Principles for proof testing of safety instrumented systems in the chemical industry

Prepared by **ABB Ltd**
for the Health and Safety Executive

CONTRACT RESEARCH REPORT
428/2002

HSE
Health & Safety Executive

Principles for proof testing of safety instrumented systems in the chemical industry

Stuart Nunns BSc, C Eng, FIEE, FInstMC
ABB Ltd
Pavillion 9
Byland Way
Belasis Hall Technology Park
Billingham
Cleveland TS23 4YS

Guiding principles for the proof testing of safety instrumented systems (SIS) in the chemical industry have been developed through research into the practices of proof testing. The proof testing of SIS is an integral component of the management of functional safety. Its purpose is to confirm the continued operation of the required safety instrumented function and to contribute to the maintenance of the required safety integrity level of the safety function.

The guiding principles were developed through direct contact with industrial end-users and suppliers of SIS components, and through searches of incident data available within the public domain. Consideration has been given to good practices as defined by international publications such as IEC 61508 and by sector guidance such as that provided by EEMUA. The guiding principles therefore provide independent guidance on proof testing issues which are of interest and concern to chemical industry end-users.

Examples of proof test practices and procedures have been provided together with a proposed checklist of recommended practices which can be used by Field Inspectors. More detailed recommendations are presented in the body of the report.

This report and the work it describes were funded by the Health and Safety Executive. Its contents, including any opinions and/or conclusions expressed, are those of the author(s) alone and do not necessarily reflect HSE policy.

HSE BOOKS

First published 2002

ISBN 0 7176 2346 7

CONTENTS

EXECUTIVE SUMMARY

A set of guiding principles upon which the proof testing safety instrumented systems (SIS) should be based has been developed via research into chemical industry practices, experience and views and via searches of data in the public domain. Interviews, questionnaires, workshops and searches identified a set of issues relating to proof testing which were of particular interest to a cross-section of the chemical industry. These issues have been used to generate guiding principles, which address the following:

- proof testing practices;
- content of proof testing procedures;
- format of proof testing procedures;
- planning and scheduling;
- proof test records;
- competence;
- awareness of hazard and risk;
- management of change.

The research indicated that the proof testing of SIS is common practice but that some organisations take a more structured and focused approach than others. The size of an organisation, and therefore its ability to deploy engineering resources, was significant as was a commonly held view that the reducing numbers of competent, experienced technical personnel is beginning to have an impact on proof testing practices.

The research confirmed the existence of conflict between the need for realistic proof testing and the need to minimise downtime, particularly within high throughput continuous processes such as refining and bulk chemical manufacture. The increasing profile of IEC61508[1] was a common theme throughout the research with manufacturing organisations expressing trepidation over its potential impact on existing installations, notwithstanding its non-retrospective nature.

Examples of good and poor practice were encountered and have been highlighted in this report, however, searches of published literature and incident databases provided no tangible evidence that incidents have been directly attributed to issues relating to proof testing.

1. INTRODUCTION

This report relates to the proof testing of safety instrumented systems (SIS). It has been produced as part of a research project funded by the Health and Safety Executive. The contract was placed with Eutech Engineering Solutions Limited.

The objectives of the research were to define a set of guiding principles upon which proof tests of SIS should be developed, to provide independent advice to HSE Field Inspectors and to report on current practices, highlighting examples of good and poor practice where relevant. The research gathered data from industry via interviews, workshops and questionnaires and executed searches of data within the public domain. This report presents the findings of the research.

The target audiences for the report are industrial end-users of SIS and HSE Field Inspectors. Industrial end users should benefit from the communication and illustration of current practices. The collation of experiences, views and examples gives an indication of what is practicable and of the issues of concern to different sectors within the chemical industry.

The data generated by the industrial research is presented 'as found' in an attempt to provide a genuine indication of the practices, experiences and concerns within industry. The data collected during the research was analysed and the results used to generate and support a set of guiding principles for the proof testing of SIS. Each principle is presented in this report and is supported by the research data and a rationale based on recognised standards and guidance. The current high profile of IEC61508[1] amongst end-users was evident throughout the research. Its principles have been used to construct the rationales supporting the guiding principles.

Detailed recommendations have been generated to provide practical guidance on the application of the guiding principles. The recommendations have been used to create a checklist for use by HSE inspectors. The checklist is presented in Appendix 2.

2. RESEARCH METHOD

The research consisted of five activities:

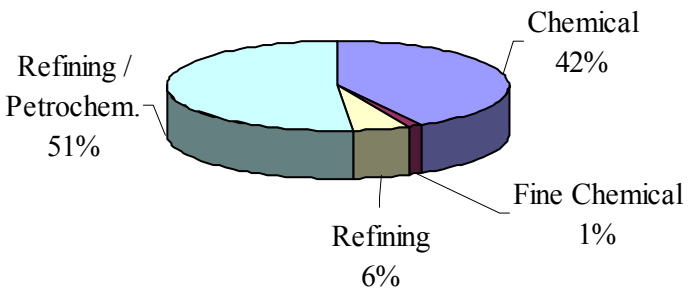
- interviews with industrial end-user organisations;
- follow-up questionnaires, discussions and interviews;
- workshops attended by end-user organisations;
- workshops attended by equipment suppliers;
- searches of data and documentation, in the public domain.

The industrial research targeted a cross section of medium to large scale chemical manufacturing organisations covering continuous and batch operators from the chemical, petrochemical, refining, fine chemical and pharmaceutical sectors. Interviews with representatives of end-user organisations were carried out via face-to-face discussions by engineering consultants using a common interview script. An analysis of the interview coverage is shown in Table 1. The reported distribution of SIS across the sectors examined is shown in Figure 1. The interviews targeted personnel involved in the proof testing of SIS, specifically those with responsibility for the management of proof testing and those responsible for its execution.

Table 1 : Analysis of interviewee characteristics

Total	Chemical	Fine Chemical	Refining	Refining / petrochemical	Pharmaceutical	Continuous	Batch
15	6	4	2	2	1	10	5

Figure 1 : Distribution of reported SIS across industrial sectors
(total reported SIS: 19,465)



Following the initial collation and analysis of the data, further targetted information was gathered through questionnaires, follow-up calls and further site visits.

Three workshops were held in order to facilitate the sharing of views and experience of chemical manufacturing organisations, hereafter referred to as end users, and SIS equipment suppliers. Workshops for end users were held at Teesside and Humberside whilst a workshop for equipment suppliers was held at Teesside. The end user workshops were supported by EPICC and HCF respectively. Analyses of the attendance of the end user and supplier workshops are shown in Tables 2 and 3 respectively. The workshops were based on a common agenda, however, the free exchange of views and experience was encouraged.

Table 2 : Analysis of end user workshop attendees

No. of companies represented	Refining	Chemical	Fine chemical	Other
22	2	8	4	8

Table 3 : Analysis of supplier workshop attendees

	SIS components supplied		
Total no. of attendees	Sensors	Logic solvers	Final elements
7	2	2	2

The search of publicly accessible data covered a variety of publications and databases. The available information was searched for specific references to the proof testing of SIS, particularly for reports of incidents arising from proof testing deficiencies. Where appropriate, the method of review of each source of data is described in the relevant sections of the research results.

3. PRESENTATION OF RESULTS

The results of the research have been used to present an independent view of the sufficient and practicable scope of proof testing. Analysis of good practice, as defined by recognised standards such as IEC61508[1], and of the interviews, workshops and searches highlighted a number of key issues associated with the proof testing of SIS. The key issues were refined to generate a set of guiding principles and supporting recommendations, which could be used to implement or assess good practice in the field of proof testing of SIS. The recommendations are summarised in Appendix 2 in the form of a checklist for use by inspectors.

The results of the research are presented in detail with the intention of reporting the views and experiences of the chemical manufacturing industry as fully and as accurately as possible. The references to specific responses aim to provide an indication of the real issues of interest to those involved, whilst the conclusions and recommendations aim to provide an independent view of the results.

The presentation of the results of interviews and workshops follows a consistent format. The statement of each guiding principle is supported by a rationale, which describes the context in which the statement is made. The rationale is followed by a collation of the relevant views and evidence obtained via the interviews, workshops and questionnaires. Examples of good and poor practices are highlighted and referenced to the relevant guiding principles. Good and poor practices are not attributed to specific sources. Conclusions and recommendations arising from the research are then presented. To aid reference, the guiding principles are collated in Appendix 1.

The appendices also contain proof test procedures, or sections thereof, which are presented to illustrate some of the issues and recommendations arising from the research.

4. GUIDING PRINCIPLES

4.1 PROOF TEST PRACTICES

4.1.1 Statements of Guiding Principles

(a) The proof test of a SIS should reflect real operating conditions as accurately as possible. If reasonably practicable, the SIS should be initiated by manipulation of the process variable without driving the process into the demand condition. Any approach which involves driving the process into the demand state should be accompanied by risk assessment and additional controls.

(b) Where process variables cannot be safely or reasonably practicably be manipulated, sufficient confidence in the correct operation of sensors should be gained by other means, such as comparison with other measurements.

(c) The inherent difficulties associated with testing valves and in-line flowmeters should be addressed during the design phase of SIS and additional provisions such as corroborative measurements should be made where necessary.

(d) Proof tests should address the necessary functional safety requirements of SIS, including functions such as response time and valve leakage class.

4.1.2 Rationale

Effective SIS proof testing should confirm the correct operation of the sensing element(s) and actuating devices, also known as final elements. There is known to be a wide range of techniques adopted by the end-user community in their approach to SIS testing and the following sections provide a summary of the techniques encountered during the research. A variety of techniques were encountered, including examples of both good and poor practice, as were examples where a deficiency was discovered and how it was addressed or improved.

The most satisfactory test of a system will manipulate the process variable in order to achieve a full end to end test. However, practicability is very much dependant on the nature of the process, the process materials and associated risk, and on the tolerable upsets to the process and to production.

4.1.3 Research Data

Testing Pressure Loops

There was unanimous agreement that process pressures should not be manipulated in order to initiate SIS due to the potential of releasing significant stored energy [*consistent with principle 4.1.1(a)*].

The most popular alternative was considered to be the injection of a pressure signal in to the measuring instrument via an isolation and vent valve arrangement positioned as close to the primary element as possible, using a suitable fluid medium. Conversely, one end-user was of the opinion that testing of pressure measuring instruments can only safely be carried out on special test rigs in a workshop environment, again, because it is not considered safe to raise the pressure of a process [*inconsistent with principle 4.2.1 (d)*]. Pressure loops are usually designed so that the process input can be isolated from the measuring instrument and a calibration pump connected at a suitable point. The pressure can then be raised to check the operation and calibration of the instrument and so test the majority of the safety system.

Pressure injection was deemed satisfactory for non-hazardous process materials but was not recommended for those of a hazardous nature. To illustrate this point, an end-user cautioned against considering "direct injection" at impulse lines as necessarily a first choice of test method. "First line breaks" with hazardous materials that are flammable, toxic or irritant have the potential to cause injury, damage plant or cause environmental incidents. There is always the possibility of leaving valves shut or not refitting blanks. Therefore, this particular end-user always considers the need for risk assessment when designing SIS hardware and writing proof test methods in order to avoid testing the plant in such a way that there is the possibility of adverse effects on persons, the environment or plant. Where the risk is deemed acceptable, precautions such as the use of protective equipment are taken. Where risk is deemed to be unacceptable, simulation techniques would be used [*potentially inconsistent with principle 4.2.1 (a)*].

A weakness of pressure injection was considered to be the inability to test the full extent of impulse lines, however, some end-users depressurise transmitters under test via the impulse line into the process, thus proving that the impulse line is clear [*consistent with principle 4.2.1 (a)*].

Two other options for dealing with hazardous process media were cited. If the measuring element is SMART, then the functionality of the device can be used to drive the signal to the trip value. If it is not, then a current signal must be injected into the loop at a suitable point to simulate the output of the measuring instrument. Neither of these techniques proves that the measuring instrument is working correctly [*principle 4.2.1(b)*], however, with a SMART instrument some confidence in the on-line measurement may be provided by self-diagnostic features. Where ‘non-SMART’ instruments are used the measurements should be corroborated [*principle 4.1.1(b)*], firstly by comparison with duplicate instrumentation or other instrumentation in the surrounding vicinity or by calibration and test under safe conditions.

Other examples of pressure SIS proof testing were cited as follows.

- On a liquid process one end-user generally uses a direct mounting instrument. This is difficult to test on-line, due to the way that the instrument would need to be tested so they wait until the plant is shutdown and then inject a pressure, ‘in-situ’ at the instrument [*inconsistent with principle 4.4.1 (b)*].
- Testing of a pressure loop is usually done, by injecting a signal into the measuring element, after isolating it from the process. However, this means that the impulse line and tapping are not being proved. Where possible the signal is injected as close to the tapping as possible to minimise this, but when the instrument is remote from the tapping, this increases the difficulty of testing [*lack of consideration of testing requirements at the design phase leads to potential inconsistency with principle 4.2.1 (a)*].
- Another end-user's method is to isolate the pressure transmitter and zero it. They then inject zero, full scale and ‘trip equivalent’ signals into signal lines and check any receivers and trip devices. Where the process materials are non-hazardous they open the vent and process tappings to check process flow through impulse lines before closing the vent and re-commissioning [*consistent with principle 4.2.1 (a)*].
- An end-user uses a "Beemax" pump to simulate a high pressure, however, on one of their most critical trips the pressure needs raising to 21.5 bar. This particular installation is on the roof of the plant and the method allows for a ‘real’ test of the system. To facilitate this, they use a nitrogen cylinder with calibrated gauges, which is situated near to the installation [*consistent with principle 4.1.1 (a)*]. Other pressure installations use either close coupled cells, generally where toxic materials are in use, or remote transmitters with impulse lines which are kept as short as possible. Where toxic materials are evident, the input to the logic solver is tested either by injecting a current signal at a suitable point, or by using the facilities of SMART transmitters to drive their outputs to trip points [*inconsistent with principle 4.2.1 (a)*]. Transmitters with impulse lines on non-toxic applications are tested by pressure signal injection.

- A bursting disk interspace trip, part of a triple redundant system, connected by an impulse line to a transmitter is tested during plant shutdown due to inadequate process isolation [*potentially inconsistent with principle 4.4.1 (b)*]. To test the element, the transmitter is removed to the workshop [*inconsistent with principle 4.2.1 (d)*] for test and calibration. The end-user would like to improve the installation in the near future by fitting double block and bleed valves to each of the three instruments, instead of the common isolation presently in place, to allow on line testing.
- Another end-user uses a direct connection to the process line for all duties via a manifold or line-specification isolation with vent and drain valves to allow 'live' process testing. Alternative measurements are generally monitored during the testing routine. The transmitter is isolated from the process and vented or injected with pressure from a test rig to simulate the required trip condition. This is seen as a fundamental test of the whole system and includes calibration. Care is needed to separately check impulse lines by way of a separate maintenance routine as they are prone to blockage [*consistent with principle 4.2.1 (c)*], and a trip test does not include the impulse lines when injecting a pressure signal at the primary element.

Testing Level Loops

As was the case for pressure systems, some end-users expressed concerns over testing level systems by manipulating the process measurement. Provided that it is concluded that it is not reasonably practicable to perform the test by manipulating the process variable as principle 4.1.1(a), the use of risk assessment and secondary instrumentation to monitor the surrounding conditions should allow this method of testing to be used.

One end-user also felt that raising or lowering levels until trips operate could lead to hazardous situations. If the trip does not operate, or operates at the wrong value, the condition being prevented could occur, therefore the only time that level SIS can be tested in a safe manner is during a shutdown of the plant when the correct level can be set up in order to test the correct operation of the level measurement [*inconsistent with principles 4.4.1 (b) and 4.1.1 (a)*]. The end-user therefore carries out online testing by injecting a signal to simulate the level measurement and so test the safety system under a defeat, but realises that this does not test the level-measuring element. It is possible to use a radioisotope system to give indication of the actual level in a vessel and compare this against the level measurement reading in order to gain confidence in the measuring device [*consistent with principle 4.1.1 (b)*].

Wherever possible, one end-user with pneumatic instrument systems increased the measured variable's actual value until the trip or alarm operated, assuming that the operating point indicated by the panel instrument would be correct. This assumption was based on the belief that they needed to have two faults giving identical errors for it to be covert. However, an incident caused them to change this practice to one of actually pressure-injecting transmitters wherever possible. The incident was caused by a large air leak affecting both the indicator and pressure switch to the same degree, which prevented a level alarm operating and resulted in an overfilled storage tank [*inconsistent with principles 4.1.1 (a) and 4.2.1 (a)*].

Another end-user's measurement philosophy involves one of three approaches; either a direct coupled pad cell, a vibrating fork level switch or, in some instances, a radar device. Due to the toxic and corrosive nature of the process, signals are injected to test the logic solver and the instrument is generally removed for calibration and testing at a shutdown to give confidence in the measuring instrument [*inconsistent with principles 4.2.1 (d) and 4.1.1 (a)*].

