

CASE STUDY: SAFETY INSTRUMENTED BURNER MANAGEMENT SYSTEM (SI-BMS)

Mike Scott
VP, Process Safety
AE Solutions
Greenville, SC 29507

Bud Adler
Director, Business Development
AE Solutions
Lake Mary, FL 32746

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, IEC 61508, IEC 61511, 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 (2) 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 1365 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 include the following:

- Development of the concept of a SIS Front End Loading package
- Project cost savings realized attributed to following the Safety Lifecycle
- Challenges encountered during the design process associated with implementation of the Safety Lifecycle with the diverse project team

INTRODUCTION

The project about which this case study encompasses was tasked with designing and installing two (2) 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. CII has done extensive research on improving project success. Towards this end CII has documented that Front End Loading “of capital facilities is an extremely important function in determining the ultimate outcome of a project.” CII through quantitative analysis of 62 projects, as noted in *Analysis of Pre-Project Planning Effort and Success Variables For Capital Facility Projects*, has stated that the Front End Loading “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 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

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.” 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 AE Solutions fully endorses the development of a Front End Loading package for all Safety Instrumented System related projects.

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.” AE Solutions 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
 - Develop Lifecycle Cost Analysis
 - Develop Interlock List

- Develop Sequence of Operations
- ❖ Conceptual Design Specification
 - Redline P&ID's
 - Develop System Architecture Diagram
 - Develop E-stop Philosophy
 - Develop SIS Logic Solver Specification – Bill of Materials
 - Develop Approved Inst Vendor List / Procure Plan for SIS
 - Develop SIL Verification Report
 - Develop Control Panel Location Sketch
 - Develop Control Philosophy Specification
- ❖ Summary Safety Report
- ❖ Construction Estimate, TIC (+- 20 %)

AE Solutions 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 based design. 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 & 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 IEC61511 Safety Lifecycle.

SAFETY AND ECONOMIC ANALYSIS

This paper will also highlight a five (5) step methodology, which was applied to perform economic analysis on Safety Instrumented Systems to ensure the “best” system has been selected.

1. Step 1 – Select an architecture for the SIS for evaluation (sensors, logic solver and final elements)
2. Step 2 – Perform SIL Calculations to determine Probability of Failure on Demand Average (PFDavg) and Mean Time To Fail Safe (MTTFS) based upon a given Functional Test Interval
3. Step 3 – Calculate Benefit-to-Cost Ratio
4. Step 4 – Calculate 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 AE Solutions to ensure the SIS design architecture selected represents a sound financial investment.

