Going Full Life Cycle with Process Safety Data

Iwan J.W.R.J. van Beurden*, Kate M. Hildenbrandt

exida, 80 N. Main St., Sellersville PA, 18960, USA
vanbeurden@exida.com

The international functional safety standard IEC 61511 provides the safety lifecycle as a steadfast guideline to assess and mitigate risk for manufacturing processes including refineries, chemical, petrochemical, pulp and paper, and power plants. To achieve a functionally safe system, it is essential to follow each requirement in the standard. However, consistent execution is difficult to achieve and often depends on the tools used to perform analysis and specification of the safety instrumented system. The need for a consistent work process was fulfilled with a fully integrated safety lifecycle software suite. Lifecycle tools often include a module for each stage of the safety lifecycle. Use of the full suite ensures quality assessment and execution of a safety instrumented system, as well as compliance to the safety standard. An integrated tool will also streamline these tasks, easily transferring data from one module to another to save the user time and money.

In this paper, the benefit of using an integrated safety lifecycle tool versus use of MS Excel™ spreadsheets or other in-house tools is quantified. The intent is to show how users of the software reduce the number of engineering hours, and therefore dollars spent, for each safety lifecycle task. It is assumed that all required information is available when needed. Through conservative estimates, this paper proves that it pays to use an integrated tool to support your safety lifecycle tasks.

1. Introduction

An integrated safety lifecycle tool will provide a suite of tools that guide users through the analysis, implementation, and operation phases of the safety lifecycle, as defined in IEC 61511. These phases include the following key tasks:

- Analysis Phase:
  - o Scope Definition and Process Design
  - o Process Hazard Analysis (PHA)
  - o Layer of Protection Analysis (LOPA)
  - o Safety Integrity Level (SIL) Selection
  - o Safety Requirement Specification (SRS)
- Design and Implementation Phase:
  - o Safety Integrity Level (SIL) Verification
  - o Detailed Design Safety Requirement Specification (Design SRS)
  - o Configuration of Safety Logic
  - o Specification of Proof Tests
- Operation Phase:
  - o Configuration of Safety Instrumented System (SIS) into field collection database
  - o Documentation of Field Failures, Proof Tests and Maintenance Activities
  - o Standard Compliance, Audit Preparedness

Use of excel or an in-house tool is believed to be a low-cost solution to support these SLC tasks and design a safety instrumented system. However, with each phase of the lifecycle comes a hefty to-do list that requires hours of preparation, discussion and documentation. As hours add up, the cost of the project increases. Use of an integrated tool reduces the time required at each phase by organizing and transferring inputs from one step to the next, providing built-in failure rate data, performing design calculations and generating necessary reports.

In the following sections, each task is described and an estimated time to complete the tasks using excel versus using an integrated lifecycle tool is provided. The time estimate for each task assumes 10 nodes are analyzed, each resulting in 5 safety instrumented functions (SIF). To attribute a cost range to the hours spent, an hourly rate of $75 is assumed, as well as a burdened rate of $150 per hour.

2. Safety Lifecycle Phase 1: Analysis

2.1 Scope Definition and Process Design

To conduct a quality process hazard analysis, participants must be equipped with preliminary piping and instrumentation diagrams, equipment layouts, manning arrangements and safety targets. It is conservatively assumed that users of an integrated lifecycle tool and excel alike will have to same start effort.

2.2 Process Hazard Analysis (PHA)

To prepare for a PHA, the process plant must be broken down into smaller pieces called nodes. Nodes are typically small sections of the plant with a specific design intent. For example, a steam drum, piping feed into a reactor, a flare, and so on. For each node, different challenges to the process parameters are analyzed. These challenges are called deviations, and can include high pressure, low pressure, no flow, reverse flow, etc. Nodes and deviations must be defined before any sessions take place. An advanced PHA module reduces this preparation time with embedded smart deviations for each node type. For this reason, preparation may take 0.3 hours per node using an in-house tool but will only take 0.1 hours per node in an integrated tool.

The objective of the PHA is to imagine all causes and consequences of a deviation to the process parameters. Risk is determined by quantifying the frequency of the cause, and the severity of the consequence. If the deviation potentially leads to a dangerous hazard, safeguards and recommendations are identified. Most often, the PHA will include process engineers, process control engineers, safety engineers, operations and maintenance engineers, as well as a facilitator and a scribe. Depending on the size of the system in question, the PHA could require multiple sessions. The cost estimate for the PHA assumes five participants would spend 6 hours analyzing one node using an in-house tool, and 4 hours per node using the PHA module in an integrated tool. The benefit of using the tool's smart deviations and built-in libraries increase as more nodes are analyzed. To analyze a unit of ten nodes, an integrated tool would save nearly 100 hours.

