩ	-
Series resistor	-	Not required

Table 2 Measured and Resistor Values for Line Fault Detection with normally de-energised SafetyNet Digital Output channels – with “reverse” test current

For normally de-energised loads, that do not incorporate a diode to faciliate line fault detection, the measured values used for reporting short circuit line faults can be configured by the user, so that the resistance of the field wiring and the load itself can be taken in to account.

The forward test current is a higher value, pulsed current which can be configured to test field wiring to lower resistance solenoids. Its value is given by the equation (BFP Voltage) / (1200Ω + R_{FIELD}), and it is never greater than 25mA. Before selecting this test, users must check that the test current is insufficient to energise the solenoid.

2.4.8.11 Intrinsically Safe Discrete Inputs and Outputs

If an intrinsically safe field connection is required, an external galvanic isolator (that meets both the hazardous area and functional safety requirements) should be used. Note: IS zener barriers would not normally be suitable for use with 8811 modules as their internal leakage currents could cause measurement errors or earth leakage problems.

2.5 Power Supplies

The SafetyNet System is intended for use with PAC8000 Power Supplies; the 8913-PS-AC to supply the 12V “System” and “Controller” power and the 8914-PS-AC to supply the 24Vdc “Bussed Field Power” from a.c. mains supplies.

Redundant power supplies can be implemented by “pairing” supplies, this is not required for the certified safety integrity level, but will improve availability.

The 8913-PS-AC and 8914-PS-AC power supplies incorporate protection against faults which could cause the output voltage to increase, which could in turn lead to a dangerous failure in the SafetyNet System.

The dangerous undetected failure rates provided for each SafetyNet System component assume that the 8913-PS-AC and the 8914-PS-AC power supplies are used, in which case no additional failure allowance is necessary.

For applications where, in any operating condition, load currents of less than 100mA may be drawn from an 8914-PS-AC power supply, it is recommended that a resistor of 220Ω (rated for 3W) should be wired between the terminals of the 8914-PS-AC. This is to ensure that the power supply can react adequately when required to rapidly supply a significantly higher current demand.

Where ac mains is not available, a 24Vdc supply may be used for the Bussed Field Power supply, if it can be shown to be adequately protected against faults that could cause the supply voltage to exceed 32V.

Such protection may be achieved:

1. if the power source is inherently incapable of producing significant overvoltage, even in the event of a fault, (for example a battery-backed supply), or

2. if the power supply has internal protection with a failure rate similar to that of 8913-PS-AC and the 8914-PS-AC These failure rates are given in appendix B., or

3. if a separate, reliable means of overvoltage protection is fitted between the power source and the SafetyNet system

Any power source used must provide adequate electrical safety protection, for example by complying with the requirements of IEC 61010-1.

It is the user’s responsibility to prove that the levels of protection provided are adequate.

The 12Vdc for System and Controller Power may be generated from a 24Vdc supply that has the overvoltage protection described above, using a 24V/12V converter. (Note, the 24V/12V converter must be of a type that cannot generate an output voltage higher than its input voltage, even under fault conditions. Most buck converters would meet this requirement.)

The BQ2320-9R-EX power supply can provide 24Vdc and 12Vdc outputs from a 24Vdc source, and meets all the above requirements.

For further information regarding the provision of power and arrangements for earthing, refer to the GE Intelligent Platforms Instruction Manual for the 8000 Series Power Supplies".

2.6 Workbench

The PAC8000 Workbench is an engineering tool for configuring parameters and writing control programs (known as Strategies) that will be downloaded to PAC8000 Controllers. Depending on the licences purchased, the Workbench can be used with both standard and/or SafetyNet Systems. Licences for the latter enable special features that are only used when working with SafetyNet Controllers.

This section describes the features of the Workbench applicable to the SafetyNet System – more general information regarding the operation and use of the Workbench can be found in the Workbench training manual.

A summary of Workbench features specific to its use with SafetyNet Systems is given below.

- Two modes of operation are defined for the SafetyNet System: “Configuration Mode”, in which configuration parameters and control strategies can be modified in the Workbench and downloaded to the SafetyNet Controller; and “Safe Mode” in which the SafetyNet Controller is running its control strategy and will not accept modifications.
- Password protection of security access is enhanced to control which personnel are allowed to perform operations related to the safety.
- A Key Switch facility is provided that can be used to further restrict access to safety aspects of each SafetyNet Controller.
- A Trusted Host Table is provided that defines which hosts – i.e. Ethernet LAN drivers - can write to each SafetyNet Controller.
- A “Static Analysis Tool” is included in to the SafetyNet Logic programming environment to capture unsafe or suspect programming structures within the safety application.
- Version management controls are enhanced to ensure compatibility between versions of the Workbench and the SafetyNet Controller firmware and hardware.
- Change control logging and event recording are enhanced within the Workbench and SafetyNet Controllers.

More detailed descriptions of these features are provided in the following sections.

2.6.1 Safe Mode

Safe Mode is the state in which the PAC8000 SafetyNet System is acting as a **safety–related system** and carrying out its **safety functions.** When the system is in this state, it is not possible to make modifications to configuration parameters or control strategies.

This is the normal, running state of the SafetyNet system.

2.6.2 Configuration Mode

Configuration Mode is the same as Safe Mode, except that changes can be made to the configuration parameters and the control programs of the SafetyNet Controller – when in this mode the SafetyNet system is not SIL 2 compliant, though the safety application will still operate.

Instructing the PAC8000 SafetyNet System to leave Safe Mode and enter Configuration Mode – allows the user to make modifications to configuration parameters or control strategies, during which time the **safety function** can still operate.

Configuration Mode can only be entered when the following conditions are met:

- a user designated as having Safety Responsibility enters an appropriate password
- the Key Switch, if one is present, is set to Unlocked.
- the particular instance of the Workbench from which the instructions are being sent is identified in the Trusted Hosts Table.

If this particular Workbench is one of those in the Trusted Hosts Table, then a command button to move between Safe and Configuration Mode is presented to the user. The current status is displayed and the button is used to switch to the other mode.

2.6.3 Workbench Password Protection

Access to the Workbench programming environment is restricted by password protection. Passwords must be a minimum of 6 characters and can be changed at any time by the user.

The Workbench does not provide an automatic log-out facility, whereby access to the Workbench is automatically locked when neither the keyboard nor the mouse has been used within a specified period of time. This must be implemented via the password protection options for the screen saver. If the screen saver protection is triggered then the user must use the screen saver password to re-enter the system. No data is lost when the Workbench is locked and unlocked in this way and the system returns to the exactly the condition it was in when the system became locked.

2.6.4 Security Levels

A number of Security Levels are defined within the Workbench, to restrict access to certain features. Higher levels have access to more features than the levels below.

- Level 0 – Disabled. No access to the Workbench.