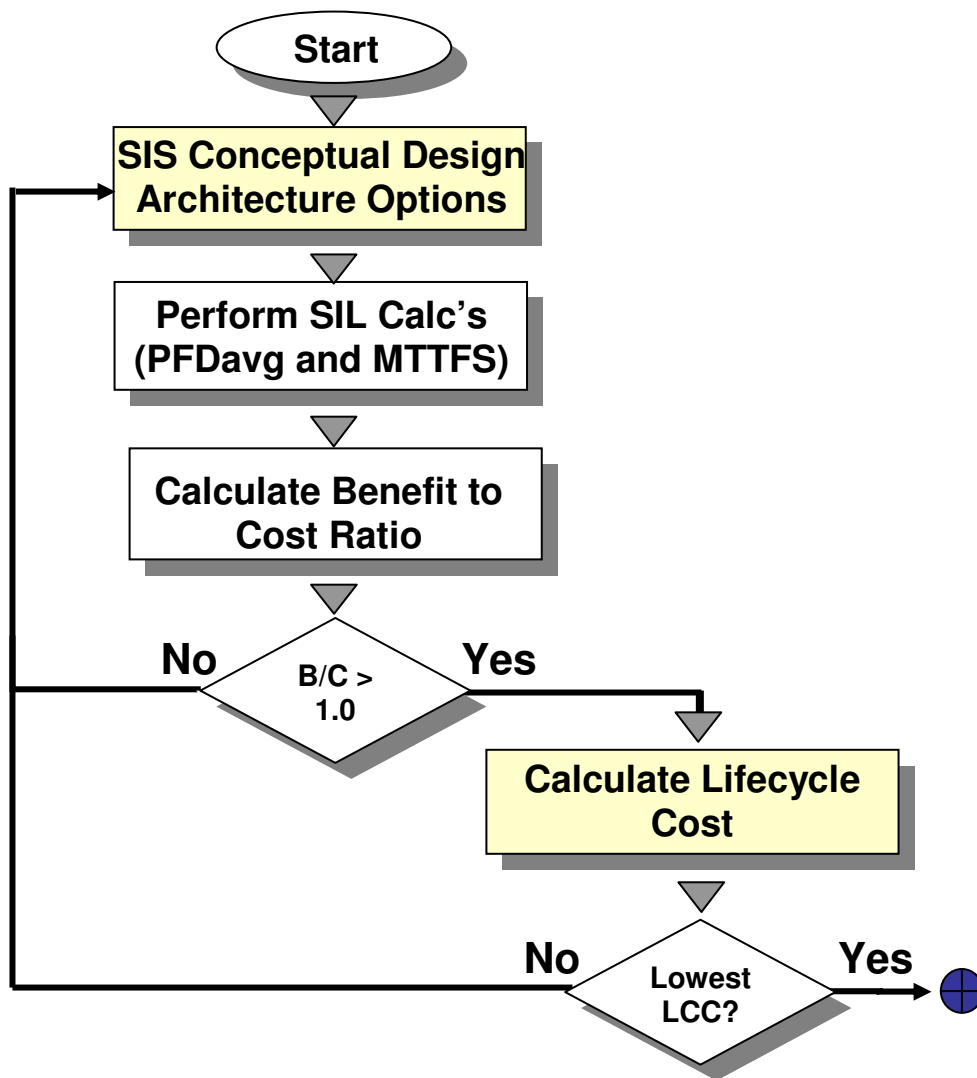


Figure 1 – Economic Analysis Flowchart

BENEFIT-TO-COST RATIO

Benefit-To-Cost Ratio is a screening tool to help one determine if the “best” Safety Instrumented System architecture has been selected by calculating the ratio of benefits to costs on a financial basis. If the ratio is greater than one, the system is 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.

Therefore, the Benefit – Cost Ratio is as follows:

$$\text{B-C Ratio} = \frac{F_{\text{No-SIS}} \times \text{EV}_{\text{No-SIS}} - F_{\text{SIS}} \times \text{EV}_{\text{SIS}}}{\text{Cost}_{\text{SIS}} + \text{Cost}_{\text{NT}}}$$

Where,

B-C Ratio	=	Ratio of benefits to cost
$F_{\text{No-SIS}}$	=	Frequency of the unwanted event without a SIS
F_{SIS}	=	Frequency of the unwanted event with a SIS
$\text{EV}_{\text{No-SIS}}$	=	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)

B-C Ratio can be calculated in two different ways. The first is based upon anticipated expected values of loss as obtained during the risk analysis with all other variables calculated as required. Thus, this method would yield an actual expected B-C Ratio. The other method is to use the 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 B-C Ratio is approximately 1.0. This method can be used as a screening tool to present the lowest cost of the 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 some time and 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 lifetime 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 span 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, functional 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 value, 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 and shipping
Installation	Construction costs associated with SIS
Start-up	Commissioning, PSAT and Initial Functional Testing of SIS
Operating Costs	Description
Engineering Changes	Engineering costs associated with maintenance
Consumption	Power, spares parts, instrument air, etc.
Maintenance	Inspection, Functional 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 for Boiler
 - 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 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.

