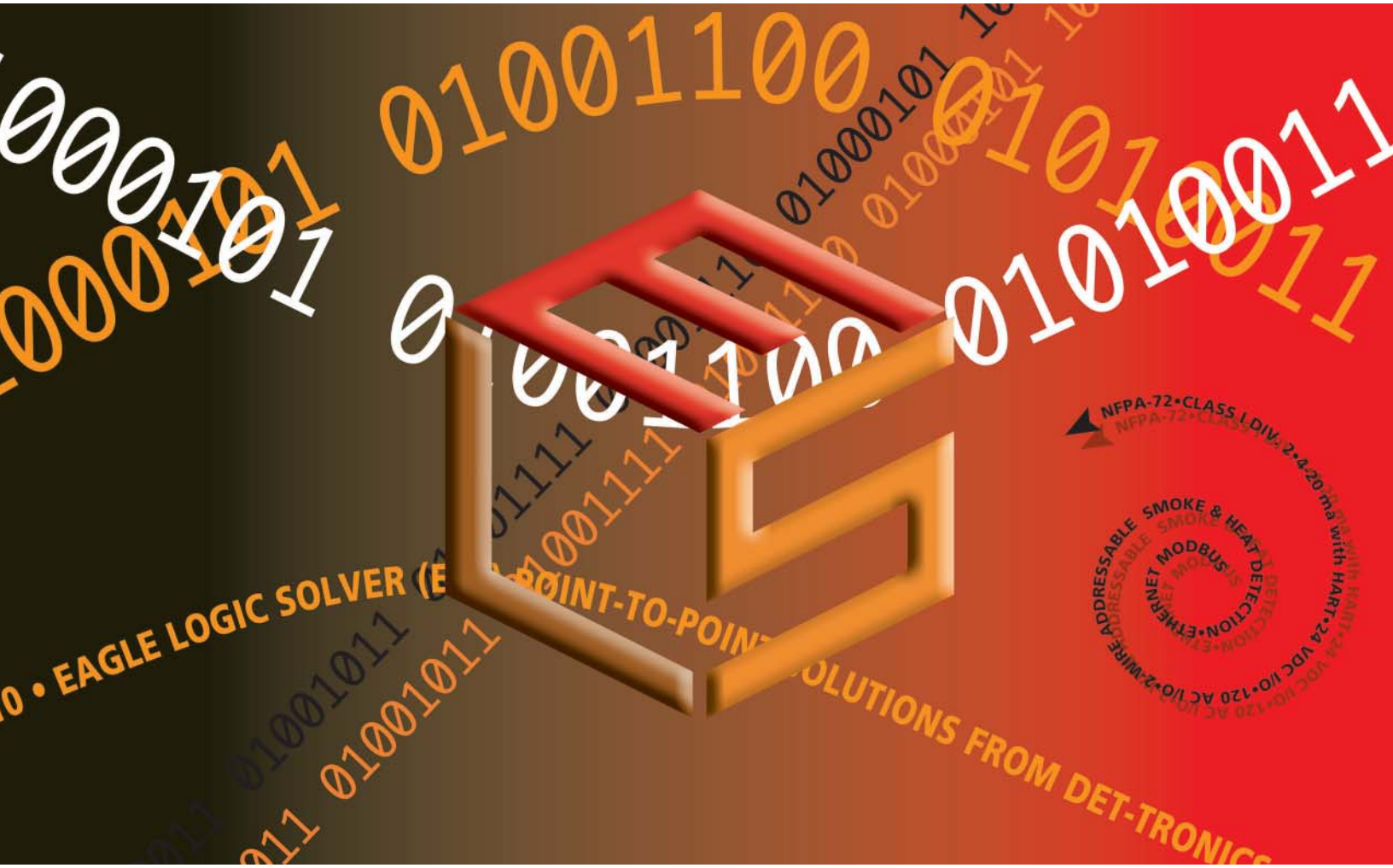


Eagle Logic Solver (ELS)

SAFETY MANUAL

SIL 2 Rated Fire & Gas System

DET-TRONICS®

95-8592-1.1

Table of Contents

Eagle Logic Solver (ELS)
SIL 2 Rated Fire & Gas System

NOTE

*In the text, any wording which is in **bold** has specific meaning within IEC 61508:2002. 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.*

INTRODUCTION

This Safety Manual describes the actions that must be taken to use the Det-Tronics ELS Safety 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 such as Manuals and Datasheets - must be referred to for information outside the scope of this document. These documents can be found on the Det-Tronics website www.det-tronics.com.

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

Further, it is the responsibility of the user to ensure that the ELS Safety System is suitable for the chosen application - and complies with the appropriate application standards.

SCOPE

The Det-Tronics ELS Safety 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 (SIL 2)**.

The ELS Safety System employs a **1oo1D** (i.e. **1 out of 1 with diagnostics**) architecture to achieve **SIL 2**. ELS Safety 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 ELS Safety System must be via a software program known as the Workbench.

In addition to completing the actions specifically related to the ELS Safety 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 requirement specification**. This work must be carried out through appropriate and competent Safety Management procedures and staff.

DOCUMENT STRUCTURE

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

Introduction

Product Overview, gives an overview of the Det-Tronics product range in general and the ELS Safety products in particular.

Maintenance Over-ride, describes the implementation of maintenance over-rides.

Proof Testing, describes the proof testing that is necessary.

Suitable Applications, describes the use of the Det-Tronics ELS Safety System in practical applications.

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 Det-Tronics ELS Safety System is given in Appendix B.

PRODUCT OVERVIEW

ELS

The ELS Process Control System (on which the Det-Tronics ELS Safety System is based) was originally developed to meet the requirements of modern process control. The system comprises (see Figure 1):

- IO modules, in both General Purpose and Intrinsically Safe format.
- Field terminals to which field wiring is terminated, incorporating fusing and loop disconnect.
- Controllers which can be programmed to carry out the control of the process.
- Carriers on which the other components can be mounted.
- Power supplies and other miscellaneous hardware.
- Workbench software which is used to configure the system and to generate the control programs which will be run by the Controllers.
- An internal and proprietary protocol known as Railbus provides communication between IO Modules and Controllers on each node.