With radioactive level and density initiators, one end-user usually isolates the radioactive sources for high trips and uses a test source for low trips. Level switches mounted directly on vessels are tested during a shutdown, during water trials or re-commissioning, following removal and examination of the switch [*potentially inconsistent with principles 4.4.1 (b), 4.2.1 (d)* and *4.1.1 (a)*].

During discussion, an end-user contended that testing of a level system depends on the installation. If it is a differential pressure (DP) installation then the item is treated as a pressure signal, and a pressure is injected at the cell to simulate level. Where it is a fixed level switch, then the level is generally raised and the system tripped 'in anger' [*inconsistent with principle 4.1.1 (a)*]. They avoid doing this type of test under a trip defeat as they feel that the potential exists for creating a hazardous situation. They have considered installing chambers on the sides of columns or tanks to allow draining and filling to test sensors under realistic conditions but this is known to be costly and where hazardous materials are present, this could endanger the people carrying out the testing.

Another example an end-user discussed, applied to a reactor where the initiator is a direct mounted level switch. They would wait until a shutdown [*potentially inconsistent with principle 4.4.1 (b)*] when they would remove the switch [*inconsistent with principle 4.2.1 (d)*] and test it with water [*inconsistent with principle 4.1.1 (a)*]. Realising the shortcomings of this, they are looking at improving this by moving towards a self-checking probe [*consistent with principle 4.1.1(b)*] or a method to test the switch in-situ with the actual process medium [*consistent with principle 4.1.1 (a)*].

One end-user provided an example involving a toluene tank analogue level and high level trip. Here, the end-user employs a flange-mounted capacitance probe with dual redundant high level switches, allowing testing on line. They would proceed as follows:

1) Remove, inspect & operate high level switch to verify operation [*inconsistent with principles 4.2.1 (d) and 4.1.1 (a)*];

2) Use software override facility to over-ride the trip off the analogue signal;

3) Fill tank until level switch trips the feed flow [*inconsistent with principle 4.1.1 (a)*];

4) Check the calibration of the analogue instrument at this datum point.

In future, they hope to use a low-level, physical dip of the tank to confirm the zero calibration [*consistent with principle 4.1.1 (b)*].

Discussions with another end-user identified the following approach. The method of testing varies depending on measurement technique. If the system uses a DP arrangement, this is treated as if it was a pressure installation and differential pressure injected at the cell to simulate the level. In other cases, they adjust the process level to the trip point if this can be done safely [*consistent with principle 4.1.1 (a)*], or remove and test the initiator in a container [*inconsistent with principles 4.1.1 (a) and 4.2.1 (d)*], for certain high level devices, where possible. For SMART devices they rely on the nature of the device to simulate the trip condition, via a hand held communicator, together with a functionality check. With devices such as radar, it is becoming increasingly difficult to carry out a total fundamental test. End-users are becoming increasingly reliant on the SMART nature of devices to test the output stages of electronics. They then assume that if the input stage is working at the current level, it will still work at the trip point [*inconsistent with principles 4.1.1 (a), 4.1.1 (b) and 4.2.1 (a)*].

One end-user devised a method to test a stock tank trip system as follows. The old system would involve draining and decontamination of the tank and disposal of the effluent, breaking of pipe-work under mask and suit conditions and draining and refilling of the system several times during testing which was very time consuming. The method was improved based on past operating data [*consistent with principle 4.5.1 (b)*] to coincide with offloading of a railcar into the stock tank from a routinely calibrated weighbridge, tripping the transfer system in anger using the weighbridge for comparison. Although the SIS may be in a demand mode, the weight measurement is used as a control measure [*consistent with principle 4.1.1 (a)*], however, it relies on the weight measurement providing an accurate representation of level. For other installations, pad cells are used and, similar to pressure measurements on systems containing toxic material, the trip values are simulated by injecting a current signal or using the SMART functionality of the transmitter to drive the output to the trip value [*inconsistent with principle 4.2.1 (a)*]. On

some stock tanks, a dip-pipe, coupled with a fluidic logic system is used. Here, a 'mini dip-pipe' and valve system has been installed locally to the fluidics which allows the system to be tested with a portable container of water, as the fluidic system only needs a few inches water gauge to operate [*consistent with principle 4.1.1 (a)*]. Where a dip-pipe measurement is used on a non-toxic system with a DP cell, the cell is pressure-injected using suitably calibrated test equipment. Although it is realised that this is not testing the dip-pipe, confidence is gained by having duplicate measurement systems on the vessel [*consistent with principle 4.1.1 (b)*].

An incident with a trip on a pumped liquor supply to a filter was reported by an end-user. When the level in the filter reached a certain point, the logic solver would close a valve in the supply line. On this occasion, the valve did not close and the level overflowed out of the filter. On further investigation, it was found that the seats of the trip valve had been contaminated with the product, which had solidified and jammed the valve open [*failure to detect this situation implies failure to adopt principle 4.2.1 (a)*]. As this could well occur again on similar installations at the same site, it was decided to modify the system by tripping the pump as well when a high level was detected. Eight filters were modified in this way to prevent any reoccurrence [*without careful consideration of the functional safety requirements, the potential exists to violate principle 4.1.1 (d)*].

The following example of proof testing using the process fluid was encountered [*consistent with principle 4.1.1 (a)*]. As shown in Figure 2, it involves the addition of a pocket around the level probe and is suitable for some types of capacitance and conductivity probe when used for high level trips. The pocket has a hole beneath the probe, which allows the process fluid to enter the pocket when the level in the vessel rises. There is a breather hole in the side of the pocket to allow vapour in the pocket to escape.

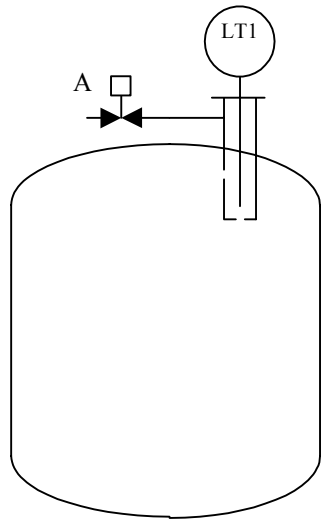


Figure 2 : An example of a level SIS proof testing arrangement

The line connected to valve A comes from a pump that is used to transfer process fluid into the reactor vessel. For trip testing, the normal process valve into the vessel (not shown) remains closed and valve A is opened. This allows process fluid to enter the pocket around the level sensor.

The sizing of the holes in the pocket and the sizing of the pipe through valve A is such that the flow rate through valve A is greater that the flow rate through the hole in the bottom of the pocket. This means that the pocket fills with process fluid and activates the level trip. On closing valve A, the process fluid in the pocket drains into the reactor and the trip can be reset. The hole in the side of the pocket is designed to take the full flow through valve A so that no pressure build-up occurs in the pocket.

The quantity of process fluid entering the reactor for testing can be measured and then used as part of the normal batch processing, or possibly returned to interim storage for re-use. Testing is carried out at any suitable point in the batch cycle.

Testing Temperature Loops

The manipulation of process temperatures is not often practicable due to the time it would take to raise or lower the temperature to the trip value and due to the high temperatures encountered in chemical processes. A common approach is to remove resistance thermometers or thermocouples from their pockets and place them in a calibrated bath or block to simulate the trip point temperature without removing them from the area. Again, this is not always practicable due to equipment being located in hazardous areas or operating temperatures being too high.

One organisation removes the elements from the pocket and does just this. They recognise that with head mounted transmitters it is more difficult to do this [*lack of consideration of testing requirements at the design phase leads to potential inconsistency with principle 4.2.1 (a)*]. If the measurement device is located in a potentially explosive atmosphere, then removal or exposure of equipment may generate a source of ignition. They also have experience of temperature elements being too short for their pockets, which could give an artificially low temperature measurement. This would not be picked up by usual forms of testing, other than a physical inspection of the element and comparison of its length with the depth of the pocket [*inconsistent with principle 4.2.1 (d), however, adverse consequences would be addressed by comparison of the element and pocket lengths*].

Another organisation operates in a similar way. Testing is generally done on-line by removing the element from its pocket and inserting it in a bath at a suitable temperature, however, this cannot be done on all installations. Alternative methods include disconnecting the element and connecting a decade resistance box or voltage source to drive the input to the trip point. Alternatively, they would rely on a SMART transmitter to drive itself to the trip point [*inconsistent with principles 4.1.1 (a) and 4.2.1 (a)*].

In another example, whether it is a ‘live’ test or ‘shutdown’ test, the end-user connects a decade box to the head of a 3-wire RTD probe. They realise that there may be a problem with pocket sensitivity and that this method does not test the pocket/probe interface and that they should check the response and calibration of the system [*currently inconsistent with principle 4.1.1 (d)*].

An end-user ensures that all temperature probes are mounted in pockets with breakaway couplings. To test a loop, the process control is placed in to manual mode, the probe is removed and a measurement of resistance or voltage at ambient temperature is checked against a standard. This suggests that the control sensor is also being used for trip duty. The logic solver is tested, by injecting a signal equivalent to the trip point. There is no duplicate system installed and it is recognised that they are ‘running blind’ whilst this is ongoing, so plan to install duplicate and comparison units.

An example of the testing of a process gas heater was provided. Elements installed in pockets are tested on-line, as they form part of triple redundant systems with 2 out of 3 voting. They use a thermocouple / PT100 simulator from the connection at the head, and check for ingress, integrity and connection security. When on line, they check for differences in readings between the three instruments to detect drift. To improve confidence and reliability, they would like to change the thermocouples regularly in addition to simulation, and check contact with the end of the pocket.

A further end-user's normal on-line test is to inject a current, voltage or resistance signal to simulate temperature and so test the operation of the safety system. The signal can be injected on some types of probes in front of the electronics and so only the sensing element is not tested. On some other probes the signal is injected after the electronics, particularly where the

transmitter is built-in to the probe, and hence the probe will not be included in the test [*lack of consideration of testing requirements at the design phase leads to inconsistency with principle 4.2.1 (a)*]. The probe can be compared to another temperature probe in the same line as a method of testing the response of the primary element. However, common mode failure may be an issue where both probes could suffer from coating, contamination or environmental conditions.

An example provided by another organisation involves the use of a pyrometer installation to measure the temperature of a converter bed, the normal operating temperature of which is greater than 900^{o}C. There is no practicable means of recreating operating conditions in a test situation and testing in anger could be hazardous, so testing is done by injecting a current signal into the trip amplifier of the SIS. There are two temperatures on the bed, so confidence in the measurement is provided by comparison. Periodically, a hand-held optical pyrometer is used through an inspection glass to confirm the temperature of the bed corresponds with the measurement [*consistent with principle 4.1.1 (b)*].

The measurement of temperature in the remainder of the plant is carried out using RTD probes mounted in pockets. Approximately 50% of these have the transmitter separate to the probe, so a resistance box can be connected to the transmitter and the corresponding resistance value to the trip point simulated. Where a transmitter is built into the head, a current signal is injected at a suitable point. It is realised that these test modes do not test the sensing element [*lack of consideration of testing requirements at the design phase leads to inconsistency with principle 4.2.1 (a)*], so on critical duties the probe would be removed, tested and calibrated on a regular basis. There is significant confidence in the measurements, as duplicate or other measurements slightly downstream accompany many systems.

An alternative approach to reliability was reported by another end-user. During shutdowns the elements are replaced on a regular basis with new ones and the old ones tested in batches for re-use at a later date [*inconsistent with principles 4.1.1 (a) and 4.2.1 (d)*].

The following example of temperature measurement shows how the process fluid can be used for the test.

Figure 3 shows a batch reactor. There are three process materials used for the reaction. It is during the reaction with all three present that there is potential for a reaction runaway. There is a high temperature trip using the sensor TT1. Independent temperature sensors are used for control.

The proof test procedure for this reactor was designed around the use of only one the liquids normally added to the reactor, thereby removing the risk of reaction. Following completion of the test, the plant operators could then add the other materials and produce a batch of product.

There are two benefits from this. One is that the trip is tested from the process fluid right through to the actuator [*consistent with principles 4.1.1 (a) and 4.2.1 (a)*]. The second is that no additional fluid is introduced into the reactor for the test and the fluid used for the test can be used to make product. However, there is a need to include a contribution for human error into the likelihood for a runaway in the reactor [*principle 4.7.1 (a)*].

One example of where errors can occur is illustrated in the following example. It is common practice to replace faulty SMART transmitters by uploading the faulty transmitter configuration to a hand held device and downloading it to a replacement spare unit. With a certain make of transmitter, this overwrites everything but the burnout direction. One end-user had around ten of these transmitters which had incorrect burnout directions because of this feature. Where this method is used for any transmitter, it is recommended to check all the parameters in the replacement before re-commissioning.

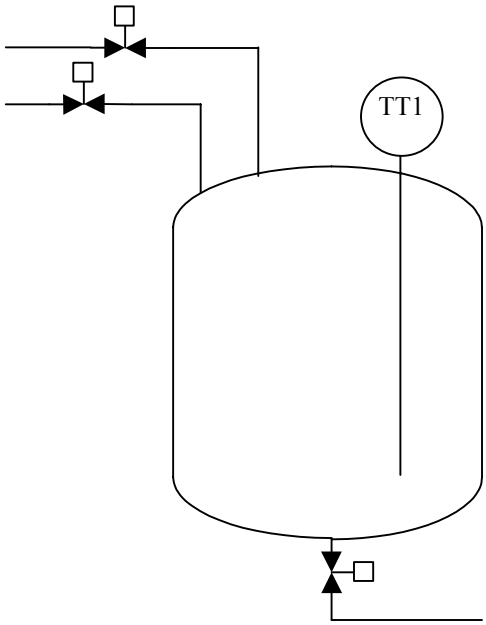


Figure 3 : An example of a temperature SIS proof testing arrangement

Testing Flow Loops

Flows under control are usually critical to the process, therefore it is not often feasible to manipulate them for the purposes of proof testing, however, there can be exceptions.

One end-user echoed this, reiterating that it is inherently difficult to test in-line flowmeters using the process fluid due to upset of process conditions. They invariably inject a signal into the electronics to simulate a trip condition and test the safety function, but realise that this does not test the 'wetted end' of the sensor [*principle 4.2.1 (a)*]. This holds true both for 'on-line' and 'off-line' testing.

Another end-user confirmed this, reporting that it is difficult to test or calibrate an in-line flowmeter whilst it is still installed in the line. The usual method of proof testing would be to inject a signal to simulate the flow measurement and so test the rest of the safety function as in the previous example. This, however, does not prove that the flowmeter is working correctly or is accurate [*inconsistent with principle 4.2.1 (a)*]. The flowmeter can be taken out of the line and tested on a proven flowmeter test rig but this usually requires a shut down. Another method is to use the flowmeter to fill a calibrated tank or compare it with another flowmeter, but any differences in density of the test fluid and actual operational fluid has to be taken into account.

If the SIS is based on a simple DP cell and orifice plate installation, the most common approach is to inject a differential pressure signal, simulating the flow, into the cell, however, this does not test the impulse lines and isolation or equalisation valves for possible blockage [*inconsistent with principle 4.2.1 (a)*]. The end-user providing this example would expect blockage to become apparent during normal operation by manifesting itself in an obviously incorrect reading. Regular maintenance and calibration of the sensor instrumentation gives the end-user confidence in the reading from the instrument [*consistent with principle 4.1.1 (b)*].

One end-user recounted an incident when a flow switch on a scrubber vent system was changed for a device designed to give a remote indication of the flow. The reason for the change was that the previous flow switch was very unreliable. The new instrument worked 'too well', as there was a small period (which was not realised in the HAZOP) in the scrubbers' cycle when the system had no flow and the previous switch did not detect this. Every time the cycle got to this

point, the reactor associated with the scrubber system would trip. On further investigation this was revealed and the trip system was moved to the fan shaft by means of a proximity switch to prevent this happening, and the flow measurement was returned to a measurement duty only. This modification is being extended to another seven similar systems.

One end-user declared that all their flows are tested by simulation, via either the electronics or injecting current signals [*inconsistent with principle 4.2.1 (a)*]. In some instances, when conditions allow, a calibrated, in-line, portable flowmeter is installed to give confidence in the accuracy of the measurement [*consistent with principle 4.1.1 (b)*].

An example was given by one end-user of a stabiliser addition system, where the flow is only a matter of litres per minute. These can be tested on-line as there would be minimal process upset. Trips on pump seal systems are never tested in anger but are always simulated to prevent damage to the equipment. For other flow trip system measurements, such as electromagnetic and vortex shedding flowmeters, it was estimated by this end-user that 95% of these are simulated by either using the electronics (30%) to simulate the trip signal or injecting a current signal (65%) at a suitable point. Only 5% of systems are tested by manipulating the process variable. This is due mainly to the difficulty of testing this type of instrumentation [*inconsistent with principle 4.1.1 (a)*].