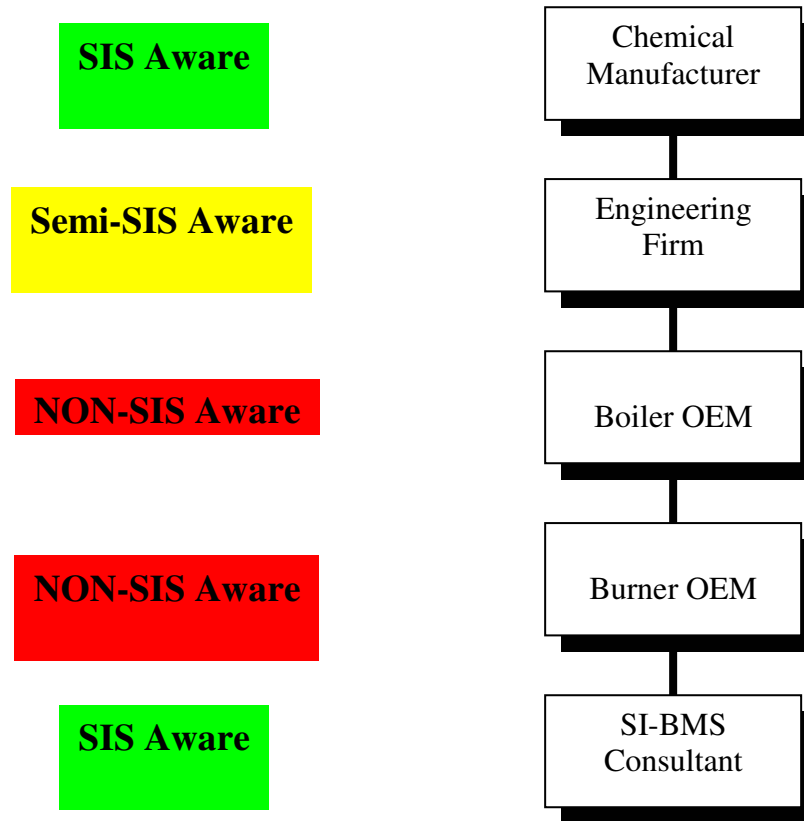


Figure 2 – Project Team Safety Lifecycle Knowledge

Step 1: SIS Conceptual Design Architecture Options

The plant that was installing the Boilers has numerous fully IEC61511 compliant Safety Instrumented Systems already installed onsite. As such, many of the key architecture decisions had already been established for this facility. This, the included the following options were to be evaluated:

- Transmitters shall be used wherever possible
- A TMR Safety PLC shall be used as the logic solver
- A 24 month test functional interval shall be provided
- Project conceptual P&ID's contained 2oo3 voting on initiating sensors across the board
- As part of this economic analysis 1oo1 voting on initiating sensors will also be reviewed

Step 2: Perform SIL Calculations (PFDavg and MTTFS)

The SIS Engineer on the project completed the following SIL calculations based upon the following Safety Instrumented Functions as identified during the Risk Analysis portion of this project.

Table 2 – SIS Architecture Analysis Summary

SIF	Description	Func Testing (mo)	Reqd SIL	Achiv'd 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	20.49
2a	Low steam drum level causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	2	2	7.10E-03	141	18.78
3	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). (2oo3) Sensor Architecture	24	2	2	5.83E-03	172	20.41
3a	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	2	2	6.47E-03	155	18.01
4	High furnace pressure causes Master Fuel Trip (MFT). (2oo3) Sensor Architecture	24	2	2	5.84E-03	171	20.52
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	18.09
5a	Low instrument air pressure causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	1	2	6.42E-03	156	18.09
6	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). (2oo3) Sensor Architecture	24	1	2	5.83E-03	172	19.79
6a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	1	2	5.85E-03	171	17.74
7	High pressure natural gas causes Master Fuel Trip (MFT). (2oo3) Sensor Architecture	24	1	2	5.84E-03	171	20.52
7a	High pressure natural gas causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	1	2	6.47E-03	155	20.3

