

EFFECT OF THE LIFE CYCLE MODEL ON A CAPITAL PROJECT

David K. Thomas
Principal
Meerkat Consulting
Houston, TX 77062

KEYWORDS

QRA, Quantitative Risk Analysis, SIL, SIS, ANSI/ISA-S84.01, Life Cycle Model, IEC-61511

ABSTRACT

ANSI/ISA-S84.01 and IEC-61511 include a Life Cycle Model, calling for establishing SIL levels between the HAZOP and the detail design. The benefits of this Life Cycle Model to the user are unstated. To determine the scope and magnitude of these benefits, a recent capital project was evaluated. The new plant was to be similar technology to an existing plant, so a preliminary design was available at the time of the SIL Assignment Meetings.

A QRA performed on the preliminary design determined that for 16 of 25 safety functions, the required SIL would not have been met. A project scope and estimate were generated to determine the cost (both capital expense and timing) to bring a plant, based on this preliminary design, up to standards.

It was found that failure to follow this Life Cycle Model would result in an inadequate instrumentation scope for the project. Start-up would be delayed several months while a project was designed, funded, and built, to remedy the shortcomings in the preliminary design.

INTRODUCTION

When the PSM (Process Safety Management) standard, CFR 1910.119, was published, it included a Life Cycle Model for a project. This was included in the standard to help show when a HAZOP (Hazards and Operability study) should be conducted. While helpful, it still left room for debate. Ideally, the

HAZOP should be performed early in the project cycle, in order to have maximum impact on the project design. But some sort of study was still needed later in the project cycle, to verify that the final design met the safety intent of the HAZOP.

ANSI/ISA-S84.01 (Application of Safety Instrumented Systems for the Process Industry) and the equivalent international code (IEC-61511) changed the project lifecycle by adding the assignment and verification of the SIL (safety integrity level) for the SIS (Safety Instrumented System). This is broken down into four steps.

1. Determine the SIL required to mitigate the hazard.

The standard was written to allow management flexibility in determining the degree of risk acceptable for the facility in question. A number of techniques are available, such as a Risk Matrix or LOPA (Layers of Protection Analysis), but management retains the ultimate responsibility to establish SIL levels which are consistent within the company and with similar operations throughout industry.

2. Define the SIS instrumentation, architecture and testing frequency.

The SRS (Safety Requirement Specification) documents functional requirements for the SIS. It defines safe state of the process for each event, process inputs and their trip points, normal operating ranges, process outputs, functional relationship between inputs and outputs, and selection of energized or de-energized to trip. The SRS must address each safety function, address diagnostic requirements, requirements for maintenance and testing, and reliability requirements if spurious trips may be hazardous.

For SIS conceptual design, the SRS defines the SIS architecture for each safety function, including separation, redundancy, technology selection, power sources, field devices, user Interfaces, security, and functional test intervals.

For SIS Detailed Design, the SRS provides detailed requirements for the design of the SIS to achieve requirements of SRS and conceptual design. This includes the logic solver. field devices, interfaces, application logic requirements, maintenance or testing design requirements

3. Verify that the SIL is met.

QRA (Quantitative Risk Analysis) typically consists of Fault Tree Analysis or occasionally Markov Modeling.

- Operate, Maintain, and Test the SIS to ensure its continued performance.

These requirements are typically laid out in the SRS.

In addition, the standard includes a modification of the earlier Life Cycle Model. This revised model calls for establishing SILs (Safety Integrity Levels) between the HAZOP and the detail design. Once the SILs are established, an SRS (Safety Requirement Specification) can be written to give guidance to the instrumentation designers, and a QRA (Quantitative Risk Analysis) can verify that the final design meets the design intent.

In establishing this Life Cycle Model as part of an ANSI standard on March 11, 1997, regulators gave it the status of “recognized, generally accepted good engineering practice”. This made the Life Cycle Model legally enforceable by OSHA and EPA, just as much as API, ASME, NFPA, and NEC codes. As companies modified their ISO procedures to account for this Life Cycle Model, experienced project personnel asked why any particular model was chosen. It was clearly a reasonable way to run a project, but what practical advantage was there to using this model? This paper was written to explore the value of the Life Cycle Model, as it pertains to a modern capital project.

THE PROJECT

To evaluate the value of the Life Cycle Model, it ideally requires a project to be designed and estimated twice, using the model, and separately without using the model. This would be an expensive and wasteful proposition. An alternative would be to intentionally ignore the model during the design process and determine the costs to correct the situation. This is also unlikely, as it would require a company to incur excessive design costs. However, this alternative could be simulated by analysis of a project to duplicate an existing plant.