For more complex flow installations employing such devices as electromagnetic, vortex shedding and coriolis flowmeters, the measurements are generally duplicated by diverse measurements in series for comparison [*consistent with principle 4.1.1 (b)*]. Current injection or the outputs of SMART devices are then used to test the logic solver. The end-user reiterated an important point that the equalising and isolation valves of DP systems must be returned to their original positions when reinstating [*principle 4.2.1 (f)*].

Discussion with another end-user centred on a DP installation. This was again treated as if it were a pressure installation. Vortex shedding and electromagnetic flowmeters are tested by using the test facility of the device or by injecting a current signal at the flowmeter output [*inconsistent with principle 4.2.1 (a)*]. The end-user does, however, recognise that this is not a complete test.

On a hydrogen flow to a hydrochloric acid burner, the process connection is a one inch Annubar tube. Due to the nature of the process, the Annubar and DP devices, and temperature and pressure transmitters are removed and all equipment sent to the manufacturer for verification and calibration [*inconsistent with principle 4.2.1 (d)*]. The safety system is then tested by simulation of the current signal. This end-user pointed out that the system is old and the reliability of the computation equipment needs to be reviewed and probably eventually replaced.

Another end-user example concerned a heat-exchanger associated with a reactor shell cooling-water installation which employs dual redundant in-line electromagnetic flowmeters. During an on-line test they use the software override facility and monitor alternative instruments. To verify the measurement they use the comparison between these instruments. They also check that the outlet temperature is of the correct order for the cooling water flow [*consistent with principle 4.1.1 (b)*]. They would like to improve the installation by including a positive displacement totaliser. They consider that removing and checking the meter on a test rig would increase reliability, however, a bypass would be needed and is considered uneconomic at the moment.

The findings of another end-user were that the calibration of in-line flowmeters relies upon the correct operation of their electronics, so they prefer to inject a current with the HART protocol removed. They recognise the reliability of HART, and the stigma associated with the corruption of electronic instruments. They find that this gives them an increase in reliability and confidence in the measurement.

Others (e.g. pH, density, speed etc.)

The majority of end-users did not provide examples of analysis instrumentation used on trip duties. Most felt that a lot of the instrumentation was not reliable enough for this purpose and only went down this route as a last resort. Of the few who did, there are examples below.

On one end-user's flare stack, on-line testing of analysers is possible due to dual redundancy. They use calibrated test gases injected into the sample impulse lines at a point near the analysers. The sample lines are proved by small flowmeters, used to set the sample flow-rate and alarm and trip on sample flow failure [*consistent with principles 4.1.1 (a) and 4.2.1 (a)*].

On pH control of a brine solution, the electrode system is situated in a bypass line. To test the system, the process control is placed in manual and the meter is buffer checked to test the trip and alarm points. The end-user recognises the shortcomings of the system and has recently installed a duplicate system using HART diagnostics to improve the loop reliability and made it a two out of two trip system.

Another end-user employed such a two out of two pH system on a bottoms analyser. This system is critical to product quality as product de-colouring or polymerisation can occur if the pH is not within tolerance. The system is calibrated every week using buffer solutions and the trip (final product to storage) is proof tested every three months using buffer solutions. The two out of two system gives confidence that the system will not trip if the electrodes become unserviceable on one of the installations.

Testing Actuators (Valves and Motors)

There was a wide and varied approach to the way that valves were tested. Some were not tested at all, some were only partially tested and, in most cases, only significantly tested during a plant shutdown. The most satisfactory way to test a final element is to check that it has the desired effect on the process under operating conditions. This is not always considered practicable due to the potential for process upset or shutdown. Some end-users indicated that they would use plant shutdowns or outages to test selected systems on a rotational basis [*potentially inconsistent with principle 4.4.1 (b)*]. Such an activity would require planning to avoid unnecessary disruption of production and consequential damage to equipment.

During discussions, one end-user indicated that they tested trip valves on-line by blocking the solenoid vent with a pressure gauge and operating the valve. This caused the valve to move slightly and also gave an indication on the pressure gauge of solenoid operation [*inconsistent with principle 4.2.1 (a) if this is the only proof test of the valve*]. This system was thought to work well though the installation and subsequent removal of the gauge would need to be very carefully controlled [*principle 4.2.1 (f)*].

One end-user stated that they need a valve to shut-off tightly within five seconds. The nature of the process is that this could not be tested on-line, so it was tested during a shutdown. Although they understood that this was not testing the valve under process conditions, it was as close as they could practicably get without tripping the plant every time a test was scheduled [*inconsistent with principles 4.1.1 (a), 4.1.1 (d) and 4.4.1 (b)*].

One end-user carried out a real test on critical shutdown valves on a rotational basis by actually tripping the plant. The philosophy used when the plants are on-line is to have multiple input test routines, then test the valve with one of these inputs on a rotational basis, when the process or plant conditions allow [*potentially inconsistent with principle 4.4.1 (b)*]. They hope to improve valve diagnostics by adding valve position feedback in the future.

The most general approach was to test valves off-line for many of the reasons stated above. One end-user does not close or open shutdown valves during on-line testing. These would be tested with a bypass in operation. During a planned shutdown, a full test is carried out, including the operation of the associated valves. This off-line testing has the disadvantage that the valve is not

being tested under operating conditions, however, this is seen by the end-user as the limit of practicability [*inconsistent with principle 4.1.1 (a)*].

Another end-user contended that valves can often only be tested when the plant is being shut down or actually shut down. Tests are generally limited to tripping the valve and observing that it moves to the open or closed position. They realise that they can only carry out limited checks on the effect on flows through the valve if there is no bypass. It is rarely possible to check that a tight shutoff has actually been achieved [*inconsistent with principle 4.1.1 (d)*]. An exception to this could be a pressure-proving scheme around gas valves on burners. To improve the test philosophy, the use of SMART positioners to confirm that valves actually close (via travel and torque feedback) is being considered. The same end-user (this was echoed by two other end-users) believed that it is not always necessary to overhaul valves, suggesting that this could be an expensive and often pointless rebuild which might result in a badly rebuilt, faulty valve going back into service. They think a better technique to use is to remove the valve from the plant, carry out a visual inspection, leak test, function-test and then flow scan the valve when it is back in-situ [*consistent with principles 4.1.1 (b) and, potentially, 4.1.1 (a) but potentially inconsistent with principle 4.2.1 (d)*].

One end-user admitted that their valves were not tested and that this would be their main area for improvement [*principle 4.2.1 (a)*]. They plan to establish a log that will automatically log the operation and travel times of key shutdown valves via open and closed limit switches during both routine and non-routine shutdowns. They will also begin routine visual inspection and maintenance to assist improvements in reliability.

One end-user's approach is to trip the valve from the initiator and record the closure time, check the leakage rate using downstream instrumentation, then overhaul any valves showing unsatisfactory results during a shutdown [*consistent with principles 4.1.1 (a) and 4.1.1 (d)*]. This is one of the most comprehensive tests that were discussed during all of the interviews but they are fortunate that they have a process that allows this.

One end-user prefers to overhaul and test their critical valves on a regular basis [*inconsistent with principles 4.1.1 (a) and 4.2.1 (d)*]. They say that this does give them the confidence in the safety loop function when combined with on-line input testing.

An example was provided for a chlorine gas system. A trip demands a shut-off seal, but this installation uses a conventional control valve for this function at present and the process needs to be off line in order to test it, however, tight shut-off cannot be verified under test conditions [*inconsistent with principle 4.1.1 (d)*]. To improve this they are going to install a dedicated shutdown valve to provide tight shut-off and employ a partial stroke testing facility to enhance its reliability.

Another example was provided for a natural gas system. An emergency gas injection system to the process must provide gas, via a double block and bleed arrangement, when demanded. Testing of the system is carried out by performing gas injection on the live process. The technician tests the system and position switches are used to confirm valve operation. The test could be improved by including a visual inspection of the valve position, although this would make it a two-man operation [*consistent with principle 4.2.1 (a)*].

With periods between plant shutdowns being extended, emergency shutdown valves (ESDV) may remain in the open position, without movement, for lengthy periods. Experience has shown that after extended periods without movement, there is a tendency for the valve to stick. This would result in the shutdown system failing to operate in the event of a genuine demand on the shutdown system, despite all other tests on the system being completed satisfactorily. A manufacturer of valve equipment contended that the application of Smart Valve Monitoring (SVM) can monitor the ESDV for faults based on comparing an original full closure fingerprint of the ESDV assembly and components, such as solenoid valves, against a partial stroke test. Their system can perform all tests at the ESDV designed closure speed without shutting the plant down. It can also include tests for connectivity between itself and a Safety PLC and claims

a 95% diagnostic coverage factor. In some cases, due to the speed of the test, full closure of the ESDV may be possible, resulting in a claimed 99% diagnostic coverage factor. The regular use of the partial test, in combination with other system tests will help to ensure that the ESDV will move when it is required, and that the ESD system is maintained in a fully operative state. These tests can be initiated and monitored by remote signals from the likes of a DCS or SCADA system. The use of such technology is being piloted by a major end-user at the moment and they hope to derive benefits form this. It is hoped that benefits will include the reduction of maintenance costs due to less frequent overhaul, reduction of spurious shutdowns due to malfunction or equipment failure, or even inadvertent inhibition of the ESD signal for long periods.

In the case of motors and drives it is most common practice to trip the drive from the initiator and check that the motor stops and that any secondary trips are operated. In general, it seems to be more acceptable to trip an on-line machine, reset the system and then restart the machine, than to trip then re-open a valve. These seem to be similar concepts, unless the consequence of tripping a valve has a more serious effect on the process. Where a motor is tripped by a SIS, it is generally done under process conditions when possible. If it is not, the off-line test consists of removing the fuses, but leaving the control fuse in place and watching the contactor operate.

4.1.4 Conclusions and Recommendations

Approaches to the proof testing of "wetted end" components are common, however the rigour varies. Amongst others, common approaches are:

- manipulation of process variables;
- pressure injection;
- current, voltage and resistance simulation;
- use of SMART features;
- comparison with alternative measurements;
- valve closure;
- inspection and overhaul.

Items that pose particular testing difficulties are valves and in-line flowmeters. The sealing capabilities of valves under operating conditions are rarely tested due primarily to the impact on process operation. Whilst it is the case that some processes may present significant risk during shutdown and start-up it is also the case that SIS should provide the specified safety functions with the specified integrity. Proof testing is an integral part of the demonstration of function and integrity and must therefore be given the attention which it deserves, however, where proof testing is likely to prove difficult then the design phase of SIS should seek to provide the specified functions and integrity in a manner which accommodates these difficulties. It is during the design phase of a chemical process that consideration should be given to the facilities that will be required to ensure the specified integrity of valves without necessarily demanding process shutdown. Consideration should therefore be given to specifying valve features that reduce the probability of malfunction and seat failure or to the targetted use of the proven capabilities of SMART positioners.

In-line flowmeters present little opportunity to apply proof tests that realistically manipulate the process variable. Differential pressure systems allow process variable simulation but introduce additional process connections and the potential for loss of containment or process contamination. The use of alternative or portable measurements to corroborate in-line flow measurements should be considered, particularly during the design phase of SIS. An interesting statistic provided by an end-user was that only 5% of flow systems are tested by manipulating the process variable. This is a subjective figure, however, it suggests that "wetted-end" testing of flow SIS may not be particularly rigorous.

The simulation of process variables and process conditions was common and is a necessity in cases where the risk associated with manipulation of process variables is not considered to be acceptable. Good practice in the application of simulation techniques would involve the comparison of sensor outputs with alternative process measurements, preferably diverse, to corroborate the measured value.

The use of SMART devices during proof testing should be treated with caution. The generation of current signals by digital electronics is no substitute for the testing of an instrument's ability to accurately measure a process variable. The use of such simulation should be accompanied by corroboration of the sensor reading unless sufficient diagnostic coverage can be demonstrated.

4.2 CONTENT OF PROOF TEST PROCEDURES

4.2.1 Statements of Guiding Principles

Purpose and Scope of Proof Testing

(a) Proof testing should be designed to expose any reasonably foreseeable unrevealed fail-to-danger fault conditions in all components including process sensors, logic solvers and final elements, and in the means of connecting the SIS to the process.

Overrides

(b) Where overrides are applied to SIS, they should be subject to strict controls to ensure their safe application and timely removal.

Partial Testing

(c) Where the partial testing of SIS or components of SIS is adopted, the impact on process operation, functional safety and overall test coverage should be established by assessment and additional controls should be applied where necessary.

System State on Trip Initiation

(d) SIS installations should be tested as found and should not be disturbed during proof testing.

Calibration

(e) All test equipment used for proof testing SIS should be calibrated and the calibration should be traceable to recognised national standards.

(f) SIS should be returned to their as-found state following testing and any necessary repair.

4.2.2 Rationale

Proof testing forms part of the routine actions that are required to maintain the required functional safety (as designed) of SIS. Their purpose is to reveal dangerous faults that would otherwise remain unrevealed and adversely affect the integrity of the SIS. Proof tests are executed using written test procedures, the content and accuracy of which govern the effectiveness of the test. The content of procedures addresses many issues, defining the scope of the testing, the test equipment to be used and the procedural controls to be adopted. Test procedures must also remain accurate throughout the lifecycle of SIS, particularly where change is encountered. The procedures communicate the required actions to the tester and should do so in a manner that takes account of human factors and seeks to minimises the risk of error and violation.

ANSI/ISA-S84.01-1996[2], the EEMUA Alarm Guide[3] and Kletz[4] provide published guidance on the scope and content of proof tests. Guidance on human factors is provided by references 5 and 6.

4.2.3 Research Data

The research revealed that industry is aware of the attributes of effective proof testing, although its implementation is variable. The research further suggested that consideration of the content of a proof test procedure tends to be dominated by the following issues:

- scope and coverage of the proof test;
- overrides;
- partial testing;
- trip initiation during testing;
- calibration of test equipment;
- the use of diagnostic facilities.

Scope and Coverage of the Proof Test

There was a unanimous view from interviews and workshops that proof tests should test all components of SIS, including the process measurement, the logic solver and the actuating device or "final element". Additionally, one end user workshop emphasised that the connection to the process in the form of impulse lines, orifice plates and dip pipes was vitally important as were services to the SIS, such as power, air and bubble gases, and external influences such as lagging, trace heating and environmental conditions. All interviewees reported executing "end-to-end" testing although one interviewee and one end user workshop reported difficulties with ageing and inherited systems, particularly where existing pipework arrangements were considered to preclude complete testing. The example procedures obtained during the research indicated examples of measurement simulation, such as current injection, rather than true process measurement.

All interviewees initially reported little difficulty in testing measuring elements and logic solver inputs, referred to by the supplier workshop as the "wetted end", although none reported explicitly inspecting the physical condition of process connections even though both end user workshops and one interviewee highlighted their importance. Further interviews and questionnaires revealed that difficulties were, in fact, encountered. One interviewee reported difficulties in achieving complete coverage of ageing or inherited systems, being able to test the field devices only [*inconsistent with principle 4.2.1 (a)*]. A batch operator reported difficulty in testing "inter-unit" trips where a number of production units would have to be aligned [*inconsistent with principle 4.1.1 (a)*]. An end user workshop reported that the majority of problems relate to impulse lines clogging but left an open question on how to test for these occasions. A workshop also stated that functional performance, such as the response of transmitters and the travel time of valves, should be tested.

The testing of the final element attracted much comment during all interviews and workshops. There was a clear division between operators of continuous processes and operators of batch or campaign processes. In general, continuous process operators perceived a conflict between the desire for high plant availability and the testing of final elements whilst batch process operators were generally able to take advantage of inter-batch downtime. Two interviewees reported the examination and testing of valves under workshop conditions, however, the supplier workshop commented that valves should be tested under process conditions [*consistent with principles 4.1.1 (a) and 4.2.1 (d)*]. Notwithstanding the impact on plant availability, there was general acceptance that the final element is the least reliable component of a SIS and demands robust testing.

The research indicated a preference for on-line testing amongst the continuous plant operators and support for this approach from the supplier workshop. This is not a surprising situation as manufacturing organisations seek to minimise plant downtime and suppliers seek to develop and market technologies that aim to satisfy this desire. It is also the case that start-up and shutdown tend to be the most hazardous periods of plant operation. Within the continuous industries, the general pattern of proof testing involves the on-line testing of measuring and initiating devices complemented by full "end-to-end" testing during maintenance activities, however, two interviewees reported the use of duplicate valves and manual bypass arrangements to allow full on-line testing [*consistent with principle 4.1.1 (a)*]. Of those two, one interviewee reported that the provision of full on-line test facilities allowing operation of the final element without process interruption is a recently adopted standard. Again, batch operators reported taking advantage of inter-batch downtime.

ANSI/ISA-S84.01-1996[2] and the EEMUA Alarm Guide[3] provide comprehensive guidance on the coverage of proof testing.

