Engineering maintenance of safety instrumented functions

Early involvement improves operations and maintenance through the safety life cycle

Fast Forward

- The work required to design an adequate platform to support maintenance and operation activities related to safety instrumented systems is frequently underestimated.
- Clear objectives and, in consequence, a well-designed strategy supported by a software platform facilitates achieving the required levels of safety and the optimization of resources.
- Engineering the maintenance of safety instrumented systems should be accomplished in parallel with the design phase.

By Henry Johnston and Fahad Howimil

International standards for safety instrumented systems (SIS) have had a profound influence on the analysis and design of these protection systems. The old prescriptive or recipe type was changed to a performance approach that designers must satisfy. The first stages of the safety life cycle (SLC) are now well known by a majority of designers and engineers involved in SIS; however, such grade of understanding and influence has not been widely accomplished at the final stages of the SLC as are the operation and maintenance (O&M).

O&M involvement in the engineering of SIS is normally passive, participating in specific analysis when requested. Such approach leaves almost the complete engineering of the protection system under project designer “responsibility.” An early involvement with a proactive approach to complement the designer experience with reliability and maintainability vision is necessary to balance the design and to manage the SIS.

The following are some of the actions for founding the basis for SIS management in the O&M phase:

Establish clear objectives

The most important factor is to establish clear objectives or goals. The standard, IEC-61511, section 16-2-2, helps us with the first objective, which is obviously safety-related: “Maintain
the as-designed functional safety of the SIS.” The second objective in many companies is economical: “Maintain the SIS efficiently.”

But what do “as-designed” and “efficiently” mean regarding safety? How are these objectives understood by the organization? The “maintain as designed” goal means to achieve during operation a safety instrumented functions (SIF) probability of failure on demand average (PFD\textsubscript{avg}) lower than required in the SIL target during the analysis phase of the SLC. The “maintain SIS efficiently” means to reevaluate tasks, methods, and frequencies to intervene where and when necessary. Once the company agrees on the objectives, resources and action will depend on them.

**Define activities to fulfill the objectives**

**Maintain the SIS “as designed” or better.**

This mandate includes two main factors:

1. Do not modify the original design, or modify it only for improvements properly evaluated and authorized through a management of change (MOC) protocol. It is easy to say, but difficult to achieve. A poor MOC is normally the main cause of introduction of systematic failures.

2. Maintain the performance of SIS components. This includes two categories of activities:
   - *Proof testing/functional test:* The objective is to reveal random dangerous undetected failures. These tasks shall be executed with a time interval lower than the test interval considered in the SIL calculations.
   - *SIF asset strategies:* these are complementary tasks to reestablish, periodically, the “as-designed conditions.”
     
   – SIF asset strategy tasks can be derived from failure mode and effect analysis (FMEA), according to IEC 60812.

It is important to realize that degradation mechanisms can be different for the same type of asset depending on the service and operating conditions. In consequence, the risk reduction measures or recommended corrective actions will also be different. Bad actors (asset with an inexplicably high failure rate) are normally the consequence of the use of general asset strategies on specific equipment whose degradation mechanisms and cause of failure are not covered by the recommended corrective actions used in the general strategy.

Tasks and associated schedule shall be synthesized in a plan. Proof testing along with the SIF asset strategies are both safety critical activities. If either of them is not executed, the mandate to maintain “as-designed conditions” will not be fulfilled.

**Maintain SIS efficiently**
Continuous evaluation and improvement is the key concept here. Data capture and analysis is needed to determine if the adopted asset strategies are effective. Initial estimation of many parameters is frequently obtained from generic data. The O&M phase generates real data that must be compared with the initial assumptions.

**Define mechanisms to evaluate the performance**

**Select your value indicators**

Think ahead; establish which are going to be your functional safety indicators as early as possible. SIS indicators show dynamic information, which could improve or decline depending on operational and maintenance actions. As with any other indicators, a reference value is needed to compare observed and expected performance. Most of the reference values were assumed in the analysis and design phase of the SLC (demand rate, failure rates, safe failure fraction, etc.). A SIF will deviate from the expected performance if real and assumed values differ.

Some value indicators give valuable information related to O&M company objectives for SIF management, but others should be specific to identify the source of deviations. The indicators are a company selection; consequently, what follows are just examples to illustrate the next stages of engineering the maintenance of SIS. This basic selection allows O&M to do what it is supposed to do: measure real observed performance and comparing against expectations, and measuring observed parameters to be compared with original assumptions.

*Compliance with the functional safety plan and schedule*

This indicator shows whether the facility is complying with the required schedule for proof testing and defined asset strategies activities for SIF components. The proof test events and asset strategies work orders shall be recorded in the computerized maintenance management system (CMMS).