When business conditions allow the construction of second plant using the same technology, it is considered an opportunity to reduce the design costs and timing, as many design questions have already been resolved on the original plant. But the second plant is designed to incorporate the experience of the first plant, improving reliability and operability. It also frequently has a different capacity than the first plant, and it is located on a different plot of land. The project team is able to perform its HAZOP

on a nearly-complete detailed design, which assumes the two plants are nearly identical. By examining this preliminary detailed design for compliance with ANSI/ISA84.01, it is possible to illustrate the types and magnitudes of problems the Life Cycle Model is designed to prevent.

The project chosen for this paper is for a manufacturing operation by a multi-national corporation. It was assumed (for the purposes of the paper) that design would continue after the HAZOP and that the SIL assignment, SRS generation, and QRA would be delayed until just before project start-up.

RESULTS

A QRA was performed on the preliminary design, using SAPHIRE software. For 16 of 25 safety functions, the required SIL would not have been met. The QRA provides an estimate of the probability to fail on demand (PFD) of the SIS in order to determine if the planned design and testing philosophy will provide sufficient system availability. The performance targets for each safety function performed by the system were evaluated and expressed in terms of a Safety Integrity Level. The probability to fail on demand correlates to safety integrity level, as follows:

	PFD _{avg}	AVAILABILITY (1-PFD)
SIL 1	0.1 to 0.01	0.90 to 0.99
SIL 2	0.01 to 0.001	0.99 to 0.999
SIL 3	0.001 to 0.0001	0.999 to 0.9999

The following table lists the 16 safety functions which failed to meet the desired SIL level.

SIS	Event Description	Potential Problem	Target TIL	Actual TIL	PFD _{avg}	Availability %
1	Furnace Purge Cycle	Explosion in Furnace	3	0	3.67E-01	63%
2	Sequencing prevents more than 3 furnaces to vent at high organic rates at same time.	Overheat Furnace	3	0	4.67E-01	53%
3	Water shutoff for Reactor	Hydrolysis and fire/explosion in Reactor	2	0	7.54E-01	25%
4	Loss of ventilation in Flammables Area	Fire or explosion in Flammables Area	2	0	4.98E-01	50%
5	Electrical system shutdown in Flammables Area	Fire and/or explosion	2	1	5.40E-02	94%
6	Furnace trip logic for	Fire/explosion in	2	0	5.76E-01	42%

SIS	Event Description	Potential Problem	Target TIL	Actual TIL	PFD _{avg}	Availability %
	controlling excess oxygen.	furnace				
7	Shutdown system for personnel entry to automated area.	Fire in automated area	1	0	4.77E-01	52%
8	Shutdown system for personnel entry to automated area	Injury	1	0	4.84E-01	52%
9	High level interlock for Reactor	Personnel exposure	1	0	5.12E-01	49%
10	High level interlock for Flammable Storage Tank	Personnel exposure	1	0	4.92E-01	51%
11	Prevent Hydrocarbon build-up in dryer	Fire/explosion	1	0	7.72E-01	23%
12	Shut down Furnace on loss of seal in seal pots	Fire/explosion	1	0	6.98E-01	30%
13	Furnace Burner Management System	Fire/explosion	1	0	3.67E-01	63%
14	Shutdown Reactor on loss of agitation	Runaway reaction	1	0	5.13E-01	49%
15	High level shutoff for Storage tank	Personnel exposure	1	0	4.99E-01	50%
16	Shut off ventilation for shelter-in-place.	Personnel exposure	1	0	4.77E-01	52%

Six of the SIS systems which did not meet the required SIL were burners/furnaces. The NFPA standard governing fired burners (NFPA 85) was generated assuming that furnaces and boilers were not located in high traffic areas. With the improved layout of the second plant, a number of burners were now in areas with high personnel traffic flow. This raised the SIL for burner explosions and the standard control package for burners did not meet this higher SIL requirement. A typical fault tree for a fired burner in a high traffic area (case 1) is in the appendix.

Two of the SIS systems which did not meet the required SIL were ventilation systems. It was determined that the ventilation systems for the original plant had been upgraded, but these changes were not reflected in the design package used for the HAZOP. Instead, a “standard vendor’s package” was reviewed.

Three of the SIS systems which did not meet the required SIL were high level interlocks. The original plant had these tanks in low-traffic areas, so the potential for personnel exposure had been rated very low.