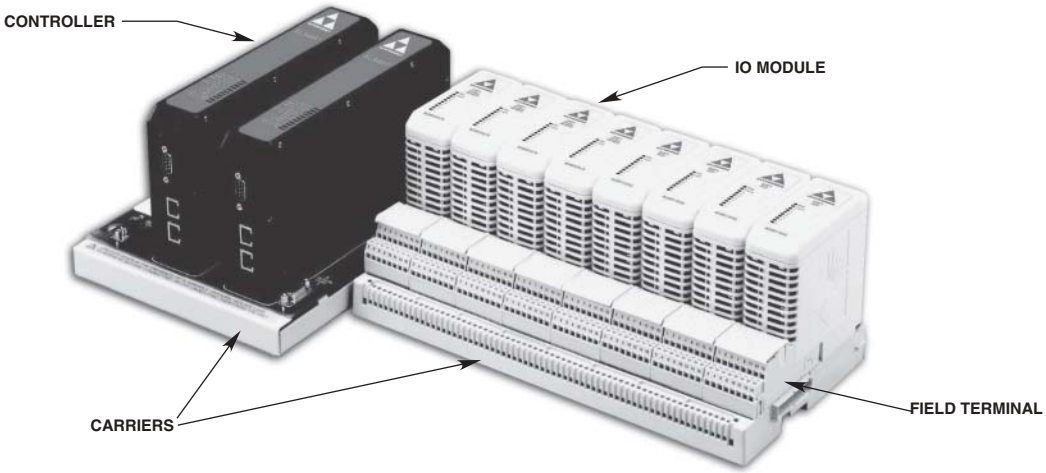


Figure 1—Basic Components of a Det-Tronics ELS System

ELS SAFETY SYSTEM

The Det-Tronics ELS Safety System uses the following specifically developed components:

- ELS Safety Controller
- ELS Safety Controller Carrier
- ELS Safety IO Modules
- Workbench software specifically for use with the ELS Safety System

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

ELS Safety System components and standard components can be used together in certain circumstances (see “Safe and Non-Interfering Data” in the “Workbench” section). A listing of which components can be used together, and under which circumstances, is maintained at www.det-tronics.com and at the TÜV website www.tuvasi.com.

ELS SAFETY SYSTEM NORMAL AND SAFE STATES

The Digital Outputs from an ELS Safety DI/DO Module can 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 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.

ELS Safety System Component Overview

Figure 2 gives an overview of the role each element of the ELS Safety System has in implementing the safety function.

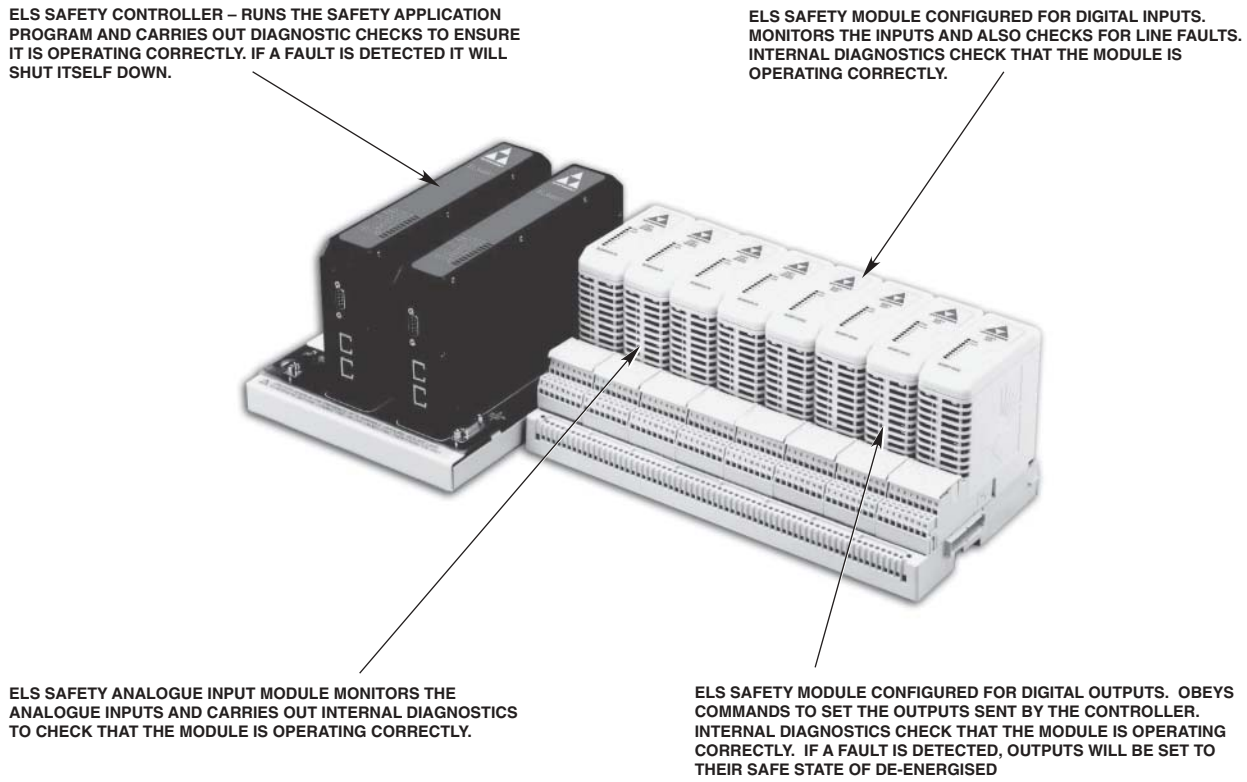


Figure 2—Det-Tronics ELS Safety System Component Overview

ELS SAFETY CONTROLLERS

The ELS4851-LC-DT Safety Controllers share a common hardware platform with standard ELS Controllers. Safety compliance is assured by constraining the Controller so that it can only perform appropriate operations and by additional diagnostic software detecting failures and taking appropriate action should errors be detected.

ELS Safety Controllers can be mounted on either the ELS4751-CA-NS or ELS4750-CA-NS Controller Carrier. The ELS4751-CA-NS provides earth-leakage fault detection capability.

If the ELS Safety Controller detects a “dangerous” fault in itself (i.e. one that would prevent the ELS Safety 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 ELS Safety 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 an ELS Safety Controller's configuration and application programmes, and then only under certain conditions. (See “Configuration Mode” in the “Workbench” section for further information.)

Controlled Shutdown by ELS Safety Controllers

A controlled shutdown involves the following steps:

- All ELS Safety Controller activity that could affect IO Modules is suspended. This leads to the IO Modules entering failsafe mode (loss of communication between the ELS Safety Controller and an ELS Safety 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 is 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 ELS Safety Controller returns to a state from which fault diagnosis can be carried out.
- Following the processor reset, the configuration, program and warm start data is CRC checked and re-loaded.
- The ELS Safety 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.
- An ELS Safety Controller in “Failed State” illuminates both red FAULT and FAILSAFE LED's.

Uncontrolled Shutdown by ELS Safety Controllers

Uncontrolled shutdown is defined for the ELS Safety System as a shutdown in which it is not possible to record the event journal and the “reason for failure” message. Uncontrolled shutdown will occur in such cases as a hardware fault or hardware watchdog triggering a reset of the processor.

