ENGINEERING SAFETY CONSULTANTS
The Global Provider of Functional Safety Expertise and Technical Consultancy

Proof testing… A key performance indicator for designers and end users of safety-related systems

David Green
Engineering Safety Consultants Ltd

ron.bell@esc.uk.net / d.green@esc.uk.net
www.esc.uk.net

Agenda

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Proof Test & Functional Test

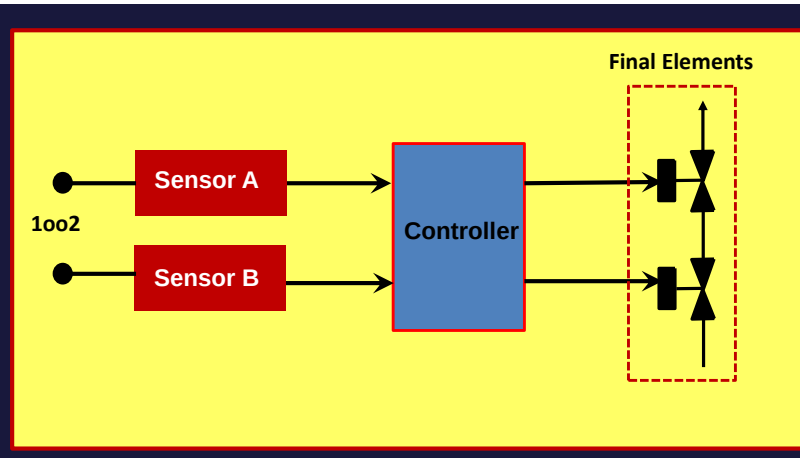
Proof Test:

Periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition IEC 61508-4 / 3.8.5 /Edition 2].

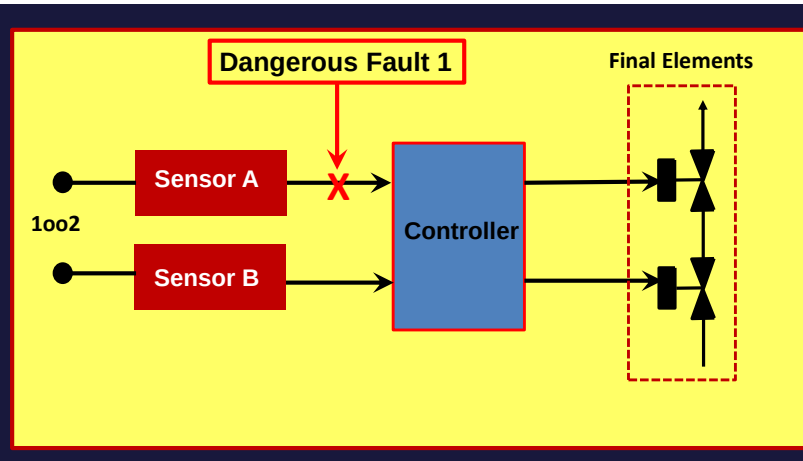
Functional Test:

Usually referred to the testing of a safety-related system to ensure that the specified function is working correctly.

Example: Functional Test & Proof Test

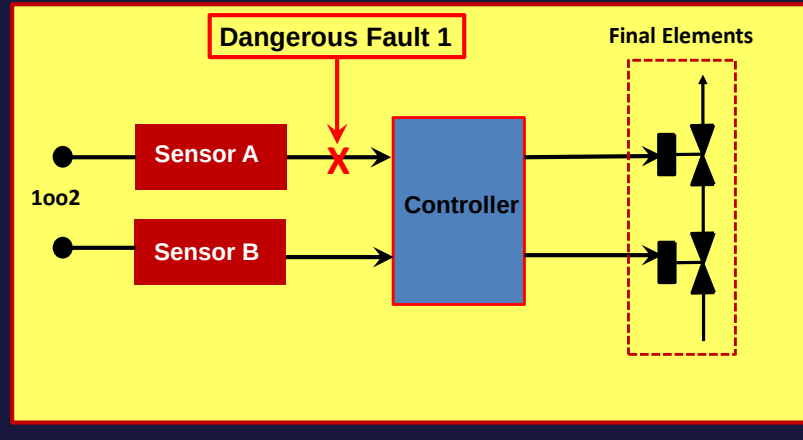


Example: Functional Test & Proof Test



A functional test would not detect Dangerous Fault 1 of Sensor A architecture.