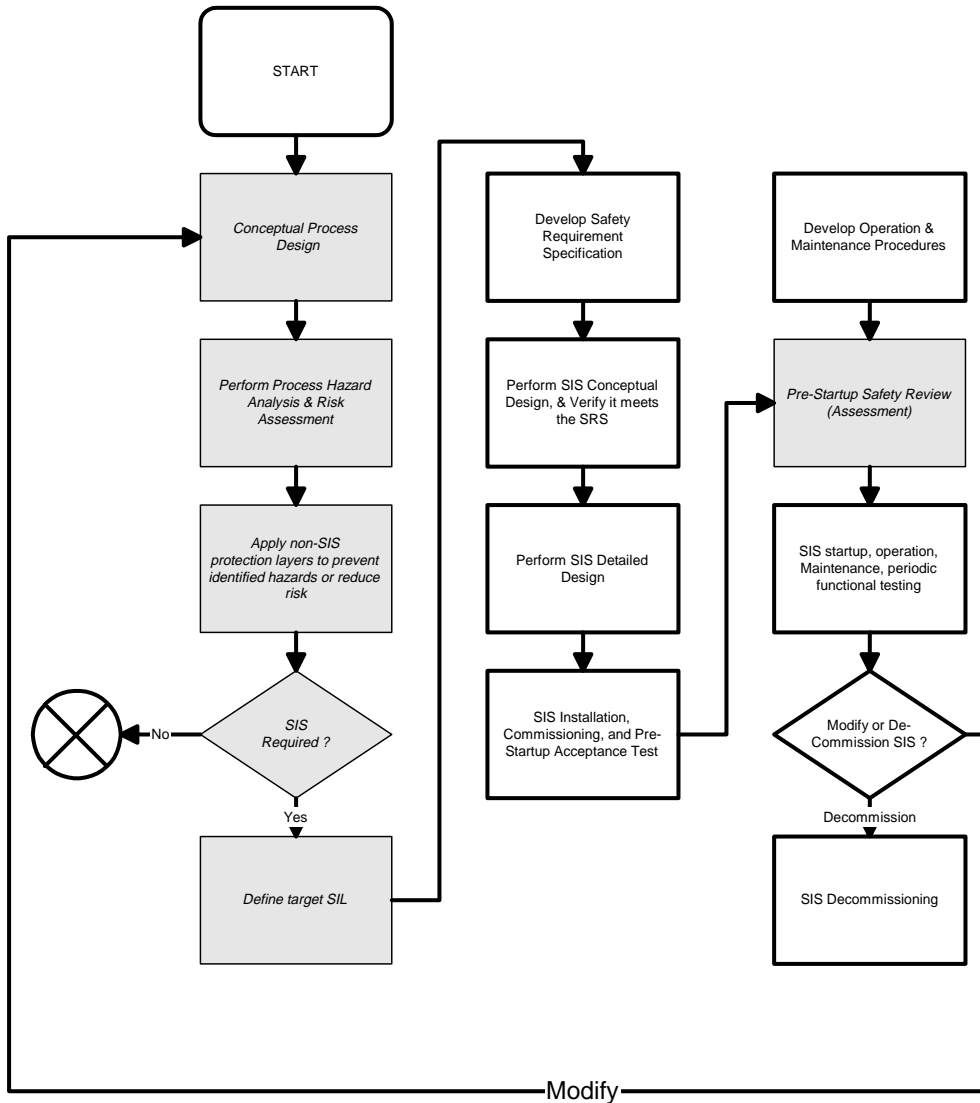
The remaining SIS systems which did not meet the required SIL were systems which had been changed significantly from the first plant to take advantage of process improvements.

A capital project was developed to determine the cost (both capital expense and timing) to bring a plant, based on this preliminary design, up to standards. This would show the potential results if the Life Cycle Model were not followed.

It was determined that the total capital cost of two projects is only slightly more than the cost of one comprehensive capital project. The cost increases were due to abandoned design and cable (which could be written off to expense) and overhead associated with maintaining the project team for longer duration.

The most notable penalty of not using the Life Cycle Model was time. Approximately 2-3 months would be required to perform the design and construction work needed to remedy the inadequate design. A significant amount of time would be needed to convince upper management to fund a project to remedy deficiencies in the original design. And project start-up would be delayed by up to six months, while the SIS's are designed and built.

Figure1 SIS Safety Life Cycle



LEGEND:

Safety Lifecycle steps not covered by S84.01

Safety Lifecycle steps covered by S84.01

Table 3
Typical Furnace QRA Results
Furnace Loss-of-Purge-Cycle Shutdown

Mincut Upper Bound -> 3.672E-001

This Partition -> 3.672E-001

Cut No.	% Total	% Cut Set	Frequency	Cut Sets
1	61.7	61.7	2.264E-001	FURNACE_PLC
2	70.7	9.0	3.316E-002	FLAME_DETECT
3	79.4	8.7	3.198E-002	FD_FAN
4	88.1	8.7	3.198E-002	ID_FAN
5	96.8	8.7	3.198E-002	FAN
6	100.0	7.1	2.594E-002	COMB_AIRFLOW
7	100.0	6.3	2.303E-002	MAIN_GAS
8	100.0	3.6	1.305E-002	AIR_PRESS
9	100.0	1.7	6.113E-003	FURNACE_PRESS
10	100.0	0.2	5.305E-004	DAMPERS_LIGHTOFF, FUEL_LIGHTOFF
11	100.0	0.1	2.488E-004	AIRFLOW, AIR_DAMPER