- Level 1 – Strategy Viewer. Access limited to running Strategy Viewer. Cannot modify or change the strategy and cannot view any other data.
- Level 2 - Workbench Viewer. Level 1 access, plus the ability to view (as read-only) all data within the Workbench. Can view (but not edit) drawings in the Strategy Builder.
- Level 3 - Workbench Editor. Level 2 access, plus the ability to edit data within the Workbench. Can create new data points, but cannot create or delete projects, controllers, or drawings. Can edit drawings within Strategy Builder and change tuning constants.
- Level 4 - Create/Delete. Level 3 access, plus the ability to create or delete projects, controllers, or drawings.
- Level 5 – Administrator. Full access to all Workbench features. Can run administrative tools and utilities and can reset passwords for all lower levels.

The Administrator defines an access level when the user is created in the Workbench. The user's password gives them access at the given level.

Users from level 3 and higher can optionally be given Safety Responsibility - this will allow them the access defined above for both standard and SafetyNet Controllers. When users at level 3 and level 4 do not have Safety Responsibility they have the access to SafetyNet Controllers defined by level 2 – i.e. can view strategies and data, but cannot change them. Users with Safety Responsibility can switch SafetyNet Controllers between Safe and Configuration Modes.

2.6.5 SafetyNet Controller Password

When a new Controller is added to a project within the Workbench, it may be added as a SafetyNet or a standard Controller. When configuring the IO of a SafetyNet Controller, the user will be given the option to enter a Controller password (this option is not presented for standard Controllers). It is recommended that such passwords are used, but it is not a requirement.

If the password is lost it cannot be recovered (even by a user with Level 5 – Administrator access). The SafetyNet Controller must be reset to clear its memories and re-programmed if the password is lost. This is done using the Network Configurator.

SafetyNet Controller Passwords must be between 6 and 15 characters in length. The password can be changed using the IO Configurator.

2.6.6 Protection by the "Key Switch" Tag

When a SafetyNet Controller is added within the Workbench, the user is given the option of selecting a tag to use as a Key Switch. This can be used – for example – to provide the means by which an Operator can lock the SafetyNet System in Safe Mode, so that taking the system out of this mode can only be done with their awareness and permission.

The Key Switch is assigned from a pull-down list launched by a right mouse click on a SafetyNet Controller icon, where all digital input tags are presented as options for selection. When a particular tag is chosen, its channel health tag is automatically entered as the Key Switch health tag. If the chosen tag does not have an identified health tag, then an additional tag may be selected that will act in this way.

Only users with Safety Responsibility can enter, delete or edit the Key Switch value and its associated health tag.

If a Key Switch is assigned then it must be set to unlocked before any of the following operations can be carried out:

- switching between Safe and Configuration Modes.
- changing the Controller password.
- Downloading application programmes and the Trusted Hosts Table.

The Key Switch is also used in confirming that Maintenance Override instructions can be accepted. See Section 3.2 for more details.

2.6.7 Trusted Hosts

A SafetyNet Controller's Trusted Hosts Table defines which devices on the LAN are allowed to write to that SafetyNet Controller (any LAN entity can read from SafetyNet Controllers). This prevents access to the SafetyNet Controller from unknown or untrustworthy devices.

Trusted Hosts would typically be computers running instances of the Workbench or asset management packages, Remote Modbus Devices and HMI stations. (Note: other Controllers are not included in the Trusted Host Table as they are subject to a different system of authenticity checking).

Each entry in the Trusted Host table consists of the following:

- MAC address of host (LAN A)
- MAC address of host (LAN B for Fault Tolerant Ethernet (FTE) Nodes)
- Modbus writes allowed or not
- Workbench writes allowed or not
- HART pass-through allowed or not
- descriptive name (for use in event logs etc) – optional

To allow Remote Modbus Devices to communicate through the serial ports, COM1 and COM2 can be added as Trusted Hosts.

A user can edit the Trusted Host Table when:

- the user is designated as having Safety Responsibility
- the Key Switch, if one is present, is Unlocked
- the user enters the appropriate SafetyNet Controller password, if one is required

Note: The Trusted Host Table can be edited from any PC on which the Workbench is installed (even one that is not listed in the Trusted Host Table) and while the SafetyNet Controller is in Safe Mode. This is to allow for the situation where the PC running the only instance of the Workbench has failed and a new instance needs to be introduced to bring the SafetyNet Controller out of Safe Mode and in to Configuration Mode.

Note: The Trusted Host Table is designed to prevent unauthorised access via the LAN to which the SafetyNet Controllers are connected. The prevention of unauthorised remote access must also be considered, and features such as network firewalls implemented.

2.6.8 IO Configurator

The 8000 IO Configurator is launched to configure the system hardware (controllers and IO modules). IO modules can be added or deleted and the specific attributes for each module can be configured.

The IO Configurator is launched from within the Workbench.

It is only possible to download an IO Configuration when the SafetyNet Controller is in configuration mode.

2.6.9 Network Configurator

The Network Configurator is a network management tool that is used to assign IP addresses to unconfigured Controllers and show network information for all Controllers on a network. When the utility is launched, the network is queried for all Controllers and those found are presented.

The Network Configurator can be launched from within the Workbench.

Before the Network Configurator is launched, the user will already have entered their username and password and the system will already have identified their Security Level. If the user has Safety Responsibility, then they will be able to write a new Network Configuration to a SafetyNet Controller, provided that:

- the Key Switch, if one is present, is Unlocked
- the SafetyNet Controller is in Configuration Mode
- the user enters the appropriate SafetyNet Controller password, if one is required

2.6.10 SafetyNet Logic Static Analysis Tools

Safety application programs must be analysed before they can be downloaded to the SafetyNet Controller. There are two analysis tools, the Integrity Analyser and the Cross Reference Analyser, which are used as follows:

- the Integrity Analyser validates that the strategy is written in one of the sanctioned languages (LD, ST, FBD) with constructs and instructions that can be easily tested.
- the Cross Reference Analyser lists all changed Programme Organisation Units (POU's) together with any dependent POU's. Users must acknowledge that the list is correct before the strategy can be downloaded to the SafetyNet Controller. (Note a POU is the basic functional element from which the application is built up, for example a function block or a routine).

The Static Analysis Tool is used to detect program structure errors in SafetyNet Logic Control Strategies. The user may decide when to run the tool, but it will not be possible to download a strategy to a SafetyNet Controller that has not passed static analysis.

2.6.11 SafetyNet Logic Differences Utility

Once a strategy is successfully compiled, it can be downloaded to a SafetyNet Controller. A Download Report text file is generated, which can be used to compare different versions of downloads.

At any time the user can generate a Master Tag Xref text report that describes the definition of each tag within a SafetyNet Controller. The Differences Utility can also be used to compare different versions of this report.