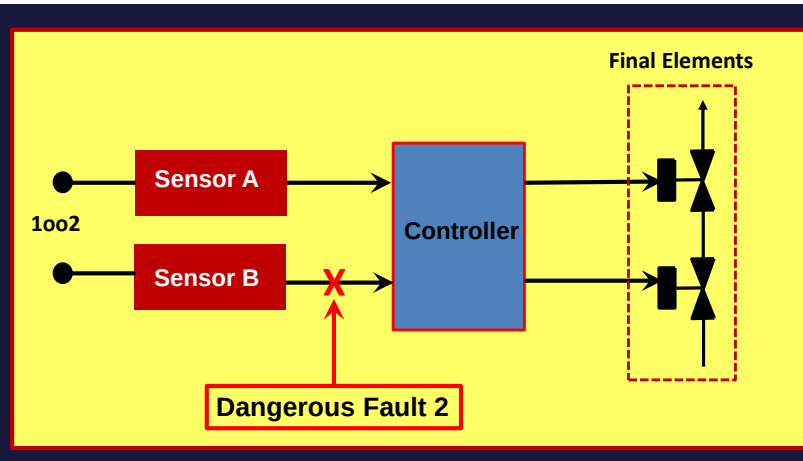
Example: Functional Test & Proof Test



A functional test would not detect Dangerous Fault 1 of Sensor A architecture.

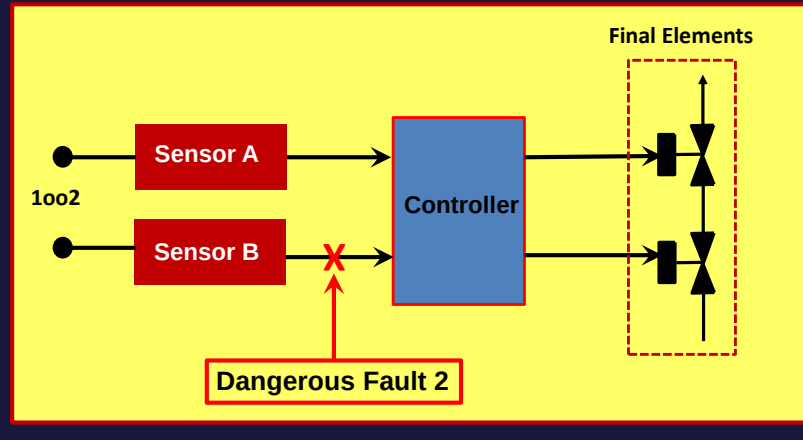
A proof test should detect such a fault since all the elements. carrying out the SIF should be tested.

Example: Functional Test & Proof Test



A functional test would not detect Dangerous Fault 2 of Sensor B architecture.

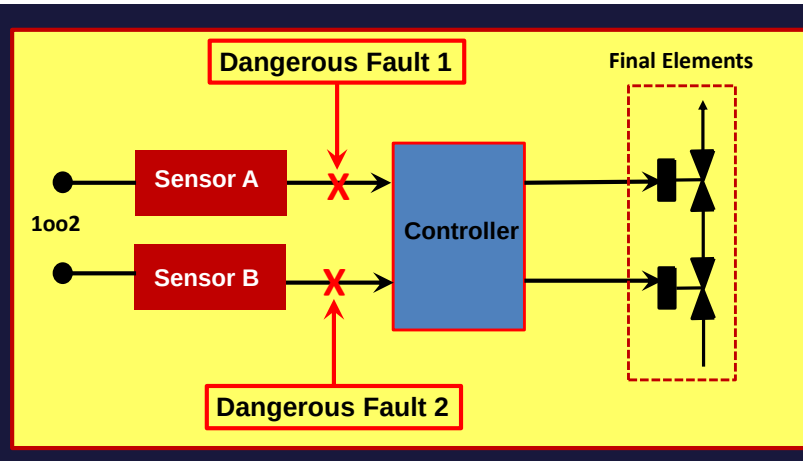
Example: Functional Test & Proof Test



A functional test would not detect Dangerous Fault 2 of Sensor B architecture.

A proof test should detect such a fault since all the elements. carrying out the SIF should be tested.

