



# IEC 61511 Implementation - The Execution Challenge

Tom Shephard and Dave Hansen - Mustang  
Published in *Control* magazine - May 2010

## ABSTRACT

The Safety Instrumented System (SIS) standard, IEC 61511, is driving the need for new engineering tools and Project Execution Plans (PEP). The standard is a lifecycle approach to defining, implementing and managing a Safety Instrumented Systems (SIS). Industry discussions tend to focus on the technical aspects of the standard however project execution is proving to have an equal or perhaps greater impact on the quality and success of an IEC 61511 project. Both challenges are driving the need for operating companies to modify and create their internal PEPs, tools, guidelines, standards and procedures. The same is true for Engineering, Procurement and Construction (EPC) and Main Automation Contractors (MAC). This article describes a few of the challenges, from the EPC and MAC perspective, and suggests approaches to enhance IEC 61511 execution and technical outcomes.

## Coordinating Project Execution and Functional Safety Plans

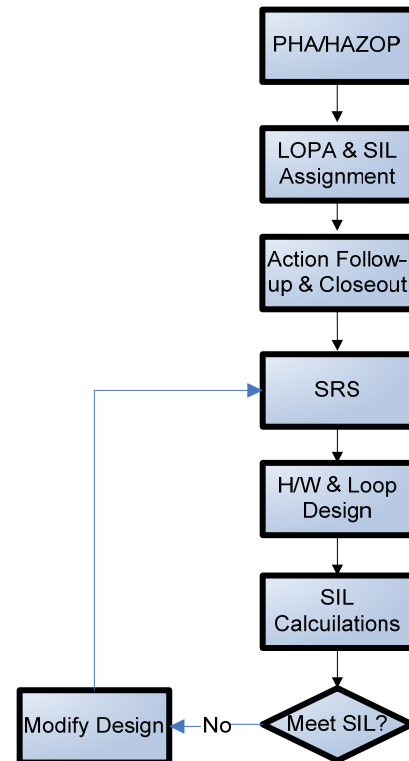
Figure 1 is an example of the elements commonly performed and supported by EPCs and MACs. For projects the PEP defines the scope of work, roles and responsibilities, work processes and procedures, QA/QC plans, etc. A Functional Safety Plan (FSP) is required by IEC61511 and encompasses many of these PEP processes and procedures but continues beyond the project to include the entire safety lifecycle through commissioning and operations. It also includes additional requirements that are specific to safety systems. The project team needs to coordinate and cross reference both documents to ensure there are no conflicts or exclusions. Some may choose to write an FSP that is specific to the project and another for operations. Both must satisfy the IEC 61511 requirements.

## Process Hazard Analysis (PHA)

The quality of the IEC 61511 implementation project begins with the PHA and the PHA team's ability to accurately identify hazards and quantify risk. PHA's have been performed for decades. The process is mature and generally understood. However IEC 61511 processes are revealing previously undetected PHA deficiencies and irregularities. The numerical aspect of the PHA and the accuracy and consistency of the assigned Consequence and Likelihood ratings are important. PHA teams tend to 'calibrate' their application of risk ratings differently. This becomes apparent when Safety Integrity Levels (SIL) resulting from a Layer of Protection Analysis (LOPA) are inconsistent for identical hazards. This variability may result in SIS over-design (unnecessary costs) or under-design (design integrity is inadequate for the true risk). Variability can also impact Operations and Maintenance (O&M) if like Safety Instrumented Functions (SIF) within a facility differ in design, maintenance intervals and operating procedures.

Specialists in rotating equipment, fired vessels and reactors are required to accurately identify and quantify operating risk. PHAs may miss or overestimate equipment-unique hazards if the appropriate specialists do not participate in the assessment. A missed hazard may become apparent if the PHA/LOPA does not require a SIF that is commonly employed to protect against a known operating risk.

Figure 1 – Simplified SIS Lifecycle (Partial)





# IEC 61511 Implementation - The Execution Challenge

Procedural and technical issues may arise during a PHA that requires expert and perhaps, corporate level clarification. The procedures, tools and standards may fail to provide adequate guidance causing the team to table the problem for later resolution and potentially delay PHA completion.