*Observed RRF avg vs. target RRF avg, per SIL class*

This indicator gives to managers a general overview of the effective risk reduction factor obtained by SIFs versus the target values required by the PHA (see Figure 1).
Spurious trip rates

This indicator shows the spurious trip rate for SIF. Observed spurious trip rates can be compared to maximum limits included in the calculation. It is usually useful to group SIF-STR by units to show its impact on reliability.

Failure rates of SIF components for main classes and types

This indicator shows failure rates for main instrument classes and types. The company should select which instrument or SIF components classes-types will supervise. A correct taxonomy is a requisite for data collection and future analysis.

Demand rates

Figure 2 shows SIF (and related initiating events) with multiple demands. This is useful to identify bad actors, specific process under control with poor stability, and the effectiveness of other non SIS IPL.
Map SIS indicators, data, and events

It is very important to establish the relation of indicators, data, and events. Such graphical representation defines an intermediate mechanism to capture, segregate, process, and, finally, calculate the indicators. Figure 3 shows a reference mapping.
The SIS mapping of indicators, data, and events has two main areas. To the left of the indicators, the data is coming from O&M events, such as trip events, proof testing, or diagnostic alarms. To the right of the indicator, the data comes from values already established in the analysis and design phase of the function. Collection of data from both sides is critical for the performance evaluation. The mapping should also delineate minimum requirements for data capture.

Using the mapping example shown above, we can derive the following requirements for capturing data from events:

_SIF trip form_

It should capture any of the three possible functional scenarios: it worked as designed, it failed spurious, or it failed dangerous. Any of them will trigger a different situation. If the SIF worked as designed, the data is important to update the demand rates. If the trip was spurious, the real spurious trip rate can be updated, but, even more important, the failure should be recorded at equipment level, to update the SFF and observed failure rates. If the SIF failed dangerous (it did not protect), then a proof test has to be done to determine the failed component. The data is used to update the observed RRF and failure rates at component level.

_Proof test form_

This form contains the step-by-step procedure to test the function. The steps should be related to components of the system, and the criteria for success or failure should be established. In case of failure, its classification should be done. The standard, ISO 14224 Petroleum and Gas Industries – Collection and exchange of reliability, and maintenance data for equipment includes failure classification of safety instrumented functions in accordance with the IEC-61508 standard. The failures are split in two categories: random or systematic. The hardware random failures of components are further split in failure modes: dangerous detected (DD), dangerous undetected (DU), safe detected (SD), and safe undetected (SU).

_Functional test form_

This is a variant of the proof test form. Here, it is only important to capture if the overall function was operational and not individual components in failure.

Influence the outcome of the project

O&M objective is to have a system able to support SIS activities since day one of operation, including data capture and processing for performance evaluation. To fulfill such a requirement, a conjunction of activities has to be done in parallel with the analysis and design phase.

Engineering specifications

Reinforce SIS FEED (front end engineering design) engineering specification:
Define the proof testing strategy (online vs. offline) and minimum test intervals. These are constraints for the designer.

Define the spurious trip limits. This is a constraint for the designer.

Define O&M system(s) for SIS management, including planning (task and scheduling), data capture of events, and performance evaluation.

Define the necessary data for performance evaluation.

Select necessary reports and their requirements for the different phases of the SLC, describing minimum information (fields).

Establish the minimum acceptable requirements for proof testing. Provide a typical example to show the level of detail necessary.

Request procedures for each one of the proof test tasks considered in the SIL calculation. These proof tests should be reviewed and approved by O&M.

Either request automatic data exchange between engineering SIS packages and O&M SIS management system(s) or impose a system that can manage the SLC.

Request the calculation of the indicator’s reference values after SIF design is completed (before commissioning). This is the first opportunity to test communication between engineering tools and O&M systems for performance evaluations.

The specifications should be finalized during the FEED so that the requirements are officially categorized as contractual for the engineering companies.

**Proof testing strategy**

After the PHA has finalized and SIFs have been identified, the SIS maintenance strategy needs to be detailed. The following shortfalls should be avoided:

- **Oversimplifications**: specifying that proof testing will be done during shutdown or every “x” years is not sufficient. It is a completely different strategy for utilities where redundancy of equipment is normally found in process units where the possibility for frequent proof testing is rare. Designers shall not be left alone with such decisions, otherwise discrepancies between engineering assumptions and real O&M conditions will promptly appear.

- **Lack of commitment for online testing of final elements**: PVST has a wide acceptance from designers to decrease the PFD; however, such level of support is rarely found by operations. Any such strategies should be carefully analyzed, communicated, and approved by the O&M team. Acceptance of the strategy shall be a commitment for compliance during operation.