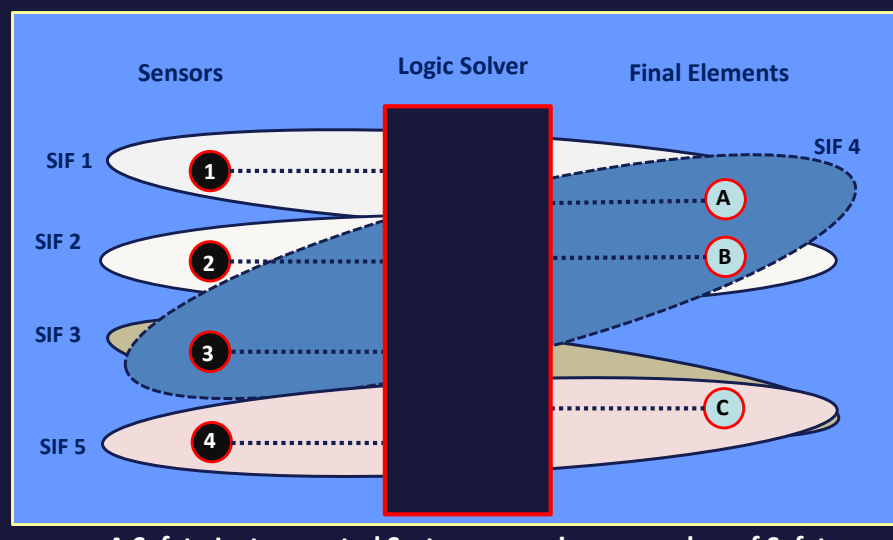
Example: Functional Test & Proof Test



A functional test would detect a Dangerous Fault of the Sensor architecture but won't highlight how many faults.

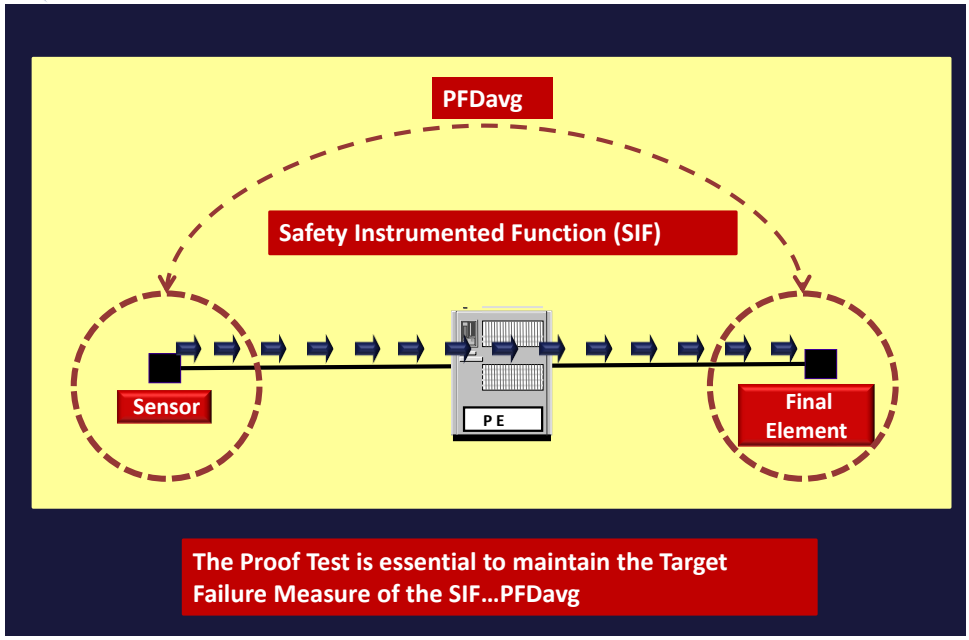
A proof test should detect all faults since all the elements. carrying out the SIF should be tested.

Safety-Instrumented System & Safety Instrumented Functions



A Safety Instrumented System comprises a number of Safety Instrumented Functions with SIF Loops

Target Failure Measure of the Safety Instrumented Function (SIF)