Cold Start by ELS Safety Controllers

Should the power supply to the ELS Safety Controller fail and then be reinstated, the ELS Safety Controller will enter cold start mode. Cold start re-initialises all data, including IO Module data.

The ELS Safety Controller cold start mode has two configurable options - Off-line, in which manual intervention is required to bring the ELS Safety Controller online, and Automatic whereby the ELS Safety Controller will automatically come on-line once the power is restored. An ELS Safety Controller that is configured to come on-line following a Cold Start will begin operating the safety application from its configured Initialised State.

ELS Safety Controller Diagnostic Checks

The ELS Safety 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 certifying authority that has granted the Det-Tronics ELS Safety System approval for use in **SIL 2 safety-related** applications has confirmed the completeness of the diagnostic tests. No further diagnostic tests need to be incorporated into the ELS Safety application by the user. Proof testing - which is the responsibility of the user - is discussed in the “Proof Testing” section of this manual.

Redundant ELS Safety Controllers

When a second Controller is added to introduce redundancy, the new Controller will only operate as a standby once it has confirmed that it has identically the same firmware and control strategy as the master. If a new Controller does not have identical firmware and/or application, then the master will update the new Controller.

If the new standby Controller has an older version of firmware or application, then the master automatically updates the standby.

If the new standby has a newer version of firmware or application, then it will start in off-line mode. If the Controller button for the new standby is then pressed, it will copy the older version from the master before coming on-line as the standby.

When used in redundant mode, ELS 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 outputs to the Railbus, 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 instructs the standby to write the agreed output, in order 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's self-diagnosis detects 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 Det-Tronics ELS Safety Controllers in redundant mode will increase their availability, but will have no effect on their ability to perform a **safety-related** function - they would still be certified for use as part of a **SIL 2** system.

When used in Redundant Mode, ELS Safety 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 cold start of one of the Controllers is initiated. Where both Controllers were in standby, once the cold start has been completed, the Controller will re-start in on-line or off-line according to its configuration (see “Cold Start by ELS Controllers” under “ELS Safety Controllers”). Where both Controllers were masters, once the cold start has been completed, the Controller will re-start in standby mode.

Download of New Controller Firmware

When permitted and approved by local operating procedures, new firmware can be downloaded to ELS Safety Controllers from the Workbench. Download of new firmware can only take place with the ELS Safety Controller in Configuration mode.

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 ELS Safety Controller is available. The new firmware is first downloaded to the standby Controller. Once this has been completed, the Controller with the new firmware re-starts in standby. It then copies the current live data from the master and, once this has been copied, a fail-over between the Controllers is initiated, so that the Controller with the new firmware becomes the master and the one with the old firmware goes off-line. The new firmware can then be downloaded and enabled in the remaining Controller - which is then brought on-line (as a standby) in the normal way.

The process of downloading new Controller Firmware is managed by the “Firmware Downloader” utility, running on the Workbench.

On-line Download of New ELS Safety Applications

When permitted and approved by local operating procedures, new safety applications can be downloaded on-line to ELS Safety 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 ELS Safety Controllers.

When downloading a new application to ELS Safety 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** (see “Calculating Response Time” in the “General Application Requirements” section). Once the new application has been downloaded and checked the Controller will automatically adopt the new application.

Downloading a new safety application to redundant ELS Safety Controllers is the same 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.

ELS SAFETY IO MODULES

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

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

Configuration

ELS Safety IO Modules are configured via the IO Configurator within the Workbench.

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

To carry out such an on-line download, the ELS Safety Controller must first be in “Configuration Mode” (see “Configuration Mode” in the “Workbench” section).

LED Indication

Each ELS Safety 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 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: • —)

Module States

ELS Safety IO Modules can be in one of four “static” 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 “transient” states:

- Power Up
- Cold Start
- Controlled Shutdown

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

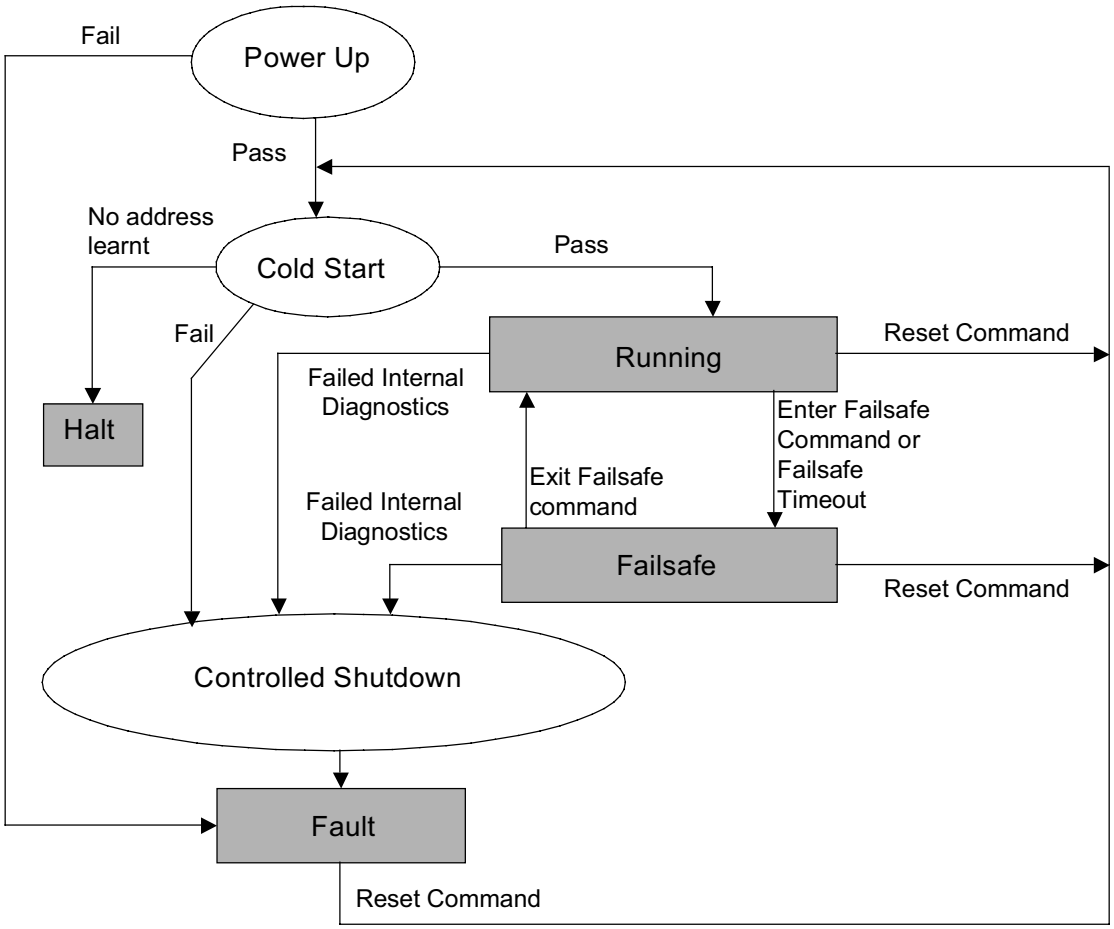


Figure 3—ELS Safety IO Module States and Transitions

Figure 3 shows the transitions between the various IO Module States.