2.6.12 Version Management Control

To ensure that the user downloads compatible versions of the control strategy and the various tables associated with that control strategy, it is only possible to download both the tables and the control strategy simultaneously.

Note: “Tables” refers to the data tables that define:

- register initialisation table
- peer-to-peer mapping table
- remote device mapping
- event recording
- register mapping

2.6.13 SafetyNet Controller Change Control Log

The Workbench maintains a Change Control Log that records change messages in a table in the master database. For standard Controllers, this function can be turned off, but for SafetyNet Controllers it cannot. The log can be viewed by executing a LogChangeReport command from the Workbench Report Generator.

A record is made in the Change Control Log when:

- IO Modules are added, deleted, or moved
- Tags are added to, removed from, or moved within an IO Module
- IO Configuration parameters are saved
- Controller IP addresses or node numbers are entered or modified
- external node numbers are entered or modified
- serial communications parameters are entered or modified
- a successful download is made to a Controller
- a strategy is deleted from a Controller
- the Controller password is changed

Note that when a table (such as the Trusted Hosts Table) is saved, a record is kept in the Change Control Log that the save took place. The Change Control Log will not store the full contents of the table – running the Download Report does this.

The Change Control Log will record the date, time, host and the instance of the application used as well as the detail of the change made.

2.6.14 SafetyNet "Strategy Heartbeat"

All SafetyNet application programmes must incorporate a dedicated function block to increment the "Strategy Heartbeat" tag on each application execution cycle. If the tag is not incremented then the SafetyNet Controller will perform a controlled shutdown. It is not possible to download a safety application to a SafetyNet Controller that does not contain a function block to increment the "Strategy Heartbeat".

3 SafeD tags and Maintenance Overrides

Maintenance overrides allow sensors and actuators to be **proof tested** and/or maintained, by temporarily suppressing the normal operation of a **safety function**. The requirements for maintenance overrides must be considered during the specification and design of the safety system – and the implementation must be tested as rigorously as the other elements of the system during acceptance testing.

The maintenance override facility may also be used to meet other requirements – for example to force a system shut-down or to re-start the safety system after a shut-down has taken place and to reset channels that have entered failsafe due to symmetry errors, once the fault has been cleared. (Special tags are provided within the Controller to allow symmetry errors to be cleared).

An example would be using a maintenance override to disable a specific part of the safety logic or to set a particular analogue input to a specific value.

When an override is in place, the safety system is not providing the level of protection that it would normally provide.

The design, test and use of maintenance overrides must be implemented so as to comply with the TÜV draft guideline (Maintenance Override Procedure – see www.tuv-fs.com/modr_3_e.htm) and the requirements specified in this Safety Manual.

The TÜV guideline defines three options for implementing maintenance overrides.

- The safety application is written so that the input from specially defined switches can be used to de-activate the sensors and actuators that are to be maintained.
- A means of electrically isolating sensors and actuators is provided, so that they can be disconnected from the logic solver for maintenance.
- Maintenance overrides are initiated by remote communication with the logic solver. The remote communication – for example – would be from an HMI or DCS.

The third of these options is such that the **logic solver** used to provide the **safety function** must accept the remote communication initiated by the HMI or DCS and take appropriate action to implement the maintenance override. This is in contrast to the first and second options which rely on actions associated with the sensors and actuators (and/or their wiring) to initiate the maintenance override and the implementation does not require anything but the normal operation of the SafetyNet system. The third option requires the SafetyNet system to act in a manner that is unique to the implementation of maintenance override. This Safety Manual therefore gives particular attention to the management of the third option – though the issues raised would apply equally to maintenance override implementations that are not initiated by remote communication with the **logic solver**.

It is recommended that the application should be designed such that a keyswitch must be used to enable the use of maintenance over-rides within the application programme, when these are initiated from the HMI or DCS.

3.1 Impact of Maintenance Override on Safety Function Availability

3.1.1 Probability of Failure on Demand – for Low Demand Mode Applications

If a **safety function** is designed with the intention of carrying out maintenance while the hazard is still present, the effect this will have on the "availability" of the **safety function** must be considered. This is achieved by including an estimate of maintenance down-time in the calculation of the average **probability of failure on demand** (**PFDavg)** for **low demand** applications. (See Section 7.1.4 and IEC 61508-6:2000 Section B.3.2.1 for further information).

3.1.2 Probability of Failure per Hour – for High Demand Mode Applications

For sub-systems that do not employ **hardware fault tolerance**, it is assumed (IEC 61508-6:2000 Section B.3.2.1) that the safety system will immediately place the **EUC** in to a **safe state** on detection of any failure.

For sub-systems that employ **hardware fault tolerance**, and which do not immediately place the **EUC** in to a **safe state** on detection of any failure, the effect that maintenance will have on the "availability" of the **safety function** must be considered. See IEC 61508-6:2000 Section B.3.2.3 for further information.

3.2 Maintenance Overrides Controlled by remote communication

A special mechanism has been developed for implementing maintenance overrides by remote communication with SafetyNet Controllers – typically from an HMI or an Operator screen or from a DCS.

This mechanism allows discrete commands to be communicated from the HMI to the SafetyNet Controller which are used to control the action of safety functions. Since this communication is not SIL 2 compliant, the restrictions defined in the TUV draft guideline (Maintenance Override Procedure – see Section 3 above) are placed on the way this must be implemented. In particular, note that when maintenance overrides are sent via Ethernet, the communication must be via the OPC Server.

The maintenance override function must be written in to the SafetyNet application and tested and approved as an integral part of the application.

There is no limit to the number of maintenance override functions that can be incorporated in to a particular SafetyNet application. Two dedicated tags control each "Override" tag: "Request Override" and "Confirm Override". Once both of these have been correctly set, the application logic associated with the particular maintenance override will be implemented. It will also set the bit in the Overview Status word that indicates that a maintenance override has been implemented (unless this has already been set by a previous maintenance override).

3.2.1 Activating a Maintenance Override by remote cCommunication

A SafetyNet Controller operating in “safe” mode can accept a maintenance override instruction transmitted by remote communication from a host – such as an HMI or a DCS – subject to the following conditions:

- the instruction is sent by a host identified in the Controller’s Trusted Hosts Table.
- the tags to be used are defined in the Controller’s external mapping table to allow writes from external sources and the external node number is enabled (this allows the use of conventional Modbus TCP protocol) OR the communication is Modbus RTU to the Controller’s serial ports OR proprietary “Safe” Modbus TCP via the OPC server to the Controller’s LAN ports.
- the SafetyNet Controller’s Key Switch (if used) is unlocked.

The process for applying the maintenance override is as follows:

- the host writes a “1” to the relevant override “Request” tags .
- the host must then read the associated “Confirm” tags and check that they have been set to "1" by the Controller. Typically the Controller will set these 2 seconds after receiving the override request.
- the host confirms that the override should take place by writing a “0” to the “Confirm” tags within the pre-configured timeout period (default 10 seconds) – and the maintenance override is then implemented. If the host does not carry out this confirmation, then the SafetyNet Controller will automatically re-set the “Request” and “Confirm” tags to “0” and the process of initiating the override must be repeated.