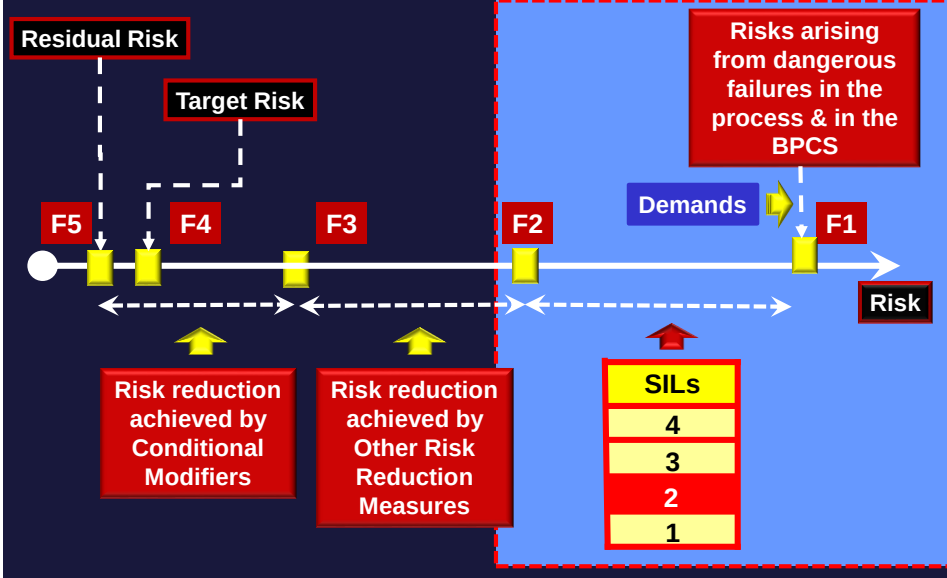
Proof Testing …. objective

- The proof test is designed to detect and expose unrevealed dangerous failures of all components making up a Safety Function
- Unrevealed dangerous failures are failures that are not detected by self test diagnostics
- Regular testing is required to detect and repair failures and restore the equipment performance to it's "as new" state
- A Safety Function can be "part tested" whereby only defined components are tested, giving the advantage that components can be proof tested at different intervals.

Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61511
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Risk Model Example: Low Demand Mode



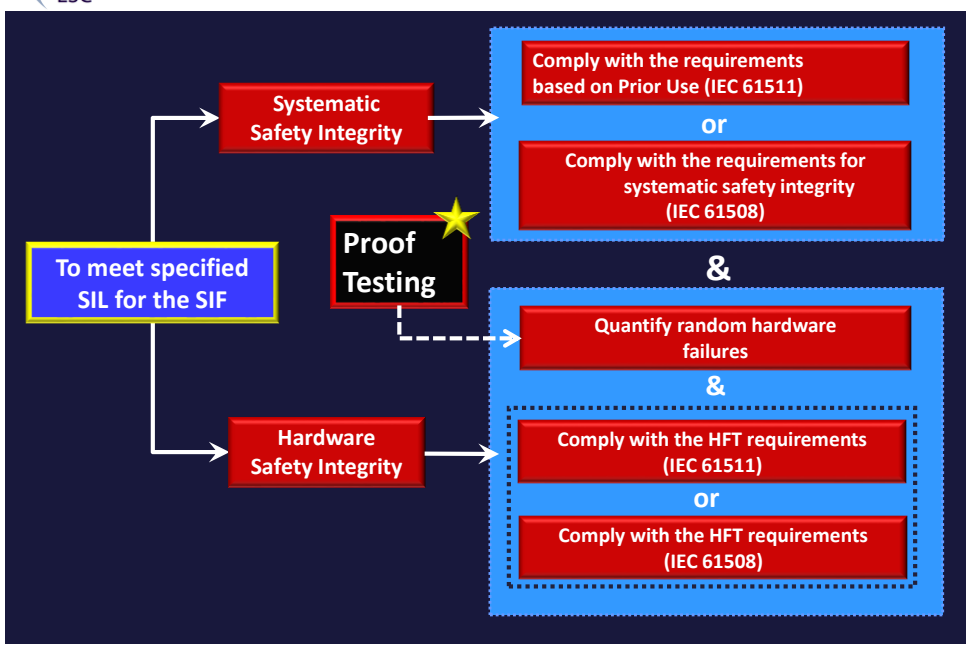
Target Failure Measures: Low Demand Mode

Safety Integrity Level (SIL)	Low demand mode of operation Average probability of dangerous failure on demand [PFDavg]	Frequency Reduction
4	$>=10^{-5}$ to $<10^{-4}$	10,000 - 100,000
3	$>=10^{-4}$ to $<10^{-3}$	1000 - 10,000
2	$>=10^{-3}$ to $<10^{-2}$	100 - 1000
1	$>=10^{-2}$ to $<10^{-1}$	10 - 100

F2 / F1 = PFDavg

F1 / F2 = Frequency Reduction

Design requirements to achieve a specified SIL (IEC 61511)



Proof Testing

Reason for Proof Testing:

- Functional safety is based on achieving a SIL with a PFD_{avg} in a defined band
- PFD increases with time, as the equipment performance decreases
- If proof testing is not carried out at the prescribed intervals the level of risk reduction assigned to the during the design phase is not achieved

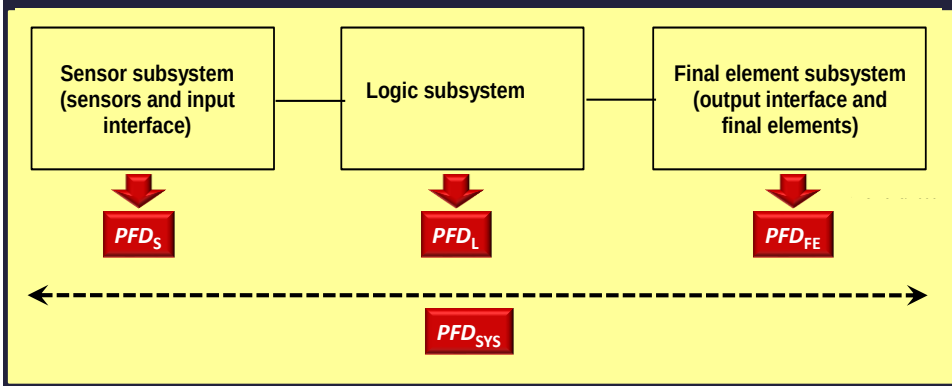
Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Proof test principles