As indicated in Figure 1, the application of IEC 61511 increases the number of analysis and design steps that can lengthen SIS design cycle. The project must be well planned, managed and correctly scheduled and resourced to keep the SIS design off of the project's critical path.

## Layer of Projection Analysis (LOPA)

LOPA is becoming a commonly accepted method for determining layers of protection and allocating safety functions. The PHA report is the LOPA starting point. For each PHA hazard and associated risk values, the LOPA team identifies and assigns one or more Independent Protection Layers (IPL) until the risk is reduced to an acceptable level. Common instrumentation IPL's are alarms and relief valves. If a risk remains after other preferred IPLs are applied, the remaining risk is typically reduced by a SIF. Like PHA's, LOPA reports are issued with recommendations and action items that may require further analysis and assessment. The report in this form is often handed off to the EPC or MAC to implement.

Once received the EPC or MAC generally reviews the LOPA report to understand its content and completeness. A month or more may lapse before this step is completed. On closer examination, questions may arise and irregularities may become apparent. A typical example is an alarm assigned as an IPL. The LOPA guidelines for the project may specify rules such as: 1) the Operator must be able to respond to the alarm and initiate corrective action within 10 minutes, 2) the Operator response and corrective action must occur within the process response time (typically within ½ the process response time) and 3) the alarm must be independent from the event and equipment that may have caused the hazard, e.g. a failure in the Basic Process Control System. On review one or more of these assumptions prove to be incorrect. Another irregularity seen in LOPA reports is variability in SIL targets when the equipment, hazard scenario and IPLs are the same. This can be symptom of a problematic PHA. For these reasons a process should be in place that allows the LOPA team to challenge and review the PHA and if necessary, make changes in the PHA if an error is confirmed. (As a counterpoint SIL variability can also result if IPLs are not applied consistently in the LOPA.)

The LOPA report does not typically provide the following information required to progress the SRS:

- SIF final elements
- Answer the question 'Does SIF activation create a new hazard?'
- Hazard process response times
- Potential sources of common cause failure
- Confirmation that the assessment addresses all modes of operation

It is not uncommon that a proposed SIF final element creates a new hazard when it moves to its safe state or position. This triggers a one-off (and unplanned) hazard assessment that may require a revisit to the PHA or LOPA. Process response time is often difficult to define and provided by different disciplines and equipment specialists. A 'fast' response time may trigger a new hazard that also requires further assessment. Identifying sources of common cause failure often requires input from several disciplines. The additional time needed to assess hazards when operating in different operating modes is often overlooked.



# IEC 61511 Implementation - The Execution Challenge

Suggestions for improving PHA and LOPA outcomes and execution include:

