Appendix 1: Process for Defining SIS Proof Testing Requirements

Figure 1: Process for the management of Proof Testing Requirements
Notes to Figure 1

Note 1: The SIS design and PFD calculation might be as a result of a new (or modified) SIS or a review of legacy SIS. See guidance below on ‘PFD calculations’.

Note 2: Refers to credible failure modes that would prevent the SIS operating in accordance with the SRS. See guidance below on ‘Identifying failure modes’.

It should also include failure modes associated with Diagnostic functions of the components. See guidance below on ‘Diagnostic Functions’.

Note 3: Direct testing in this case refers to normal testing typically carried out by instrument technicians at the defined proof test interval (PTI). See guidance below on ‘Direct Test Methods’.

Note 4: Other methods in this case refers to any other test completed at the defined proof test interval (PTI). See guidance below on ‘Other Methods’.

Note 5: See guidance below on ‘Partial Proof Testing’.

Note 6: The PFD calculation should be modified to show the effects of partial proof testing. See guidance below on ‘Partial Proof Testing’.

Note 7: The methods identified should be recorded within the Proof Test Procedure. See guidance below on ‘Proof Test Procedures’.

Note 8: See guidance below on ‘Redesign’. 
**PFD Calculations**

1. The purpose of a PFD calculation is to show that the SIS has sufficient integrity to reduce the risk of the defined hazards to that assumed within the risk assessment.

2. PFD calculations are normally based upon the undetected dangerous failure rates of the components, the proof test interval and other parameters such as the mean time to repair (MTTR), etc.

3. Only failures that prevent the SIS from operating in accordance with the safety requirement specification (SRS) should be included within the calculation.

4. Sources of failure rate data can be from equipment manufacturers, industry standard data or from site specific failure records. Dutyholders should ensure that the failure data used is applicable to the SIS and associated operating and environmental setting.

5. Good practice BS EN 61511 clause 5.2.5.3 requires that the performance of the SIS is monitored during its lifecycle to ensure that the observed failure rate of components is not higher than that assumed within the design, i.e. the PFD calculation.

6. If this performance monitoring indicates that component failure rates are higher than assumed, then the SIS might not be providing the necessary risk reduction and therefore it might be necessary to make changes to the SIS or the proof test interval to remedy this. This could be costly and disruptive.

7. It follows therefore, that the use of more conservative failure data within the design PFD calculation is less likely to require changes later on in the lifecycle. However, it is the responsibility of the dutyholder to select appropriate failure rate data and monitor SIS performance throughout the lifecycle.

8. It should also be noted that although a PFD calculation is a quantitative analysis, it is based upon data and assumptions that has potentially significant errors and therefore dutyholders should be mindful of the potential sensitivities within the calculation.

9. Failure rates often increase when the components are operated past their expected lifetime. In such cases, the dutyholder should consider replacing the components or taking other measures, such as increasing test frequency, to ensure the overall integrity of the SIS meets that required.

**Identifying Failure Modes**

10. Good practice requires that proof tests reveal undetected dangerous failure modes that prevent the SIS from operating in accordance with the safety requirement specification (SRS).

11. This therefore requires knowledge of the potential failure modes and a clear understanding of the SRS – for example if tight shutoff of a valve is required then failure to achieve this would be a failure mode, otherwise it would not be.
Equally, response times are part of the SRS and need to be considered as a potential failure mode.

12. Some legacy plants may not have a single documented SRS consistent with BS EN 61511 clause 10. However, there should be a description (e.g. within cause and effect diagrams) that, along with other documents and site standards, is sufficient to describe the safety function and allow the failure modes that would prevent the SIS operating in accordance with its design to be determined.

13. It is not necessary to systematically record the failure modes, but the proof test procedure should record the tests or other methods used to reveal them.

14. However, in some cases, for example on larger sites, a dutyholder may optionally choose to record failure modes for different types of components to facilitate generation of consistent proof test procedures.