- Assess the best way to undertake the proof test taking. For example:
  - Optimised testing
  - Partial testing
  - Testing of redundant channels
  - End to end testing versus part testing
  - Use of signal manipulation

PFD Calculations



$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

PFD for Undetected Failures

Configuration	λ_{SYS}	PFD
1oo1	λ_{DU}	$\lambda_{DU}.T_P / 2$
1oo2	$\lambda_{DU}^2.T_P$	$\lambda_{DU}^2.T_P^2 / 3$
2oo2	$2.\lambda_{DU}$	$\lambda_{DU}.T_P$
1oo3	$\lambda_{DU}^3.T_P^2$	$\lambda_{DU}^3.T_P^3 / 4$
2oo3	$3.\lambda_{DU}^2.T_P$	$\lambda_{DU}^2.T_P^2$
3oo3	$3.\lambda_{DU}$	$3.\lambda_{DU}.T_P / 2$
1oo4	$\lambda_{DU}^4.T_P^3$	$\lambda_{DU}^4.T_P^4 / 5$
2oo4	$4.\lambda_{DU}^3.T_P^2$	$\lambda_{DU}^3.T_P^3$
3oo4	$6.\lambda_{DU}^2.T_P$	$2.\lambda_{DU}^2.T_P^2$
4oo4	$4.\lambda_{DU}$	$2.\lambda_{DU}\ T_P$

Remember!

- PFD = $PFD_{Undetected}$ + $PFD_{Detected}$
- Proof Testing focussed on Undetected Failures

PFD Calculations

PFD is the numerical value that describes the probability that the will fail to operate when required.

The PFD of a single channel element is:

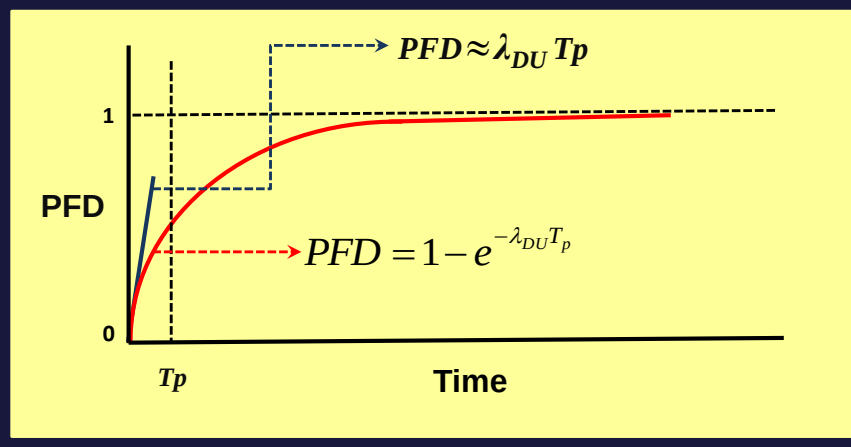
$$PFD = 1 - e^{-\lambda_{DU} T_p}$$

If $\lambda_{DU}\ Tp$ is small (<0.1) then:

$$PFD \approx \lambda_{DU}\ Tp$$

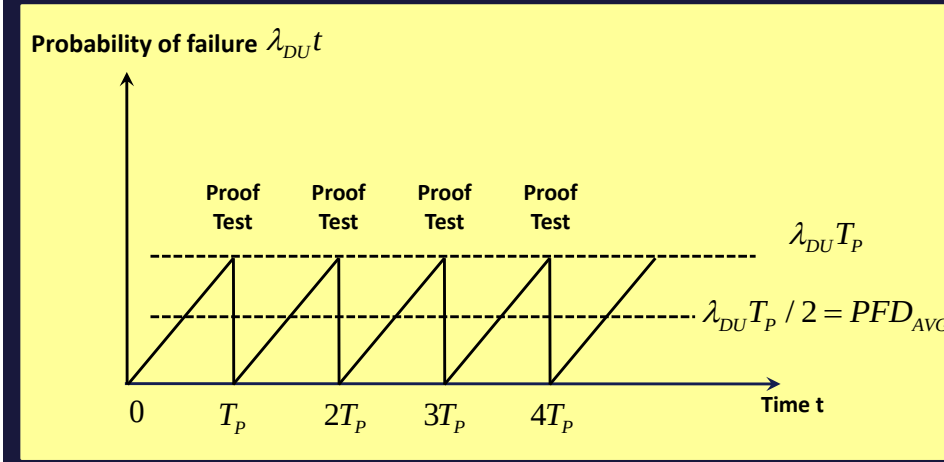
- λ_{DU} is the dangerous undetected failure rate per hour;
- T_p is the proof test frequency