Table 1: Process Hazard Analysis (PHA) Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Total Hours per node	Unit Total (10 nodes)	Total Hours per node	Unit Total (10 nodes)
Process Hazard Analysis (PHA)	30.3	303.0	20.1	201.0

2.3 Layer of Protection Analysis (LOPA)

The LOPA defines protection measures necessary to reduce the frequency of a dangerous hazard. The groundwork for this analysis is completed in the PHA. Safeguards identified in the PHA are analyzed as independent protection layers (IPL). The frequency of an initiating event is multiplied by the probability of failure of each protection layer, bringing the actual frequency of the hazard to a tolerable level. The protection layers can include anything from an alarm and operator intervention, basic process control function, a device such as a relief valve, or a safety instrumented function. Proper analysis requires a process engineer, a process control engineer and a safety engineer at a minimum.

In an integrated tool useful information is transferred from the PHA module to the LOPA instantly, with the push of a button. In addition, the user can select applicable initiating event frequencies and probability of failure on demand for IPL's straight from the LOPA database in the tool. For this reason, preparation for a LOPA may take 3 hours per hazard scenario using an in-house tool. However, hours needed to prepare using an integrated tool are negligible.

This cost estimate assumes each node analyzed in the PHA has five hazard scenarios to be analyzed in the LOPA. In this case, one hazard scenario will take 2 hours using an in-house tool, but only 1 hour using an integrated tool. If three engineers are required to perform the LOPA and they analyze 50 hazard scenarios, use of an integrated tool would save 300 engineering hours.

Table 2: Layer of Protection Analysis (LOPA) Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Total Hours per hazard scenario	Unit Total (50 hazard scenarios)	Total Hours per hazard scenario	Unit Total (50 hazard scenarios)
Layer of Protection Analysis (LOPA)	10.5	525.0	4.5	225.0

2.4 Safety Integrity Level (SIL) Selection

If the LOPA concludes a SIF is necessary to reach the target frequency for a hazard scenario, the risk reduction factor (RRF) and the safety integrity level (SIL) for that SIF must be defined before design and implementation. For each SIF, the RRF is the ratio of the actual frequency of the hazard divided by its target frequency. The value of this factor correlates to a safety integrity level as shown in the chart below.

Table 3: Safety Integrity Level relation to PFD_{AVG} and Risk Reduction Factor

Safety Integrity Level (SIL)	Target average probability of failure on demand (PFD_{AVG})	Target Risk Reduction (RRF)
4	$\geq 10\text{-}5$ to $< 10\text{-}4$	> 10,000 to ≤ 100,000
3	$\geq 10\text{-}4$ to $< 10\text{-}3$	> 1,000 to ≤ 10,000
2	$\geq 10\text{-}3$ to $< 10\text{-}2$	> 100 to ≤ 1,000
1	$\geq 10\text{-}2$ to $< 10\text{-}1$	> 10 to ≤ 100

This task is straightforward provided the PHA and LOPA are done well. However, if many SIFs are required, the number of hours spent add up. An integrated tool would automatically perform the SIL selection based on the LOPA, which should save up to 15 minutes per SIF. Assuming each hazard scenario analyzed in the LOPA requires one SIF, about 12 hours can be saved by using an integrated tool for SIL selection.

Table 4: SIL Selection Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
SIL Selection	0.3	12.5	0.0	0.0

2.5 Safety Requirement Specification (SRS)

The safety requirement specification outlines the purpose and target SIL of each SIF. The specification should answer many questions, including the following:
- What is the safe state?
- What equipment needs to be protected?
- What actions must be taken?
- What is the response time of those actions?

This document summarizes findings from the entire analysis phase of the safety lifecycle and becomes the guideline for design and realization. To write the SRS from scratch may take 3 hours per SIF. However, with use of an integrated tool information from PHA, LOPA, and SIL selection is pre-populated into the SRS tool. This automatically generates a report, with little more than 1 hour needed per SIF to customize as needed. For 50 SIFs, use of an integrated tool can save 100 hours.