15. Identification of failure modes requires expert knowledge, typically held by competent Instrument Engineers and Technicians, and the component manufacturers. The proof test should include those undetected dangerous failure modes:

   a. Identified in the component manufacture’s documentation.

   b. Associated with ancillary components such as impulse lines, heat tracing etc.

   c. Associated with redundant parts of the SIS, for example failure modes of a single channel in a voted sub-system.

   d. That are known or credible predicted failure modes.

   e. Directly associated with the safety function.

16. A proportionate approach should be taken to the identification of failure modes, i.e. more rigor should be applied for higher integrity SIS and higher assumed component reliability (i.e. longer proof test intervals).

17. It will be necessary to ensure that if, during normal lifetime, additional failure modes are identified that these are considered for all similar components.

18. Some common failings observed with respect to identification of failure modes are provided in Appendix 4 for information.

**Diagnostic Functions**

19. Diagnostic features are often used to improve the integrity and safe fail fraction of equipment. This may include diagnostic functions built into components by manufactures (e.g. memory checking) or diagnostics implemented during the design of the SIF (e.g. transmitter under/over range) within the logic solver.

20. Note the difference between diagnostic coverage and proof testing: diagnostic coverage refers to methods which detect dangerous failures within the MTTR time assumed within the PFD calculation. Whereas, proof testing is a method of revealing undetected dangerous failures at the defined proof test interval.

21. Proof testing should include appropriate testing of diagnostic functions to reveal dangerous failures of the diagnostic systems since they contribute to meeting
the PFD and fault tolerance requirements and therefore the safety requirements specification.

22. Some component ‘built-in’ diagnostic functions (e.g. memory checking in safety PLCs or smart instruments) may be difficult to fully test since the initiating conditions cannot be simulated. In these cases reasonable efforts should be made during the test to confirm that the diagnostics are operational based upon discussions with the component manufacturer.

**Direct Test Methods**

23. Direct testing is used to reveal undetected dangerous failure modes by subjecting the components to specified methods, usually using test equipment to create specific conditions and then observing the response of the component.

24. Direct test methods should be recorded within the proof test procedure along with the expected success criteria and where necessary tolerances etc.

25. The direct test methods must be conducted at the proof test interval assumed within the PFD calculation.

26. Typical direct test method include: simulating process conditions, calibration, stroking valves, simulating trip conditions, simulating electrical signals etc.

27. In general, direct testing methods should attempt to simulate process conditions as realistically as possible, without putting the process in a dangerous condition.


**Other Methods**

29. Other methods may be used to reveal dangerous failure modes when direct testing is not possible. They are sometimes known as ‘confidence building measures’ or ‘indirect test methods’.

30. The other methods should be recorded within the proof test procedure and include success criteria.

31. These other methods must be conducted at the proof test interval assumed within the PFD calculation.

32. Typical other methods include: cross checking sensor history data against other instruments where the range is covered, periodic replacement and sampled testing of single-use components, valve overhauls to ensure tight shutoff, etc.

**Partial Proof Testing**

33. The decision on whether to implement partial proof testing requires judgement by a competent person based on the component types, relative costs of periodic maintenance, replacement and overhaul and the access to the equipment.

34. Good practice BS EN 61511 clause 11.2.5 requires that testing requirements are considered during the design stage, and therefore for new or significantly
modified SIS, facilities for testing should be built into the design and therefore requirements for partial proof testing can often be avoided.

35. However, sometimes, and especially for legacy SIS systems, it is not possible to reveal all of the undetected failure modes at the proof test interval assumed within the PFD calculation, for example due to operational constraints, or due to personal safety issues. In these cases, a partial proof testing strategy can be a valid approach so long as the overall integrity requirements of the SIS are met.

36. A partial proof testing strategy requires the definition of two or more proof test intervals. Normally, this is defined as a more frequent partial test followed by a less frequent full test (typically to fit in with normal plan shutdown periods).

37. For each of the defined proof test intervals, the dutyholder should define which failure modes of the components will be tested, and which won’t be tested. This split may be at the component level (for example sensor and logic solver every 1 year, and final elements every 2 years) or be split by specific component failure modes (for example, sensor, logic solver, and solenoid valves + partial valve stroke test every 1 year and full valve stroke test every 2 years).