Probability of failure with time



- λ_{DU} is the dangerous undetected failure rate per hour;
- T_p is the proof test frequency

Probability of failure with time



- λ_{DU} is the dangerous undetected failure rate per hour;
- T_p is the proof test frequency

Undetected Failures between proof tests: Focus on the PFD parameter for Low Demand Mode

Configuration	PFD
1oo1	$\lambda_{DU} \cdot T_P/2$
1oo2	$\lambda_{DU}^2 . T_P^2 / 3$
2oo2	$\lambda_{DU} . T_P$
1oo3	$\lambda_{DU}^3 . T_P^3 / 4$
2oo3	$\lambda_{DU}^2 . T_P^2$
3oo3	$3.\lambda_{DU} . T_P / 2$
1oo4	$\lambda_{DU}^4 . T_P^4 / 5$
2oo4	$\lambda_{DU}^3 . T_P^3$
3oo4	$2.\lambda_{DU}^2 . T_P^2$
4oo4	$2.\lambda_{DU} T_P$

The frequency of the Proof Tests have an impact of the PFD achieved for a specified dangerous undetected failure rate per hour (That is: λ_{DU}).

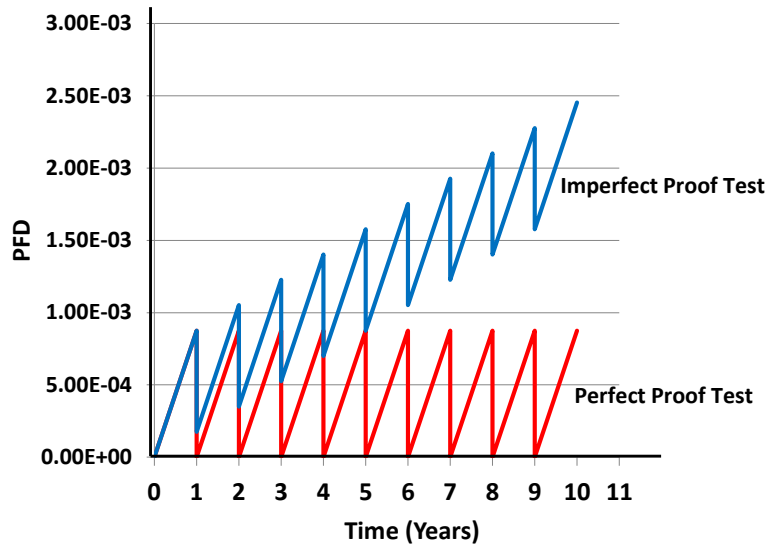
However, the resource implications and competence requirements of undertaking the Proof Test should be thoroughly thought out.

Perfect and Imperfect Proof Testing

Reasons for Imperfect Proof Testing:

- Proof test is not carried out under exact process conditions, including:
  - Pressure (total and differential)
  - Temperature
  - Flow rate
  - Process fluid density
- Difficulty of testing, such as:
  - Ensuring a valve is gas tight after operation;
  - Testing of flow meters (requirement for a reference meter).

Effect of Proof Testing on PFD
Imperfect Proof Testing



Perfect and Imperfect proof testing

- Cannot assume automatically the proof testing will detect 100% of dangerous undetected failures (i.e. perfect proof testing)… in practice this is difficult to achieve.
- Failures that are not detected by proof testing will increase the PFDavg of the year on year despite regular proof testing
- Given enough time the PFD_{avg} will increase to an unacceptable level
- Some examples of imperfect proof testing are:
  - ✓ not testing the system under normal operating process conditions
  - ✓ not testing impulse lines for blockages
  - ✓ failure to check valves close fully and to the required shut off class.