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

POWER UP

De-powering and re-powering an ELS Safety IO Module will cause it to enter the 'Power-Up' and subsequent processes, irrespective of the module's state prior to the removal of the power. (These transitions are not shown on the above diagram for simplicity). All data stored within the module - IO data, diagnostic, status and any event logs not yet transmitted to the Controller - will be lost in doing this.

If an ELS Safety IO Module fails Power Up, it will enter the Fault State, if it passes it will carry out a Cold Start.

COLD START

During a Cold Start, the ELS Safety 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.

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).

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.

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.
- Outputs are de-energised.
- Background diagnostics are running and if a failure is detected, then the module will enter Controlled Shutdown.

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 IO Module is re-initialised.
- 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 address the module.

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

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). The module will enter a cold start when re-starting from the Fault State.

ELS Safety IO Module Failsafe Timeout

ELS Safety 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 ELS Safety Controller does not take place within the failsafe timeout, then the Module will enter a controlled shutdown. The failsafe timeout cannot be increased beyond 5s (the **diagnostic test interval** of the ELS Safety system), but for certain applications, it may be useful to decrease the failsafe timeout for particular IO Modules. (Note the **diagnostic test interval** will remain at 5s, even when the IO Module failsafe timeout is reduced).

ELS Safety IO Module Diagnostics

The ELS Safety 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 ELS Safety 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 the “Proof Testing” section of this manual.

Downloading new IO Module Firmware

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

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

ELS Safety Analogue Input Module

The ELS4810-HI-TX ELS Safety 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. The inputs are suitable for use in **SIL 2** 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 is otherwise identical in operation to a standard Analogue Input Module with HART.

Detailed information regarding the use of the ELS Safety 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.

HART DATA

In the initial release of the ELS4810-HI-TX Analogue Input Module, the HART capabilities are disabled. When using this product, each entry in the Trusted Host Table must have the HART capability disabled.

When using HART enabled product, the HART data retrieved by the ELS Safety 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 ELS Safety 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 in ensuring that these instruments may not be re-configured by 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) needs to be given careful consideration.

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 time constants
- 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 processing on that channel is disabled.

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 returns to the normal operating range.

Figure 4 shows the operation of alarms with the unfiltered input value.

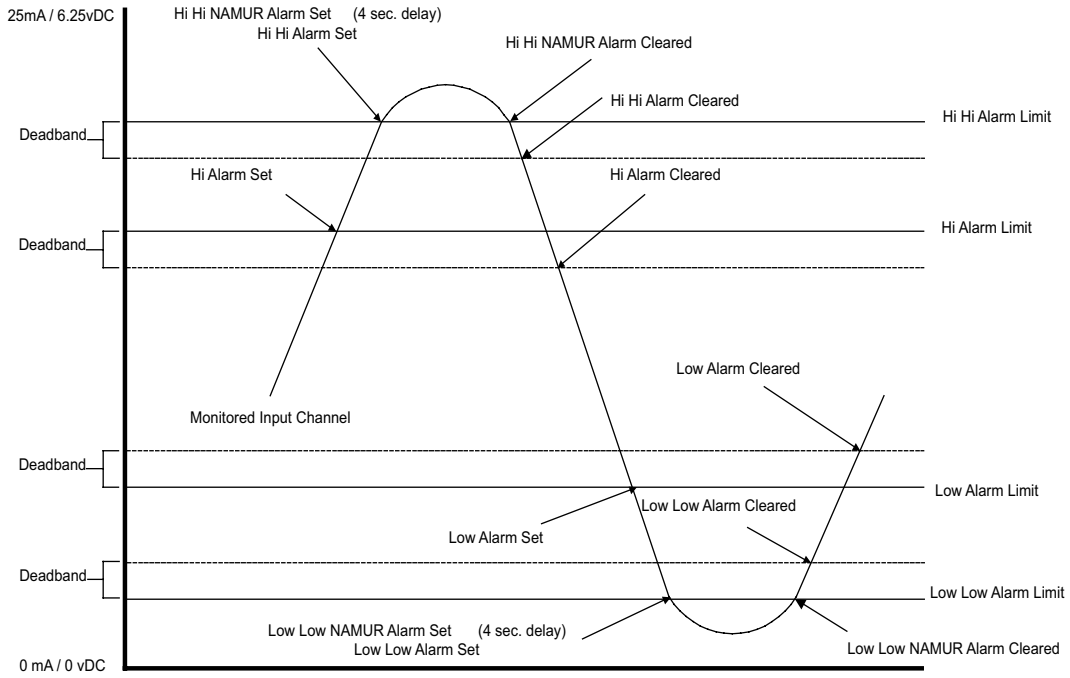


Figure 4—The operation of alarms for the ELS Safety Analogue Input Module

ANALOGUE INPUT DIAGNOSTICS

The ELS Safety 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 will be 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).

ELS Safety Digital Input/Output Module

The ELS4811-IO-DC ELS Safety 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 **SIL 2 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 **SIL 2 safety functions**. The architecture is **1oo1D**. Line fault detection should normally be enabled for normally de-energised loads*. 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).

*NOTE**

If line fault detection is not enabled, then the installer must establish that the reduction in diagnostic coverage that this will entail, is acceptable in the given application.

The ELS Safety Digital IO Module can be in one of four states - Running, Failsafe, Fault, or Halt. (See “Module States” in the “ELS Safety IO Modules” section.)

Detailed information regarding the use of the ELS Safety 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.

Inactive Digital IO Channels

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

- The channel's input state is set to zero and it is de-energised. If the de-activation command is received while the output is ON, it will be immediately de-energised.
- 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.

ELS Safety Digital Input Channel Configuration

An ELS Safety Digital Input channel can be configured as a discrete or latching input. In both these modes the channel may also be configured to be a pulse counter.

ELS Safety 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 ELS4751-CA-NS Controller Carrier. Further information can be found in the relevant Installation Manuals.