SIF	Description	Func Testing (mo)	Reqd SIL	Achiv'd SIL	PFD _{avg}	Risk Reduction Factor	MTTF Spurious (Years)
10	Flameout caused by low fuel oil pressure causes Master Fuel Trip (MFT). (2oo3) Sensor Architecture	24	1	2	5.83E-03	172	19.79
10a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	1	2	5.85E-03	171	17.74
11	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	1	1	3.66E-02	27	14.48
11a	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). (1oo1) Sensor Architecture	24	1	1	3.66E-02	27	14.48
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	48.01
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	48.01
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 Architecture	24	1	1	3.10E-02	32	1501.7
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	146.06
14	Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence. (2oo3) Sensor Architecture	24	1	1	8.58E-06	116508	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	4345	28.54

Step 4: Calculate Benefit-to-Cost Ratio

To calculate the Benefit-to-Cost ratio several additional pieces of information are required and are available as a result of completing the SIL Selection process. For this project, the following data was utilized:

$$F_{\text{No-SIS}} = \text{Frequency of Hazardous Event from LOPA}$$

- F_{SIS} = Calculated based upon ($PFD_{avg} \times F_{No-SIS}$)
- EV_{No-SIS} = Iterate to determine limiting SIF with B-C Ratio close to 1.0
- EV_{SIS} = Iterate to determine limiting SIF with B-C Ratio close to 1.0
- $Cost_{SIS}$ = Varies per SIF architecture considered
- $Cost_{NT}$ = Evaluate \$75,000 events

Table 3 – SIS Benefit-to-Cost Ratio Analysis Summary – 1001 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	0.05555556	7.10E-03	0.00039444	18.78	\$ 3,994	13.28
SIF-003a	\$5,125,000	\$5,125,000	0.00546448	6.47E-03	0.00003536	18.01	\$ 4,164	1.30
SIF-004a	\$5,125,000	\$5,125,000	0.05555556	6.47E-03	0.00035944	20.30	\$ 3,695	13.48
SIF-005a	\$5,125,000	\$5,125,000	0.05555556	6.42E-03	0.00035667	18.09	\$ 4,146	13.19
SIF-006a	\$5,125,000	\$5,125,000	0.05555556	5.85E-03	0.00032500	17.74	\$ 4,228	13.15
SIF-007a	\$5,125,000	\$5,125,000	0.05555556	6.47E-03	0.00035944	20.30	\$ 3,695	13.48
SIF-010a	\$5,125,000	\$5,125,000	0.05555556	5.85E-03	0.00032500	17.74	\$ 4,228	13.15
SIF-011a	\$5,125,000	\$5,125,000	0.05555556	3.66E-02	0.00203333	14.48	\$ 5,180	12.21
SIF-012a	\$5,125,000	\$5,125,000	0.00546448	3.09E-02	0.00016885	48.01	\$ 1,562	1.44
SIF-013a	\$5,125,000	\$5,125,000	0.05555556	3.15E-02	0.00175000	146.06	\$ 513	15.48
SIF-014a	\$5,125,000	\$5,125,000	0.05555556	2.30E-04	0.00001278	28.54	\$ 2,628	14.29