Table 5: Safety Requirement Specification (SRS) Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
Safety Requirement Specification (SRS)	3.0	150.0	1.0	50.0

3. Safety Lifecycle Phase 2: Design and Implementation

3.1 Safety Integrity Level (SIL) Verification

The design and implementation phase of the lifecycle starts with SIL verification. In this task, SIFs are designed to meet their target SIL level with guidance from the SRS. Each SIF includes a combination of three types of devices: sensors, logic solvers, and final elements. The achieved SIL level of a safety instrumented function is the lowest value of the following factors:

- The SIL level based on PFD_{AVG} (low demand) for the sum of all pieces of equipment in the SIF.
- The SIL level based on minimum architectural constraints of each element in the SIF.
- The SIL level based on systematic capability for each piece of equipment in the SIF.

Minimum architectural constraints are determined based on redundancy levels of the SIF. Users of an integrated tool do this simply by modelling the SIF in a SIL verification module. In some cases, the quality of the failure rate data must be validated per IEC 61508 Route 2_H. In a SIL verification module, this compliance should be confirmed through its calculation engine. To demonstrate systematic capability, selected equipment must be IEC 61508 certified or a proven in use justification must be documented. In an integrated tool, the SIL verification module should automatically consider IEC 61508 compliance and/or allow easy documentation of proven in use justification.

Finally, the PFD_{AVG} calculation is based on the failure rate and failure modes of each device, mission time, mean time to restore, probability of initial failure, redundancy, and proof test intervals and effectiveness. To gather this information and perform the calculation could easily take 8 hours per SIF. However, an integrated tool's SIL verification module should have industry failure data embedded in the tool. Users can model the SIF, specify the equipment, and automatically calculate the achieved SIL level. If the SIF does not meet the target SIL level, simply select a different device and/or adjust one of more of the other conceptual design parameters. For these reasons, modelling one SIF in an advanced SIL verification module takes approximately one hour. If modeling 50 SIF's, one can save 350 hours by utilizing an integrated tool. A detailed overview of parameters that should be included in a PFD_{AVG} calculation can be found in The Key Variables Needed for PFD_{AVG} Calculation are documented by van Beurden I.J.W.R.J., Goble W.M., 2018,

Table 6: SIL Verification Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
SIL Verification	8.0	400.0	1.0	50.0

3.2 Detailed Design Safety Requirement Specification (Design SRS)

Once conceptual design of your SIF is completed, a Design SRS outlines how the SIF should be implemented. Hardware requirements are defined here, as well as logical relationship information between inputs and outputs. The Design SRS defines, among others:

- Application level diagnostics
- Analog signal health range
- Voting arrangements
- Repair time requirements
- Process connection requirements
- Auxiliary inputs and outputs

Writing a Design SRS from scratch may take approximately 3 hours per SIF. In an integrated tool, most of the required information is input or calculated during SIL verification and can be transferred to the Design SRS module from the SIL verification. Additional information like auxiliary inputs and outputs can be defined and linked to existing library items easily. From there, the document is automatically generated. This should take the user only 0.5 hours per SIF. If one is documenting 50 SIFs, use of an integrated tool will save 125 hours.

Table 7: Design SRS Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
Design SRS	3.0	150.0	0.5	25.0

3.3 Configuration of Safety Logic

With the detailed design complete, SIF information can be configured in the safety logic solver. Information from the Design SRS like inputs, outputs, voting arrangement, trip delays, etc., must be converted to application program function blocks. For many SIFs this is a simple, yet time consuming process averaging 5 hours per SIF, including and review and re-work necessary. An integrated lifecycle tool may have a SIS configuration module that will automatically convert the SIL verification and Design SRS information into an application program. This will allow for significant time savings, with the ability to convert all SIFs in one import. In addition, the automatic conversion eliminates the need for a programmer to interpret the Design SRS information and the creation of intermediate logic diagrams like cause and effect matrices. With this module, programming of the PLC should take no more than 0.5 hours per SIF including final review. For 50 SIFs, use of an integrated tool should save roughly 225 hours.

Table 8: Configuration of Safety Logic Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
Configuration of Safety Logic	5.0	250.0	0.5	25.0

A significant project execution time savings is expected as the application program is in once the design is complete. Contrastingly to typical project execution where the application program is created while the design is still being finalized resulting in design changes and updates needed to be made to the application program.

3.4 Specification of Proof Tests

The proof test interval and effectiveness for each device in a SIF are key variables in SIL verification. A user will need to define a specific proof test for each device. Manufacturers of IEC 61508 compliant equipment are required to publish a proof test in their safety manual. These must be collected and documented in one specification to guide operators through the proof test. On average, 3 hours per SIF are required to complete the proof test specification. However, users of an integrated lifecycle tool can automatically generate a proof test report based on an integrated equipment database, saving 2.5 hours per SIF in the process. For a total of 50 SIFs, integrated tool users will save 125 hours on proof test specification.