Note: it is not sufficient to write to the “Request” tag and then write to the “Confirm” tag after a suitable delay. The “Confirm” tag must be read between the two write commands.

Once the maintenance override is implemented, the Key Switch should be re-locked to prevent further access to the SafetyNet Controller (any existing overrides remain in place, until the Key Switch is unlocked and they are removed by the appropriate instructions). While the maintenance override is active, the safety function (or functions) that is (or are) affected, will no longer be operating normally.

Further maintenance override instructions may be sent and – if they satisfy the above requirements for trusted hosts, Key Switch and communication exchange – they will be accepted in addition to any maintenance override instructions that are already in place.

3.2.2 Removing a Maintenance Override by remote communication

Removing the maintenance override by remote communication with a host such as an HMI or a DCS is the reverse of the process for setting.

A SafetyNet Controller in “safe” mode can accept an instruction to remove a maintenance override transmitted by serial communication from a host – such as an HMI or a DCS - subject to the following conditions:

- the instruction is sent by a host identified in the Controller’s Trusted Hosts Table.
- the tags to be used are defined in the Controller’s external mapping table to allow writes from external sources and the external node number is enabled (this allows the use of conventional Modbus TCP protocol) OR the communication is Modbus RTU to the Controller’s serial ports OR proprietary “Safe” Modbus TCP via the OPC server to the Controller’s LAN ports.
- the SafetyNet Controller’s “Key Switch” is unlocked.

The process for clearing a maintenance override is as follows:

- the host writes a “0” to the relevant override “Request” tags.
- the host must then read the associated “Confirm” tags and check that they have been set to "1" by the Controller. Typically the Controller will set these 2 seconds after receiving the override request.
- the host confirms that the override should be removed by writing a “0” to the “Confirm” tags within the pre-configured timeout period (default 10 seconds) – and the maintenance override is then removed. If the host does not carry out this confirmation, then the SafetyNet Controller will automatically re-set the “Request” and “Confirm” tags and the process of removing the override must be repeated.

Note: it is not sufficient to write to the “Request” tag and then write to the “Confirm” tag after a suitable delay. The “Confirm” tag must be read between the two write commands.

Once the maintenance override is cleared, the Key Switch should be re-locked to prevent further access to the SafetyNet Controller.

The tags used to set and clear Maintenance Overrides are known as SAFED tags.

It is often useful to confirm that the **safety function** that has been subject to the maintenance override does not immediately trip once the override is removed. To facilitate this, the SafetyNet Controller will report the actual input values from any over-ridden inputs and the application and HMI/DCS displays can be written such that this information can be viewed by the operator prior to removing the override.

3.3 Removing a Maintenance Override using SafetyNet Inputs

By preference, maintenance overrides should be removed by a switch connected to a SafetyNet Digital Input channel – normally set manually by an operator. Different switches can be used to clear particular overrides and/or a switch could be used to clear all overrides from a particular SafetyNet Controller.

The use of such a switch would satisfy the TÜV draft guideline requirement that there should be an “alternative” method of clearing the maintenance override, other than via remote communication.

The application could automatically remove the maintenance override, perhaps after a given time period, but experience has shown that removing them in this way is neither a practical nor a safe approach.

The application can clear the maintenance override by writing a “0” directly to the “Override” tag.

Once the maintenance override is cleared, the bit in the Overview Status word that indicates that a maintenance override has been implemented will also be cleared (unless there are other maintenance overrides still in place).

Note: if a function is required that will “clear all overrides” this can simply be implemented by writing the application so that setting a particular input (perhaps by operating a dedicated push-button) clears all maintenance overrides. This can be designed to operate over a number of SafetyNet Controllers if required.

3.4 Recording Maintenance Override Activity

The TÜV guideline for maintenance override requires that the identity of the person initiating the maintenance override, the time at which it took place, which override was initiated and the time that it was removed should all be recorded – preferably electronically. The SafetyNet System does not support this recording, and if electronic recording is to be implemented, it should be carried out within the host HMI or DCS.

3.5 Additional Measures when using Maintenance Overrides

The TÜV guideline defines the following measures that must or should be adopted during maintenance override:

- the time span for a given override shall be limited to the duration of one operator shift (normally 8 hours) unless hardwired lamps/indicators are provided on the operator console.
- a program in the HMI or DCS host regularly checks that there are no discrepancies between the override requested by the host and that implemented by the SafetyNet System.
- a loss of communication between the HMI or DCS host and the SafetyNet Controller on which the maintenance override is initiated must be indicated to the operator and maintenance engineer. This must be implemented on the HMI or DCS.

3.6 Using SAFED tags to reset a tripped Safety Function

The features of SAFED tags can be useful in re-setting a tripped **safety function**. Once the reason for the trip has been removed, the **safety function** can be reset prior to being brought back on line.

3.7 Using SAFED tags to clear symmetry errors

Symmetry errors occur as a result of field wiring (line) faults or from the failure of the output switch testing of the 8811 module.

Symmetry errors from field wiring faults clear when those faults are repaired.

Symmetry errors caused by failures in the switch health tests are latched.

In certain circumstances field wiring faults can cause the switch health tests to fail (which latches the channel as faulty).

Symmetry errors can be cleared either via the Workbench (Clear Symmetry Error is an option in the Tools menu) or via an HMI using the special “Symmetry” tag, which clears all latched symmetry errors from a particular node. (Note, symmetry errors caused by field wiring faults that are still apparent will not be cleared).

Clearing symmetry errors from the HMI using the “Symmetry Tag” operates in the same way as SAFED tags (a request and confirm cycle must be implemented and communication must be via SAFE Modbus Protocol using the OPC server, or via standard Modbus TCP using the external register mapping table).

4 Peer to Peer communication with PAC8000 Controllers

4.1 SafetyNet data via SafetyNet P2P protocol

SafetyNet P2P is a proprietary Ethernet based protocol used to communicate safe data between SafetyNet controllers on the same network. It can be used to implement SIL 2 safety functions where the input and output are connected to different nodes.

The protocol is based on Modbus TCPIP with additional features to ensure the communication meets the requirements for SIL 2 and the draft standard IEC 61784-3 for safety related communication.

SafetyNet P2P is designed so that if the communication is lost or the communication becomes unacceptably “noisy” this is flagged and users can use this information to design their safety functions appropriately for the particular application.

This is programmed using a tag based “drag and drop” process – with the communication itself being managed automatically by the system.

4.2 Peer to peer communication between PAC8000 Controllers

Non-safety data is transmitted between all types of PAC8000 Controller (including SafetyNet Controllers) via peer-to-peer communication.

