Case Study of a Safety Instrumented Burner Management System (SI-BMS)

aeSolutions Technical Team

Keywords

Burner Management System, BMS, Boilers, Construction Industry Institute, CII, Detailed Design, Front End Loading, FEL, Safety Integrity Level, SIL, Safety Instrumented System, SIS, SI-BMS, Safety Instrumented Burner Management System, ANSI/ISA 84, NFPA 85, Lifecycle Cost Analysis, Benefit-To-Cost Ratio

Abstract

This case study will discuss the application of the safety lifecycle as defined by ANSI/ISA 84.00.01-2004 (IEC 61511 mod) to two single burner multiple fuel boilers. Each boiler is capable of firing natural gas, oil and/or waste gas, in order to supply the plant header with 1,365 psig steam at a maximum capacity of 310,000 lb/hr. The project team included the end client task force at the manufacturing facility, the engineering firm with design/procurement responsibility, the boiler OEM, the burner/gas train OEM, and the safety instrumented system consultant. This paper will cover:

- the development of a SIS front end loading package,
- the project cost savings realized attributed to following the safety lifecycle, and
- the challenges encountered during the design process associated with the implementation of the safety lifecycle across a diverse project team.

Introduction

This study summarizes the design and installation of two large packaged boilers. The project was implemented following a staged engineering approach to engineering and financial decision making. The Construction Industry Institute (CII) describes a staged approach to projects, where engineering is divided into two phases; front end loading and detailed design. The CII has done extensive research on improving project success. Towards this end, the CII has documented that front end loading of capital facilities "is an extremely important function in determining the ultimate outcome of a project." The CII, through quantitative analysis of 62 projects, as noted in *Analysis of Pre-Project Planning Effort and Success Variables for Capital Facility Projects* (1), has stated that the front end loading (FEL) "effort level directly affects the cost and schedule predictability of the project." This includes the following conclusions:

As the level of front end loading tasks increases, the project cost performance from authorization decreases by as much as 20%

As the level of front end loading tasks increases, the variance between project schedule performance versus authorization decreases by as much as 39%

As the level of front end loading tasks increases, the plant design capacity attained and facility utilization improved by as much as 15%

As the level of front end loading tasks increases, the project scope changes after authorization tend to decrease

As the level of front end loading tasks increases, the likelihood that a project met or exceeded its financial goals increased

The CII further concludes that the “design work hours to be completed prior to project authorization should be from 10% to 25% of the total design effort depending upon the complexity of the project.” The CII also notes that “expenditure of less effort should be accompanied with an understanding of the implications of not providing this effort is decreasing the probability of project success.” With this information in mind, aeSolutions fully endorses the development of a front end loading package for all safety instrumented system projects.

The CII defines a front end loading package for a capital facility as “the process of developing sufficient strategic information for owners to address risk and decide to commit resources to maximize the chance for a successful project.” aeSolutions defines the following tasks as being part of a typical SIS FEL.

SIS FEL

- Hazard identification
  - Conduct HAZOP
- Risk assessment
  - Perform LOPA
  - Develop SIF list
  - Develop SIS design basis support report
- Safety requirements specification (SRS)
  - Develop lifecycle cost analysis
  - Develop interlock / safety instrumented function list
  - Develop sequence of operations
- Conceptual design specification
  - Redline P&ID’s
  - Develop system architecture diagram
  - Develop E-stop philosophy
  - Develop testing philosophy
  - Develop UPS philosophy

- Develop bypassing philosophy
- Develop wiring philosophy
- Develop SIS logic solver specification – Bill of materials (BOM)
- Develop approved instrument vendor list / Procure plan for SIS
- Develop SIL verification report
- Develop control panel location sketch
- Develop control philosophy specification

- Summary safety report
- Construction estimate, total installed cost (+- 20%)

aeSolutions defines the following tasks as being part of a typical SIS detailed design package. One should also note that new projects, versus retrofit SIS upgrade projects, will tend to have different detailed design tasks. Thus, a new project might involve extensive piping and/or civil/structural tasks. A retrofit job may simply be replacing an outdated control system with a newer safety instrumented system. Thus, this type of project will tend to be very controls intensive with limited tasks required to be performed by other disciplines.