Overrides

The subject of overrides and bypasses was an integral part of the consideration of coverage yet generated sufficient discussion to warrant consideration in its own right. The need for overrides and bypasses was unanimously reported as arising from a wish to carry out routine testing without adversely affecting production. Nine interviewees specifically reported the use of override or bypass facilities with only one reporting no bypasses being used on shutdown systems. Of the nine, seven reported that input overrides are provided as a matter of course whilst two emphasised that overrides are the exception to the rule. Two interviewees in the refining and petrochemical sectors reported the use of process bypasses for final element testing under strictly controlled conditions [*consistent with principle 4.2.1 (b)*]. An instance of the use of overrides was reported by a batch operator, indicating that the use of overrides is not restricted to continuous processes. One example encountered involved the use of duplicate valves or valve trains whilst another involved the use of manual bypass valves around trip valves, controlled by the use of Castell key systems. One interviewee from the chemical industry reported that the provision of process bypasses is not deemed to be cost effective. One interviewee reported tests on two-out-of-three systems being carried out without overrides. The supplier workshop suggested that overrides should be designed out and one interviewee explicitly stated that the emphasis is to design systems to allow testing without overrides.

Overrides were highlighted as an area of concern by all workshops and the need for strict controls to ensure their safe application and timely removal was unanimously stressed. Typical controls reported were management authorisation, alarm generation, continuous indication and the continued functioning of process alarms during the override period. Override switches were unanimously reported as being key-operated and manual process bypasses were reported as being subject to mechanical interlocks. Valve jamming / clamping and pneumatic solenoid bypass arrangements were also reported as a means of override. Management procedures for the control of overrides and bypasses were stressed by three of the interviewees. One interviewee reported that bypass authorisation requires the signature of the Site Director and is valid for a twenty-four hour period. Another interviewee reported the adoption of two classes of override based on risk and vulnerability with the higher risk overrides requiring the dual authorisation of both Shift and Operations Management. The same interviewee reported the use of unique keys for each override to which access is strictly controlled.

Both end user workshops stated that overrides should be time-dependent, with one interviewee reporting that overrides associated with a DCS will accommodate a re-alarm function after six hours to ensure that they are not overlooked [*consistent with principle 4.2.1 (b)*]. One end user workshop and one interviewee stressed that process alarm functionality is maintained throughout override periods. An end user workshop reported that the application of overrides is

reviewed and that copies of override records are displayed in the control room for daily review [*consistent with principle 4.2.1 (b)*].

Partial Testing

In the context of this research, the partial testing of SIS describes two situations; the testing of system components at different times and frequencies or the testing of sub-sets of functions of single components.

Whilst the need for complete testing of all components of safety-related systems was unanimously supported it was equally unanimously recognised that production pressures, particularly associated with continuous processes, significantly affect the ability to carry out such tests in their entirety at the appropriate frequencies [*inconsistent with principle 4.4.1 (b)*]. The research found that it is common practice amongst continuous operators to use overrides to allow the on-line testing of measuring and initiating devices and to schedule the testing of logic solvers and final elements to coincide with production outages. Only two interviewees reported routinely testing final elements in-line.

Providing less agreement was the partial testing of individual components. The discussions concentrated on valves, although the shortcomings of injection testing of sensors was stressed by one interviewee citing an example of a proof test procedure which specifies the use of thermocouple simulators, arguably a partial test. All workshops raised the issue of partial operation of valves. The supplier workshop questioned the usefulness of partial closure tests and commented that partial stroke testing with feedback is of limited use but that the deployment of effective intelligent diagnostic facilities could improve the usefulness of the information gathered. One end user workshop suggested that process constraints dictate that certain valves can only be operated through a small range of their travel and commented that risk assessment is necessary to establish the impact on process operation, however, concern was raised that similarly rigorous risk assessment might not be applied to the impact on functional safety. The other end user workshop recognised the option of partially operating valves but stressed that valves can fail to seal, particularly in harsh environments, and cited an example of pebbles being found on inspection. Recognising this possibility, one interviewee reported leak testing all safety-related valves on a two to eight year basis [*consistent with principle 4.1.1 (a) but potentially inconsistent with principle 4.4.1 (b)*]. One interviewee reported limiting the opening travel of a ball valve during testing to avoid breaking of the seal. This was due to asset and environmental issues and was risk assessed.

The partial stroking of safety block valves has been examined in an article by Angela Summers and Bryan Zachary[7] which proposes that failure mode and effects analysis (FMEA) and data from the Offshore Reliability Data (OREDA) Handbook[8] can be used to demonstrate that the maximum percentage of failures which can be detected by a partial stroke test is 70%. The FMEA and reliability data must be applicable to specific SIS, however, the article demonstrates an objective approach to partial testing.

Trip Initiation

The issue of appropriate methods of initiating SIS emerged as a common theme throughout the research. Both end user workshops and three interviewees specifically highlighted the need to ensure that the initiation of safety-related systems under test should be consistent with operational conditions.

Initiation by driving the process variable to its demand condition clearly provides the most accurate evaluation of the SIS and two interviewees reported striving for this situation. The EEMUA Alarm Guide[3] recommends driving the alarmed process variable into the alarmed state, however, this does not imply that the process itself should be driven into a hazardous state. If processes are driven into potentially hazardous states and SIS do not operate as expected, there is a real possibility that hazardous situations may arise, indeed an end user workshop cited two

examples of organisations being criticised by the HSE for raising vessel levels in order to test trips.

The use of simulation techniques was reported by an end user workshop and the use of thermocouple simulation was evident in an example proof test procedure. One interviewee reported investigating the use of equipment suppliers' own in-built test capabilities for some sensors, such as RF admittance level probes, in order to initiate SIS on-line without driving the process variable to the demand condition. The use of alternative process fluids was raised by a workshop, however, one interviewee suggested that adopting this approach over using the actual process fluid must be justified [*consistent with principle 4.1.1 (a)*].

An end user workshop commented that proof testing can disturb equipment such as temperature sensors and questioned whether installations should be tested as found. SIS should indeed be proof tested as found in order that any fault conditions are recognised and installations are not unnecessarily disturbed. To further illustrate this point, Kletz[4] describes a situation where a trip was removed from its case before testing but when it was required to operate in anger, a pointer fouled the case and could not move freely [*the incident illustrates inconsistency with principle 4.2.1 (d)*].

Calibration

Six interviewees representing all industrial sectors explicitly stated that all test equipment is calibrated and that the calibration is traceable to national standards. The necessity for traceable calibration was supported by all workshops.

Diagnostics and Diagnostic Coverage

Three interviewees reported interest in the application of intelligent diagnostic facilities and in-built test facilities, with two interviewees trialling such facilities with a view to improving production availability. Both end user workshops perceived benefit from the use of diagnostics, but both cited reluctance to implement such technologies. One workshop reported confusion over the relationship between diagnostic coverage and proof testing whilst the other reported difficulty in obtaining diagnostic coverage data from suppliers. Not surprisingly, the supplier workshop proposed benefits from the use of intelligent diagnostics.

It is not the intention of this research to provide a detailed examination of diagnostic coverage. However, it is useful to reiterate that the purpose of proof testing is to detect unrevealed faults at the time of testing whilst diagnostic coverage allows the detection and remediation of fail-to-danger fault conditions between proof tests. The perceived benefit for industry is that the application of diagnostic techniques where none previously existed has the potential to decrease the proof test frequency and the scale of routine testing, however, it does not necessarily render components any more reliable.

4.2.4 Conclusions and Recommendations

Scope and Coverage of the Proof Test

The research suggests that the achievement of complete proof test coverage of SIS is a unanimous desire of the chemical industry but that there is some recognition that it is not being fully realised. The process connection is an integral component of a SIS and may possess dangerous failure modes, often attributable to blockage or deposition, which could cause the SIS to fail on demand. Such failure modes should be detectable by proof tests. Nevertheless, there is strong evidence that comprehensive "end-to-end" testing is practicable and is being undertaken. With respect to proof test coverage, the following recommendations are made:

- proof testing should test all components of SIS which could lead fail-to-danger conditions;

- proof test procedures should address the condition of process connections, particularly impulse lines;
- proof test procedures should address the condition of any necessary services such as power, instrument air, gas supplies, trace heating etc.

Overrides

Overrides of SIS in the form of input overrides or final element bypasses are common in the chemical industry. Interviews and workshops suggested that considerable care is taken over the use of overrides and, whilst there is considerable pressure to maintain production during proof testing, there is recognition that the inappropriate application of overrides can render SIS inoperative. There is evidence that overrides are being avoided where practicable, for example during the testing of multiple channel SIS. There is also evidence that procedural controls are put in place where overrides are applied and that the application of overrides is reviewed.

When used in the presence of adequate controls overrides provide a means of maintaining both functional safety and process availability, however, if deployed without controls they have the potential to significantly undermine functional safety. Opinion varies over whether overrides should be provided within standard well-proven designs and controlled by robust well-understood operational practices or whether they should be avoided where possible. They are certainly a recognised feature of manufacturing processes, being addressed by publications such as ANSI/ISA-S84.01-1996[2]. Ultimately, functional safety must not be compromised by the application of overrides so, whether they are favoured or not, they must only be applied after consideration of risk.

Based on the research, the following recommendations are made:

- the application of overrides and bypasses should be subject to a process of risk assessment which should be documented and reviewed where modification occurs;
- the application of overrides should be subject to robust control processes involving authorisation by personnel competent to assess the risk involved.

Partial Testing

The research suggested that the proof testing of components of SIS at different frequencies and times is common practice. Specifically, it is common to test initiating devices on-line and to test the associated logic and final elements during planned outages. This is an entirely appropriate approach to the maintenance of functional safety provided that the combination of on-line and off-line tests lead to adequate coverage at an adequate frequency and adequately represents the operating environment. Less common, but present nevertheless, is the partial testing of individual components in the form of measurement simulation and the partial stroking of valves. Such partial testing arises when the complete testing of components is not deemed to be reasonably practicable and must be subjected to rigorous justification. Based on the research, the following recommendation is made:

- where partial testing of SIS or their components is adopted, its justification should be documented and it should be explicitly addressed within the demonstration of achieved functional safety.

Trip Initiation

The methods of initiating SIS are many and varied but whatever the method it must provide adequate confidence that the SIS would be initiated if required under operating conditions. A distinction must be drawn between manipulation of the process variable and manipulation of the process. Manipulation of the process variable without driving the process into a potentially hazardous situation should be achieved where reasonably practicable. Manipulation of the

process may be necessary to provide a realistic test of functionality but this must be accompanied by a risk assessment to ensure that the probability of achieving an unsafe state remains acceptably low. Equally, any departure from realistic operating conditions during proof testing must be accounted for within the safety integrity assessment of the SIS. Based on the research, the following recommendations are made:

- a method of SIS initiation should be adopted which adequately establishes that the SIS would operate under operating conditions;
- where reasonably practicable, SIS initiation should be via manipulation of the process variable using process fluids. The provision of facilities for achieving this should be considered during design of SIS;
- the initiation of SIS should not involve placing the process in a state where failure of the SIS under test could lead to a hazardous situation;
- SIS should be proof tested as found rather than being disturbed, thereby reducing the potential for unrealistic tests, loss of as found system failure data and introduction of faults on system reinstatement.

Calibration

The research established unanimous agreement that traceable calibration should exist for all test equipment, therefore, the following recommendations are made:

- calibration records should exist for all test equipment and should be traceable to national standards;
- the recording of test equipment serial numbers and calibration due dates should form part of proof test procedures.

Diagnostics

The research identified varying amounts of uncertainty and confusion over the use of diagnostic facilities and over the application of the term "diagnostic coverage" to proof testing. An exercise to establish the extent of the implementation of diagnostic coverage, together with examples of good practice would be of benefit to industrial users.

4.3 FORMAT OF PROOF TEST PROCEDURES

4.3.1 Guiding Principles

(a) The written proof test protocol should take account of recognised human factors in order to reduce the potential for errors and violations.

(b) The written proof test protocol should be subject to formal document control procedures.

4.3.2 Rationale

A proof test is a set of sequential actions which, when correctly executed, will verify the correct operation of a SIS at the time of testing. The procedure to be followed by a tester is generally presented as written text and the format of the written procedure can introduce weaknesses into proof testing. The involvement of human beings has the potential to introduce behavioural issues, such as error and violation, where an error is an unintentional deviation from a procedure and a violation is a deliberate deviation from a procedure. Both error and violation can influence the effectiveness of proof tests and lead to an undesirable outcome, therefore test procedures should be constructed and presented in such a way that the potential for error and violation are

minimised. Guidance on producing procedures that minimise the potential for error and violation can be found in references 5 and 6 respectively.

It is also imperative that the test procedure describes a sufficient examination of the SIS and is recognisable as the currently applicable version. In short, it should be generated in line with the principles of Quality Management. Clause 9 of ANSI/ISA-S84.01-1996[2] provides guidance on minimum general content of a test procedure, which covers preparation for test, the test and expected results and reinstatement after test.

4.3.3 Research Data

The research found some differences of opinion over the general approach to proof test procedures. One interviewee reported a preference for generalised procedures executed by experienced people whilst four reported a preference for explicit procedures to minimise the need for specific knowledge. Three interviewees specifically reported the use of generic procedures although only two interviewees specifically reported the deployment of generic designs. An end user workshop offered the general view that proof tests need to be more prescriptive, suggesting that the Electrical Engineering community benefits from such prescriptive procedures. The other workshop explicitly recommended that proof test procedures should be presented as a collection of sequential steps with each step being verified.

A debate restricted to the pros and cons of detailed and generic procedures fails to address the accepted issues associated with human factors as described by references 5 and 6. Proof test procedures should be based upon an understanding of the task and the users. Thought must be given to those who will use proof test procedures and the level of information they need, therefore, the competence of the tester must be understood and procedures must be supported by training in order to promote their effective use.

The examples of test procedures collected from nine interviewees demonstrated a common approach of describing each sequential step. Of the eight, three demonstrated the use of a tick or comment facility for each step with one of the three providing a separate results sheet for each test allowing the recording of the result of each test. The remaining five examples did not provide the facility to verify each step. Six of the examples provided sign-off facilities for the tester with four of the six allowing for counter-signature.

Three interviewees specifically reported the provision of additional information in support of proof test procedures. Such documentation includes cause and effect charts, sequential flow charts, system descriptions and function diagrams. One interviewee stated that test protocols do not normally reference or include the design intent, although newer procedures have a short section detailing the purpose of the test and the equipment upon which it is being performed.

Appendix 3 reproduces examples of test procedures, or sections thereof, which illustrate elements of good practice. The example of Appendix 3.1 is presented in a structured manner with a title page providing an overview of the test, precautions and preparation followed by a procedure broken down into clearly defined steps. The use of short sentences is evident, as is the use of highlighted text to provide warnings and draw attention to important information. Lower case font is used throughout; research has shown that test written entirely in uppercase font is slower and more difficult to read.

The examples of Appendices 3.1 and 3.2 provide mechanisms for the tester to verify the successful completion of test steps with the latter providing the facility to describe the test results in the form of a code for input to and manipulation by a database application. Both examples demonstrate simple revision control. Appendix 3.3 reproduces an example of a document control sheet that clearly defines the responsibilities and definitions associated with approval of the proof test procedure.

The trend appears to be to ensure that test procedures are sufficiently detailed to eliminate the requirements for experienced technicians to be involved in testing, however, the assumption that

there is a best way to present a proof test procedure irrespective of the attributes of the tester is an indication of poor practice and a lack of understanding of the potential impact of human factors [*inconsistent with principle 4.3.1 (a)*]. An appreciation of the competence of the tester is an integral part of the construction of proof tests. Providing too much information may lead to less use of the procedure if it becomes too difficult to follow whilst too little information may mean that an inexperienced person will not be able to carry out the task.

A clear example of a violation arising from an inadequate proof test procedure was encountered during an end user workshop and involved a tester who tested a SIS differently to the written procedure because the written procedure was not workable [*inconsistent with principle 4.3.1 (a)*]. The SIS was tested in this way for a number of years but when the tester left the company the new staff reverted to the written procedure. The ongoing violation of the proof test procedure could have been prevented or stopped in a number of ways, for example, by involving the tester in the production and maintenance of the procedure or by undertaking a robust validation process prior to fully implementing the procedure.

4.3.4 Conclusions and Recommendations

The research suggests that consideration of the format of proof tests appears to be based on authors' perceptions of testers' competencies rather than on objective understanding. The approach should be adequate provided that the perceptions are correct and the attributes of the tester community remain stable over time, however, this is unlikely to be the case in an environment where skilled personnel are reported as being in short supply and there is an increasing reliance on temporary contract personnel. The lack of evidence of proof test procedures being designed for defined user groups coupled with the lack of evidence of the competence of user groups being maintained accordingly, increases the potential for error and violation in the execution of proof tests.

The absence of a single test procedure that exhibits all of the attributes associated with good practice suggests that proof test procedures could be generally improved. Whilst many attempt to apply approvals and gather similar information, the styles vary. The chemical industry would benefit from a structured approach to procedure writing based on the need for validation, data recording and an appreciation of human factors. References 5 and 6 and related publications should be reviewed by authors of proof test procedures and used as the basis of a common approach.