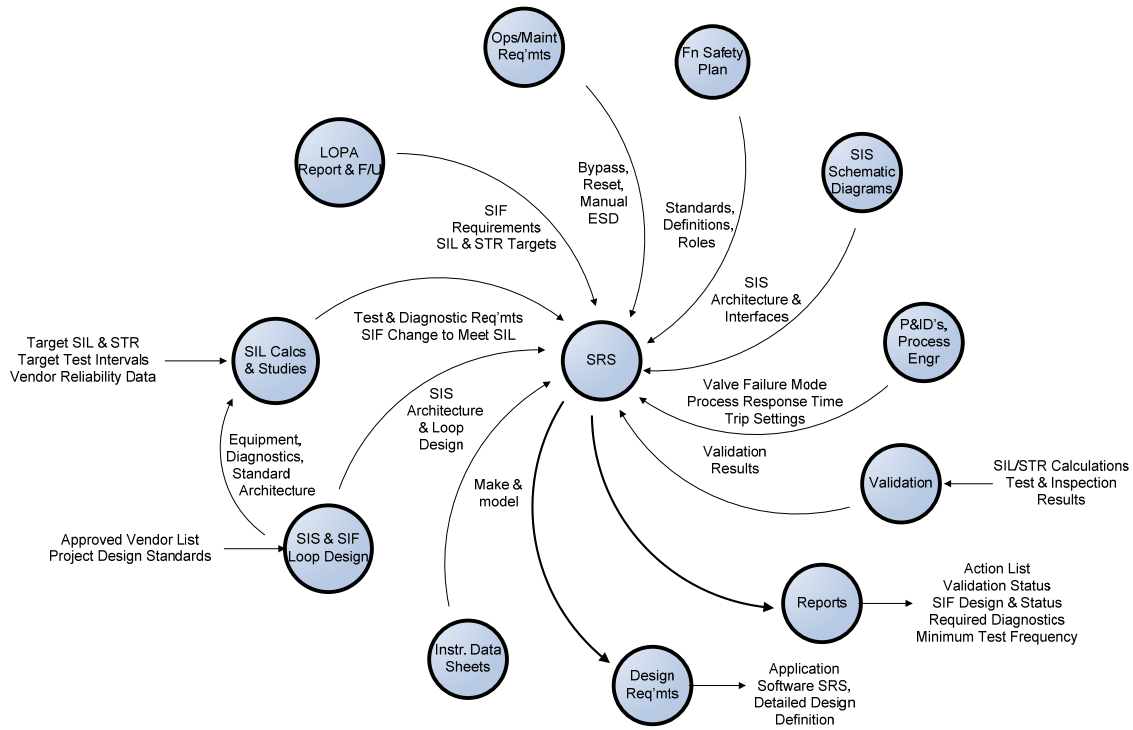
- Provide the FSP before the project starts. It should clearly define the site or corporate approach, tools, processes and personnel for implementing IEC 61511. It should include a process to resolve problems that are not directly addressed in the PEP and FSP, and how to provide the analysis information typically missing in the LOPA report, e.g., SIF response time.
- Project teams should resist the temptation to shortcut or truncate the analysis phase to save money or reduce project schedule. This can cause a team to miss a critical hazard or define unnecessary requirements that result in higher SIS lifecycle costs.
- Provide equipment and risk specific PHA and LOPA examples (corporate approved) that clearly show the expected application of the corporate and project tools, risk matrices and IPL rules. This should help to achieve more accurate and consistent outcomes.
- Align the PEP with the Function Safety Plan. Revise the plan to address challenges that are unique to an IEC 61511 implementation.
- Increase training for PHA and LOPA teams on the correct use and application of the supplied tools, standards and procedures.
- Provide checklists that define the recommended steps to assess hazards for common equipment types such as fired vessels and rotating equipment.
- Provide a documented process to track, expedite and resolve PHA and LOPA recommendations and action items.
- Provide a Quality Assurance plan to confirm the requisite procedures are followed.
- Assign a team to verify and consolidate PHA and LOPA recommendations and replace “consider” recommendations and action items with actionable decisions. The team should be empowered to correct PHA and LOPA errors and omissions identified after the report is issued.
- Have technical specialist conduct pre-assessments of specialty equipment to reduce analysis time and improve results.
- Insure PHA and LOPA teams include the necessary technical expertise.
- Ensure Management of Change procedures encompass all steps in the IEC 61511 process.

## Safety Requirements Specification (SRS)

This phase begins the shift from analysis to SIS engineering and design. When compared to traditional SIS specifications, the SRS is a major expansion in both depth and breadth. Example content is identified in Figure 2. The SRS may be one document or a compilation of documents. The SRS is the master document. Referenced documents are subordinate to the SRS. The global SIS content is more comprehensive when compared to historical SIS specifications. It should not use generalizations that were often common to these specifications. The time and effort needed to complete this section is generally understood. In contrast, the time and effort needed to fully specify individual SIFs can vary widely. On projects having a large number of SIFs (common to large floating production platforms) this new activity may noticeably increase the SIS engineering effort. In response, EPCs and MACs must modify and adapt their procedures, execution plans and cost estimating tools accordingly.