SIS Detailed Design

- SIS panel design
  - Develop system engineering & specification
  - Develop panel layout drawings
  - Develop panel internal wiring drawings
- SIS field wiring design
  - Develop field wiring design – loop sheets, schematics and/or motor elementaries
- SIS instrumentation specification
  - Develop instrumentation / controls datasheets
- Software design specification
  - Develop architectural design specification
  - Develop detailed sequence of operations
  - Perform SIS configuration
- Procure system hardware and software
  - Procure SIS system panel materials
- SIS panel integration / fabrication
  - Perform SIS panel fabrication
  - Perform factory acceptance testing
  - Perform client acceptance testing

The project highlighted in this case study was implemented based upon the above FEL and detailed design concepts and followed the ISA84/IEC61511 safety lifecycle.

Safety and Economic Analysis

This paper highlights a five step methodology, which was applied to perform economic analysis on the safety instrumented systems, to ensure that the "best" system was selected.

1) Select an architecture for the SIS for evaluation (i.e., sensors, logic solver and final elements)
2) Perform SIL verification calculations to determine probability of failure on demand average (PFD_{avg}) and mean time to fail safe ($MTTF_S$) based upon a given proof test interval
3) Calculate the benefit to cost ratio
4) Calculate the lifecycle cost in terms of net present value (NPV)
5) Repeat above steps for each possible SIS architecture being considered for the project

Note: Steps 1 and 2 represent tasks associated with the safety lifecycle and are typically already being performed by designers of safety instrumented systems. The remaining steps have been added by aeSolutions to ensure the SIS architecture selected represents a sound financial investment.

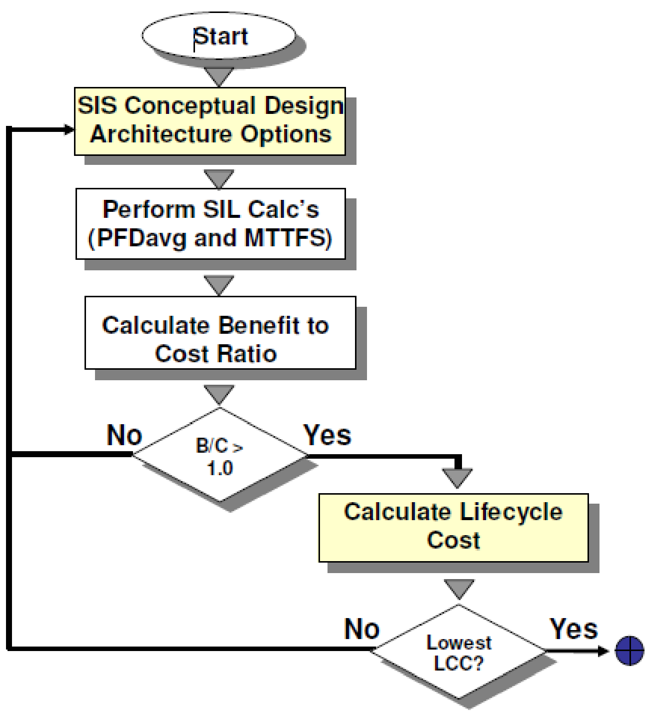

Figure 1: Economic Analysis Flow Chart

Benefit To Cost Ratio

The benefit to cost ratio is a screening tool to help one determine if the “best” safety instrumented system architecture has been selected. It is performed by calculating the ratio of financial benefits to costs. If the ratio is greater than one, the system is considered cost effective. For example, if a system has a benefit to cost ratio of 1.5, for every $1.00 invested, the system will return $1.50.

The benefit to cost ratio is as follows:

$$B - C\ Ratio = \frac{F_{No-SIS} * EV_{No-SIS} - F_{SIS} * EV_{SIS}}{Cost_{SIS} + Cost_{NT}}$$

Where:

$B - C\ Ratio$ = Ratio of benefits to cost
F_{No-SIS} = Frequency of the unwanted event without a SIS
F_{SIS} = Frequency of the unwanted event with a SIS
EV_{No-SIS} = Total expected value of loss of the event without a SIS
EV_{SIS} = Total expected value of loss of the event with a SIS
$Cost_{SIS}$ = Total lifecycle cost of the SIS (Annualized)
$Cost_{NT}$ = Cost incurred due to nuisance trips (Annualized)

The benefit to cost ratio can be calculated two different ways:

1) The ratio is based upon anticipated expected values of loss as obtained during the risk analysis, with all other variables calculated as required. This method yields an expected benefit to cost ratio.
2) Use project specific values for all other variables with an assumed expected value of the event in question. The value of the expected event is modified in an iterative fashion to yield the cost where the benefit to cost ratio is approximately 1.0. This method can be used as a screening tool to determine the lowest cost of a hazardous event where the SIS is financially justified. This route works well when the hazardous event being considered has not occurred at this facility in a long time, or it is difficult for the project team to estimate its cost impact.