This is programmed using a tag based “drag and drop” process – with the communication itself being managed automatically by the system.

5 SafetyNet as an Integrated Control and Safety System (ICSS)

5.1 SafetyNet Controllers with release 1.12 and earlier

A SafetyNet application program for SafetyNet Controllers with release 1.12 or earlier can only read data from other SafetyNet application programs, SafetyNet Controllers or SafetyNet IO Modules. This data is known as “safe data” within the SafetyNet documentation. No other data can be read by the SafetyNet application.

5.2 SafetyNet Controllers with release 1.13 and higher

SafetyNet Controllers with release 1.13 or higher can be used as Integrated Control and Safety Systems.

Non-SafetyNet sources of data such as PAC8000 Controllers, standard IO Modules, 3rd party remote connected Modbus devices and other entities on the Ethernet LAN (such as 3rd party HMI screens, PLC’s and DCS systems) can be used in SafetyNet applications that are also managing SIL 2 safety functions.

All data within the SafetyNet application programme has a label which indicates if it is safe (SafetyNet data) or unsafe (non-SafetyNet data). SafetyNet allows safe data to be written to SafetyNet outputs, but will ensure unsafe data cannot be.

If SafetyNet data is combined with other SafetyNet data (safe with safe) the result is also labelled safe. If unsafe data (non-SafetyNet data) is combined with other unsafe data (unsafe with unsafe) the result is labelled unsafe. However if safe data is combined with unsafe data, the result is labelled as safe.

Combining safe and unsafe data must be done so that the unsafe data could never prevent the correct operation of a safety function. For example safe data can be logically “OR-ed” with unsafe data and this can still be part of the safety function. (When an OR function is used, the unsafe data cannot prevent the correct action of the safety function). When an AND function is used however, the unsafe data *could* prevent the correct action of the safety function, so that this is not allowed.

5.3 SafetyNet Controllers with release 1.31 and higher

SafetyNet Controllers with release 1.31 or higher have an additional feature to simplify the use of SafetyNet as an ICSS. From release 1.31, users can set certain tags to be both import and export. This allows the tag to be written to by the application logic (for example to set an alarm) and also to be written to by an external node (such as an HMI, to clear that same alarm).

5.4 Writing to internal tags via remote communication

When SafetyNet is used as an ICSS, it is often necessary for HMI, DCS or other 3rd party systems to write to tags within the SafetyNet controller - for example, to change the set point of a control PID loop – and to do this while the SafetyNet Controller is in Safe Mode. The tags used are ISG tags.

A special mechanism has been developed for this communication The mechanism is similar to that for SAFE D tags, but has a lower level of protection, as in this case the instruction is being used to modify a control function, whereas maintenance overrides are used to disable safety functions.

A SafetyNet Controller operating in "safe" mode can accept a write transmitted by remote communication from a host – such as an HMI – subject to the following conditions:

- the instruction is sent by a host identified in the Controller's Trusted Hosts Table.
- the setpoint should be accepted following a request and confirm procedure

ISG type tags are used for non-interfering data and can be written to using the default or the external node number, as long as the Discrete control tag mapping form is properly configured to allow the tag import or export rights to the control program. When an ISG type tag is created in Workbench, it must be mapped to a controller using the Discrete Control mapping form and then configured as either import, export, or both, to allow the HMI read\write access to the tag

6 Installation

Installation instructions are found in the instruction manuals for the PAC8000 Process Control Products, which include details specific to the SafetyNet product range.

In common with other PAC8000 products, the SafetyNet product range is IP20. It is necessary to mount the SafetyNet products in a suitable enclosure to provide additional mechanical and ingress protection appropriate to the particular application.

It is recommended that a means of providing ESD (electrostatic discharge) protection during maintenance is provided – such as a point to which a personal ESD wrist strap can be connected. For fire and gas applications according to EN54-2, this is a mandatory requirement.

For applications that require earth-leakage fault detection, the 8751-CA-NS must be used and a single channel of an 8811-IO-DC Digital IO Module must be wired and configured as described in the Instruction Manual INM8100.

7 Suitable Applications

The PAC8000 SafetyNet System can be used to provide **safety functions** up to **Safety Integrity Level 2** (**SIL2**). It can be used in both **low demand** and **high demand** applications.

Typical low demand applications are:

- Fire and Gas protection systems, which monitor for the presence of fire or a release of gas
- Emergency Shut-Down or Process Shut-Down systems that are used to monitor the correct operation of a process and its process control system and which will perform a controlled shut-down if safety limits are exceeded or a dangerous situation is detected
- Burner management systems, which – in combination with a combustion control system – ensure the correct and safe operation of a burner.

In all cases, the **process safety time** must be greater than the **response time** of the **safety function** (i.e. the response time of the PAC8000 SafetyNet System, together with the response times of the sensors and actuators involved in the particular **safety function**).

For high demand applications, the PAC8000 SafetyNet System is restricted in its use by the length of the **diagnostic test interval** (5-seconds). This restricts its use to those applications where the **process safety time** is longer than the 5-second **diagnostic test interval** plus **the fault reaction** time**.** The PAC8000 SafetyNet System will have a **response time** typically in the range of 50 to 200 milliseconds, to which must be added the response time of the input **sensors** and the output **final elements** to give the total **response time**.

7.1 General Application Requirements

7.1.1 Operator Interface

The PAC8000 SafetyNet System will normally be connected to operator interfaces made up of a combination of PC consoles, matrix panels, mimic panels and press switches.

These interfaces allow the operator to monitor the operation of the system and to override the automatic system in some instances (such as to prevent extinguishant release or to manually initiate alarms).

The SafetyNet System will allow detected faults (from line fault monitoring, internal SafetyNet System diagnostics etc.) to be displayed or indicated via the chosen Operator Interfaces according to the application program.

Loss of communication between the HMI and the SafetyNet System should be alarmed in the HMI – for example by a watchdog timer that would detect such a communication loss.

The operator interface can initiate maintenance override functions, but use of this capability is restricted – see Section 3.

7.1.2 Programming Interface

Programming, downloading **safety-related** parameters and programs and switching between operating states is carried out from an engineering workstation running the PAC8000 Workbench.

Access to the Programming Interface shall only be permitted for authorised and suitably qualified personnel. Access must be restricted by the use of passwords (and the options to do this are provided for within the PAC8000 Workbench) and/or some other forms of restricting access, such as safety management procedures or locks and restricted access keys.

The Programming Interface may also be used as the Operator Interface, but its use as a Programming Interface must be restricted as described above.

Programming may be carried out while the safety system is performing **a safety function**, but the system will not be SIL 2 compliant (i.e. the system is not in "Safe" mode, it is in "Configuration" mode).

Instructions for using the Workbench and typical application examples are provided in the "Getting Started Guide".