Based on the research and on the consideration of human factors by reference 5, the following recommendations are made:

- the design of proof test procedures should be based on a firm understanding of the test and the requirements and competence of the tester;
- ownership should be promoted by involving testers in the preparation and maintenance of procedures;
- proof test procedures should be presented in a consistent format, including, for example:
    - the purpose of the procedure;
    - precautions which must be observed to avoid potential hazards;
    - special tools or equipment needed;
    - initial conditions which must be satisfied before starting;
    - references to other relevant documents such as data sheets, manuals etc.;
    - procedural steps to perform the task safely and efficiently;
    - actions to be taken on discovery of a fault;
- warnings should be clear and conspicuous and precautions reiterated in procedural steps;

- the style of proof test procedures should promote ease of use by:
    - keeping sentences short and precise;
    - using positive active sentences such as 'open valve A then valve B";
    - using normal lower case text rather than ALL CAPITAL LETTERS;
    - retaining open spaces and avoiding cluttered pages;
- proof test procedures should be subject to strict document control.

4.4 PLANNING AND SCHEDULING

4.4.1 Guiding Principles

(a) Proof testing should be an integral and explicit part of the planning and scheduling of the safety management system.

(b) The timing of proof tests should be dictated by the need to demonstrate and maintain functional safety and should not be compromised by operational or business considerations.

4.4.2 Rationale

The proof testing of at least some components of SIS requires those components to be taken out of service for some time. This is not necessarily a problem for batch and campaign manufacturing organisations as advantage can be taken of inter-batch downtime, however, no such opportunities exist for continuous process manufacturing organisations and the need for proof testing often conflicts with the need to maintain high levels of plant availability. Proof testing may be scheduled to coincide with planned equipment downtime, provided that it results in sufficiently frequent proof testing.

4.4.3 Research Data

All participants in the research reported the routine testing of SIS, although, the rationale and planning behind the routine testing varied. The frequency of routine proof testing was set by one of three means; reliability analysis, the application of standard rules and, in one case, a subjective historical decision. A common practice, reported explicitly by six interviewees, was to calculate maximum allowable intervals between tests then apply standard testing based on these limits [*consistent with principle 4.4.1 (b)*]. Standard intervals for partial or complete proof testing were three months, six months, one year and two years. One interviewee reported the allocation of test frequencies based on classification of the SIS and therefore on a standard design. Another interviewee reported establishing test frequencies through reliability analysis but applied a maximum allowable period between tests of two years. One interviewee reported adopting a twenty-six month period between tests for a long established installation based on the historical decisions of an Operations Manager [*potentially inconsistent with principle 4.4.1 (b)*].

The planning of proof testing is carried out by a variety of resources. Five interviewees explicitly reported the use of computer-based maintenance scheduling systems, with one being dedicated to SIS. There were reports of planning being carried out by engineering teams, process teams, maintenance teams and planning teams.

The research revealed a unanimous aspiration to execute proof testing without impacting on production. This was particularly obvious amongst continuous process manufacturing organisations but was also evident amongst batch and campaign manufacturing organisations, with one batch manufacturer reporting being driven by pressures to minimise disruption to production. A workshop reported a "constant battle" between production and downtime for testing [*inconsistent with principle 4.4.1 (b)*]. The general approach was to schedule the proof testing of some or all of the components of SIS to coincide with planned production outages

such as shutdowns, overhauls or batch changes. Only two interviewees reported addressing the conflict between production and proof testing by striving for full on-line testing. Eight interviewees explicitly reported scheduling proof tests to coincide with shutdowns or overhauls, however, one of the eight reported difficulty in matching resource availability to plant availability implying an opportunistic rather than planned approach. A further one of the eight explicitly reported taking advantage of unplanned outages where practicable and rescheduling subsequent proof tests accordingly.

Two further approaches to minimising production disruption were encountered. A fairly common practice, reported explicitly by four interviewees and one workshop, was the grouping of proof tests which could be conveniently executed as a single activity, concentrating disruption into a single time window. Such a group might include all SIS associated with a single plant item such as a vessel or reactor. Another approach, reported by two interviewees and one workshop was the alignment of proof tests with statutory inspections made under regulations covering pressure vessels, nominally performed on a biannual basis [*potentially inconsistent with principle 4.4.1 (b)*].

There was evidence that proof test intervals are being stretched to maximum theoretical limits, for example, a workshop reported a case of the period between routine shutdowns being extended to two years resulting in the existing proof test frequencies being reduced accordingly, thus invalidating the basis of the SIL [*inconsistent with principle 4.4.1 (b)*]. There is now pressure from external authorities to return the proof test frequencies to justifiable values.

The supplier workshop raised the issue of "occasional use" systems such as research and mothballed batch facilities, suggesting that these may tend to require SIL3 systems and require regular testing. In this case, the proof testing of SIS could be carried out prior to operation then at the appropriate frequency during operation. This is an example of the need to address proof testing requirements during development of a maintenance regime.

4.4.4 Conclusions and Recommendations

Proof testing is an integral component of the maintenance of the safety of an operating plant and should therefore be fully integrated into maintenance regimes. Indeed, given the relatively high frequency of the tests and the potential impact on production, the scheduling of proof tests should account for a significant amount of maintenance planning effort. Additionally, care must be taken to ensure that production pressures and mathematical proofs do not override practical considerations and lead to undetected reductions in functional safety.

The following recommendations are made:

- proof test frequencies should be based on objective and justifiable criteria and any alignment of proof testing with planned outages should be justified, particularly where the time between outages exceeds twelve months;
- proof testing should be treated as an integral component of the safety management system planning activities.

4.5 RECORDS OF PROOF TESTING

4.5.1 Statements of the Guiding Principles

(a) The results of proof testing should be recorded and maintained for the purposes of periodic reporting, audit and historical analysis.

(b) Data arising from proof testing should be collated, reviewed and acted upon in order to maintain or improve functional safety.

4.5.2 Rationale

The records of proof tests are required to enable the review of the design basis and performance of SIS and to demonstrate compliance with safety requirements. The initial reliability analysis of a SIS is based on data such as required risk reduction, component failure rates, component fail-to-danger rates and operational demand rates, gathered from a number of sources. Although performed by competent personnel, the application of these figures to particular situations may involve some judgement and the review of data collected during proof testing affords an opportunity to validate the design basis of SIS or to modify SIS design in line with actual process and SIS performance.

4.5.3 Research Data

Recording

The research found that the results of SIS proof tests and details of failures under test are widely recorded but that the data generated is rarely subjected to analysis or reporting. Typically, test records indicate whether the test was successful and provide a description of any faults found, details of any corrective action taken and details of the tester. Two interviewees reported that failure data is not normally gathered [*inconsistent with principle 4.5.1 (a)*]. Interviewees unanimously reported the completion and retention of test records in paper form with the records generally being held by a local Engineer. In some cases the completed test procedure constituted the record of test whilst in other cases separate results sheets were preferred. An end user workshop reported strong views to move towards common electronic repositories for test records. The same workshop queried the length of time that records should be kept and suggested that the retention period of results should be specified on each test procedure based on frequency of test.

Only four interviewees reported the transfer of pertinent information from paper records to electronic formats for the purpose of subsequent analysis and reporting. One interviewee reported that alarms associated with safety-related systems are logged by a central information management system allowing reporting of SIS initiation but suggested that no further analysis was performed. One interviewee reported the use of plant item record sheets to capture and collate test information associated with major plant items. Another reported that failure data is held and analysed to provide reliability norms [*consistent with principle 4.5.1 (b)*]. The allocation of fault codes was explicitly reported by two interviewees and observed in an example test procedure provided by another (reproduced in Appendix 3.2). The use of codes allows simple analysis and reporting using database and spreadsheet applications.

The supplier workshop suggested that strict reporting of component faults would improve the credibility of reliability data but suspected that many components are considered to be throw-away items and that their failures are not reported [*inconsistent with principle 4.5.1 (a)*]. This suspicion was supported by an interviewee who stated that the visibility of operational downtime takes precedence over SIS analysis. The supplier workshop also raised the possibility of using intelligent devices to record component and system performance and some evidence of data gathering using intelligent valve positioners was presented at an end user workshop. An end user workshop also commented that key reliability data is not available for ageing or inherited systems, however, the research suggests that the data is available somewhere but is simply not collated into a useable form and is not easily traceable.

Traceability was a key issue at both end user workshops with one workshop reporting the examination of a paper trail by the Regulatory Authority. The other workshop presented a general view that the Regulatory Authority does not give credit for past experience, however, the research suggested that the quality of record keeping and general traceability of data is insufficient to formally demonstrate valid previous experience.

Review

The research identified the following review processes relevant to proof testing:

- the review and reporting of overdue tests;
- the review of SIS component failures under test and the associated remedial actions;
- the review of SIS component failures in operation;
- the review of SIS and process performance against the assumptions of the risk and reliability analysis;
- the review of the quality of proof test execution.

Seven interviewees representing all participating industrial sectors explicitly reported the analysis and reporting of overdue proof tests to senior management, some via computer-based maintenance management systems. Reporting, review and action was on a monthly or quarterly basis. An end user workshop suggested that the number of overdue tests could be used as a key performance indicator (KPI).

The approach to the review of failures under test varied greatly involving, for example, formal quarterly reporting to senior management, ad-hoc review based on the experience and judgement of the tester or no review at all. One interviewee reported that the E/I Manager reviews reported failures, suitably coded and grouped to identify trends and reports the findings to senior management via a quarterly report [*consistent with principle 4.5.1 (b)*]. One interviewee explicitly reported the use of a computer-based maintenance management system to store condition reports. One interviewee reported the instigation of root cause analysis investigations of failures under test [*consistent with principle 4.5.1 (b)*], one interviewee reported reliance on the local quality management system and four interviewees reported review of failures under test by local E/I Engineers. One interviewee reported a feedback mechanism which relies wholly on testers bringing concerns to the attention of maintenance management which then has the opportunity to review areas of concern [*potentially inconsistent with principle 4.5.1 (b)*]. In this case, the appreciation of trends and concerns remains with the Maintenance Engineer [*inconsistent with principle 4.5.1 (a)*]. Two interviewees reported identifying and reviewing fail-to-danger figures [*consistent with principle 4.5.1 (b)*]. No interviewees reported reviewing repair times, however, one interviewee reported reviewing process availability losses. Five interviewees explicitly reported the use of formal incident investigation procedures to address failures of SIS under test or on demand during operation.

The review of SIS performance was reported by four interviewees whilst one reported plans to instigate such reviews in the future and two reported a general review of critical equipment and process hazards. Two interviewees explicitly reported reviewing SIS fail-to-danger rates whilst one reported reviewing demand rates. In these cases it was reported that design and testing of SIS were modified accordingly [*consistent with principle 4.5.1 (b)*]. One interviewee reported that a formal review of the test frequency is required after a maximum of five tests and involves the review of the records of previous tests.

The review of the quality of execution of proof tests was raised by three interviewees. One interviewee reported a formal review of the execution of proof tests after a maximum of five tests whilst another explicitly defined the responsibility for such reviews. Another interviewee reported the instigation of such reviews at a local level by plant Engineers.

Examples of the output of reviews were few. One interviewee reported that experience revealed very few complete or catastrophic failures of shutdown systems against a slightly higher incidence of out of tolerance failures. Another interviewee reported only one SIS failure to date, involving a calibration error. A review of fail-to-danger rates was undertaken in an attempt to demonstrate that proof test frequencies could be reduced, however, the exercise revealed that frequencies were at or near their lower limits.

The identification and reporting of incidents was a common issue for the workshops with all workshops suggesting that a formal approach to incident and failure reporting and analysis should be adopted. The supplier workshop highlighted the availability of intelligent field devices, which can provide data to information management systems for the purpose of analysis and review.

A reliability problem that was identified by one end-user involved the regular breakdown of transmitters on a compressor due to excessive vibration. This was picked up by the trip test records system [*consistent with principle 4.5.1 (b)*], and the installations were modified to include flexible connections to the process.

4.5.4 Conclusions and Recommendations

The research suggested that a significant amount of data is not recorded, and that the data which is recorded, is rarely reviewed or in a form which allows easy analysis. The ability to review SIS performance against design data or to provide data in support of claims of past operating experience is similarly rare. Evidence of effective SIS performance was anecdotal, in some cases based on the experience of long-serving personnel. The inability to reproduce or review performance data raises doubt over whether the demonstration and improvement of functional safety of SIS are considered a priority.

The lack of performance data could be attributed in part, to the treatment of many components as throwaway items. It was suggested that many malfunctioning components are simply replaced and discarded leaving their true reliability unreported.

Recording

Although records of tests are generally kept they are rarely kept in a form which facilitates future analysis. The time required to be invested tends to preclude the analysis of recorded data, however, failure to record data could lead to maintenance problems in the future and many of the perceived historical issues could be overcome in the medium term by effective reporting and analysis. Additionally, traceable records could be used to influence Regulatory Authority perceptions and practices.

The following basic data should be recorded:

- the steps undertaken during testing;
- the results of steps;
- details of all faults;
- details of corrective actions including time to repair and effectiveness of remedial action;
- the duration of the test (start time / end time);
- details and signature of the tester;
- validation details and signatures.

Additional recommendations are made as follows:

- the purpose of making, retaining and tracing records should be understood;
- the procedure for the generation, retention and retrieval of records should form part of the general procedures covering the management of SIS;
- any initial processing of the data, such as the input to database systems and the allocation of fault codes, should be carried out immediately after testing.

Review

The research suggests that a significant quantity of data is generated by proof testing but that most is not reviewed. With only two examples of the review of fail-to-danger figures and no reported reviews of repair times, it appears that there is significant reliance on assumptions made during the SIS design process. It further suggests that effective review of such data is practicable and can provide information that can be used to validate or modify SIS, leading to the maintenance or improvement of functional safety. The availability of desktop spreadsheet and database applications provides the ability to store, organise and review data, however, the ability to review data generated by proof testing depends largely on the quality of recording at the time of proof testing. A formal yet manageable approach to recording and review is therefore required.

A formal approach to capturing and reviewing proof test data brings two main benefits. Firstly, it provides evidence of efforts to continually improve safety management procedures and maintain functional safety. Secondly, it will, over time, increase the quality of information such as fail-to-danger rates, demand rates and repair times on which the design and operation of new and existing SIS are generally based. This will allow proof test intervals to be optimised and will help to alleviate some of the concerns over ageing and inherited systems.

Based on the research, the following recommendations are made:

- the purpose and benefits of effective recording and review should be understood and the requirements defined by the safety management system;
- the review of proof test data should be facilitated by organising recorded data immediately after proof testing, for example, by inputting it into database applications and allocating fault codes.

4.6 COMPETENCE

4.6.1 Guiding Principles

(a) Personnel participating in all aspects of the proof testing process should be demonstrably competent to carry out their allotted tasks.

(b) The responsibilities for all aspects of proof testing should be clearly identified and communicated.

(c) Documented verification by competent persons should be applied to the appropriate stages of the proof testing process to ensure that each test is sufficient in terms of content and execution.

4.6.2 Rationale

The need for people to be competent to carry their allotted tasks is a fundamental and obvious prerequisite for the avoidance of unsafe situations, particularly when the tasks involve the maintenance of safety-related systems. With respect to proof testing, there is a need to ensure that those individuals involved in the design of SIS, in the writing of proof test procedures, in the execution of proof tests and in associated approval processes recognise their responsibilities and are demonstrably competent. There is also a need to ensure that appropriate standards and competencies are applied to proof testing via a structured approval process.

The need to formally identify and measure competence has been addressed by the collaborative publication, Competency Guidelines for Safety-Related System Practitioners[9]. Appendix B of that document provides guidance on competency assessment relating to the maintenance and modification of safety-related systems.

4.6.3 Research Data

Competence

Whilst some views were expressed on the need for appropriate competence to be deployed in the design of SIS and in the writing of the associated test procedures, the interviewees and workshops concentrated upon the competence applied to the testing activities. The research found that although there was unanimous agreement that appropriate competence is essential, there is little evidence that it is addressed in a formal manner. Only four interviewees reported a formal approach to competence, the majority reporting no formal processes for the specification, establishment, recording and maintenance of SIS proof testing competence. Two interviewees reported the provision of formal training, a further three reported the provision of initial training but no interviewees reported the provision of refresher training.

An interview highlighted a structured approach to competence assessment and certification [*consistent with principle 4.6.1 (a)*]. The process involves all staff and contract Instrument Technicians attending a training course explaining the corporate and local requirements for proof testing of safety systems. After the training, technicians are certified to work on safety systems subject to limitations of authorisation and confidence in understanding of the underlying principles. There are two levels of certification; Part A covers general principles and mainly focuses on the field side whilst Part B contains several sections and addresses specific plants (in Manufacturing Groups) and also covers calibration and issue of test equipment. Contract Technicians are generally certified to Part A, however, established contract technicians, may be certified to specific sections of Part B.