Lifecycle Cost

Lifecycle cost is a technique that allows those responsible for system selection to consider all of the costs incurred over the life of the safety instrumented system, rather than just the initial purchase costs. This is especially important where the cost of equipment failure can be significant. The intent of this evaluation is to include all costs of procurement and ownership over the life of the safety instrumented system. Procurement costs represent costs that occur only once during life of the project. Operating costs occur over the life of the safety instrumented system and can be repetitive. Costs associated with system failure can dominate overall lifecycle costs.

A lifecycle cost evaluation can show one how to minimize overall cost of ownership by initially selecting the "best" safety instrumented system architecture. The evaluation considers the costs for design, purchase, installation, start-up, proof testing, energy, repair, a failure event, and lost production. To obtain the complete lifecycle cost, all yearly operating costs are converted to "present value". All future expenses are converted into their current valve, accounting for discount rate (interest/inflation). Initial costs and the present yearly costs are added to obtain total lifecycle cost. Refer to reference (5) for additional information regarding lifecycle cost calculations. The proposed architecture for each safety instrumented system should be evaluated for minimum lifecycle cost.

Table 1 Lifecycle Cost Components

Lifecycle Costs	
Procurement Costs	**Description**
System design	Engineering costs associated with front end loading and detailed design
Purchase	Cost of equipment including factory acceptance testing (FAT) and shipping
Installation	Construction costs associated with the SIS
Start-up	Commissioning, pre startup acceptance testing (PSAT)
Operating Costs	**Description**
Engineering changes	Engineering costs associated with maintenance
Consumption	Power, spares parts, instrument air, etc.
Maintenance	Inspection, proof testing
Cost of System Failure	**Description**
Lost production	Cost of lost production
Asset loss	Cost of lost equipment

Project Specifics

Implementation of the phased approach to engineering was critical to the overall success of this project. Once detailed design was begun, the project was commercially structured as follows:

- Engineering firm prime contractor with engineering and procurement responsibilities
- Boiler OEM prime contractor
    - Burner manufacturer sub-contractor for BMS, burners, fuel trains
        - Safety instrumented system firm sub-contractor for BMS and safety lifecycle implementation

This type of multiple prime and sub-contractor arrangement can lead to significant cost increases to a project when a large number of change orders are encountered through multiple mark-ups of each change through the contractual chain. By completing the SIS FEL, most design changes to the SI-BMS architecture were implemented early in the design process, which limited their impact to the project team members.

Another challenge for the project team was the varied knowledge of the safety lifecycle by the various team members. Figure 2 below depicts the various organizations and their respective level of knowledge regarding the safety lifecycle. Thus, early communication and initial training efforts were required to align all project team members to ensure successful implementation of the safety lifecycle.