A change in input state is only recognised if the new input state is observed at both the start and at the end of the filter time interval (to ensure that noise is not incorrectly interpreted as a change in the input state). If the readings taken at the start and end of the filter time interval 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 ELS Safety 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. When using the counter as part of a safety function, the safety application must monitor the health of the associated input channel and ensure that appropriate action is taken if the channel is in fault (which will lead to the counter value being incorrect).

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.

ELS SAFETY 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.

ELS SAFETY INPUT LINE FAULT DETECTION

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.
Figure 5 describes this and gives the values for the resistances.

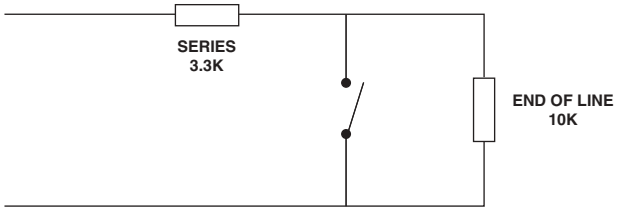


Figure 5—Resistor Values for Line Fault Detection

Table 1—Measured and Resistor Values for Line Fault Detection with ELS Safety Digital Input channels

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

Table 1 shows how the measured values of line resistance are interpreted according to NFPA 72:

ELS SAFETY 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 line fault detection disabled), or to self-test the module'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 open 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.

Output channels in single pulsed mode can be configured to be “Inactive”. When in this state:

- The channel is de-energised. If the de-activation command is received while the output is ON, it will be immediately de-energised.
- The stored Output State (the value returned to the Controller) is set to zero and all signal processing for the channel is discontinued, including line fault detection.
- The channel fault flag is set to healthy.

ELS SAFETY OUTPUT CHANNEL - CONTINUOUS PULSED MODE CONFIGURATION

When configured as a continuous pulsed mode output, a channel is suitable for use - for example - with sounding 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 open 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.

Table 2—Output 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

ELS SAFETY 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.

The output will de-energise or remain de-energised when the channel is de-activated.

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 open 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.

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 be briefly opening or closing each switch and then returning it to its normal 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. Table 2 shows the situations that arise in the event of various switch failure scenarios.

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 switch failures and the ELS Safety 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.

READING BACK THE ACTUAL OUTPUT STATE

Each output channel has tags allocated to it called “DO Desired” and “DO Echo”. The value of “DO Desired” is the state that the ELS Safety Controller has requested. The “DO Echo” value is the state that the ELS Safety IO Module measures on the actual output. Diagnostics check that the requested value is matched by the actual output value and set the channel to failsafe when an error is detected.

In certain circumstances, the internal diagnostics of the ELS Safety system will fail to detect that the desired value has not been set. The user must therefore incorporate a function in to the safety application, which also 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.

Table 3—Measured Resistance and Resistor Values for Line Fault Detection with normally de-energised Output channels.

Output mode	Open circuit detect	Short circuit detect — forward test current	Short circuit detect — reverse test current
Open line (measured as)	>45kΩ	—	—
Shorted line (measured as)	—	User configured between 1Ω and 14kΩ	User configured between 1Ω and 14kΩ
End of line resistor	—	—	10kΩ for diode blocked loads

ELS SAFETY 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).

The test for short-circuit line faults can be configured to use either a forward or reverse test current. The nominal resistance threshold at which a short circuit is reported can also be configured. The actual value at which a short-circuit is reported will depend on the nominal resistance value and the measurement accuracy at that value (see the module datasheet for further information).

When the load incorporates a diode the short-circuit line fault detection must be configured to use a “reverse” test current, and a 10kΩ end of line resistor needs to be wired in parallel with the load, as shown in Figure 6:

The test for open circuit line faults always uses reverse test currents and will always report an open circuit fault for line resistances above 45kΩ.

Table 3 gives the measured values that are used for reporting open and short circuit line faults:

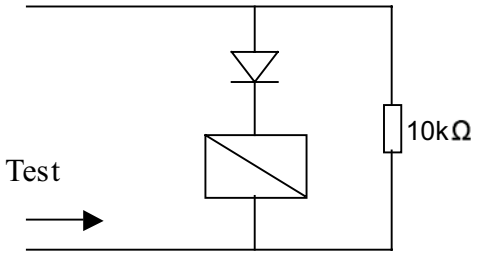


Figure 6—Resistor Values for Short-Circuit Line Fault Detection with Loads Incorporating Blocking Diodes

NOTE

The “reverse” test current is never more than 1.5 mA, the “forward” test current is never more than 25 mA. In the case of the forward test current, it must be confirmed that this current is not sufficient to energise the load.

POWER SUPPLIES

The ELS Safety System is certified for use with Det-Tronics ELS Power Supplies; the ELS4913-PS-AC to supply the 12V “System” and “Controller” power and the ELS4914-PS-AC to supply the 24 Vdc “Bussed Field Power”. Use of any other power supplies will invalidate the certification for use in **safety-related** applications.

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

For applications where, in any operating condition, load currents of less than 100 mA may be drawn from an ELS4914-PS-AC power supply, it is recommended that a resistor of 220Ω (rated for 3W) should be wired between the terminals of the ELS4914-PS-AC. This is to ensure that the power supply can react adequately when required to rapidly supply a significantly higher current demand.

WORKBENCH

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

This Section describes the features of the Workbench applicable to the ELS Safety 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 ELS Safety Systems is given below.

- Two modes of operation are defined for the ELS Safety System: “Configuration Mode”, in which configuration parameters and control strategies can be modified in the Workbench and downloaded to the ELS Safety Controller; and “Safe Mode” in which the ELS Safety Controller is running its control strategy and will not accept modifications.
- ELS Safety Controllers can retrieve peer-to-peer data from other ELS Safety Controllers or from standard Controllers, but only data that is “safe” can be used in the ELS Safety Logic application.
- Only “safe” data can be used in the ELS Safety Logic application - the user is prevented from using any other data.
- Password protection of security access is enhanced to control which personnel are allowed to perform safety-related operations.
- A “Key Switch” facility is provided that can be used to further restrict access to safety aspects of each ELS Safety Controller.
- A “Trusted Host Table” is provided that defines which hosts - i.e. Ethernet LAN devices - can write to each ELS Safety Controller.
- A “Static Analysis Tool” is included in the ELS Safety 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 ELS Safety Controller firmware and hardware.
- Change control logging and event recording are enhanced within the Workbench and ELS Safety Controllers.
- Maintenance over-ride features allow the ELS Safety application to be set to a pre-defined state, to allow work to be carried out on field instrumentation.