There was evidence of differing opinions over the true meaning of 'competence' as applied to proof testing. For example, a suggestion was made that test procedures should not rely on the knowledge of the technician performing the test to ensure correct execution whilst it was also suggested that the competence of persons carrying out proof testing is a key factor in determining effectiveness. Additionally, eight interviewees reported reliance upon general technical qualifications to demonstrate competence in proof testing with one interviewee making no distinction between the testing of SIS and the testing of other instrumented systems. One interviewee commented that compliance with standards and procedures is most threatened by the loss of competent personnel.

The use of third party contractors in proof testing was reported by eight interviewees with five explicitly reporting avoiding the practice. Of those who use third parties, only one interviewee reported doing so as a matter of course, using preferred suppliers to test all SIS, whilst the remainder reported using third parties to supplement permanent resources during periods of high demand. Only one interviewee reported applying the same formal competency certification to contract staff as is applied to permanent staff, however, only long-term contract technicians would be certified to the higher level of competence. One interviewee reported an almost total reliance on the experience of permanent staff due to very low staff turnover, and is concerned about the risk of key staff leaving and the difficulty of succession planning. Another interviewee reported the retention of experienced personnel to be a key concern.

The subject of competence generated significant discussion at the workshops. It was suggested by the supplier workshop that users seem to ask for SIS information as part of the general documentation package for equipment based on little understanding of the principles of IEC61508[1]. It was also suggested that, whilst warranties require that equipment be maintained by competent personnel, there is little definition of 'competent' in this context.

One end user workshop suggested that a general movement towards using contract technical personnel rather than permanent staff reflected a change in the nature of industry and it was further suggested that a rapidly changing workforce leads to difficulties in controlling competence. The workshop observed a trend towards ensuring that proof test procedures are sufficiently detailed to eliminate the requirement for experienced technicians to be involved in

proof testing. To arrest the slide in expertise the workshop suggested the possibility of requiring NVQs for proof testing and of specifying competency requirements within proof test procedures. It was also suggested that the use of process operators to perform proof tests appears to be a growth area and questions were raised over whether competency issues have been adequately addressed.

The other end user workshop suggested that management structures can lead to ignorance of competencies, especially when technicians responsible for executing proof tests respond to a Maintenance Manager who may not be able to judge technical competence.

Responsibility

Thirteen interviewees were able to explicitly name the appointed role responsible for the operation and testing of SIS whilst one senior engineer was not aware of such an appointment [*inconsistent with principle 4.6.1 (b)*]. Of the thirteen, eleven reported that proof testing is the responsibility of a senior Responsible Engineer whilst two reported that proof testing is the responsibility of Operations Management. For large installations, the Responsible Engineer generally has the power to delegate responsibility to local plant Engineers. One interviewee reported the use of a responsibility matrix to communicate responsibilities [*consistent with principle 4.6.1 (b)*]. Making asset owners responsible for the execution of proof testing was cited as an effective mechanism for managing any conflict between routine proof testing and plant availability.

The supplier workshop cited an example of the responsibility for the provision of probability of failure on demand analysis being passed to a supplier without all of the necessary data, implying a lack of appreciation of accountability by the user [*potentially inconsistent with principle 4.6.1 (b)*]. An end user workshop stressed the need to distinguish between responsibility and accountability, a particularly important aspect of the practice of delegation. In this context, the Duty Holder may delegate responsibilities associated with proof testing to suitably competent persons but remains accountable for the successful execution of the proof testing process. The same workshop stressed the need to clearly define ownership, roles and responsibilities. Additionally, an example was encountered of plant Engineers delegating testing to a maintenance group but having no control over who performs the tests [*inconsistent with principles 4.6.1 (b) and 4.6.1 (a)*].

An attendee at the other end user workshop reported that the Operations / Asset Manager has the responsibility to ensure that proof testing is carried out but often delegates to the Engineering group. The workshop stressed that someone must be clearly appointed to own trip testing and control which personnel can execute the tests, suggesting that company procedures should define who has responsibility for taking decisions in the event of failures during proof tests. It was further suggested that only the asset owner should be authorised to give dispensation from carrying out proof testing.

Approval

The research identified the following approvals relating to proof testing:

- approval of the proof test procedure;
- approval of the proof test execution;
- approval of proof test deferrals;
- approval of overrides and bypasses.

Three interviewees and both end user workshops reported the practice of having an independent person witness the first implementation of a proof test to ensure that it is practicable and clear and to ensure that any relevant feedback from the tester is captured. A further three interviewees reported the independent approval of proof test procedures by Responsible Engineers or by a combination of engineering and operations personnel [*consistent with principle 4.6.1 (c)*]. One interviewee suggested that the designer should witness the initial test, however, design personnel have often moved on by the time of commissioning, especially when large design contractors are employed. Nevertheless, the feedback of operational practicalities to design personnel was supported by both end user workshops [*consistent with principle 4.5.1 (b)*].

Competence and independence were raised as key issues. There was general agreement that approvers should be competent and should bring a level of objectivity through independence, however, whilst stating that approvals and peer reviews should be carried out by demonstrably competent personnel, one end user workshop observed that the number of such people has diminished significantly. This indicates that skill shortages may become a significant issue.

Independent approval of the execution of proof tests was evident from four interviews and two example procedures, however, the nature of the independent approval varied from operations personnel to maintenance personnel to engineering personnel. The purpose of the independent approval of execution was generally to show that the outcome of tests had been reviewed.

An example of an incident attributable to a failure to adequately validate a test procedure was given during an end user workshop and involved a tester who tested a SIS differently to the written procedure because the written procedure was not workable. The SIS was tested in this way for a number of years but when the tester left the company the new staff reverted to the written procedure. The suggested learning from the workshop was that feedback from testing is essential in order to initiate change where it is necessary, however, a robust validation process involving approval by appropriately competent personnel could have prevented the ongoing violation of the proof test procedure [*principles 4.6.1 (c)*].

The approval of proof test deferrals and dispensations was raised by an end user workshop, which agreed that it should be considered as a guiding principle. This is covered generally by principle 4.6.1 (c)..

4.6.4 Conclusions and Recommendations

Competence

There is limited evidence of formal controls associated with the competence of those individuals responsible for proof testing, particularly those responsible for its execution. There is a general view that generic technical qualifications coupled with some initial training is sufficient to ensure the maintenance of functional safety, especially where the tasks involved can be expressed in a prescriptive manner. Where prescriptive procedures are employed, care must be taken to ensure that human factors are taken into account.

There is recognition that an industry trend towards outsourcing has the potential to reduce the competence applied to proof testing unless appropriate controls are put in place, although, examples of effective controls are few. The provision of initial training for new or contract personnel appears to be common practice although its future provision will depend on the maintenance of a core of permanent expertise in an environment where the retention of such expertise is already proving difficult. Experienced and skilled personnel are also more likely to identify and act on issues which less experienced personnel may miss, particularly during exceptional or unexpected conditions.

Based on the research, the following recommendations are made:

- a competence profile for proof testing should be generated by the Duty Holder which details the necessary knowledge, training and experience required;

- the competence necessary to perform a proof test should be specified within the proof test procedure;
- records of those deemed competent to test SIS should be retained;
- personnel regularly engaged in proof testing should receive refresher training;
- succession planning should be adopted in an effort to maintain access to sufficient competent personnel;
- where the maintenance of competence is an issue, periodic audits of proof testing and related issues by experienced and skilled personnel (internal or external) should be undertaken.

Responsibility

Large organisations were found to exhibit clearly defined management structures, which lead to clear definitions and communication of individual responsibility. Smaller organisations recognise the need to define roles and responsibilities but do not necessarily experience the same pressures of scale to adopt a formal approach. Whatever the practical pressures, the need to maintain the functional safety of SIS is paramount and structures and processes should be deployed accordingly. To this end, the roles and responsibilities associated with the proof testing of SIS should be clearly defined and communicated. The following recommendations are made:

- the responsibility for proof testing should be assigned to a nominated role who should be clearly informed of, and accept, their responsibilities and accountabilities;
- any delegations of responsibility should be made in a structured manner to suitably competent persons who should be informed of, and accept, their responsibilities;
- roles and responsibilities should be clearly documented and communicated.

Approvals

It is extremely important to recognise that approval is a process of verification and validation, not simply the application of a signature. The questions;

"what are we trying to demonstrate?" and

"what does approval mean in this case?"

should be asked, before deciding which documents should be approved by whom. In the context of proof testing the process of approval should ensure that:

- the proof test procedure describes a sufficient test of a SIS;
- the proof test procedure is safe to apply to the process or equipment under control;
- the outcome of the proof test has been reviewed and any appropriate actions initiated.

It is therefore necessary to ensure that the correct competencies are brought to bear, for example:

- an experienced Engineer or technician would be able to assess the sufficiency of a test;
- the asset owner or plant manager should be able to assess the safety of the test in the operating environment;
- a Maintenance Engineer might be best placed to ensure that any necessary corrective actions are undertaken.

It is equally important to recognise that the process of approval can be a time-consuming activity, particularly the approval of proof test procedures associated with large assets. Nevertheless, the process of ensuring that SIS proof testing provides the appropriate functional safety is not optional and the accountability for functional safety cannot be delegated by the Duty Holder, therefore, the provision of appropriate resources and budgets must be planned.

Involvement in the process of verification and validation allows design personnel to appreciate the practicalities of testing SIS which they design and, where applicable, the proof test procedures which they write. It also allows operations and maintenance personnel to appreciate the design intent of the SIS. Such involvement may be possible where design personnel remain available to a site or facility but may be not be possible where third parties are involved.

Based on the research, the following recommendations are made:

- a robust process of verification and validation should be applied to the design and execution of proof test procedures;
- the involvement of competent people in the design of proof tests should be maximised, for example, the experience of operations personnel could significantly benefit the design process;
- the initial execution of a proof test should be independently witnessed leading to modification where necessary;
- the purpose of every approval should be defined and understood;
- personnel should be demonstrably competent to provide approvals.

4.7 AWARENESS OF HAZARD AND RISK

4.7.1 Guiding Principles

(a) The written proof test protocol should describe all identified hazards associated with undertaking the test together with the any necessary precautions.

4.7.2 Rationale

Although the purpose of proof testing is to maintain functional safety, the very action of testing has the potential to expose the equipment under control and the tester to risk. It is therefore important that those involved in the execution of proof tests take precautions to minimise risk.

The equipment owner has a duty of care to ensure that the action of proof testing does not lead to an unsafe state. In order to achieve this, the hazards and risks must be understood and suitable precautions put in place. Risk can be minimised by ensuring that proof testing is carried out by informed, competent personnel, following well structured risk-assessed procedures.

The proof test procedure is the means of providing the tester with an awareness of the risks associated with the test and must therefore be written in a manner which the tester understands and which clearly and conspicuously conveys warnings and precautions. Human factors must be considered; references 5 and 6 provide further guidance.

4.7.3 Research Data

Only three interviewees reported carrying out formal risk assessments of proof test procedures [*suggests general inconsistency with principle 4.7.1 (a)*] with a further two stating reliance upon risk assessments associated with the issuing of permits to work. Of the three interviewees which reported risk assessment of proof tests, two reported that it was done as a matter of course [*consistent with principle 4.7.1 (a)*]. Of those two, one reported that all procedures are risk

assessed by a multi-functional team, the other reported that the precautions taken during testing, specifically the quantity and level of authorisation required for overrides, are based upon an assessment of risk and vulnerability.

The research revealed two distinct views on the minimisation of risk during proof testing. One approach is to provide prescriptive, unambiguous procedures, which fully define the necessary activities and constrain the tester to a set of actions which are unlikely to result in an unsafe state. For example, one interviewee reported that test procedures are written in a clear and concise way to minimise the need for specific knowledge of a system and reduce the risk of making mistakes. The second approach is to provide less detailed procedures and rely upon the expertise of the tester. For example one interviewee reported that tests are not generally detailed exhaustively but the expertise of technicians is recognised and equipment suppliers' manuals are used where necessary. Of those interviewees which specifically addressed this issue, three reported generating prescriptive proof test procedures whilst one reported reliance upon the expertise of the tester. The common feature of these approaches is the reliance on someone's competence; that of the tester, the author or the assessor(s) of the proof test procedure [*potentially inconsistent with principle 4.3.1 (a)*].

The supplier workshop suggested that proof test procedures should include a description of the safety function and an explanation of the process of SIL determination. Whilst a description of the safety function could help the tester to understand the purpose of the SIS and the risks associated with its testing, a description of the SIL determination process may be less useful. One end user workshop suggested that risk assessment should be undertaken in order to understand and, by implication, communicate the hazards associated with proof testing to the tester.

Of the nine example proof test procedures obtained, four provided a mechanism for explicitly defining the precautions to be taken and for providing the tester with additional information [*consistent with principle 4.7.1 (a)*]. None of the examples explicitly defined the process hazard being addressed by the SIS, however, one of the examples used bold typeface to describe precautions and the reasons why they were being taken [*consistent with principle 4.7.1 (a)*]. Examples of sections of procedures, providing supporting information that were encountered, are:

- purpose;
- scope;
- initiating variable(s) / items actuated;
- references;
- definitions;
- pre-requisites / process conditions for testing;
- preparation (including test equipment requirements);
- notes (free format).

The proof test procedure of Appendix 3.1 uses a title page to provide a subset of this information in tabular form.

4.7.4 Conclusions and Recommendations

A key consideration in the execution of proof testing is the avoidance of unsafe states during the testing. To this end, all personnel involved in proof testing, including the tester and the equipment owner, should be aware of the risks associated with their actions and with the necessary precautions. The awareness of risk and hazard, together with a description of the associated precautions, should be provided in a conspicuous manner to complement the general competence of the tester. To this end, the following recommendations are made:

- a risk assessment of each proof test procedure should be carried out to identify potential hazards to the equipment under control, to the tester and to the wider operating environment;
- the differences between the testing environment and the operating environment should be clearly understood by those managing and executing proof testing;
- the risks associated with each test should be summarised in the proof test procedure together with the associated precautions;
- warnings should be conspicuous, using bold typeface or other means of attracting the attention of the tester;
- a brief description of the purpose of the proof test and the equipment under control should be included in the proof test procedure enabling the tester to fully understand the impact of the test;
- the risks associated with the proof test should be reviewed after any change to the SIS and the proof test procedure should be modified accordingly.

4.8 MANAGEMENT OF CHANGE

4.8.1 Guiding Principles

(a) Management of change should explicitly require consideration of the impact of change on proof testing.

4.8.2 Rationale

Change is common in the process industries. Well-managed change has the potential to improve safety and business performance, however, poorly managed change has the potential to undermine the functional safety provided by SIS. It is therefore essential that the full impact of change on SIS is properly considered in its widest context. The impact of change on the testing regimes of SIS, from timing of routine tests to the detailed stepwise procedures, is as important as the impact on system design, though arguably less obvious to those charged with implementing the change.

Change Management is a recognised issue throughout industry, indeed it is a fundamental element of a Quality Management System (QMS). Whilst a documented QMS applies strict change control to product-related activities the same pressures of certification do not necessarily apply to SIS and their related documentation. Guidance, however, does exist, for example, ANSI/ISA-S84.01-1996[2] provides specific guidance on the management of change, specifically within clause 10, "SIS Management of Change". With respect to proof testing, it states that all changes to operating procedures, process safety information and SIS documentation (including software) shall be noted prior to start-up, updated accordingly and that all SIS documentation shall be revised, amended, reviewed, approved and be under the control of an appropriate document control procedure. The UKOOA guidelines[10] also promote a rigorous change management system.

4.8.3 Research Data

The research highlighted a number of initiators of change which impact on the operation and testing of SIS, namely:

- process modifications;
- chemistry modifications such as catalyst changes;
- product changes;

- batch changes (one organisation reported that one loop can have up to 6 sets of settings);
- small scale manufacturing improvement projects;
- large scale capital projects;
- SIS improvements based on a review of operational data;
- proof test procedure modification based on feedback from testers;
- organisational changes due to divestments, acquisitions and mergers (seven interviewees reported some form of organisational change resulting in the need to adopt, or otherwise deal with, systems and procedures from new or past owners);
- proof testing itself, where temporary measures such as overrides are introduced.

An additional issue, put forward as a potential initiator of change, was the perceived increased pressure to address ageing and inherited systems. This was raised in the end user and supplier workshops. Notwithstanding the existing duties of end users, the emergence of IEC61508[1] has raised concerns over its impact on those systems that have been inherited or have been in service for many years.

The research suggests that procedures controlling the management of change are widely adopted, indeed all of the organisations interviewed operate some form of documented change management procedure with nine interviewees explicitly reporting change management as being based on some form of risk assessment. With respect to proof testing, only three interviewees explicitly refer to proof test procedures within their change management procedures [*suggests general inconsistency with principle 4.8.1 (a)*]. Additionally, an end user workshop commented that although "modification forms" are completed for set point changes, they are not always completed for a change to the procedure for a trip test [*inconsistent with principle 4.8.1 (a)*]. Notwithstanding the reported current practices, the research showed an overwhelming belief by end users and equipment suppliers that the operation and testing of SIS, and especially supporting documentation, should be subject to rigorous change management.