Proof Test Coverage (PTC)

- **When it is not possible to carry out a perfect proof test this must be accounted for in the PFD calculation using the concept of Proof Test Coverage (PTC)**

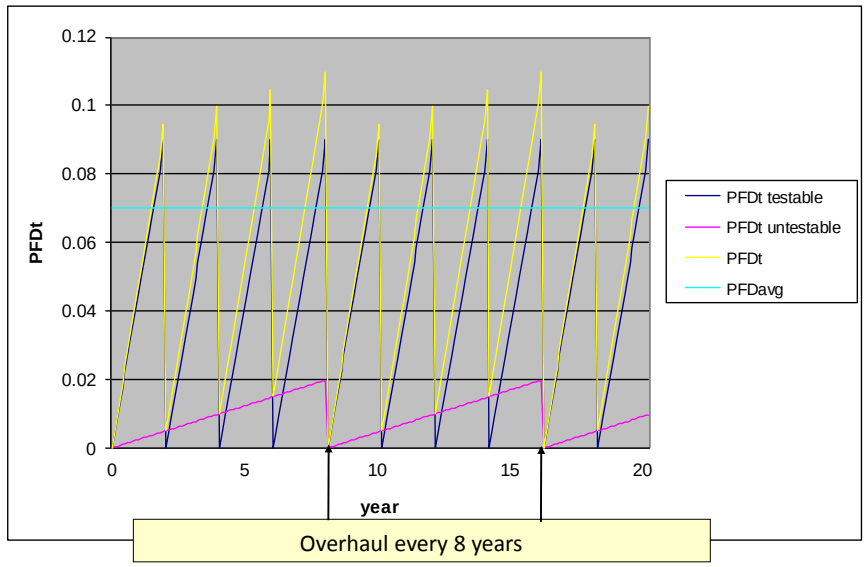
– PTC is the percentage of dangerous undetected failures that are exposed by a defined proof test procedure

- This can be done by assigning a PTC percentage for each subsystem based on the estimated amount of dangerous undetected failures that would be revealed by the proof test.

Proof Test Coverage (PTC)

- The PTC can be estimated by means of a Failure Mode and Effect Analysis (FMEA)……in conjunction with engineering judgment based on sound evidence can be used.

Effect of Overhaul Test on PFD



Impact of reducing PTC on PFD

Year	PFDavg					
	100% PTC	90% PTC	80% PTC	70% PTC	60% PTC	50% PTC
1	4.38E-04	4.38E-04	4.38E-04	4.38E-04	4.38E-04	4.38E-04
5	4.38E-04	6.13E-04	7.88E-04	9.64E-04	1.14E-03	1.31E-03
10	4.38E-04	8.32E-04	1.23E-03	1.62E-03	2.01E-03	2.41E-03

Based on λ_{DU} = 1.0E-7 and Tp = 8,760 hours

Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Proof Test Practical Issues

- If reasonably practicable, the Safety Function should be initiated by manipulating the process variable
- If manipulating the process to initiate the Safety Function into the demand state is used, a risk assessment should be carried out to ensure failure of the proof test won't create the hazard which is trying to be protected.
  - This may result in the implementation of additional safeguards being implemented during testing.

Proof Test Practical Issues

- References can be made to the manufacturers documentation (e.g. safety manual)
  - For any specific test requirements
- All test equipment should be calibrated to a recognised national standard and the calibration certificate number recorded against the test equipment records.
- The proof test results document should detail the test equipment used for traceability.

Proof Test Practical Issues

- Components should be visually inspected
  - ✓ **Excessive wear/ corrosion**
  - ✓ **Weather ingress**
  - ✓ **Physical installation – mounted correctly, holding bolts in place, labelled correctly, Hazardous Area requirements in good order.**
  - ✓ **Ancillaries – supplies correctly installed and in good condition, Air supplies secure, trace heating or cooling operational**
- Defects found during proof test failures should be reported to the functional safety manager (or equivalent).
- Ensure system is put back into the operable state as defined in the Proof Test Procedure.
- Ensure that no overrides are left on after completion of proof test.

Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Resource Implications

- The incorrect frequency of testing impacts the business costs:
  - ✓Production losses
  - ✓Labour costs
  - ✓Costs of calibration gasses
  - ✓Cost of test equipment (including re-calibrations)
  - ✓Transport costs
- Therefore the correct interval optimisation will not only mean that there are fewer opportunities to introduce errors but also reduce costs to the business.

Resource Implications example

- Test takes 5 hours and requires the unit to be shutdown and de-contaminated therefore 8 hrs production losses. Requires a pressure calibrator.
  - Production losses
    - £10k/hr = £80k
  - Labour costs
    - 2 people at £50/hr = £500 (10 man hours)
  - Costs of calibration gasses: None in this test
  - Cost of test equipment (including re-calibrations):
    - £2.5k per device + £200 annual calibration
      - (annualised (5 year life of device) is £500/yr + £200 = £700/yr)
  - Transport costs
    - £40 per day = £40