7.1.3 Hardware Fault Tolerance, Safe Failure Fraction and Sub-system Type

The PAC8000 SafetyNet System is a **Type B** system, with a **hardware fault tolerance** of 0 and a **safe failure fraction** of >90%, it is therefore suitable for use in **safety functions** requiring a **safety integrity level** of 2.

7.1.4 Calculating PFD for Low Demand Applications

This Section gives a basic introduction to calculating the **average probability of failure on demand** (**PFD_{avg}**) for a **safety function** incorporating the PAC8000 SafetyNet System.

The application is a typical pressure relief application – with a transmitter to measure the pressure and a valve that must be opened if the pressure is higher than a specific limit.

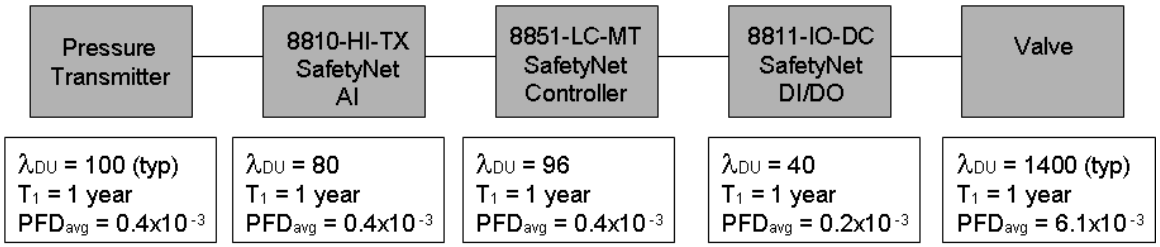
The example is "**low demand**" because the frequency with which the safety function is expected to operate is once a year or less.

For the purpose of this example, the following assumptions have been made:

- all components are certified as suitable for use in **SIL2 safety-related** applications
- all elements are used in **1oo1** arrangements
- the Mean Time to Repair is not considered, as any fault will activate the **safety function** (so the requirement described in Section 3.1.1 does not apply)
- the approximation **PFDavg = 1/2 T_1 λdu** is valid for the **proof test interval** considered

PFD_{avg} for a particular safety function is the sum of the probabilities of the average failure on demand of each element of the system, taking in to account the **proof test interval** of each element.

Figure 5 below includes a pressure transmitter for an input device, an 8810-HI-TX Analogue Input Module, a SafetyNet Controller, an 8811-IO-DC Digital IO Module configured as an output and a valve.



λ_{DU} is failure rate per 10^9 hours, T_p of 1 year = 8760 hours, PFD_{avg} is the probability of dangerous failure

$$PFD_{avg} = \Sigma(_{1/2} * T_1 * \lambda_{DU})$$

Figure 5 Typical Low Demand Application

PFDavg = $0.4 \times 10^{-3} + 0.4 \times 10^{-3} + 0.4 \times 10^{-3} + 0.2 \times 10^{-3} + 6.1 \times 10^{-3} = 7.5 \times 10^{-3}$

Using the table given in the standard, this value would be suitable for a **SIL 2 safety function**. Other conditions (**hardware fault tolerance** and **safe failure fraction**) also allow its use in a **SIL 2** application.

See IEC 61508-6 for a more comprehensive guide to the calculation of **PFDavg**.

7.1.5 Calculating PFH for High Demand Applications

As an example of a high demand application, consider taking the **safety function** for which the final element is now an exhaust valve, and calculate the **probability of dangerous failures per hour** (**PFH**).

The example is "**high demand**" because the frequency with which the safety function is expected to operate is more than once a year (which would not be typical in the process industries).

For the purpose of this example, the following assumptions have been made:

- all components are certified as suitable for use in **SIL2 safety-related** applications
- all elements are used in **1oo1** arrangements
- the Mean Time to Repair is not considered as any fault will trigger the **safety function**

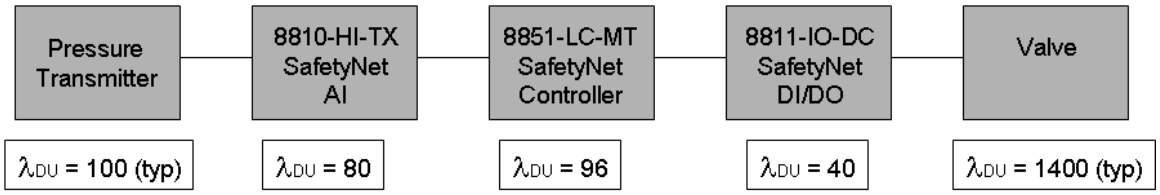


Figure 6 Typical High Demand Application

Adding the individual PFH values gives:

PFH = 100 x 10^{-9} + 80 x 10^{-9} + 96 x 10^{-9} + 40 x 10^{-9} + 1400 x 10^{-9} = 1716 x 10^{-9}

Using the table given in the standard, the **PFH** value of 1716 x 10^{-9} (or 1.7 x 10^{-7}), which is suitable for a **SIL2 safety function**, as is the **hardware fault tolerance** and **safe failure fraction** of each element of the **safety function**.

See IEC 61508-6 for a comprehensive guide to the calculation of **PFH**.

7.1.6 Calculating Response Time

The **response time** of the PAC8000 SafetyNet System (i.e. the time taken from an input transition being detected to an output being asserted), under worst case conditions, can be estimated by the following formulae:

For single SafetyNet Controller systems –

25ms +
4ms x number of IO Modules +
2ms x number of communications links +
30ms if analogue input or 10ms if digital input +
10ms (for digital output)

For redundant SafetyNet Controller systems –

35ms +
4ms x number of modules +
2ms x number of communications links +
30ms if analogue input or 10ms if digital input +
10ms (for digital output)

For example, a node comprising redundant SafetyNet Controllers, 25 IO modules, dual redundant ethernet LANs and a serial interface (a total of 5 communication links) will have response times as calculated below.

For a digital input being switched to a digital output being set:

35ms + 4ms x 25 + 2ms x 5 + 10ms + 10ms = 165ms

For an analogue input – from a trip point being exceeded to a digital output being set:

35ms + 4ms x 25 + 2ms x 5 + 30ms + 10ms = 185ms

The formulae provide only an estimate of the **response time** of the PAC8000 SafetyNet System – the actual response time will vary with each installation and depend on the complexity of the SafetyNet Logic program as well as the number of IO modules. When a system is assembled and the SafetyNet Logic program is downloaded, the system will report the actual response time achieved.

Note – the **process safety time** must be compared with the response time of the entire **safety function**. In addition to the response time of the PAC8000 SafetyNet System, the response time of the input sensors and output actuators must be included.