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

Safe Mode

Safe Mode is the state in which the Det-Tronics ELS Safety System is acting as a **safety-related system** and carrying out its **safety function**. When the system is in this state, it is not possible to make modifications to configuration parameters or control strategies.

Configuration Mode

In Configuration Mode changes can be made to the configuration parameters and the control programs of the ELS Safety Controller - the **safety function** can still operate, but it will no longer be **SIL 2** compliant.

Instructing the Det-Tronics ELS Safety 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.

Safe and Non-interfering Data

An ELS Safety application program can read data only from other ELS Safety application programs, ELS Safety Controllers or ELS Safety IO Modules. This data is known as “Safe Data” within the ELS Safety documentation. No other data can be read by the ELS Safety application.

In some instances, the ELS Safety *Controller* can read data that is not sourced from the ELS Safety application programs, Controllers or IO Modules - but this does not affect the ELS Safety *application program*. This data is known as “non-interfering” within the ELS Safety documentation. The ability of the ELS Safety Controller to read and subsequently write “non-interfering” data is the route by which standard IO Modules and remote Modbus devices mounted on an ELS Safety node, can communicate and be controlled by standard application programs.

The ELS Safety Logic Application can write data to any location (standard or ELS Safety IO Modules, standard or ELS Safety Controllers, remote Modbus devices, HMI or other networked hosts).

Peer-to-Peer Communication with other Controllers

ELS Safety Controllers can use peer-to-peer communication to retrieve “safe” data from other ELS Safety Controllers and “non-interfering” data from standard Controllers.

Communication with Remote Modbus Devices

ELS Safety Controllers can write data to Remote Modbus devices that may or may not form part of the safety function, but any data read from such devices is not recognised as “safe” and cannot be used in a safety application.

Workbench Password Protection

Access to the Workbench software program 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 if 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 exactly to the condition it was in when the system became locked.

Security Levels

A number of Security Levels are defined within the Workbench, to restrict access to certain features. The levels are common to both standard and ELS Safety Workbenches. 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.

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

ELS Safety Controller Password

When a new Controller is added in the Workbench, it may be added as an ELS Safety or standard Controller. When configuring the IO of an ELS Safety 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.

Without the ELS Safety Controller password access to Configuration Mode and to the Trusted Hosts Table is denied.

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

ELS Safety Controller Passwords must be between 6 and 15 characters in length. The password can be changed via the IO Configurator.

Protection via the "Key Switch" Tag

When an ELS Safety 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 ELS Safety 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 an ELS Safety 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 when any of the following operations are carried out:

- switching between Safe and Configuration Modes.
- changing the Controller password.
- downloading the Trusted Hosts Table.

The Key Switch is also used in confirming that Maintenance Over-ride instructions can be accepted.

Trusted Hosts

An ELS Safety Controller's Trusted Hosts Table defines which entities on the LAN are allowed to write to that ELS Safety Controller (any LAN entity can read data from ELS Safety Controllers). This prevents access to the ELS Safety 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 Nodes)
- Modbus writes allowed or not
- Workbench writes allowed or not
- HART passthrough allowed or not
- descriptive name (for use in event logs etc) - optional

To allow Remote Modbus Devices to communicate via the serial ports, COM1 and COM2 can be added as Trusted Hosts. (Note the ELS Safety application can only write to such remote devices, it cannot read from them. Only conventional control strategies can read data from these devices via peer-to-peer communication).

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 ELS Safety Controller password, if one is required

NOTE

The Trusted Host Table can be edited from any instance of the Workbench (even one that is not listed in the Trusted Host Table) and while the ELS Safety 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 ELS Safety 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 ELS Safety Controllers are connected. The prevention of unauthorised remote access must also be considered, and appropriate network security measures implemented.

IO Configurator

The IO Configurator should be launched from within the Workbench.

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

Network Configurator

The Network Configurator should be launched from within the Workbench.

When 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 an ELS Safety Controller, provided that:

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

ELS Safety Logic Static Analysis Tool

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

ELS Safety Logic Differences Utility

Once a strategy is successfully compiled, it can be downloaded to an ELS Safety Controller. A Download Report text file is generated, which can be used for comparison with earlier downloads using a differences utility within the Workbench.

At any time the user can generate a Master Tag Xref (cross-reference) text report that describes the definition of each tag within an ELS Safety Controller. The Differences Utility can also be used to compare different versions of this report.

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 simultaneously download both the tables and the control strategy.

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

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

ELS Safety 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 ELS Safety Controllers it will always be on. 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 removed
- 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.

ELS Safety "Strategy Heartbeat"

All ELS Safety application programmes must incorporate a function block to increment the "Strategy Heartbeat" tag on each application execution cycle. This monitors that the safety application is correctly completing execution cycles. If the tag is not incremented then the ELS Safety Controller will perform a controlled shutdown.

It is not possible to download a safety application to an ELS Safety Controller that does not contain a function block to increment the "Strategy Heartbeat". An ELS Safety Controller will reject the download of any strategy that does not include instructions to import and export the strategy heartbeat register.

MAINTENANCE OVER-RIDE

Maintenance over-rides 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 over-rides 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 over-ride facility may also be used to meet other requirements - for example to force a system to shutdown or to re-start the safety system after a shutdown has taken place.

The basic action of the maintenance over-ride function is to set one or a number of digital tags. The safety application then carries out a pre-determined action, which is only carried out if a particular tag is set. An example would be setting a tag that is only activated when a particular transmitter is being maintained. When this tag is set, the analogue tag that would normally be read from the transmitter is set to a pre-determined value. This would remain for the period that the maintenance over-ride instruction is in place.

When an over-ride 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 over-rides must be implemented so as to comply with the TÜV draft guideline (Maintenance Over-ride Procedure) and the requirements specified in this Safety Manual.

The TÜV guideline defines three options for implementing maintenance over-rides.

- 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 over-rides are initiated by serial communication with the logic solver. The serial 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 serial communication initiated by the HMI or DCS and take appropriate action to implement the maintenance over-ride. 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 over-ride and the implementation does not require anything but the normal operation of the ELS Safety system. The third option requires the ELS Safety system to act in a manner that is unique to the implementation of maintenance over-ride. This Safety Manual therefore gives particular attention to the management of the third option - though the issues raised would apply equally to maintenance over-ride implementations that are not initiated via serial communication with the **logic solver**.

IMPACT OF MAINTENANCE OVER-RIDE ON SAFETY FUNCTION AVAILABILITY

Calculation of average 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 downtime in the calculation of the average **probability of failure on demand (PFDavg)**, for **low demand** applications. (See IEC 61508-6: Section B.3.2.1 for further information).

Calculation of 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: 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: Section B.3.2.3 for further information.

