5th Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 29-30, 2002

EFFECT OF THE LIFE CYCLE MODEL ON A CAPITAL PROJECT

David K. Thomas
Principal
Meerkat Consulting
609 Oak Harbor
Houston, TX 77062
Phone: (281) 286-5206
Email: davcathy@swbell.net

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 not stated in either standard. 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 determined 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) regulation, 29 CFR 1910.119, was published, a debate started throughout industry on when a HAZOP (Hazards and Operability study) should be performed. 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. Efforts were even mounted in some companies to determine how to HAZOP a software package and an electrical design.

ANSI/ISA-S84.01 (Application of Safety Instrumented Systems for the Process Industry) and the equivalent international code (IEC-61508 and IEC-61511) resolved this debate with a project lifecycle model which included 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. It is also recommended to have input from a broad spectrum of employees into this SIL determination.

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

   The SRS (Safety Requirement Specification) documents functional requirements for the SIS. It defines the 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 the 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. It is further stated that the QRA must be computer-based, to reduce the potential for human error giving false results, and to better deal with common-mode failures.

4. 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 earlier Life Cycle models. 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, ideally one would designed and estimated a project 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 intentionally 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 project 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 shaped 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. This allows a high quality HAZOP, as the design is well understood. Additionally, by examining this preliminary detailed design for compliance with ANSI/ISA-S84.01, 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 a manufacturing operation by a multi-national corporation. It was assumed (for the purposes of the paper) that design and construction 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:

TABLE 1 – SAFETY INTEGRITY LEVEL VS. PROBABILITY OF FAILURE ON DEMAND

Safety Integrity Level (SIL)	Probability of Failure on Demand Average Range (PFD avg)
1	10^{-01} to 10^{-02}
2	10^{-02} to 10^{-03}
3	10^{-04} to 10^{-04}
4	$< 10^{-05}$

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 to 2 or 3 for burner explosions and the standard control package for burners does not meet this higher SIL requirement.

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 in the HAZOP.

Three of the SIS systems which did not meet the required SIL were high level interlocks on tanks with flammable or toxic contents. 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.

CONCLUSIONS

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 additional time would be needed to convince upper management to fund a project to remedy deficiencies in the original design. A significant effort would be needed to keep key members of the project team available for the additional design work. And project start-up would delayed by (conservatively) six months, while the SIS's are designed built, and tested.

REFERENCES

1. "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA-S84-01-1996, ISA, Research Triangle Park, NC, 1996

2. "Guide for Pressure-Relieving and Depressurizing Systems", API Recommended Practice 521, Fourth Edition, American Petroleum Institute, March 1997.

3. "Pressure Vessels with Overpressure Protection by System Design", Section VIII, Divisions 1 and 2, ASME Code Case 2211-1, The 1995 Boiler Pressure Vessel Code, American Society of Mechanical Engineers, 1995.

4. *"OREDA: Offshore Reliability Data Handbook,"* 2nd Edition, Det Norske Veritas Industri Norge as DNV Technica, Norway, 1992.

5. *"Guidelines for Process Equipment Reliability Data,"* Center for Chemical Process Safety of the American Institute of Chemical Engineers, NY, NY, 1989.