Although all interviewees adopt change management procedures, some differences in approach were noticeable. The research suggested that strict adherence to a widely deployed QMS within the pharmaceutical industry delivers a robust approach to change management and more particularly to the control of documentation such as operating instructions and instrumentation test procedures. Two interviewees reported a "standard design" approach to SIS, with one organisation going as far as to prohibit any change to the design of a SIS once the standard design has been deployed. As stated previously, only three interviewed organisations explicitly address proof test procedures via their change management procedure with the remaining organisations relying upon the competence and experience of discipline Engineers to address the impact of change on proof test procedures.

The competence of personnel involved in the change management process was identified as a key issue through interviews and workshops. One interviewed organisation reported that its recommended approach to the modification of proof test procedures is to involve the author of the test procedure in addition to those with responsibility for testing. An end-user workshop reported evidence of the person carrying out the test writing up any changes to the proof test procedure, a situation which must be backed up with appropriate checks to ensure that the proof test remains appropriate in the wider context. Another organisation reported that training, including any special requirements for maintenance or testing, is provided for all site personnel when any major change is made. An end user workshop commented that peer review is an essential part of the approvals process and must include all disciplines and questioned whether the person who approves a change is always competent to assess that change, particularly with respect to technological judgements. To illustrate the need for appropriate authorisation of

change, Kletz[4] suggests that set points should be changed only after authorisation in writing at an agreed level of management.

Interviewees and workshops highlighted the scope and coverage of change management processes. One organisation commented that every change is managed through a standard change control process with inputs from operations, quality, all engineering disciplines and others. Two interviewees specifically mentioned that original risk assessments and design intent are referenced when executing changes to SIS, ensuring that the purpose of the SIS remains clear. The point was made by one interviewee that the like-for-like replacement of components should not constitute a change. The validation of changes was raised by an end user workshop which suggested that although it was common for the initial performance of a proof test to be witnessed, it was not necessarily as common for this to be done if the test method were changed.

The control of SIS documentation emerged as a key issue. A common suggestion for a guiding principle was that SIS documentation should be properly controlled with the appropriate expertise and review processes being deployed where change occurs. However, concern was raised via an end user workshop over the amount of approvals that may be necessary and the point was made that some end users do not enjoy the benefit of a large engineering resource. Whilst this is a genuine concern, the employment of sufficient resource remains the responsibility of the Duty Holder. An example of a robust SIS-specific change control procedure was encountered requiring approval, by both Engineering and Operations Management, however, even in this case, the interviewee reported a general problem with availability of personnel. An end user workshop commented on the need to ensure that the information for the trip settings for different batches should be stored in one place only. On this subject, five interviewees reported using, or planning to use, electronic document handling techniques to ensure version control of "master" proof test procedures and other SIS documentation.

4.8.4 Conclusions and Recommendations

Although evidence of the use of formal change management procedures was widespread, only three interviews revealed explicit reference to the need to assess the impact on proof test procedures. There was evidence of reliance on Instrument Engineers to gauge the impact of changes on instrument maintenance documentation and therefore, by implication, on proof tests. Even changes to plant maintenance frequencies can have an impact on proof test procedures, especially where they have been based on specific planned outages.

The following recommendations are made on the basis of the research:

- changes to proof tests must be based on an unambiguous statement of required functional safety;
- change management procedures should explicitly state a need to consider the impact of change on proof tests;
- testers and the original authors should be involved in modifications to proof tests to ensure that tests remain practicable and consistent with the design intent. Where original authors are unavailable, other suitably competent design authorities should be nominated;
- changes to proof tests should be accompanied by appropriate training, especially for testers and operators.

5. SEARCHES

The following sections present the findings of searches of information available in the public domain. In general, specific references to proof testing are rare, hence little information relevant to the research was encountered.

5.1 LOSS PREVENTION JOURNAL

The following documents were reviewed:

Vol.7 – 1,4;

Vol.8 – 4,5,6;

Vol.9 – 1,2,3,4,5,6;

Vol.10 – 1,2,3.

The literature was reviewed with respect to any specific references to proof testing and any contribution it may have had towards any incident, e.g., bad practice, failure to carry out etc.

It was found that the articles in the journal were mainly of a 'mathematical' and 'process modelling' nature and that no reference was made to proof testing either in the articles or the references used.

5.2 IChemE LOSS PREVENTION BULLETIN

Literature from incident bulletins from the last several years was reviewed with respect to any specific references to proof testing or maintenance and any contribution it may have had towards the incident.

In bulletin 143, an analysis of past incidents, the frequency of primary causes of incidents where it was possible that proof testing 'elements' were involved were reported as follows:

- equipment or mode of operation modified – 7.9% (37);
- safety instrumentation failures – 5.8% (27);
- wrong equipment opened up or operated – 3% (14);
- shut valve passing fluid flow – 1.9% (9);
- control or motor operated valve stuck – 1.3% (6);
- control valve bypass left open – 0.6% (3).

5.3 MISCELLANEOUS LITERATURE SEARCHES

A broad search of publications, journals and conference proceedings was undertaken to extract and analyse those entries relevant to the research topic under consideration.

The following reference material was reviewed:

- Chemical Abstracts 1998 - 2001;
- Loss Prevention Bulletin 1999 – 2001;
- Chemical Engineering Journal 2000 – 2001;
- Computing & Control Abstracts 1999 – 2001;
- UKOOA Guidelines for Instrument-Based Protective Systems Issue 2 Nov 1999;

- Loss Prevention and Safety Promotion in the Process Industries – 9th International Symposium;
- EWICS TC7 publications;
- Safety Critical Systems Club symposia;
- IEE Computing & Control Journal 2000 – 2001.

5.3.1 Method of Search

The method chosen reflected the need to be able to undertake a first-cut analysis of the material using key words such as 'safety', 'protection', 'trips' and 'alarms' in the case of journals, bulletins and abstracts, followed by a more detailed review of those specific references cited from the first-cut.

For conference proceedings the first-cut analysis consisted of searching the paper titles for relevance to the subject under review, and if pertinent the second cut a review of the abstract followed if required by review of the contents of the paper. For other material (books, trade association material) the first cut consisted of a search of contents and index for appropriate subject matter with detailed review of sections and chapters if relevant.

5.3.2 Findings

Many of the publications provide information relating to the maintenance of SIS, however, none explicitly address proof testing. Some publications provide detailed guidance on the management of SIS during their operational life and make recommendations that support the guiding principles developed from the industrial research. The content of these publications is summarised as follows.

UKOOA Guidelines for Instrument-Based Protective Systems – Issue 2, November 1999

Section 7, Operations & Maintenance, provides guidance on responsibilities (7.2), Maintenance and Testing (7.3), Documentation and Records (7.4), Control of Changes (7.5) and Assessment of Protective System Integrity (7.6). The document also makes the following comments and recommendations relating to proof testing.

- Each responsible person is accountable for ensuring that the systems continue to perform to the required performance standards. Specific responsibilities include:
  - ensuring appropriate test procedures are available;
  - assurance of competency of the operator and maintenance technicians who work with or on the system;
  - control of access to the system including use of key words and passwords;
  - control of overrides;
  - co-ordinating testing of the system;
  - control of changes;
  - ensuring appropriate records are maintained;
  - accessing results of testing, demands rates, system failures etc.
- The maintenance, testing scope, frequency and responsibilities should be clearly documented.

- Maintenance overrides should be formally authorised and documented and the status regularly assessed.
- Results of periodic testing should be assessed and appropriate measures taken to maintain required system integrity.

HSE PES 2[11]

The document provides comprehensive checklists which, whilst not specific to proof testing, does promote the need for a formal operational management system to include:

- fault reporting and analysis;
- supervision to ensure the continued adherence to agreed procedures;
- training provided appropriate to the tasks to be undertaken and personnel involved;
- review of maintenance and test procedures;
- prevention of unauthorised access to systems.

CCPS Guidelines for Safe Automation of Chemical Processes

This publication includes a section (6.4.3) on Functional Testing. Whilst this covers testing prior to operation it provides a complete list of validation requirements to be covered in a test, which can be taken forward and used in follow-on proof testing. A specimen proforma for functional test checklists is provided.

Section 6.5 covers testing frequency requirements. In addition to the routine testing it recommends additional testing:

- after upgrading the vendor-supplied operating system;
- after major work that changes system communications network configuration;
- after major upgrades of hardware components.

Section 6.6 provides guidance on installed test connections and necessary bypasses. It recommends that written procedures exist that prevent having more than one signal bypassed at the same time. All instances of bypassing should be documented and the return-to-normal position should be a requirement prior to signing off that any work has been completed. Where a SIS allows, changes in positions of all bypass switches should be automatically logged. Only those bypasses that are truly required for maintenance or testing should be allowed in the system and no master bypass switches should be allowed.

5.3.3 Conclusions on the Literature Search

Whilst this literature search was extensive it did not reveal specific factors directly relating to proof testing, nor did it identify any dangerous occurrences or incidents where the root cause was directly linked to proof testing. However, there are a number of points drawn from the material, which can underpin the development of the set of guiding principles. The majority of these apply to management and operational systems, rigorous change control and responsibilities.

5.4 INDUSTRY INCIDENT DATABASE

The database (on 30 Jan 2001) contained details of 23 incidents. The majority of the incidents recorded are associated with maintenance problems, modifications or line ruptures, however, one suggests a lesson that relates to protective systems and is described in Table 4 in a generalised manner to preserve confidentiality.

Table 4 : Summary of findings of a review of the industry incident database

Description of Incident	Relevance to SIS Proof Testing
An incident resulted from a pair of block valves (series) which were both passing when notionally closed and a third valve, intended to bleed dilution air into the oxidiser was shut by the control system.	The inability of both block valves to seal adequately remained an unrevealed dangerous fault.

5.5 MAJOR ACCIDENT REPORTING SYSTEM (MARS) DATABASE SEARCH

The MARS search facility was used to query the database, however, no accidents were reported as being attributable to proof testing issues.

5.6 HSE PROSECUTIONS DATABASE (HTTP://WWW.HSE-DATABASES.CO.UK)

The database (checked on 30 Jan 2001) contained details of incidents from a wide range of industrial and other sectors. This review focuses on the 'Manufacturing Sector' and the 'Extractive and Utility Supply Sector' as being most relevant to the chemical industry.

There are 55 incidents recorded for the 'Manufacturing Sector' and 6 for the 'Extractive and Utility Supply Sector', covering the period from 1994 to 2000. The majority of the incidents recorded are associated with 'unsafe systems of work' and no incidents could be directly attributed to proof testing.

5.7 GENERAL CONCLUSIONS FROM SEARCHES

Documented evidence of causal links between incidents and deficiencies in proof testing is rare, although references to the general management of SIS are more common. The searches have identified instances of criticism, corrective action and recommendation associated with the maintenance of SIS though not with proof testing. Furthermore, the results of the searches do not suggest a need to develop guiding principles beyond those developed as a result of the industrial research

The lack of documented evidence might be thought to indicate that weakness of proof testing practices is not a significant contributing factor to incidents, however, the style and content of the reviewed publications and databases indicate that reporting mechanisms are simply too coarse to identify proof testing as a contributing factor.

APPENDIX 1 : GUIDING PRINCIPLES FOR PROOF TESTING

Proof Testing Practices (4.1.1)

(a) The proof test of a SIS should reflect real operating conditions as accurately as possible. If reasonably practicable, the SIS should be initiated by manipulation of the process variable without driving the process into the demand condition. Any approach which involves driving the process into the demand state should be accompanied by risk assessment and additional controls.

(b) Where process variables cannot be safely or reasonably practicably be manipulated, sufficient confidence in the correct operation of sensors should be gained by other means, such as comparison with other measurements.

(c) The inherent difficulties associated with testing valves and in-line flowmeters should be addressed during the design phase of SIS and additional provisions such as corroborative measurements should be made where necessary.

(d) Proof tests should address the necessary functional safety requirements of SIS, including functions such as response time and valve leakage class.

Content of Proof Test Procedures (4.2.1)

(a) Proof testing should be designed to expose any reasonably foreseeable unrevealed fail-to-danger fault conditions in all components including process sensors, logic solvers and final elements, and in the means of connecting the SIS to the process.

(b) Where overrides are applied to SIS, they should be subject to strict controls to ensure their safe application and timely removal.

(c) Where the partial testing of SIS or components of SIS is adopted, the impact on process operation, functional safety and overall test coverage should be established by assessment and additional controls should be applied where necessary.

(d) SIS installations should be tested as found and should not be disturbed during proof testing.

(e) All test equipment used for proof testing SIS should be calibrated and the calibration should be traceable to recognised national standards.

(f) SIS should be returned to their correct state following testing.

Format of Proof Test Procedures (4.3.1)

(a) The written proof test protocol should take account of recognised human factors in order to reduce the potential for errors and violations.

(b) The written proof test protocol should be subject to formal document control procedures.

Planning and Scheduling (4.4.1)

(a) Proof testing should be an integral and explicit part of the planning and scheduling of the safety management system.

(b) The timing of proof tests should be dictated by the need to demonstrate and maintain functional safety and should not be compromised by operational or business considerations.

Records of Proof Testing (4.5.1)

(a) The results of proof testing should be recorded and maintained for the purposes of periodic reporting, audit and historical analysis.

(b) Data arising from proof testing should be collated, reviewed and acted upon in order to maintain or improve functional safety.

Competence (4.6.1)

(a) Personnel participating in all aspects of the proof testing process should be demonstrably competent to carry out their allotted tasks.

(b) The responsibilities for all aspects of proof testing should be clearly identified and communicated.

(c) Documented verification by competent persons should be applied to the appropriate stages of the proof testing process to ensure that each test is sufficient in terms of content and execution.

Awareness of Hazard and Risk (4.7.1)

(a) The written proof test protocol should describe all identified hazards associated with undertaking the test together with the any necessary precautions.

Management of Change (4.8.1)

(a) Management of change should explicitly require consideration of the impact of change on proof testing.

APPENDIX 2 : PROPOSED CHECKLIST FOR USE BY INSPECTORS

This checklist has been designed to assist Field Inspectors to assess the quality of an organisation's approach to proof testing.

It is designed as a series of high-level statements that can be used directly or to develop more detailed questions. The assumption made is that SIS will be one of a number of topics to be addressed during site visits by inspectors. Therefore, the emphasis is on seeking quick and effective feedback from the organisation, making a judgement, and if confidence in respect of the responses is low, seeking further expert support leading to more detailed examination of evidence. The statements are designed to encourage the collection of evidence to support responses. This evidence may take a number of forms including:

- proof test procedures;
- calibration records;
- test sign-off sheets;
- training records;
- change control records;
- scheduling tools;
- management reviews;
- risk assessment reports;
- incident reporting procedures;
- authorisation levels;
- lists of ‘Responsible Engineers’;
- override and bypass management reviews.

Principle : Proof Test Practices and Procedures	
Guidance	Inspector's Observations
Proof testing should be carried out in an environment that is as consistent as practicable with operating conditions. (*Tests performed under maintenance conditions may not necessarily demonstrate that a SIS would function under operating conditions*).	
Proof testing should attempt to manipulate the process variable. (*Note that manipulation of the process variable does not imply manipulation of the process under control*).	
Proof testing should not have the potential to place process, plant or equipment in a dangerous state. (*Driving process variables, particularly pressure and level, into high states has the potential to create hazardous situations if SIS fail to operate*).	
Risks associated with manipulation of the process variable should be identified and assessed.	
Proof testing should provide adequate confidence in the correct operation of in-line devices, particularly in-line flowmeters and safety valves. (*Note that the use of built-in simulation facilities alone does not demonstrate a device's ability to operate under operating conditions*)	
Proof testing should address dynamic SIS performance by testing features such as response time and valve leakage class.	
Proof testing should be designed to test all components of SIS *(Evidence could be documentation which shows that reasonably foreseeable fail to danger faults have been identified and captured in proof test)*.	
Proof testing should address the condition of process connections, particularly impulse lines.	
Proof testing should be designed to address the condition of all necessary services such as power, instrument air, gas supplies, trace heating etc.	
The use of overrides and bypasses should be subject to a documented process of risk assessment.	
The application of overrides should be subject to authorisation by competent personnel.	
Access to override initiation facilities should be controlled.	

Principle : Proof Test Practices and Procedures	
Guidance	Inspector's Observations
Operators should be made aware of the presence of overrides.	
Procedures should be in place to ensure that overrides are removed in a timely manner.	
If partial testing of SIS and component parts is undertaken, its justification should be documented.	
Proof testing should not unnecessarily disturb SIS *(SIS should be tested as found)*.	
SIS failures identified during proof testing should be repaired in a timely manner.	
Calibration records should exist for all test equipment and should be traceable to recognised national standards.	
Proof testing should be based on a firm understanding of the test and the requirements and competence of the tester.	
There should be evidence of a culture of 'ownership' of the proof test procedure, for example the testers should be involved in the preparation and maintenance of procedures.	
Proof testing procedures should be provided in a consistent and standard form.	

