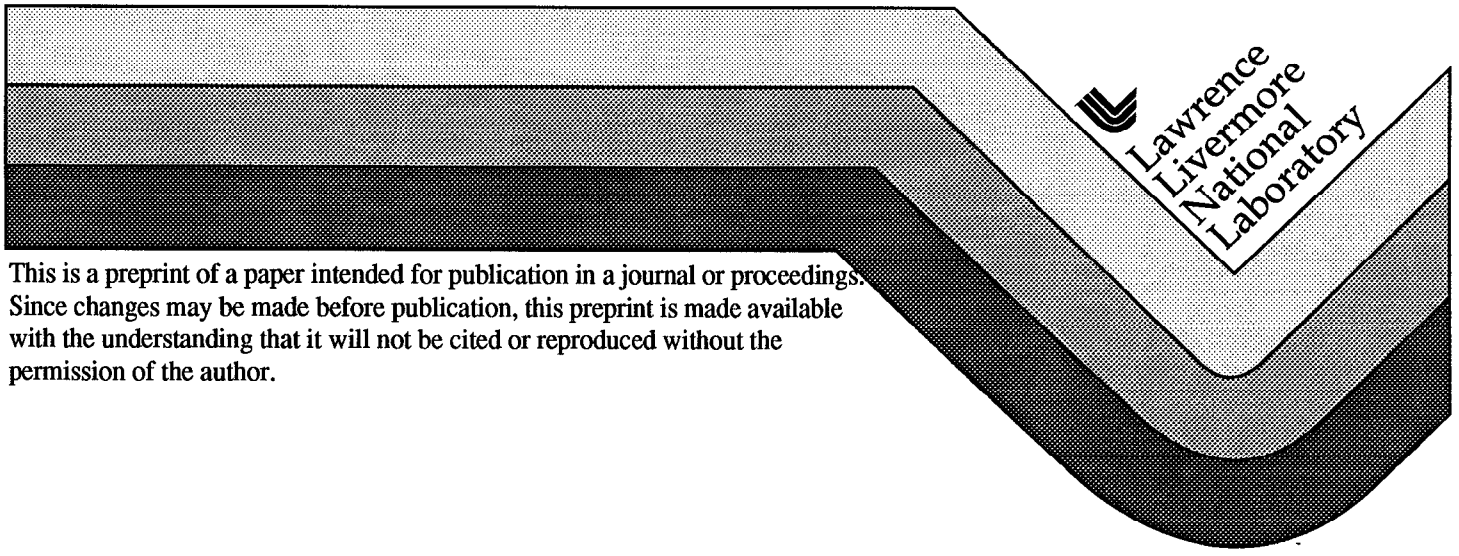
UCRL-JC-132368
Preprint

Systems Engineering Applied to Integrated Safety Management for High Consequence Facilities

R. H. Barter and B. G. Morais

This paper was prepared for submittal to
9th Annual International Symposium
of the Council on Systems Engineering
Brighton, England
June 6, 1999

November 10, 1998



Systems Engineering Applied to Integrated Safety Management for High Consequence Facilities

Robert H. Barter
Lawrence Livermore National Laboratory
7000 East Ave., Livermore, CA 94550, USA

Bernard G. Morais
Synergistic Applications, Inc.
Suite 107, 333 Cobalt Way, Sunnyvale, CA 94086, USA

Abstract. Integrated Safety Management is a concept that is being actively promoted by the U.S. Department of Energy as a means of assuring safe operation of its facilities. The concept involves the integration of safety precepts into work planning rather than adjusting for safe operations after defining the work activity. The system engineering techniques used to design an integrated safety management system for a high consequence research facility are described. An example is given to show how the concepts evolved with the system design.

BACKGROUND

System Boundary. Integrated Safety Management (ISM) at Lawrence Livermore National laboratory (LLNL) is managed at two levels. The site level safety system describes the institutional safety management functions that apply to the Laboratory as a whole. Facility, activity and task safety management is managed at the facility level. Figure 1, below shows the relationship between site, facility, activity and task activities.

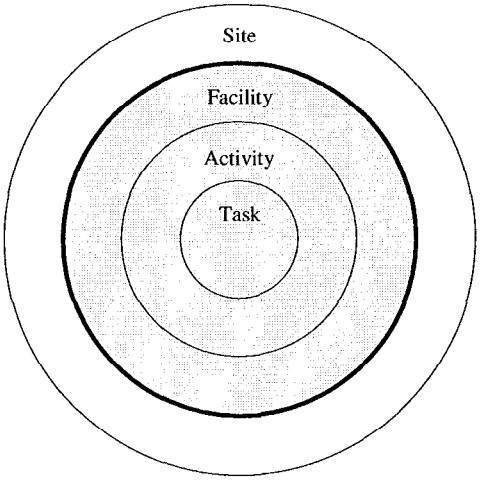


Figure 1.
Safety Hierarchy

Objectives. The Defense Technology Engineering Division's Systems Engineering Center at LLNL was asked to look at ISM requirements as they pertain to high consequence facilities. The goal of the effort was to develop a system that would increase work efficiency and assure regulatory compliance while providing appropriate levels of protection to workers, the public and the environment.

Regulatory Environment. There is a complex regulatory environment that ultimately drives the safety environment. The U.S. Code of Federal Regulations (CFRs) establish some safety requirements that are directly applicable to LLNL. Other CFRs drive the Department of Energy Acquisition Regulations (DEARs) which, in turn, drive contract requirements for Integrated Safety Management. The Defense Nuclear Facility Safety Board (DNFSB) is chartered by the U.S. Congress to provide nuclear safety oversight of Department of Energy (DOE) defense nuclear facilities. The DNFSB role is similar to the role played by the Nuclear Regulatory Commission for civilian nuclear facilities. The DNFSB has developed its own set of ISM guidance documents.