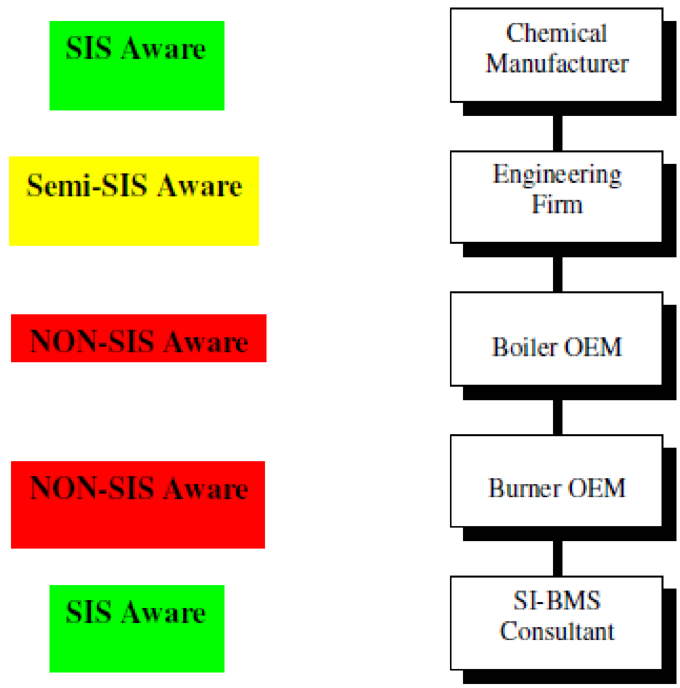

Figure 2 Project Team Safety Lifecycle Knowledge

Step 1: SIS Conceptual Design Architecture Options

The plant installing the boilers already has numerous safety instrumented systems that are fully compliant with ISA84/IEC61511. As such, many of the key architecture decisions had already been established for this facility. Thus, the following options were to be evaluated:

- Transmitters shall be used wherever possible
- A TMR (Triple Modular Redundant) safety PLC shall be used as the logic solver
- A 24 month proof test interval shall be followed
- Project conceptual P&IDs contained 2oo3 voting on initiating sensors across the board
- As part of this economic analysis, 1oo1 voting on initiating sensors was also be reviewed

Step 2: Perform SIL Calculations (PFD_{avg} and $MTTF_S$)

The SIS engineer on the project completed the following SIL calculations based upon the following safety instrumented functions identified during the hazard analysis portion of this project.

Table 2 SIS Architecture Analysis Summary

SIF	Description	Functional Testing (months)	Required SIL	Achieved SIL	PFD_{avg}	Risk Reduction Factor	MTTF Spurious (Years)
2	Low steam drum level causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	24	2	2	5.86E-03	171	20.5
2a	Low steam drum level causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	2	2	7.10E-03	141	18.8
3	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT).	24	2	2	5.83E-03	172	20.4
3a	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	2	2	6.47E-03	155	18.0
4	High furnace pressure causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	24	2	2	5.84E-03	171	20.5
4a	High furnace pressure causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	2	2	6.47E-03	155	20.3
5	Low instrument air pressure causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	2	6.42E-03	156	18.1
5a	Low instrument air pressure causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	2	6.42E-03	156	18.1
6	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	24	1	2	5.83E-03	172	19.9
6a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	2	5.85E-03	171	17.7
7	High pressure natural gas causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	24	1	2	5.84E-03	171	20.5

SIF	Description	Functional Testing (months)	Required SIL	Achieved SIL	PFD_{avg}	Risk Reduction Factor	MTTF Spurious (Years)
7a	High pressure natural gas causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	2	6.47E-03	155	20.3
10	Flameout caused by low fuel oil pressure causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	24	1	2	5.83E-03	172	19.8
10a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	2	5.85E-03	171	17.7
11	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	1	3.66E-02	27	14.5
11a	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	24	1	1	3.66E-02	27	14.5
12	Proof of “gun in position” signal is required prior to startup of fuel oil firing. **(1oo1) Sensor Architecture**	24	2	1	3.09E-02	32	48.0
12a	Proof of “gun in position” signal is required prior to startup of fuel oil firing. **(1oo1) Sensor Architecture**	4	2	1	3.09E-02	32	48.0
13	Safe purge conditions must be satisfied prior to introducing an ignition source into furnace during pilot light-off. **(2oo3 FT, 2oo3 PDT, 1oo1 ZSC) Sensor**	24	1	1	3.10E-02	32	1,500.
13a	Safe purge conditions must be satisfied prior to introducing an ignition source into furnace during pilot light-off. **(1oo1 FT, 1oo1 ZSC) Sensor Architecture**	24	1	1	3.15E-02	32	146.
14	Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence. **(2oo3) Sensor Architecture**	24	1	1	8.58E-06	116,000	14.5
14a	Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence. **(1oo1) Sensor Architecture**	24	1	1	2.30E-04	4,350	28.5

Step 3: Calculate Benefit to Cost Ratio

To calculate the benefit to cost ratio, several additional pieces of information are required, which were available as a result of completing the SIL selection process. For this project, the following data was utilized:

F_{No-SIS} = Frequency of hazardous event from LOPA

F_{SIS} = Calculated based upon (PFD_{avg} * F_{No-SIS})

EV_{No-SIS} = Total expected value of loss of the event without a SIS. Iterate to determine limiting SIF with B-C ratio close to 1.0.