IMPLEMENTATION OF MAINTENANCE OVER-RIDES INITIATED BY SERIAL COMMUNICATION

A maintenance over-ride function must be written into the ELS Safety application and tested and approved as an integral part of the application.

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

Activating a Maintenance Over-ride

An ELS Safety Controller which is operating in “safe” mode can accept a maintenance over-ride instruction transmitted by serial communication from a host - such as an HMI or a DCS - on the following conditions:

- the instruction is sent by a host identified in the Controller's Trusted Hosts Table.
- the ELS Safety Controller's “Key Switch” is unlocked.

The process for applying the maintenance over-ride is as follows:

- the host writes a “1” to the “Request Over-ride” tag (or tags).
- the host must then read the “Confirm Over-ride” tag and check that it has been set to "1" by the Controller. (Updating the host on the basis of having sent the request is not sufficient, it must be read back from the Controller to ensure that the tag has been set).
- the host confirms that the over-ride should take place by writing a “0” to the “Confirm Over-ride” tag - and the maintenance over-ride is then implemented. If the host does not carry out this confirmation, then the ELS Safety Controller will automatically re-set the “Request” and “Confirm” over-ride tags to “0” and the process of initiating the over-ride must be repeated.
- the host could cancel the requested over-ride by writing a “0” to the “Request Over-ride” tag.

Instructions to activate a particular maintenance over-ride must be Modbus RTU and can be received from a trusted host either via the Ethernet LAN or the serial interface.

Once the maintenance over-ride is implemented, the Key Switch should be re-locked to prevent further access to the ELS Safety Controller. While the maintenance over-ride is active, the ELS Safety Controller will not satisfy all the requirements for operating the **safety function** which is subject to the over-ride.

Further maintenance over-ride 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 over-ride instructions that are already in place.

Removing a Maintenance Over-ride via Serial Communication

Removing the maintenance can be over-ride via serial communication with a host such as an HMI or a DCS is the reverse of the process for setting.

An ELS Safety Controller which is operating in “safe” mode can accept an instruction to remove a maintenance over-ride instruction transmitted by serial communication from a host - such as an HMI or a DCS - on the following conditions:

- the instruction is sent by a host identified in the Controller's Trusted Hosts Table.
- the ELS Safety Controller's “Key Switch” is unlocked.

The process for clearing a maintenance over-ride is as follows:

- the host writes a “0” to the “Request Over-ride” tag (or tags).
- the host must then read the “Confirm Over-ride” tag and check that it has been set to "1" by the Controller. (Updating the host on the basis of having sent the request is not sufficient, it must be read back from the Controller to ensure that the tag has been cleared).
- the host confirms that the over-ride should be cleared by writing a “0” to the “Confirm Over-ride” tag - and the maintenance over-ride is then cleared. If the host does not carry out this confirmation, then the maintenance over-ride will remain in place.

Instructions to clear a particular maintenance over-ride must be Modbus RTU and can be received from a trusted host either via the Ethernet LAN or the serial interface.

Once the maintenance over-ride is cleared, the Key Switch should be re-locked to prevent further access to the ELS Safety Controller.

It is often useful to confirm that the **safety function** that has been subject to the maintenance over-ride does not immediately trip once the over-ride is removed. To facilitate this, the ELS Safety 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 over-ride.

Removing a Maintenance Over-ride via ELS Safety Inputs

Maintenance over-rides can be removed by a switch connected to an ELS Safety Digital Input channel - normally set manually by an operator. Different switches could be used to clear particular over-rides and/or a switch could be used to clear all over-rides from a particular ELS Safety 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 over-ride, other than via serial communication.

The application could automatically remove the maintenance over-ride, 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 over-ride by writing a “0” directly to the “Over-ride” tag.

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

NOTE

If a function is required that will “clear all over-rides” 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 over-rides. This can be designed to operate over a number of ELS Safety Controllers if required.

Recording Maintenance Over-ride Activity

The TÜV guideline for maintenance over-ride requires that the ID of the person initiating the maintenance over-ride, the time at which it took place, which over-ride was initiated and the time that it was removed should all be recorded - preferably electronically. The ELS Safety 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.

ADDITIONAL MEASURES WHEN USING MAINTENANCE OVER-RIDES

The TÜV guideline recommends that the following measures should be adopted during maintenance over-ride:

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

USING MAINTENANCE OVER-RIDE TO RESET A TRIPPED SAFETY FUNCTION

The features of maintenance over-ride can be useful in re-setting a tripped **safety function**. Once the reason for the trip has been removed, the **safety function** can be put in to maintenance over-ride while it is reset prior to being brought back on line.

PROOF TESTING

The proof test interval for the Det-Tronics ELS Safety 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.
- take the ELS Safety Controller and IO Modules through a power cycle - i.e. turn the power OFF and back ON (this ensures that the start-up procedures are tested).

INSTALLATION

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

In common with other Det-Tronics ELS products, the ELS Safety product range is IP20. It will be necessary to mount the ELS Safety products in a suitable enclosure to provide mechanical and ingress protection appropriate to the particular application.

For applications that require earth-leakage fault detection, the ELS4751-CA-NS and a single channel of an ELS4811-IO-DC Digital IO Module must be wired and configured according to the relevant Installation Manual.

SUITABLE APPLICATIONS

The ELS Safety System can be used to provide **safety functions** up to **Safety Integrity Level 2 (SIL 2)**. 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 Shutdown or Process Shutdown systems that are used to monitor the correct operation of a process and its process control system and which will perform a controlled shutdown if safety limits are exceeded or a dangerous situation is detected

In both cases, the **process safety time** must be greater than the **response time** of the ELS Safety System.

For high demand applications, the ELS Safety 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 ELS Safety 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**.

GENERAL APPLICATION REQUIREMENTS

Application Standards

The ELS Safety System is certified to meet the requirements of a number of application standards that are listed in this Safety Manual and on the TÜV certificate. Users must ensure that they comply with all the requirements of the standard, not just those which apply to the ELS Safety System.

Operator Interface

The ELS Safety 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 over-ride the automatic system in some instances (such as to prevent extinguishant release or to manually initiate alarms).

The ELS Safety System will allow detected faults (from line fault monitoring, internal ELS Safety 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 ELS Safety System should be alarmed in the HMI - this would normally be implemented by some sort of watchdog timer that would detect such a communication loss.

The operator interface can initiate maintenance over-ride functions, but use of this capability is restricted (see the “Maintenance Over-Ride” section).

Engineering Workstation - the Workbench

Programming, downloading **safety-related** parameters and programs and switching between operating states is carried out via an engineering workstation using the ELS 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 ELS Workbench) and/or some other forms of restricting access.

The Programming Interface may be used as the Operator Interface, but use of the Programming Interface must be restricted to authorised and qualified personnel.