# IEC 61511 Implementation - The Execution Challenge

Figure 2 – Safety Requirements Specification Inputs and Reports



The simple task of issuing the SRS requires discussion. The global section should be issued for approval early. Issuing the SIF section may need to occur on a SIF by SIF basis since completion depends on when PHA/LOPA action items are completed and when information available. The SRS for a SIF can be several pages. If the SRS is issued as a single document, the Client is challenged with reviewing a complex document that may be 100's of pages. The traditional project review period is 5-10 days.

Suggested in Figure 2, the information required to fully define and document a SIF may entail 40 or more unique data items. The source and detail required to document each item (e.g., proposed SIF architecture) must be clearly defined. The effort to gather, track and review this data can be significant. For a large project the work includes migrating and recording large amounts of data that may be provided in different formats, at different times and by different disciplines and organizations. Companies are beginning to develop in-house SRS data base tools to improve productivity, reduce errors and track SIF development and approval status. These tools may also be used to create SRS deliverables, status reports, and action items lists and provide a central repository to manage the SRS over the SIS lifecycle. Information provided by different disciplines and organizations represents an interface challenge that should be addressed in the PEP Interface Management Plan. The potential for data transfer and transcriptions errors should be addressed in the PEP Quality Plan.

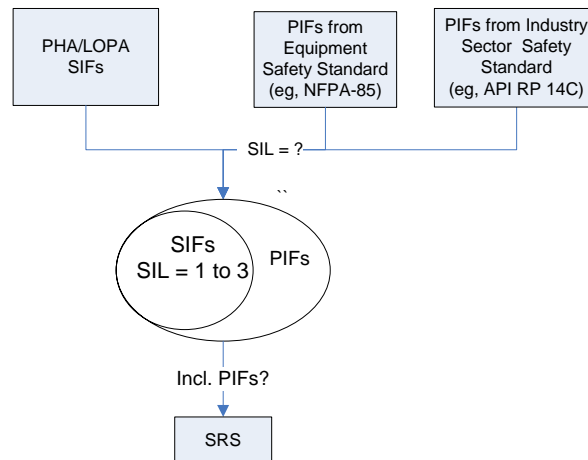
Completing the SIF section can be challenging and typically requires a SIS engineer that has significant depth and breadth. Once completed a 'cold eyes' quality check by a by a senior competent person should be considered. The Quality Plan should define the approach to these checks, e.g., verify all SIFs, only complex SIFs, or a randomly selected percentage.

# IEC 61511 Implementation - The Execution Challenge

The SIF specification process may identify problems that can trigger a secondary work process or design change. Example, the LOPA defines a hazard in an exothermal reactor as a ‘hot spot’ that can exceed metallurgy limits. The report proposes 2 out of 3 sensor voting. Project P&ID’s show three thermocouples mounted vertically. If this were a large reactor this design may fail to detect the hot spot, and the three sensors will see very different temperatures. The design does not appear to meet the intent. The SIS engineer should contact the LOPA owner to confirm the intent which may trigger a design change.

Figure 3 identifies a common scope question. What are the project requirements for documenting Protective Instrumented Functions (PIF) that are not required by the LOPA/PHA? PIFs may be provided for safety (not SIL rated), environmental, regulatory (proscriptive), and asset protection. Are PIFs documented in the SRS? Do the SIF analysis and verification steps apply to PIFs? Will the SRS differentiate between SIFs and PIFs? These questions need to be answered before budgets are firming up and schedules developed.

Figure 3 – Protective Instrumented Functions (PIF) in the SRS?



The approach to verifying SIF response time is a typical scope question. Example, will it be calculated during detailed design using published performance data and valve supplier test records? Perhaps it is only verified during pre-commissioning which can be risky if the response time target is not met.

Suggestions for improving SRS outcomes and execution include:

- Define what information is included in the SIF specification section, the level of detail required, who provides the information, and who records it in the SRS. (This can impact proposals, project scope and schedules.)
- Provide an example specification for common SIF types and indicate the level of detail required.
- Define the approach to assessing and documenting PIFs that are not SIL rated.