EV_{SIS} = Total expected value of loss of the event with a SIS. Iterate to determine limiting SIF with B-C ratio close to 1.0.

$Cost_{SIS}$ = Total lifecycle cost of the SIS (annualized). Varies per SIF architecture considered.

$Cost_{NT}$ = Cost incurred due to nuisance trips (annualized). Evaluate $75,000 events.

Table 3 SIS Benefit-to-Cost Ratio Analysis Summary – 1oo1 Architecture

	EV_{No-SIS}	EV_{SIS}	F_{No-SIS} (1/Yrs)	PFD_{avg}	F_{SIS} (1/Yrs)	Nuisance Trip Rate (Yrs)	$Cost_{NT}$ ($/Yr)	B-C Ratio
SIF-002a	$5,125,000	$5,125,000	5.56E-02	7.10E-03	3.94E-04	18.8	$3,994	13.3
SIF-003a	$5,125,000	$5,125,000	5.46E-03	6.47E-03	3.54E-05	18.0	$4,164	1.30
SIF-004a	$5,125,000	$5,125,000	5.56E-02	6.47E-03	3.59E-04	20.3	$3,695	13.5
SIF-005a	$5,125,000	$5,125,000	5.56E-02	6.42E-03	3.57E-04	18.1	$4,146	13.2
SIF-006a	$5,125,000	$5,125,000	5.56E-02	5.85E-03	3.25E-04	17.7	$4,228	13.2
SIF-007a	$5,125,000	$5,125,000	5.56E-02	6.47E-03	3.59E-04	20.3	$3,695	13.5
SIF-010a	$5,125,000	$5,125,000	5.56E-02	5.85E-03	3.25E-04	17.7	$4,228	13.2
SIF-011a	$5,125,000	$5,125,000	5.56E-02	3.66E-02	2.03E-03	14.5	$5,180	12.2
SIF-012a	$5,125,000	$5,125,000	5.46E-03	3.09E-02	1.69E-04	48.0	$1,562	1.44
SIF-013a	$5,125,000	$5,125,000	5.56E-02	3.15E-02	1.75E-03	146.	$513	15.5
SIF-014a	$5,125,000	$5,125,000	5.56E-02	2.30E-04	1.28E-05	28.5	$2,628	14.3

Table 4 SIS Benefit-to-Cost Ratio Analysis Summary – 2oo3 Architecture

	EV_{No-SIS}	EV_{SIS}	F_{No-SIS} (1/Yrs)	PFD_{avg}	F_{SIS} (1/Yrs)	Nuisance Trip Rate (Yrs)	$Cost_{NT}$ ($/Yr)	B-C Ratio
SIF-002	$5,125,000	$5,125,000	5.56E-02	5.86E-03	3.26E-04	20.5	$3,660	10.6
SIF-003	$5,125,000	$5,125,000	5.46E-03	5.83E-03	3.19E-05	20.4	$3,675	1.04
SIF-004	$5,125,000	$5,125,000	5.56E-02	5.84E-03	3.24E-04	20.5	$3,655	10.6
SIF-005	$5,125,000	$5,125,000	5.56E-02	6.42E-03	3.57E-04	18.1	$4,146	10.4
SIF-006	$5,125,000	$5,125,000	5.56E-02	5.83E-03	3.24E-04	19.8	$3,790	10.5
SIF-007	$5,125,000	$5,125,000	5.56E-02	5.84E-03	3.24E-04	20.5	$3,655	10.6
SIF-010	$5,125,000	$5,125,000	5.56E-02	5.83E-03	3.24E-04	19.8	$3,790	10.5

	$EV_{No\text{-}SIS}$	EV_{SIS}	$F_{No\text{-}SIS}$ (1/Yrs)	PFD_{avg}	F_{SIS} (1/Yrs)	Nuisance Trip Rate (Yrs)	$Cost_{NT}$ ($/Yr)	B-C Ratio
SIF-011	$5,125,000	$5,125,000	5.56E-02	3.66E-02	2.03E-03	14.5	$5,180	9.71
SIF-012	$5,125,000	$5,125,000	5.46E-03	3.09E-02	1.69E-04	48.0	$1,562	1.10
SIF-013	$5,125,000	$5,125,000	5.56E-02	3.10E-02	1.72E-03	1500.	$50	11.9
SIF-014	$5,125,000	$5,125,000	5.56E-02	8.58E-06	4.80E-07	14.5	$5,172	10.1