7.1.7 Diagnostic Test Interval and Fault Reaction Time

For **high demand** applications, the **process safety time** must also be greater than the worst case combination of **diagnostic test interval** and **fault reaction** time for the **safety function**. This is to ensure that if a failure occurs simultaneously in the **EUC Control System** and the **safety function** that the safety system can still prevent the hazardous event from occurring – by detecting the fault and taking appropriate action sufficiently rapidly.

The worst case combination of **diagnostic test interval** and **fault reaction time** will depend on the particular implementation of the **safety function**.

The **diagnostic test interval** for the PAC8000 SafetyNet System is 5 seconds. The **fault reaction** time can be calculated from the **response time** equations in the previous Section.

In practice, the **diagnostic test interval** of the sensor, the SafetyNet System and the final element must all be considered and the worst case scenario established. It is possible that the worst case will be for a fault in any of the different elements and each must be considered.

7.1.8 Applicable Standards

- IEC 61508 7 parts: 1999 - 2002. "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems".
- IEC 61511 3 parts: 2004. "Functional Safety - Safety Instrumented Systems for the Process Sector".
- EN 54-2:1998. "Fire Detection and Fire Alarm Systems Part 2: Control and indicating equipment".
- NFPA 72: 2002. "National Fire Alarm Code".
- EN 50270:1999. "Electromagnetic Compatibility - Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen".
- EN 50130-4:1996 Re-affirmed 2004. "Electromagnetic compatibility- Product family standard: Immunity requirements for components of fire, intruder and social alarm systems".
- IEC 61131-2: 2003. "Programmable controllers, Equipment requirements and tests".
- EN 61326-1: 2005. "Electrical Equipment for Measurement, Control and Laboratory Use – EMC requirements".
- EN 60079-15:2003. "Electrical apparatus for explosive gas atmospheres Part 15: Type of protection 'n'".
- FM 3611: 2004. "Non-incendive Electrical Equipment for use in Class I and II, Division 2, and Class III Divisions 1 and 2, Hazardous (Classified) Locations".
- CSA C22.2 No 213-M1987, Reaffirmed 2004. "Non-incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations".
- ISA-S71.04-1985. "Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants".

7.1.8.1 Burner Management Applications according to NFPA 85

PAC8000 SafetyNet is compliant with the following standard:

- NFPA 85:2004. “Boiler and Combustion Systems Hazards Code”.

This standard makes a particular requirement* - that is not covered elsewhere in this safety manual - that:

- An external watchdog timer is provided (see NFPA 85 part 4.6.3.2.9) which will initiate a master fuel trip for boilers or a duct burner trip for heat recovery steam generators.

A watchdog timer may be implemented in PAC8000 SafetyNet by allocating a discrete output channel to the watchdog function, which is turned ON and OFF by the safety application programme with a time period of less than 1 second. An external device must monitor the pulsing of this output, and if it does not pulse correctly, take the specified action.

7.1.8.2 Burner Management Applications according to IEC 50156

PAC8000 SafetyNet is compliant with the following standard:

- EN 50156-1:2004. “Electrical Equipment for furnaces and ancillary equipment”

This standard makes a particular requirement* - that is not covered elsewhere in this safety manual - that:

- The “interval of operation between two functional tests” is less than or equal to 6 months (see Annex B, “Modes of operation” for “Configuration 1oo1”).

This “functional test” is taken to be the equivalent of a proof test. PAC8000 SafetyNet is here considered to be a 1oo1 configuration, with a “high-grade” diagnostic coverage.

8 Proof Testing

The proof test interval for the PAC8000 SafetyNet System operating in low demand mode will normally be between one and three years, depending on the application. As a minimum, the tests should achieve the following:

- proving that each safety function operates as required.
- checking that digital outputs are neither stuck ON nor stuck OFF.
- calibrating analogue input modules.
- taking the SafetyNet Controller and IO Modules through a power cycle – i.e. turning the power OFF and back ON (this checks the correct operation of the hardware watchdogs, which can only be tested at start-up).

* These requirements are specific to this standard. The requirement need not be met in order to comply with any other standard.

Appendix A – Glossary of terms and abbreviations for IEC61508

Note: where a definition of the term or abbreviation is given in IEC61508-4 “Definitions and abbreviations”, the definition from the standard is given first in quotation marks, followed by further explanation if this is necessary.

1oo1D – a system which has no **hardware fault tolerance** and some level of diagnostic coverage to detect faults.

1oo2D – a system which has a **hardware fault tolerance** of “one” and some level of diagnostic coverage to detect faults.

Average probability of failure of protection on demand – or **PFDavg** is the probability that a safety system will be unable to carry out its required **safety function** when a hazardous situation arises and a **demand** – in other words a request for the safety function to act – occurs. This probability is used to determine the suitability of safety systems in **low demand** applications. The value of **PFDavg** of a particular element within the safety system is determined by its dangerous undetected failure rate, combined with the length of time between **proof tests**. As defined by the standard, it is “the safety integrity failure measure for **safety-related** protection systems operating in **low demand** mode”

Continuous mode – also known as **high demand**. A **safety function** for **high demand** or **continuous mode** may be required to carry out its **safety function** more often than once per year. The alternative is a **low demand** application, in which the **safety function** would normally be required to operate once per year, or less.

Diagnostic test interval – “interval between on-line tests to detect faults in **a safety-related system** that has a specified **diagnostic test coverage**”. The **diagnostic test interval** is an important factor (when combined with the **fault reaction** time), in determining if a particular **safety-related system** (with no tolerance to **hardware faults**) is suitable for use in a given **high demand/continuous mode** application.

Electrical, electronic or programmable electronic system (E/E/PES) – “system for control, protection or monitoring based on one or more electrical/electronic programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices.”

Equipment under control (**EUC**) – the equipment, plant and machinery that is the source of the **risk**.

EUC control system – “system which responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner”.

EUC risk – “risk arising from the **EUC** or its interaction with the **EUC control system**”.

External risk reduction facility – “measure to reduce or mitigate the risks which are separate and distinct from, and do not use, **E/E/PE safety-related systems** or **other technologies safety-related systems**”. Examples: A drain system, a fire wall and a bund are all external risk reduction facilities.

Fault avoidance – "use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety-related system".

Fault reaction time – the time taken for a **safety function** to perform its specified action - to achieve or maintain a **safe state** from when a fault is detected. This should be considered along with the **diagnostic test interval** and the **process safety time** for systems that have a **hardware fault tolerance** of zero and which are operating in **high demand mode**.

Final elements – the actuators (such as valves, solenoids, solenoid valves, pumps, alarms etc.) that carry out an action to control the process or carry out the **safety function**.

Functional safety – "part of the overall safety relating to the **EUC** and **the EUC control system** which depends on the correct functioning of the **E/E/PE safety-related systems**, **other technology safety-related systems** and **external risk reduction facilities**".

Hardware fault tolerance – IEC 61508 defines **fault tolerance** as "ability of a functional unit to continue to perform a required function in the presence of faults or errors**". Hardware fault tolerance** is obviously fault tolerance specifically related to hardware.

