Appendix 2: Process for Implementing SIS Proof Testing

Figure 2: Process for Implementing SIS Proof Testing

Notes to Figure 2

Note 1: The maintenance management system may be computer or paper based but needs to be effective at scheduling tests at suitable times with appropriate competent resource to achieve the proof test strategy as per design.

Note 2: The proof test should be conducted to schedule and recorded when completed for auditing purposes.

Note 3: See guidance below on ‘Managing Failures’.

Note 4: See guidance below on ‘Auditing and Monitoring performance’.

Note 5: See guidance above on ‘Redesign’.
Managing Failures

1. All SIS component failures should be recorded, even if they are immediately repaired (often called recording the before and after state). Where failures are identified, the relevant parts of the proof test should be repeated to ensure that the repair is successful.

2. All SIS component failures should be investigated to determine if it is a safe or dangerous failure, and if the failure is a random failure or systematic to its design or use (e.g. due to environmental considerations) and its potential on wider functional safety (e.g. in this or other installations). Actions should be taken to ensure that that functional safety is maintained.

3. Safe and dangerous failures should be recorded to generate observed failure data. This is typically recorded at the component level, although the methodology for assessing SIS performance remains with the dutyholder.

4. It is noted that SIS component populations are typically quite small and therefore might not be statistically significant. In these cases, the dutyholder may wish to combine this data with more generic failure data from across the site where the same components are used, for example, in the control system. However, it is not expected that the failures in the wider population are subject to the same level of investigation, and may consist of only numbers of failures in the population – assumptions may need to be made of the ratio of dangerous undetected failures based upon the SIS component data or manufacturer’s data.

Auditing and Monitoring Performance

5. Measures should be in place to audit that the proof test procedures are completed correctly to ensure that human error during proof testing is minimised. This should include measures for ensuring adequate management of competency for those managing, specifying, or undertaking proof testing and consideration of the appropriate human factors.

6. Monitoring should be in place to ensure that proof tests are completed at the specified proof test intervals and repairs carried out within the times specified in the design. Procedures should be implemented to address situations where proof tests that have not been completed within the required time, for example to assess the risk, take other measures or otherwise make the plant safe so far as is reasonably practicable.

7. Periodic monitoring should be in place to assess the failure rate performance of the SIS compared to that assumed during design. This should include ensuring that the observed failure rates do not exceed those assumed during design. Note that it is not required that the PFD calculation is updated to show the observed failure rates so long as they remain better than that assumed during design.