As can be seen by the above benefit to cost numbers, all architectures being considered represent a sound financial investment. The cost of the event was iterated to determine what dollar value represents a benefit to cost ratio of approximately 1.0 on the limiting SIF(s), which in this case were SIF-003 and SIF-0012. This dollar value was then presented to the project team as the lowest event cost where the SIS was financially justified. The project team readily felt that $5.125MM was much lower than the outcomes being considered by the risk analysis. Thus, all SIF's above were considered to have a benefit to cost ratio greater than 1.0. The project did not attempt to specifically quantify the event cost for each SIF. Instead, the benefit to cost ratio was used as a screening tool based upon the lowest credible event that still allowed the SIF to maintain a benefit to cost ratio greater than 1.0.

Step 4: Calculate Lifecycle Costs

Several additional pieces of information are required in order to calculate lifecycle costs. For this sample problem, the following data was utilized:

The plant discussed two scenarios regarding the cost of a nuisance trip. The first was based upon the loss of a boiler where the plant steam header lost enough pressure and/or temperature to possibly impact production. This event was estimated to cost the facility $75,000 per event. The second scenario was based upon the second boiler being able to pick-up the existing steam load without significant impact to production. The costs for this type of event were limited to the re-start efforts associated with the offline boiler. This event was estimated to cost the facility $6,000 per event. Both of these events were reviewed during the lifecycle cost analysis phase of this project.

Table 5: SIS Lifecycle Cost Analysis Summary - $75,000 and $6,000 Nuisance Trip Cost

SIF	Description	Life Cycle Cost Estimate ($75K Trip)	Delta Life Cycle Cost ($75K Trip)	Life Cycle Cost Estimate ($6K Trip)	Delta Life Cycle Cost ($6K Trip)
2	Low steam drum level causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	$207,455	$17,156	$92,174	$27,650
2a	Low steam drum level causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$190,299		$64,524	

SIF	Description	Life Cycle Cost Estimate ($75K Trip)	Delta Life Cycle Cost ($75K Trip)	Life Cycle Cost Estimate ($6K Trip)	Delta Life Cycle Cost ($6K Trip)
3	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	$207,946	$11,802	$92,213	$27,222
3a	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$196,144		$64,991	
4	High furnace pressure causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	$207,272	$27,208	$92,159	$28,454
4a	High furnace pressure causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$180,064		$63,705	
5	Low instrument air pressure causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$211,237	$15,724	$80,665	$15,724
5a	Low instrument air pressure causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$195,513		$64,941	
6	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	$211,886	$13,573	$92,529	$27,364
6a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$198,313		$65,165	
7	High pressure natural gas causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	$207,272	$27,208	$92,159	$28,454
7a	High pressure natural gas causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$180,064		$63,705	
10	Flameout caused by low fuel oil pressure causes Master Fuel Trip (MFT). **(2oo3) Sensor Architecture**	$211,886	$13,573	$92,529	$27,364
10a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$198,313		$65,165	
11	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$246,614	$15,724	$83,495	$15,724
11a	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). **(1oo1) Sensor Architecture**	$230,890		$67,771	

<table>
<tr><th>SIF</th><th>Description</th><th>Life Cycle Cost Estimate ($75K Trip)</th><th>Delta Life Cycle Cost ($75K Trip)</th><th>Life Cycle Cost Estimate ($6K Trip)</th><th>Delta Life Cycle Cost ($6K Trip)</th></tr>
<tr><td>12</td><td>Proof of “gun in position” signal is required prior to startup of fuel oil firing.
(1oo1) Sensor Architecture</td><td>$122,793</td><td rowspan="2">$15,724</td><td>$73,589</td><td rowspan="2">$15,724</td></tr>
<tr><td>12a</td><td>Proof of “gun in position” signal is required prior to startup of fuel oil firing.
(1oo1) Sensor Architecture</td><td>$107,069</td><td>$57,865</td></tr>
<tr><td>13</td><td>Safe purge conditions must be satisfied prior to introducing an ignition source into furnace during pilot light-off.
(2oo3 FT, 2oo3 PDT, 1oo1 ZSC) Sensor Architecture</td><td>$83,860</td><td rowspan="2">$12,693</td><td>$82,287</td><td rowspan="2">$27,294</td></tr>
<tr><td>13a</td><td>Safe purge conditions must be satisfied prior to introducing an ignition source into furnace during pilot light-off.
(1oo1 FT, 1oo1 ZSC) Sensor Architecture</td><td>$71,167</td><td>$54,993</td></tr>
<tr><td>14</td><td>Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence.
(2oo3) Sensor Architecture</td><td>$259,209</td><td rowspan="2">$115,658</td><td>$96,314</td><td rowspan="2">$35,530</td></tr>
<tr><td>14a</td><td>Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence.
(1oo1) Sensor Architecture</td><td>$143,551</td><td>$60,784</td></tr>
</table>