**Planning**

After SIL calculations have finalized, a proof-testing plan can be structured.

- **Task and schedule impact**: from a report containing the list of SIF, associated tasks, and scheduling, analyze the impact over the O&M organizations. Communicate results to management and prepare and follow recommendations.

- **Procedures**: review and approve proof testing procedures and include them in the SIS O&M management system or CMMS.

**Spurious trip rate (STR) review**
It is very important to calculate the STR individually per SIF and the global influence of all SIF over the unit. O&M shall define unit SIS STR limits.

There are many approaches. One of them is to assume the maximum limit as a percentage of the total unplanned shutdowns. The unplanned shutdown takes into account all sources of possible shutdowns (rotating, static, electrical, instrumentation, process control, human errors, etc.). Most of the unplanned shutdowns are related to rotating and static equipment so that the SIS percentage of unplanned shutdown is normally less than 10 percent of the total value. The reliability and maintainability (RAM) study is a source of information for the calculation. The following table is an example for a crude distillation and coker units. These units could have in excess of 25 SIF each, so in some cases the global limit (contribution of all SIF in a unit) could be the constraint difficult to satisfy. This method gives a conservative value for the STR (see Table 1).

**Table 1.**

<table>
<thead>
<tr>
<th>Unit</th>
<th>Unplanned SD</th>
<th>Turnaround</th>
<th>Total days/yr</th>
<th>Operational availability</th>
<th>SIS SD (% of unplanned SD)</th>
<th>SIS SD days/yr</th>
<th>Start up time (hr)</th>
<th>Global STR (1/yr)</th>
<th>Years between trip (1/STR) 25 SIFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD U</td>
<td>100</td>
<td>4.17</td>
<td>40</td>
<td>10</td>
<td>14.17</td>
<td>96.12%</td>
<td>7.50%</td>
<td>0.31</td>
<td>8</td>
</tr>
<tr>
<td>Coker</td>
<td>175</td>
<td>7.29</td>
<td>45</td>
<td>11.25</td>
<td>18.54</td>
<td>94.92%</td>
<td>5.00%</td>
<td>0.36</td>
<td>24</td>
</tr>
</tbody>
</table>

Once the STR figures are reviewed and agreed upon, STR requirements should be included in the FEED specifications. If not, engineering contractors are released to follow their own best practices. After SIL calculations are done, an official report should be submitted.

**Supporting tools for SIS management**

The ideal tool should manage all the safety life cycle phases with seamless integration. It should include risk analysis (or connection to risk analysis packages), SIL assessment, and safety requirement specifications (SRS) in the analysis phase, SIL validation calculations with access to SIS component failure rate databases in the design phase, and proof testing procedures, task management (definition and scheduling), and event management during the O&M phase.

It is also important to manage a workflow for creation, update, and approval for change management and revision history, and exchange of information with the CMMS.
If such software is not selected or enforced by the owner, integration of information from the different phases will be difficult to achieve or sustain at last (see Figure 4).

![Figure 4](image)  

O&M participation in the engineering of SIS is essential to establish solid bases to maintain “as-designed conditions” since the startup of the facilities. The owner knowledge of the process and requirements for operation and maintenance complement the designer vision of safety with reliability and maintainability.

Take a backward perspective, defining SIS key performance indicators and SIF reevaluation needs, the requirements for equipment taxonomy, MMS, and SIS, management software organization and interrelation are then established. Actions and activities derived from these requirements should be incorporated in the project and the safety lanning, with procedures supporting the processes. This approach allows the foundation for a correct management of the SIF since day one of operation, facilitating data collection, analysis, and decision making during the O&M phases of the safety life cycle to minimize risk efficiently.

ABOUT THE AUTHORS

**Henry Johnston** ([henry.johnston@aeolns.com](mailto:henry.johnston@aeolns.com)) is a principal specialist in functional safety in aeSolutions. He has more than 25 years of experience in engineering, maintenance, and reliability analysis of instrumentation, controls, and safety systems. He has worked in the development of instrument maintenance strategies for large-scale projects. Johnston holds a M.Sc. in electrical engineering from Missouri University of Science and Technology.
Fahad Howimil (fahadlm@hotmail.com) is a senior project engineer. He executed projects in the field of instrumentation and process control and worked in engineering support for the same field. Howimil works in engineering and project management at SABIC Saudi Arabia.

Source:

http://www.isa.org/InTechTemplate.cfm?Section=Focus_Areas1&template=/ContentManagement/ContentDisplay.cfm&ContentID=93361