Principle : Proof Test Practices and Procedures	
Guidance	Inspector's Observations
Proof test procedures should address the following key attributes: • a clear statement of the 'purpose and scope'; • due consideration and documentation of all precautions that must be observed whilst performing the tests in order to avoid potential hazards; • clear identification of any special tools or equipment required and evidence that the personnel are competent to use such equipment; • any initial conditions which must be satisfied prior to undertaking the test; • adequate cross references to any other documents, manuals etc.; • clear and concise procedural steps which adequately define the tasks necessary to perform the test safely and efficiently; • any warnings or specific issues that should be drawn to the attention of the tester should be clearly and conspicuously stated.	
The procedures should promote 'ease of use' by way of: • short, precise sentences and instructions; • use of positive active sentences such as 'open valve A then valve B'. (*Further guidance on human factors is given by HSE publication ' HSG48 - Reducing Error and Influencing Behaviour'*).	
Management systems should encourage active feedback from testing personnel, designed to highlight issues, difficulties and anomalies in the proof test.	
When undertaking the test for the first time, there should be a process in place for independent witnessing of the test.	
Proof test procedures should be explicitly referenced by any formal change control regime. (*Evidence suggests that the revision of proof test procedures after a process modification relies on the thoroughness of the C&I Engineer and may be neglected*).	

Principle : Planning and Scheduling	
Guidance	Inspector's Observations
There should be evidence that proof testing is a integral and explicit part of the planning and scheduling of the safety management system within the organisation.	
There should be evidence that that the organisation plans proof testing in a structured and managed way.	
The scheduling of proof tests should take full account of the availability of competent resources.	
What is the longest period between proof tests?	
Proof test intervals should not be 'stretched' to the point of compromising functional safety. (*The justification for claimed SIL should be documented and should specify a required proof test interval. This can be compared with the timing of planned maintenance activities.*)	
Any steps to minimise production disruption due to proof testing should be taken without compromising functional safety. (*Such steps may include alignment of proof testing with statutory inspections or the grouping of tests associated with related equipment into a single activity*.)	
The deferral of any proof test should be authorised by a suitably responsible and competent person and the justification should be documented.	

Principle : Records of Proof Testing	
Guidance	Inspector's Observations
Records and results of proof testing activities should be retained and be readily accessible.	
Records and results of proof testing activities should be maintained in a form that facilitates future analysis. (*This does not imply a necessity to create electronic records*).	
There should be evidence that the data associated with the tests is subject to analysis and review. (*Such data should include component failure rates, operational demand rates etc. Reviews can provide opportunities to validate the design basis of the SIS or to modify the SIS in line with actual process and SIS performance*).	
The organisation should take steps to ensure that those with responsibility for the management of functional safety have access to the necessary records and reports.	
Records of proof testing should cover: • verification of the satisfactory execution of proof test steps; • details of all faults encountered (*for example, by the use of specific fault codes to facilitate later analysis*); • details of any corrective actions, including time to repair and effectiveness of remedial actions; • duration of test; • signature of tester and validator/approver; • ability to record any recommendations, and evidence that these recommendations have been subject to review.	

Principle : Records of Proof Testing	
Guidance	Inspector's Observations
The organisation should have in place appropriate review mechanisms to cover: • reporting of overdue tests; • SIS component failures under test and any remedial actions; • SIS component failures in operation; • SIS and process performance against the assumptions of the risk and reliability analysis; • the review of the quality of proof test execution. (*Such reviews provide evidence of efforts to continually improve safety management procedures and maintain functional safety*)	

Principle : Competence	
Guidance	Inspector's Observations
Procedures should be in place to ensure that personnel engaged in the execution and management of proof testing are suitably competent. (*Job descriptions and training records could provide supporting evidence.*)	
Competency profiles for proof testing should be available which detail the necessary knowledge, training and experience required of testers and approvers.	
Records of personnel deemed competent to undertake proof testing should be maintained.	
Personnel regularly engaged in proof testing should receive refresher training.	
The competence necessary to perform the proof test should be specified within the proof test procedure or easily accessible to those staff involved in performing the tests.	
If outside agencies are employed to execute proof tests their staff should be subject to competency assessment which is at least as robust as that applied to permanent staff.	
The responsibility for proof testing should be assigned to a nominated role. The person filling that role should be clearly informed of, and accept, the responsibilities and accountabilities.	
Responsibilities for all aspects of proof testing should be clearly identified and communicated to the responsible personnel.	
The delegation of responsibility should be managed in a structured manner.	
The 'approval' process should check that: • the proof test procedure describes a sufficient test of the SIS; • the proof test is safe to apply to the process or equipment under control; • the outcome of the proof test has been reviewed and any appropriate actions initiated.	

APPENDIX 3.1: EXAMPLE OF A FORMATTED PROOF TEST PROCEDURE

The following example is included to illustrate some, though not all, of the principles of an effective proof test procedure.

Attention is drawn to the following characteristics:

- the use of a title page giving an overview of the proof test and detailing any necessary preparation and pre-requisites [*consistent with principle 4.3.1 (a)*];
- an estimate of the time to be taken (an implied time limit);
- highlighted precautions to avoid a hazardous situation during testing [*consistent with principle 4.7.1 (a)*];
- a step-by-step approach with each step carrying a unique number;
- tick-boxes where the tester is required to confirm an action or status;
- boxes for the recording of measured values;
- recording of "as found" details (step 2) [*consistent with principle 4.2.1 (f)*];
- the return to "as found" conditions (step 6) [*consistent with principle 4.2.1 (f)*];
- document details appearing on each page;
- the use of a summary page allowing the detailed recording of any faults [*consistent with principle 4.5.1 (a)*];
- the requirement for signature by the tester [*consistent with principle 4.6.1 (c)*];
- counter-signature by engineering and operations personnel [*consistent with principle 4.6.1 (c)*];
- signature to confirm that the results of the test have been checked and recorded [*consistent with principle 4.6.1 (c)*];
- final sign-off by the proof test initiator and the responsible Engineer [*consistent with principle 4.6.1 (c)*].

INSTRUMENT SAFETY METHOD (ISM)

Trip Linkage:		Description:	

Plant Section:	*Chemical* Plant	Testing Frequency:	26 Weeks	Time Taken:	1hour

Initiating Variable(s):	***Items Actuated:***

Process Conditions for Testing:

In order to ensure that this test does not create a [*hazardous situation*], it is essential to ensure that both stream feed hoppers have been run empty for the last 45minutes.

Preparation:

Agreement for trip testing to be obtained from the Process Manager.

Operator to check that all [processing is] complete before commencing tests as per instructions above.

Notes:

Obtain a Permit to Work.

INSTRUMENT SAFETY METHOD (ISM)

Trip Linkage:		Description:	

Method:

1) Make sure that the following drives are running:

[drive 1]

[drive 2]

[drive 3]

Confirm running status from the DCS:

[drive 1] Yes ☐ No ☐

[drive 2] Yes ☐ No ☐

[drive 3] Yes ☐ No ☐

2) Note the positions of the [drive 3] Fan Inlet and Outlet damper positions.

Inlet – V[nnn] - %Open	Outlet – V[nnn] - %Open

3) Slowly close the inlet damper until the fan trips on undercurrent. The damper should be between 10% open and 20% open. **It is acceptable to use the inlet or outlet damper for this test, but ensure that if either is found to be faulty, that the fault is reported to process and commented on the results sheet.** Note the damper position at the fan tripped.

Damper Position - %Open

4) Confirm that the [drive 3] fan has tripped on undercurrent: Yes ☐ No ☐

5) Confirm that the [drive 1] has tripped Yes ☐ No ☐

6) Return all dampers to their original positions – see item 2.

7) Reset the drives and restart the [drive 1] and the [drive 3], confirm running on the DCS.

[drive 1] Yes ☐ No ☐

[drive 2] Yes ☐ No ☐

[drive 3] Yes ☐ No ☐

INSTRUMENT SAFETY METHOD (ISM)

Trip Linkage:		Description:	

8) Initiate a stop of the [drive 2] using the local stop pushbutton, confirm the following drive trips:

[drive 1] Yes☐ No ☐

9) Reset the drives and leave drives in a running state and fill in the report sheet overleaf.

10) Sign off the Permit to Work.

INSTRUMENT SAFETY METHOD (ISM)

Trip Linkage:		Description:	

Comments:

Where any faults discovered? **YES/NO**

If yes, which loop item(s) were faulty/had failed *(please tick relevant box)*

Push Button		Relay(s)		SOV(s)	
Ball Valve(s)		Wiring		Terminals	
Power Supply		Air Supply		Pneumatics	
Other(s), *please specify*					

Describe fully the faults/failures for each item (continue on separate sheet if necessary):

Describe fully the corrective action taken for each item (continue on separate sheet if necessary)

Signature – Test Complete:	

Power & Control Technician		**Process Technician**	
Name:		Name:	
Signature:		Signature:	
Date:		Date:	

Return Completed Form Responsible Instrument Engineer

Checked and Recorded:	

Responsible Engineer		Comments:
Name:		
Signature:		
Date:		

Revision No:		Note:	

Initiator		**Checked (Responsible Instrument Engineer)**	
Name:		Name:	
Signature:		Signature:	
Date:		Date:	

APPENDIX 3.2: EXAMPLE OF THE RECORDING OF PROOF TEST RESULTS

The following example is included to illustrate a structured approach to the recording of results.

Attention is drawn to the following characteristics:

- the specification of test equipment;
- the requirement to record calibration and corrective actions (step 1) [*consistent with principle 4.2.1 (e)*];
- the specification of acceptable tolerances (heading panel and step 10);
- instructions detailing the action to be taken on discovery of a fault (step 11);
- the recording of the test result in the form of a code number allowing future analysis, reporting and review [*consistent with principle 4.5.1 (b)*].

TRIP & ALARM TESTING

LOOP : (CLASS A)

	SETTING	LIMITS		UNITS	TEST INTERVAL :
PROCESS					
INSTS					

TEST METHOD

TITLE :

ACTION OF TRIP :

TEST EQUIPMENT :

LOOP NO :

DATE :

***** This Trip/Alarm protects against a SERIOUS hazard *****

Note : This test to be carried out during plant SHUT DOWN.

1. Ensure that there is a valid PERMIT to WORK for this test. Inform the Panelman that testing is about to be carried out.

   Check calibrate, note values in Comment box and correct as necessary.
   Setting : ☐

2. Panelman to open valves [1], [2], [3], [4], [5]. ☐

3. One man to remain in the Control Room, the other to carry out the outside work. ☐

4. Isolate the impulse lines. SLOWLY open the LP vent needle valve to allow the pressure to fall SLOWLY, the high [process] alarm will be initiated but continue to allow the pressure to fall until the Extra high [process] trip annunciator is initiated. ☐

5. When the annunciator is initiated, note the recorder/indicator reading in the Comments box. ☐

RESULTS

0	PASS					0	RETESTED OK
1	OPERATED EARLY	1	BLOCKAGE	1	INITIATOR	1	NO SPARES
2	OPERATED LATE	2	CALIBRATION ERROR	2	LOGIC	2	NO TIME/LAB
3	DID NOT OPERATE	3	BREAKAGE	3	SOLENOID VALVE	3	NOT KNOWN
		4	FOUND DEFEATED	4	S/D MECHANISM	4	NEEDS S/D
		5	WET/STUCK	5	DESIGN		
9	NOT DONE	9	OTHER	9	OTHER	9	OTHER

TEST RESULT

1 PROCESS LIMITATION
2 NO ACCESS
3 NO TEST EQUIPMENT
4 PLANT IS SHUTDOWN
5 UNABLE TO DEFEAT
6 NO I-E EFFORT
7 NO PROCESS EFFORT
8 PLANT SHUTDOWN REQD
9 OTHER

COMMENTS :

INSTRUMENT : .....

PROCESS:..... ELECTRICAL:..... DATE ...../...../.....

6. Check that valves [1], [2], [3], [4], [5] have tripped closed. ☐

7. Recommission the D/P cell. ☐

8. When conditions are stable, reset the trip using the Reset button. ☐

9. Ask an authorised person to reset all conditions [1], [2], [3], [4], [5]. Check that the associated data alarms have returned to normal. ☐

10. Check and record the zero reading of the transmitter at process pressure. If it is in error by more than 2.5% of full scale, then the test has FAILED. ☐

11. If any part of the system failed to operate correctly or if the reading did not correspond with the required trip or alarm setting within the prescribed limits then the test has failed. Check each item of the loop. Repair where necessary and re-test If extensive repairs have to be carried out, inform the Process Supervisor. ☐

12. Check that the [process] indication and annunciator(s) have returned to normal. Ensure that valve(s) [1], [2], [3], [4], [5] have returned to normal. ☐

13. Inform the Panelman that testing has been completed. ☐

14. END of TEST. ☐

APPENDIX 3.3: EXAMPLE OF PROOF TEST DOCUMENT CONTROL

The following example is included to illustrate some of the principles of effective document control.

Attention is drawn to the following characteristics:

- reference to company, plant and unit;
- unique document reference number [*consistent with principle 4.3.1 (b)*];
- reference to the specific SIS;
- revision history [*consistent with principle 4.3.1 (b)*];
- specific reference to risk assessment [*consistent with principle 4.7.1 (a)*];
- multiple approvals [*consistent with principle 4.6.1 (c)*];
- definitions of the meanings of the different approvals [*consistent with principle 4.6.1 (b)*];
- reference to a controlling procedure for the management of controlled documents [*consistent with principle 4.3.1 (b)*].

Company – Plant – Unit

Procedure Number:

SIS Reference Number

DOCUMENT CONTROL SHEET

Document Issue	A	B	C	D	E
Date					
Risk Assessment No.					

Responsibility	**Print Name**	**Signature**	**Date**
Document Owner Author of change or new procedure			
Document Approver (Technical) Procedure is correctly structured and technically accurate			
Document Approver (Process) Procedure is correctly structured and achieves purpose & scope without adversely affecting process			
Document Administrator (Technology) Procedure has been risk assessed and will be filed as master copy			

Refer to document number xx/xxx/002 – Management of Controlled Documents for explanation of individual responsibilities.

REFERENCES

1 INTERNATION ELECTROTECHNICAL COMMISSION (IEC)
Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7
IEC 61508 :1998 - 2000

2 AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)
Application of Safety Instrumented Systems for the Process Industries
ANSI/ISA-S84.01-1996

3 Engineering Equipment and Materials Users Association (EEMUA)
Alarm Systems - A Guide to design, management and procurement
EEMUA 1999
ISBN 0 85931 076 0

4 KLETZ, TREVOR
Lessons from Disaster
Institution of Chemical Engineers, 1993

5 HEALTH & SAFETY EXECUTIVE (HSE)
HSG48 - Reducing Error and Influencing Behaviour
HSE Books, 1999
ISBN 0 7176 2452 8

6 HEALTH & SAFETY EXECUTIVE (HSE)
Improving Compliance with Safety Procedures - Reducing Industrial Violations
HSE, 1995
ISBN 0 7176 09707

7 SUMMERS, ANGELA AND ZACHARY, BRYAN
Partial-Stroke Testing of Safety Block Valves
Control Engineering, 2000
Control Engineering On-line
www.controleng.com/archives

8 DET NORSKE VERITAS
Offshore Reliability Data Handbook - Third Edition
1997

9 THE INSTITUTION OF ELECTRICAL ENGINEERS (IEE)
Competence Guidelines for Safety-Related System Practitioners
IEE, 1999

10 UNITED KINGDOM OFFSHORE OPERATORS ASSOCIATION (UKOOA)
Guidelines for Instrument-Based Protective Systems Issue 2
UKOOA, Nov 1999

11 HEALTH & SAFETY EXECUTIVE (HSE)
Programmable Electronic Systems in Safety Related Applications: 2. General Technical Guidelines
HSE, 1987

GLOSSARY

DCS	Distributed Control System
E/E/PES	Electrical / Electronic / Programmable Electronic Safety-Related System(s)
EPICC	European Process Industries Competitiveness Centre
HCF	Humberside Chemical Focus
PFD	Probability of Failure on Demand
PLC	Programmable Electronic Controller
Proof Test	A periodic test performed on a SIS in order to determine unrevealed failures of all safety-related components (from sensors through to final elements) which would cause a reduction in the safety integrity achieved.
QMS	Quality Management System(s)
RF	Radio Frequency
SIL	Safety Integrity Level
SIS	Safety Instrumented System

Printed and published by the Health and Safety Executive
C1.25 04/02

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 2WA
Tel: 01787 881165
Fax: 01787 313995
Website: www.hsebooks.co.uk

RETAIL
HSE priced publications
are available from booksellers

HEALTH AND SAFETY INFORMATION
HSE InfoLine
Tel: 08701 545500
Fax: 02920 859260
e-mail: hseinformationservices@natbrit.com
or write to:
HSE Information Services
Caerphilly Business Park
Caerphilly CF83 3GG

HSE website: www.hse.gov.uk

CRR 428

£15.00

ISBN 0-7176-2346-7

9 780717 623464