The above table underscores how the cost of a nuisance trip can dominate the overall cost of ownership. In Table 5, even with a nuisance trip cost being assumed at $75,000, the optimum SIS architecture consists of simplex pressure transmitters.

Conclusion

Based upon the scenarios evaluated, it is readily apparent that one should not simply stop at completing a SIL calculation to determine if the required SIL has been achieved. When lifecycle costs were compared for two design options on this project, one can see that an estimated cost savings of over $550,000 could be achieved for a 1oo1 sensor architecture (versus 2oo3), regardless of which cost basis was used for a nuisance trip. However, not all SIFs were selected to use a 1oo1 architecture across the board. Both client and OEM input into past performance, and ease of maintenance, resulted in additional fault tolerance being included in some SIFs.

Table 6 Final SIS Analysis Summary

SIF	Description	Life Cycle Cost Estimate ($75K Trip)	Delta Life Cycle Cost ($75K Trip)	Life Cycle Cost Estimate ($6K Trip)	Delta Life Cycle Cost ($6K Trip)
Case 1	2oo3 Architecture	$4,354,860	**$572,086**	~~$1,940,226~~	**$553,008**
Case 1A	1oo1 Architecture	$3,782,774		$1,387,218	

In summary, in today's competitive business environment, there can be significant financial benefits in performing a financial justification of different design options during the conceptual stage of a safety instrumented system project.

The Construction Industry Institute defines a front end loading package for a capital facility as "the process of developing sufficient strategic information for owners to address risk and decide to commit resources to maximize the chance for a successful project." When the concept of a front end loading package is coupled with the concepts contained in the safety lifecycle, all parties involved have the opportunity to better control costs on their projects. aeSolutions stands behind the concept of SIS FEL and believes the project contained within this case study is a good example of the benefits and overall success of a phased/gated approach to project execution.

By implementing a SIS FEL approach, which also included completion of lifecycle cost analysis and benefit to cost ratio analysis, significant savings were realized by selecting the most appropriate architecture based upon meeting all performance requirements for the lowest total cost of ownership.

Disclaimer

The following paper is provided for educational purposes. While the authors have made reasonable efforts in the preparation of this document, aeSolutions makes no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of this document.

References

1) Construction Industry Institute, Analysis of Pre-Project Planning Effort and Success Variables For Capital Facility Projects, SD105
2) ANSI/ISA 84 (IEC 61511 Mod) -2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, International Society of Automation
3) Barringer, H. P, Life Cycle Cost and Good Practices, NPRA Maintenance Conference, 1998
4) Marszal, E & Scharpf, E, Safety Integrity Level Selection – Systematic Methods Including Layer of Projection Analysis, 2002, ISA, Research Triangle Park, NC

5) Dieter, G. E., Engineering Design: A Materials and Processing Approach, McGraw-Hill, 1983
6) Goble, W.M., Control Systems Safety Evaluation & Reliability, 2nd Edition, ISA, 1998
7) NFPA 85, *Boiler and Combustion Systems Hazard Code*, 2007, 2011, 2015

Abbreviations and Definitions

1oo1	1-out-of-1
2oo3	2-out-of-3
BMS	Burner Management System
CII	Construction Industry Institute
FEL	Front End Loading
IEC	International Electrotechnical Commission
LCC	Lifecycle Cost
MTTFS	Mean Time To Fail Spurious
NPV	Net Present Value
FV	Future Value
PFDavg	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
RRF	Risk Reduction Factor
SI-BMS	Safety Instrumented Burner Management System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System