Programming may only be carried out while the safety system is not performing a **safety function** (i.e. the system is not in "Safe" mode).

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

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

The ELS Safety 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.

Calculating PFD for Low Demand Applications

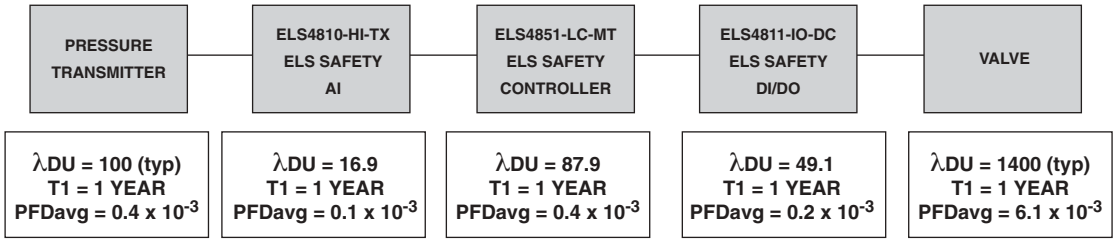
This Section gives a basic introduction to calculating the **average probability of failure on demand (PFDavg)** for a **safety function** incorporating the ELS Safety System.

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**
- the approximation **PFDavg = 1/2 T_1 λdu** is valid for the proof test interval considered

PFDavg 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 7 includes a pressure transmitter for an input device, an ELS4810-HI-TX Analogue Input Module, an ELS Safety Controller, an ELS4811-IO-DC Digital IO Module configured as an output and a valve.



λDU IS FAILURE RATE PER 10^9 HOURS, T_P OF 1 YEAR = 8760 HOURS, PFD_{avg} IS THE PROBABILITY OF DANGEROUS FAILURE.

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

Figure 7—Typical Low Demand Application

PFDavg for each element is calculated according to the equation above, where λ_{DU} is the **undetected dangerous failure** rate per 10^9 hours and T_1 is the **proof test** interval. (In this example, T_1 is chosen as 1 year (8760 hours) for all components of the **safety function**).

The value for **PFDavg** for each element is approximately half of the product of T_1 and λ_{DU}.

The value of **PFDavg** for the system is the sum of **PFDavg** for the individual elements.

PFDavg = $0.4 \times 10^{-3} + 0.1 \times 10^{-3} + 0.4 \times 10^{-3} + 0.2 \times 10^{-3} + 6.1 \times 10^{-3} = 7.2 \times 10^{-3}$

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 and AN90025 for a more comprehensive guide to the calculation of **PFDavg**.

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)**. (See Figure 8.)

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**

Adding the individual PFH values gives:

PFH = $100 \times 10^{-9} + 16.9 \times 10^{-9} + 87.9 \times 10^{-9} + 49.1 \times 10^{-9} + 90 \times 10^{-9} = 343.9 \times 10^{-9}$

Using the table given in the standard, the **PFH** value of 343.9×10^{-9} (or 3.4×10^{-7}), which is suitable for a **SIL 2 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**.

Calculating Response Time

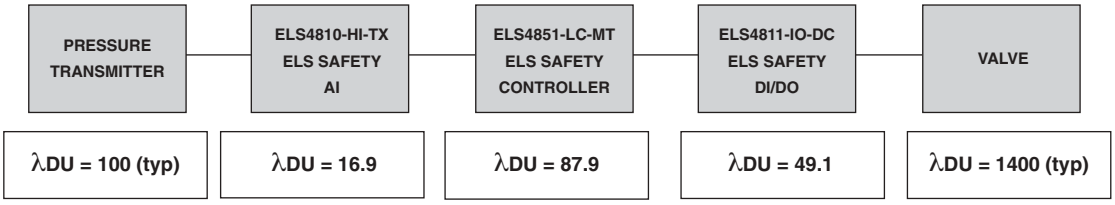
The **response time** of the ELS Safety System (i.e. the time taken from an input transition being detected to an output being asserted), under worst case conditions, can be estimated by the following formulae:

For single ELS Safety Controller systems -

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

For redundant ELS Safety Controller systems -

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



λ_{DU} FOR ALL ELEMENTS IS FAILURE RATE PER 10^9 HOURS.

$$\mathbf{PFH} = \Sigma\lambda_{DU}$$

Figure 8—Typical High Demand Application

For example, a node comprising redundant ELS Safety 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:

35 ms + 4 ms x 25 + 2 ms x 5 + 10 ms + 10 ms = 205 ms

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

35 ms + 4 ms x 25 + 2 ms x 5 + 30 ms + 10 ms = 225 ms

The formulae provide only an estimate of the **response time** of the ELS Safety System - the actual response time will vary with each installation and depend on the complexity of the ELS Safety Logic program as well as the number of IO modules. When a system is assembled and the ELS Safety 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 ELS Safety System, the response time of the input sensors and output actuators must be included.*

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 ELS Safety 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 ELS Safety 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.

Applicable Standards

- IEC 61508:2002. “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”.
- IEC 61511:2003. “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: 1997. “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”.

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 that 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 intrinsic reliability, but also by 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** (see **low demand** and **high demand**).

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**.

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 firewall 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 - the time taken for **safety function** to perform its specified action - to achieve or maintain a **safe state**. 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** - where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-check frequency.

Low demand - where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency.

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 (PFDavg) - "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 output device (**final element**) 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 detected 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)- “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”.

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.

APPENDIX B

SUMMARY OF SAFETY RELATED DATA

SUMMARY OF 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)	
ELS Safety Controller	ELS4851-LC-MT	87.9	
AI ELS Safety Module	ELS4810-HI-TX	16.9	
DI/DO ELS Safety Module - configured as input	ELS4811-IO-DC	50.3	
DI/DO ELS Safety Module - configured as output	ELS4811-IO-DC	49.1	

Detector Electronics Corporation

CORPORATE OFFICES
6901 West 110th Street
Minneapolis, Minnesota 55438
U.S.A.

Tel +1 (952) 941 5665
Fax +1 (952) 829 8745

www.detronics.com

System Solution Centers

HOUSTON
1296 North Post Oak Road
Houston, Texas 77055
U.S.A.

Tel +1 (713) 812 0088
Fax +1 (713) 812 0099

LONDON
Detector Electronics (UK) Limited
Mathisen Way, Colnbrook
Slough, Berkshire
SL3 OHB ENG
United Kingdom

Tel +44 1753 683059
Fax +44 1753 684540

SINGAPORE
438 Alexandra Point
#17-01/04, Alexandra Point
Singapore 119958

Tel +(65) 6424-7979
Fax +(65) 6424-7978

95-8592-1.1