38. Note that all undetected dangerous failure modes must be revealed at some point, otherwise these failure modes eventually become dominant and will result in the SIS having a lower than required PFD.

39. Therefore, partial proof testing requires a more detailed understanding of the components failure modes and their relative failure rates. For each component it is necessary to determine which failure modes are revealed at each of the defined proof test intervals and capture this with the PFD calculation. Additional guidance is provided in Appendix 3.

40. If the result of the PFD calculation meets the required PFD then the partial proof testing strategy is valid.

41. If the result of the PFD calculation does not meet the required PFD then the partial proof testing strategy is not valid. In these cases, guidance is provided below – see ‘Redesign’.

42. The partial proof test strategy should be recorded in the proof test procedure and may include direct testing methods and/or other methods at each stage.

43. Note that some component manufacturers design and provide test and diagnostic facilities within their components such that the unrevealed failure modes are so small that they can be effectively ignored during the components expected lifetime. This is a valid approach. However, this remains a partial test only, and if the component is to be operated past its expected lifetime, then these remaining failure modes must be revealed. In practice, many dutyholders choose to replace the equipment at its defined expected lifetime to address this issue. Details about this can often be found in the manufacturer’s safety manual or functional safety certificate details.

**Proof Test Procedures**

44. A proof test procedure should be provided for each SIF.
45. In practice the proof test procedure may be made up of several documents, for example:
   a. It may make reference to other procedures, for example standard test methods for common components along with specification sheets showing the settings, tolerances, ranges for each specific SIF.
   b. It may include procedures for testing different parts of the SIS at different times, for example for partial proof test strategies or for testing different parts of the SIF when the plant is in different operating modes. This is acceptable so long as measures are taken to ensure no failure modes or components are missed.
   c. It may include partial test procedures and full test procedures.

46. In all cases, the proof test procedure (or associated documents) should include:
   a. Relevant descriptions and information for those completing the tests.
   b. A full end-to-end test (process connection to process connection) at the specified proof test interval(s) even if different parts of the loop are tested at different times.
   c. Revealing all undetected failure modes that would prevent the SIS operating in accordance with the safety requirements specification, even if this is completed at different intervals, e.g. due to a partial testing strategy.
   d. Actions to be taken in the event of failure being detected – see BS EN 61511 clause 11.3.
   e. Requirements to record the outcome and any failures.

47. The proof test procedures should be designed to minimise human error, for example including tick boxes to help prevent missing steps, sign-offs and / or cross checking for critical steps and where possible structuring the test so that errors that could be introduced are revealed by subsequent test steps.

48. All SIS should also be subject to periodic visual inspection, including all components (e.g. junction boxes) to detect unauthorised modifications or deterioration etc. Inspection requirements may be captured within the proof test procedures or within other procedures.

49. The level of inspection should be proportionate to the site conditions and access controls, for example it may be appropriate for more frequently inspection inside a junction box that is subject to corrosion or more regular access, but less frequent inspection for one which is clearly in good condition and has not been accessed.

50. All SIS components should also be subject to appropriate maintenance, usually described by the component manufacturer. For example, cleaning, replacement of consumable parts etc.

51. The fact that a component passes a proof test, does not negate the requirements for inspection and maintenance, which are designed to proactively prevent future failures.
Redesign

52. If the required PFD cannot be met, for example because all undetected dangerous failure modes are not revealed at the defined proof test interval, then the SIS will not provide the necessary risk reduction.

53. In these cases the approach will need to be modified by either:
   a. Changing the proof test strategy, e.g. more frequent testing etc.
   b. Changing the design of the SIS, e.g. more reliable or more redundant components etc.
   c. Reduce the integrity requirements on the SIS so that the SIS meets its requirements, e.g. provide other protection layers, etc.

54. For new plant and significant modifications, good practice should be applied and therefore the above modifications must be completed.

55. For legacy plant, the above modifications should be applied, so far as is reasonably practicable. In these cases the risk assessment should be updated to include the actual integrity achieved by the SIS and then the dutyholder should consider what further measures are reasonably practicable.