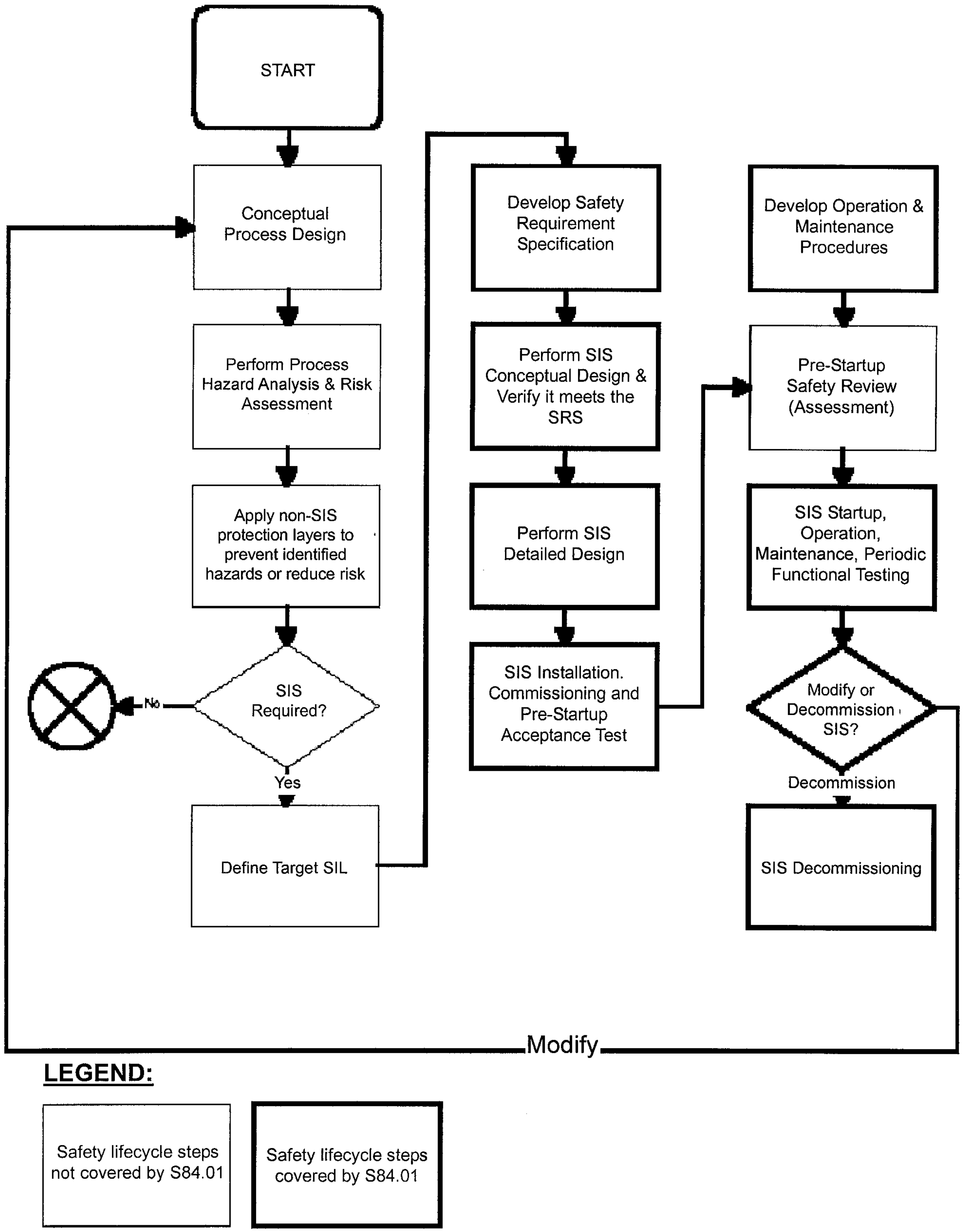
6. "*Guidelines for Quantitative Risk Assessment,* Center for Chemical Process Safety of the American Institute of Chemical Engineers, NY, NY, 1989.

7. *"Non-Electronic Parts Reliability Data,"* Reliability Analysis Center, Rome, NY, 1995.

8. *"Failure Mode/Mechanism Distributions,"* Reliability Analysis Center, Rome, NY, 1991.

9. *"IEEE Standard 500-1984 Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations"*, The Institute of Electrical and Electronics Engineers, New York, NY, 1983.

10. Lees, F.P, *Loss Prevention in the Process Industries,* Butterworth- Heinemann, 1996.


START
Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
SIS Required?
No
Yes
Define Target SIL
Develop Safety Requirement Specification
Perform SIS Conceptual Design & Verify it meets the SRS
Perform SIS Detailed Design
SIS Installation. Commissioning and Pre-Startup Acceptance Test
Develop Operation & Maintenance Procedures
Pre-Startup Safety Review (Assessment)
SIS Startup, Operation, Maintenance, Periodic Functional Testing
Modify or Decommission SIS?
Decommission
SIS Decommissioning
Modify
LEGEND:
Safety lifecycle steps not covered by S84.01
Safety lifecycle steps covered by S84.01