Harm – "physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment"

Hazard – "a potential source of harm". The standard covers harm caused in both the short-term – such as harm from an explosion – and the long term – such as harm from the release of a toxic substance.

Hazard and risk analysis – part of the development of the overall safety requirements.

Hazardous event – "a **hazardous situation** which results in **harm**".

Hazardous situation – "circumstances in which a person is exposed to hazard(s)".

High demand – also known as **continuous mode**. A **safety function** in **high demand** or **continuous mode** may be required to carry out its **safety function** more often than once per year. The alternative is a **low demand** application, in which the **safety function** would normally be required to operate once per year, or less.

Low demand – a **safety function** for **low demand** applications may be required to carry out its **safety function** once per year or less. The alternative is a **high demand/continuous mode** application, in which the **safety function** would normally be required to operate more than once per year.

Other technologies – IEC 61508 is concerned with the use **of electrical, electronic and programmable electronic systems** to provide safety systems. "**Other technologies**" are neither electrical, electronic nor programmable electronic, but the standard recognises that such protection based on alternative technologies – such as a hydraulic system - can be used in risk reduction.

Probability of dangerous failure per hour (**PFH**) - "is the safety integrity failure measure for **safety-related** protection systems operating in **high demand** mode".

Probability of failure on demand (**PFD_{avg}**) – "is the safety integrity failure measure for **safety-related** protection systems operating in **low demand** mode".

Process safety time – "the period of between a failure occurring in the **EUC** or the **EUC control system** (with the potential to give rise to a **hazardous event**) and the occurrence of the **hazardous event** if the **safety function** is not performed".

Programmable electronic system – "system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices".

Proof test – "periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition".

Random hardware failures – "failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware".

Residual risk – "risk remaining after protective measures have been taken". This level of risk should typically be lower than the **tolerable risk** once protective measures have been taken. Note, it is not necessary that this risk is zero – but it should be below what is considered a **tolerable risk**.

Response time – the standard does not specifically define **response time**, but for convenience in this safety manual, it is taken as if it were a defined concept. Given that condition, **response time** is the time taken from the input to the **sensor** (or input device) associated with a particular safety function being set, to the **final element** (output device) completing its required action. This time period includes the time taken for the E/E/PE system to carry out any software applications and communicate with the sensors and **final elements**.

Risk – "the combination of the probability of occurrence of **harm** and the severity of that **harm**".

Safe failure fraction – "of a subsystem is defined as the ratio of the average rate of safe failures plus dangerous undetected failures of the subsystem to the total average failure rate of the subsystem".

Safe state – "state of the EUC when safety is achieved".

Safety function – "function to be implemented by an **E/E/PE safety-related system, other technology safety-related system** or **external risk reduction facilities**, which is intended to achieve or maintain a **safe state** for the **EUC**, in respect of a specific **hazardous event**".

Safety integrity level (**SIL**) – "a discrete level (one out of a possible four) for specifying **the safety integrity** requirements of the **safety functions** to be allocated to **the E/E/PE safety-related systems**, where **safety integrity level** 4 has the highest level of **safety integrity and safety integrity level** 1 has the lowest".

Safety life cycle – "necessary activities involved in the implementation of **safety-related** systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the **E/E/PE safety-related systems**, **other technology safety-related systems** and **external risk reduction facilities** are no longer available for use".

Safety-related systems – "designated system that both

- implements the required **safety functions** necessary to achieve or maintain a **safe state** for the **EUC**; and
- is intended to achieve, on its own or with other **E/E/PE safety-related systems, other technology safety-related systems** or **external risk reduction facilities**, the necessary **safety integrity** for the required **safety functions**".

Safety requirements specification – "specification containing all the requirements of the **safety functions** that have to be performed by the **safety-related systems**". This should include the action the **safety function** is required to perform and also the **safety integrity** requirements of the **safety function**.

Sensors – input devices to the **safety function**.

SIL – see **safety integrity level**.

Systematic failure – "failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the way the manufacturing process, operational procedures, documentation or other relevant factors".

Techniques and Measues to Control failures – a number of techniques are specified in the standard. These techniques, when combined with the techniques specified for **fault avoidance** in all stages of the **safety life cycle**, play an important part in ensuring that the **E/E/PE safety-related system** attains its **safety integrity level**.

Tolerable risk – "risk which is accepted in a given context based on the current values of society"

Type A system – "a subsystem can be regarded as type A if, for the components required to achieve the **safety function** can satisfy the following requirements:
(a) the failure modes of all the constituent components are well defined
(b) the behaviour of the subsystems under fault conditions can be completely determined
(c) there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met."

Type B system – "a subsystem will be regarded as type B if, for the components required to achieve the **safety function**:
(d) the failure mode of at least one constituent component is not well defined
(e) the behaviour of the subsystems under fault conditions cannot be completely determined
(f) there is insufficient dependable failure data from field experience to support the claims for rates of failure for detected and undetected dangerous failures."
Note that if any element of the system is **Type B**, then the whole of the **safety function** must be treated as **Type B**. It is likely that any component using a microprocessor will be **Type B**.

Appendix B – Summary of Safety Related Data

Summary of Key Data for Safety-related applications

Certified for use up to	SIL 2	Configuration	1oo1D
Architecture Type	B	Hardware Fault Tolerance	0
Safe Failure Fraction	> 90%		
Failure Rate Data			
Part	Model	λ_{DU} (dangerous undetected failure rate per 10^9 hours) – all data given for 70^oC operating ambient temperature	
SafetyNet Controller – ESD Function	8851-LC-MT	96	
SafetyNet Controller – F&G Function	8851-LC-MT	226	
AI SafetyNet Module	8810-HI-TX	80	
DI/DO SafetyNet Module - configured as ESD input	8811-IO-DC	43	
DI/DO SafetyNet Module - configured as F&G input	8811-IO-DC	81	
DI/DO SafetyNet Module - configured as ESD output	8811-IO-DC	40	
DI/DO SafetyNet Module - configured as F&G output	8811-IO-DC	76	

This summary shows the undetected dangerous failure rates only, which can be used for simple safety functions such as those used for the examples in Sections 7.1.4 and 7.1.5. Comprehensive data covering all failure modes, and for use in more complex safety functions, is available on request from GE Intelligent Platforms.

The contribution to overall System Failure rates by 8913 and 8914 power supplies is given below. This is to be used when justifying alternative power supply arrangements as per Section 2.5.

	λ_{DU} (dangerous undetected failure rate per 10^9 hours) – all data given for 70^oC operating ambient temperature	
	Single power supply	Dual power supply
8851 controller	1	1
8810 AI module	1	2
8811 DCI/O, as input	1	2
8811 DCI/O, as output	1	2