Table 4 – SIS Benefit-to-Cost Ratio Analysis Summary – 2003 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	0.05555556	5.86E-03	0.00032556	20.49	\$ 3,660	10.59
SIF-003	\$5,125,000	\$5,125,000	0.00546448	5.83E-03	0.00003186	20.41	\$ 3,675	1.04
SIF-004	\$5,125,000	\$5,125,000	0.05555556	5.84E-03	0.00032444	20.52	\$ 3,655	10.60
SIF-005	\$5,125,000	\$5,125,000	0.05555556	6.42E-03	0.00035667	18.09	\$ 4,146	10.40
SIF-006	\$5,125,000	\$5,125,000	0.05555556	5.83E-03	0.00032389	19.79	\$ 3,790	10.54
SIF-007	\$5,125,000	\$5,125,000	0.05555556	5.84E-03	0.00032444	20.52	\$ 3,655	10.60
SIF-010	\$5,125,000	\$5,125,000	0.05555556	5.83E-03	0.00032389	19.79	\$ 3,790	10.54
SIF-011	\$5,125,000	\$5,125,000	0.05555556	3.66E-02	0.00203333	14.48	\$ 5,180	9.71
SIF-012	\$5,125,000	\$5,125,000	0.00546448	3.09E-02	0.00016885	48.01	\$ 1,562	1.10
SIF-013	\$5,125,000	\$5,125,000	0.05555556	3.10E-02	0.00172222	1,501.70	\$ 50	11.94
SIF-014	\$5,125,000	\$5,125,000	0.05555556	8.58E-06	0.00000048	14.50	\$ 5,172	10.08

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 B-C Ratio of approximately 1.0 on the limiting SIF, which in this case was SIF-003 and SIF-0012. This dollar value was then presented to the project team as the lowest event cost was the SIS is 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 are considered to have a B-C > 1.0. The project did not attempt to specifically

quantify the event cost for each SIF. Thus, instead B-C Ratio was used as a screening tool based upon lowest credible event that still allows the SIF to maintain a B-C > 1.0.

Step 3: Calculate Lifecycle Costs

To calculate the Lifecycle Costs several additional pieces of information are required. For this sample problem, the following data was utilized:

The plant discussed two scenarios regarding cost of a nuisance trip. The first was based upon loss of a boiler such that the plant steam header losses significant pressure / temperature such that a production impact could be possible. This event was deemed to potentially cost the facility approximately \$75,000 per event. The second scenario was based upon the 2nd boiler being able to pick-up the existing steam load without significant production impacts. Costs for this type of event were limited to re-start efforts associated with the offline boiler. This event was deemed to potentially cost the facility approximately \$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	Delta Life Cycle Cost \$75K	Life Cycle Cost Estimate \$6K	Delta Life Cycle Cost \$6K
2	Low steam drum level causes Master Fuel Trip (MFT). (2003) Sensor Architecture	\$207,455	\$17,156	\$92,174	\$27,650
2a	Low steam drum level causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$190,299		\$64,524	
3	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). (2003) Sensor Architecture	\$207,946	\$11,802	\$92,213	\$27,222
3a	Loss of combustion air flow (or differential pressure) causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$196,144		\$64,991	
4	High furnace pressure causes Master Fuel Trip (MFT). (2003) Sensor Architecture	\$207,272	\$27,208	\$92,159	\$28,454
4a	High furnace pressure causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$180,064		\$63,705	
5	Low instrument air pressure causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$211,237	\$15,724	\$80,665	\$15,724
5a	Low instrument air pressure causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$195,513		\$64,941	

SIF	Description	Life Cycle Cost Estimate \$75K	Delta Life Cycle Cost \$75K	Life Cycle Cost Estimate \$6K	Delta Life Cycle Cost \$6K
6	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). (2003) Sensor Architecture	\$211,886	\$13,573	\$92,529	\$27,364
6a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$198,313		\$65,165	
7	High pressure natural gas causes Master Fuel Trip (MFT). (2003) Sensor Architecture	\$207,272	\$27,208	\$92,159	\$28,454
7a	High pressure natural gas causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$180,064		\$63,705	
10	Flameout caused by low fuel oil pressure causes Master Fuel Trip (MFT). (2003) Sensor Architecture	\$211,886	\$13,573	\$92,529	\$27,364
10a	Flameout caused by low pressure natural gas causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$198,313		\$65,165	
11	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$246,614	\$15,724	\$83,495	\$15,724
11a	Low atomizing steam supply (low flow) causes Master Fuel Trip (MFT). (1001) Sensor Architecture	\$230,890		\$67,771	
12	Proof of "gun in position" signal is required prior to startup of fuel oil firing. (1001) Sensor Architecture	\$122,793	\$15,724	\$73,589	\$15,724
12a	Proof of "gun in position" signal is required prior to startup of fuel oil firing. (1001) Sensor Architecture	\$107,069		\$57,865	
13	Safe purge conditions must be satisfied prior to introducing an ignition source into furnace during pilot light-off. (2003 FT, 2003 PDT, 1001 ZSC) Sensor Architecture	\$83,860	\$12,693	\$82,287	\$27,294
13a	Safe purge conditions must be satisfied prior to introducing an ignition source into furnace during pilot light-off. (1001 FT, 1001 ZSC) Sensor Architecture	\$71,167		\$54,993	