## IEC 61511 Implementation - The Execution Challenge

- Define if the SRS will differentiate instrumented functions by type, e.g., safety, environmental, regulatory or asset protection.
- The PEP Quality Plan should define the quality checks required.
- The global SRS narrative section should be completed and approved before SIF specification work begins.
- Confirm which document, e.g., the SRS or project instrument database, is the 'master' repository for alarm and trip settings.
- Define how and when the individual SIF specifications will be issued for approval.
- Utilize electronic tools to manage the SRS SIF definition section, support electronic data transfer to and from other systems, and to manage SRS data over the SIS life-cycle.
- Develop tools for tracking SIF specification design and completion status.

### SIL and Spurious Trip Rate (STR) Calculations

SIL and STR targets are verified using project approved calculation tools and reliability data sets. The SRS typically provides the information needed to correctly model the SIF. Final SIL calculations are generally provided late in the project. To support early equipment procurement, preliminary SIL calculations are often recommended to confirm that SIL 2 and 3 SIFs and the more complex SIL 1 SIFs can meet the SIL and STR targets. Failure to meet a target typically triggers a study to identify alternate designs. Individual studies may require a few hours to a few days to complete. The elapsed time may be weeks or longer when the available design options deviate from the project or facility standards, or the project impacts are assessed. Studies to find alternatives for complex or difficult SIFs can take significantly longer.

If not defined in the FSP, the reliability data used in SIL calculations should be selected early in the project. The FSP or PEP must define how new data will be assessed and formally approved for use. Overly conservative data can drive SIF design towards unnecessarily high capital and lifecycle costs. Data provided from commercial resources can be significantly more conservative when compared to Client collected or product vendor provided data. Conversely, inaccurate data can lead to a deficient design and a faulty verification step.

Suggestions for improving verification calculations and execution include:

- The FSP or PEP should identify the calculation software and the source of the reliability data used.
- Provide rules to guide how SIFs are modeled, named and documented, target PFD safety factor, applicable Common Cause factors, etc.
- Define what information and detail is recorded in free form fields.
- Provide example calculations for common equipment and complex SIFs.
- Define the process for approving third party reliability data used in preliminary and final calculations and its introduction to the team.
- Define what test interval is used, e.g., use the interval specified in the SRS or perform iterative calculations to determine the maximum interval possible and still meet SIL and STR targets.
- Define the process for issuing and approving calculations.



# IEC 61511 Implementation - The Execution Challenge

## Miscellaneous

The following are additional topics and recommendations to consider:

- Define project requirements for factory testing, site validation testing and checklists, on-line and off-line proof test procedures, record keeping, and the process to track, correct and verify inspection and test deficiencies. Provide procedure examples to confirm scope and format requirements.
- Determine how IEC 61511 processes, documents and procedures are coordinated and integrated with existing facility O&M practices and Safety Management programs. Changes in organizational boundaries, work process and technical procedures may be required. This process and implementation should be framed and budgeted as a separate, standalone project to better ascertain its success and timeline.

## Conclusion

Implementing IEC 61511 requires changes in historical work processes, procedures, tools and execution plans. Operating companies should continue to develop corporate standards, guidelines and tools to guide project teams and improve consistency between projects. EPCs and MACs will continue to develop the execution and technical plans, procedures, tools and resources required to successfully implement this standard in today's complex project environment.

## Author Bio's

**Tom Shephard** is an automation Project Manager and Main Automation Contractor (MAC) Program Manager at Mustang Engineering. He has 28 years of control and safety system experience in the Oil & Gas, refining, marketing and chemical industries. Tom is a *Certified Automation Professional* (ISA) and a certified *Project Management Professional* (PMI). He holds a B.S. in Chemical Engineering from Notre Dame University.

**Dave Hansen** is the Safety System Practice Lead at Mustang Engineering. He has over 20 years of control and safety system experience in Oil & Gas, refining and chemical industries. He is a Southern Alberta Institute of Technology (SAIT) instrumentation technology graduate, a *Certified Engineering Technologist* (Instrumentation) and a *Certified Functional Safety Expert*.