Table 9: Proof test Specification Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
Proof test Specification	3.0	150.0	0.5	25.0

4. Safety Lifecycle Phase 3: Operation and Maintenance

The final phase of the safety lifecycle, operation and maintenance, includes tasks required for standard compliance and to validate each SIF's conceptual design SIL verification. These tasks include recording process demands, device failures, proof test results, and completion of routine maintenance.

4.1 Configuration of SIS into field collection database

Tracking field failures, proof tests, and routine maintenance is mandatory per IEC 61511. To properly keep track of all devices, physical device locations, maintenance activities and proof test due dates, a structured database is most effective. However, populating information into such a database can be a time-consuming task taking on average 6 hours per SIF. Users of an integrated tool can transfer SIF information from the SIL verification and Design SRS modules into the life event recorder module. This one import will configure the plant hierarchy, device information, device locations, and procedures for proof tests and routine maintenance. This import will take 0.5 hours per SIF. To configure 50 SIFs, use of an integrated tool will save 275 hours.

Table 10: Configuring SIS into database Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
Configuring SIS into database	6.0	300.0	0.5	25.0

4.2 Documentation of Field Failures, Proof Tests, and Maintenance Activities

During normal operation, field failures, proof tests, and process demands must be recorded. Though it is expected that recording with an integrated tool will be easier than a home-grown database due to ease of use, this cost benefit analysis conservatively assumes an equal amount of time will be spent on this task.

4.3 Proof of Standard Compliance (Audit Preparedness)

It is important to have the ability to prove compliance to safety standards such as IEC 61511 in the event of a safety audit. These can be random or as a result of an incident. At such a time, all relevant functional safety documentation will be reviewed. This includes PHA, LOPA, SRS, and SIL Selection reports, as well as SIL Verification, Design SRS, and Proof Test reports. Evidence of life event recording including proof tests, maintenance activities, failure recording must also be shown. Collection of this information can be quite challenging if not stored in a centralized location. For users of an integrated tool, all necessary information is embedded in the integrated tool file. For this comparison, it is conservatively estimated that use of an integrated tool will save nearly 30 hours when preparing for an audit.

Table 11: Proof of Standard Compliance Cost Estimate

SLC Task	Hours spent - using excel		Hours spent - using Integrated tool	
	Hours per SIF	Unit Total (50 SIFs)	Hours per SIF	Unit Total (50 SIFs)
Configuring SIS into database	32.0	32.0	4.0	4.0

5. Conclusions

It should be a top priority throughout the process industry to perform high quality analysis, implementation and operation of a safety instrumented system. To prove compliance to a functional safety standard like IEC 61511, it is important that the information be organized, accurate and properly documented. An integrated tool allows to easily perform and document all SLC tasks, while at the same time improving overall efficiency, and therefore saving time and money. This analysis highlights how use of an integrated tool can impact the bottom line of each new project.

In the end, analyzing 10 nodes and subsequently analyzing, implementing, and maintaining 50 SIFs using excel or an in-house tool will take a grand total of approximately 2,300 hours. For users of an integrated tool these same tasks should take about 630 hours. Depending on the hourly rate of the engineers assigned to each task, an integrated tool will save $120K-$240K per 10 nodes and 50 SIFs. It is possible for a system in the process industry to have hundreds of nodes and SIFs. Based on the analysis documented in this paper, it can be assumed that use of excel or an in-house tool is nearly 4 times more expensive then use of a completely integrated safety lifecycle tool.

Table 12: Proof of Standard Compliance Cost Estimate

Item	Hours Spent – Using Excel	Hours Spend – Using Integrated tool	Time/Cost Delta
SLC Analysis Phase	990.50	476.0	514.5
SLC Design and Implementation Phase	950.00	125.0	825.0
SLC Operation & Maintenance Phase	332.00	29.0	303.0
Grand Total	2272.50	630.0	1642.5
Cost (Hourly Rate: $75/hour)	$170,437.50	$47,250.00	$123,187.50
Cost (Burdened Rate: $150/hour)	$340,875.00	$94,500.00	$246,375.00

References

exSILentia User Guide, exida, Sellersville, PA, USA

Hildenbrandt K.M., van Beurden I.J.W.R.J., 2018, Reducing Project Lifecycle Cost with exSILentia®, Whitepaper, exida, Sellersville, PA, USA.

van Beurden I.J.W.R.J., Goble W.M., 2018, The Key Variables Needed for PFD_{AVG} Calculation, version 2.1, Whitepaper, exida, Sellersville, PA, USA.