SIF	Description	Life Cycle Cost Estimate \$75K	Delta Life Cycle Cost \$75K	Life Cycle Cost Estimate \$6K	Delta Life Cycle Cost \$6K
14	Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence. (2oo3) Sensor Architecture	\$259,209	\$115,658	\$96,314	\$35,530
14a	Proof of no flame in firebox (by flame scanner) prior to initiating purge sequence. (1oo1) Sensor Architecture	\$143,551		\$60,784	

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 to be \$75,000, the best SIS architecture consists of simplex pressure transmitters.

CONCLUSION

Based upon the scenarios evaluated it is readily apparent that one cannot simply stop at completing a SIL calculation to determine if the required SIL has been achieved. When Lifecycle Costs are compared for both boilers, one can see that a significant cost savings of over \$500,000 can be achieved if a 1oo1 architecture is selected regardless of which cost basis is used for a nuisance trip. Note that not all SIF were selected to use a 1oo1 architecture across the board. Client and OEM input into past performance and ease of maintenance resulted in additional fault tolerance being included in some SIF's.

Table 6 – Final SIS Analysis Summary

SIF	Description	Life Cycle Cost Estimate \$75K	Delta Life Cycle Cost \$75K	Life Cycle Cost Estimate \$6K	Delta Life Cycle Cost \$6K
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 sound financial justification of a project must be performed during the Safety Instrumented System conceptual design process.

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.” When the concept of a Front End Loading package is coupled to the concepts contained in the Safety Lifecycle, manufacturers have the opportunity to better control costs and schedule performance on their projects. AE Solutions stands behind the concept of a 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 engineering execution.

By implementing a SIS FEL design, which also included completion of Lifecycle Cost Analysis and Benefit-to-Cost Ratio Analysis, significant savings were realized by selecting the “best” architecture based upon meeting all Safety Availability requirements for the lowest cost of ownership.

DISCLAIMER

Although it is believed that the information in this paper is factual, no warranty or representation, expressed or implied, is made with respect to any or all of the content thereof, and no legal responsibility is assumed therefore. The examples shown are simply for illustration, and, as such, do not necessarily represent any company’s guidelines. The reader should use data, methodology, formulas, and guidelines that are appropriate for their own particular situation.

REFERENCES

1. Scott, M.D. & Adler C.B, *How to Select a Safety PLC*, ISA Automation West Conference, 2003.
2. ANSI/ISA S84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*, The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 1996.
3. IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Safety-related Systems, Part 1-7*, Geneva: International Electrotechnical Commission, 1998.
4. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Parts 1-3*, Geneva: International Electrotechnical Commission, 2003.
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. Barringer, H. P, *Life Cycle Cost and Good Practices*, NPRA Maintenance Conference, 1998
8. Marszal, E & Scharpf, E, *Safety Integrity Level Selection – Systematic Methods Including Layer of Projection Analysis*, 2002, ISA, Research Triangle Park, NC

9. Construction Industry Institute, *Analysis of Pre-Project Planning Effort and Success Variables For Capital Facility Projects*, SD105

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