Each test costs ~ £81.2k

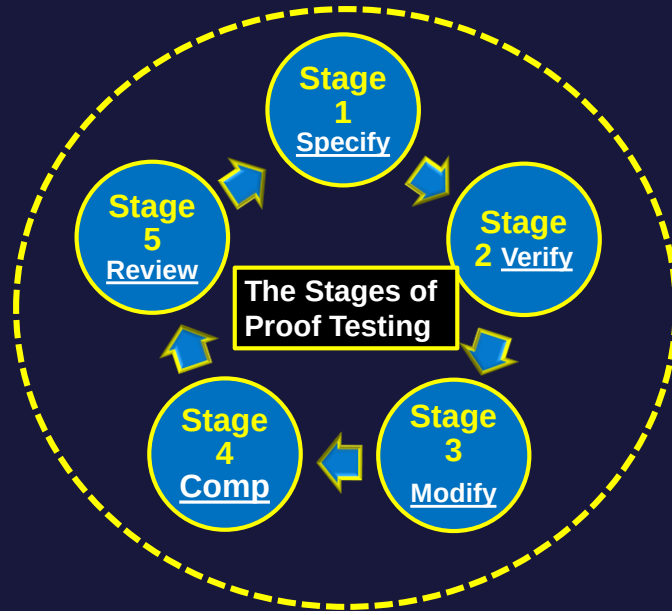
Proof Testing

1. **What is proof testing?**
2. **Overview of the requirements of IEC 61508**
3. **Proof test principles**
4. **Practical issues**
5. **Resource Implications**
6. **Proof Test Procedures**
7. **Example**
8. **Importance of Recording Proof Test Results**
9. **Concluding comments**

Proof Test Procedures

There are five key Stages in the development and implementation of Proof Test Procedures:

- **Stage 1: Development of Proposed Proof Test Procedures for the specified SIFs;**
- **Stage 2: Verification of the proposed Proof Test Procedures;**
- **Stage 3: Modification to the Proposed Proof Test Procedures;**
- **Stage 4: Ensuring that those undertaking the Proof Test Procedures are competent.**
- **Stage 5: Review and amend the Proof Test Procedure once in use.**



Proof Test Procedures

- Documented and auditable
- Concise and understandable by the person who will be conducting the test.
  - e.g. 'Apply 8.5 barg pressure' rather than 'Apply 20% more pressure than the setting of the trip point at 7.1 barg'.
- Developed in a systematic manner with the objective of determining the dangerous failures that have not been detected by other means
- The degree of detail should take into account the training and competence of the persons who are carrying out the proof tests.

Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Proof Testing: Example, Pressure Transmitter

Proof Test 1:

Manipulate mA output using HART communicator, above and below the trip point and check the mA output with a calibrated current reference meter.

Proof test coverage = 50%

Proof Test 2:

Manipulate mA output using pressure calibration instrument, above and below the trip point and check the mA output with a calibrated current reference meter.

Proof test coverage = 99%

Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Importance of Recording Proof Test Results

- Recording results from proof test procedures is of utmost importance:
  - Allows evaluation of the failure modes being experienced on your plant;
  - Allows failure rate analysis in order to determine if the assumptions made in design are correct;
  - Allow demonstration that the proof tests are being completed for internal and external audits.

Benefits of Result Analysis

- Result analysis and Investigations into the equipment in operation on the site, gives the benefits of:
  - To prevent or limit any repeats of the incident;
  - To eliminate the chance that the system isn't available when called upon;
  - Detect installation issues affecting the devices 'nearby steam leaks, regular impact with people / vehicles etc'
  - Detect trends in which devices are starting to enter the 'wearout' phase of it's life, therefore leading to change out where necessary.

Proof Testing

1. What is proof testing?
2. Overview of the requirements of IEC 61508
3. Proof test principles
4. Practical issues
5. Resource Implications
6. Proof Test Procedures
7. Example
8. Importance of Recording Proof Test Results
9. Concluding comments

Conclusions

1. The inability to fully test a complex Safety-Related System will have adverse effects on the risk reduction it provides if incorrect assumptions on the PTC have been made. The tolerable risk target may not be met.

2. Procedures for proof testing should be addressed at the design stage and this should involve the end user which may influence the design.
   - ✓(e.g. complexity of the proof test procedures, frequency of the proof tests, whether an imperfect proof test approach should be adopted).

3. Proof Test procedures should be developed which are effective and precisely specified.

Conclusions

4. **The development of Proof Test Procedures should be developed in a systematic manner and take into account the practicalities of undertaking the Proof Tests (i.e. Stages 1-5)**

5. **It is essential the those involved in proof testing are competent to carry out the defined proof tests.**

6. **Proof Test results should be effectively recorded and reviewed to assess what further action may be required.**

ENGINEERING SAFETY CONSULTANTS

The Global Provider of Functional Safety Expertise and Technical Consultancy

Thank you

©

d.green@esc.uk.net
www.esc.uk.net