CONCEPTS

At the beginning of the project, the customer expressed the desire that we incorporate three operational concepts into any Integrated Safety Management System (ISMS).

Work and Safety Envelopes. Research and Development (R&D) involving hazardous material requires a careful balance between safety controls and operational flexibility. Experience has shown that a well defined work envelope inside a well defined safety envelope will allow the flexibility desired by researchers while maintaining safety conditions. As shown in Figure 2 below, the challenge is to properly define and assure that the

work envelope stays within a correctly defined safety envelope.

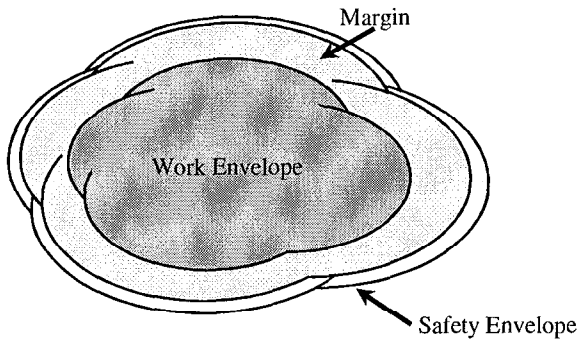


Figure 2.
Work and safety Envelopes

Reduced Development Time. R&D efforts are requiring increasingly complex facilities and apparatus to complete their research objectives. Increasing complexity increases the time needed to develop new experiments and to get those experiments approved. There is also a tendency for each experimenter to re-invent the approval process for each new experiment. There was a general belief that standard approval processes could be used to lower the approval threshold and reduce the time to complete experiments.

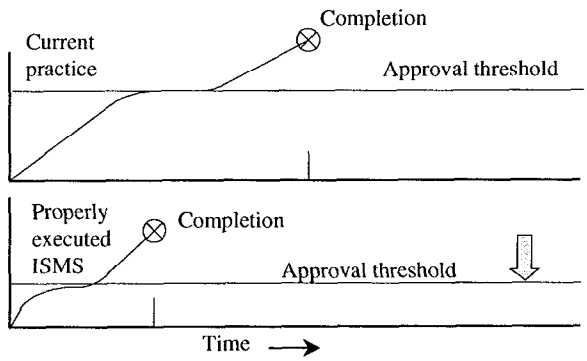


Figure 3.
Reducing the Approval Threshold

Structured Work Procedures. In any hazardous operation there is a tradeoff between the skill of the worker and the specificity of work procedures. Production environments will often use a strategy of developing highly specific work procedures and using less skilled workers to follow the detailed procedures. A nuclear reactor is an example of such an environment. The demolition industry uses highly trained explosives handlers and relatively simple written procedures. In an R&D environment it is desirable to rely upon the skill of the worker, but it is also necessary to be able to demonstrate that the workers are trained for the work that they are being asked to accomplish.

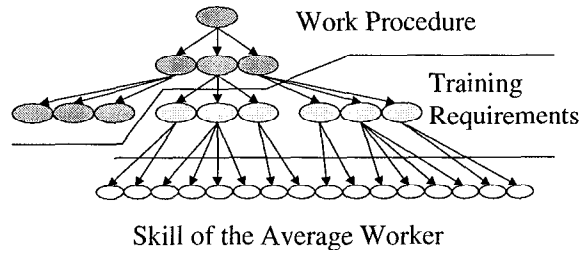


Figure 4.
Structured Task Definitions

Structured task definitions form the basis for developing work procedures and training requirements. The task definitions also document the expected level of worker competency for which no further additional training is required.

ENGINEERING METHODOLOGY

Basic Methodology. The approach to determining how to *do work safely while satisfying the objective of integrating work planning with worker, public and environmental protection* required the identification of the functions that would have to be performed to define the work. This analysis determined the work objectives, defined the work to be performed, analyzed the hazards, identified the constraints applicable for those hazards, and then established the controls that would mitigate the hazards. There was also a recognition that there needed to be some process monitoring and oversight that would allow for adjustment for changes. Having this in place would allow work to be performed safely.
The systems engineering analysis for an integrated safety management system paralleled the functions for the ISMS. The ISMS had the functional flow of:

- Define the Work
- Analyze the Hazards
- Develop the Controls
- Do the Work
- Monitor the Performance and provide feedback for improvements

The systems engineering analysis had the following functions:

- Define the Customer need
- Define the functions that satisfy the need
- Develop the requirements for how well those functions have to be performed
- Develop the answer that will perform those functions and satisfy the requirements
- Test and iterate on the design for further enhancement functionality and performance

This engineering analysis used the FRAT methodology of Mar and Morais (Mar, 1994, Morais and Grygiel, 1994, Mar and Morais, 1997) for developing definition for an integrated system. That methodology took the top level function, that is

- what has to be done and in this case - *Do Work Safely.* The requirements for how well this function must be performed are- *Meet The Orders and Regulations* and *Meet The Work Task Needs.* The answer, in this case, was a *Facility Integrated Management System (ISMS),* and was mandated by the orders and regulations. The Facility ISMS recognized that there was a larger system that this system was a part of and that this system would have to be meet the larger system's functionality, requirements and constraints. That larger system was The Site ISMS. The test was - *Approval by Management.*

After defining the top level FRAT for the system, subsequent decomposition provided further details of the system description. The functional decomposition that is only a part of this system description is shown in the following figure:

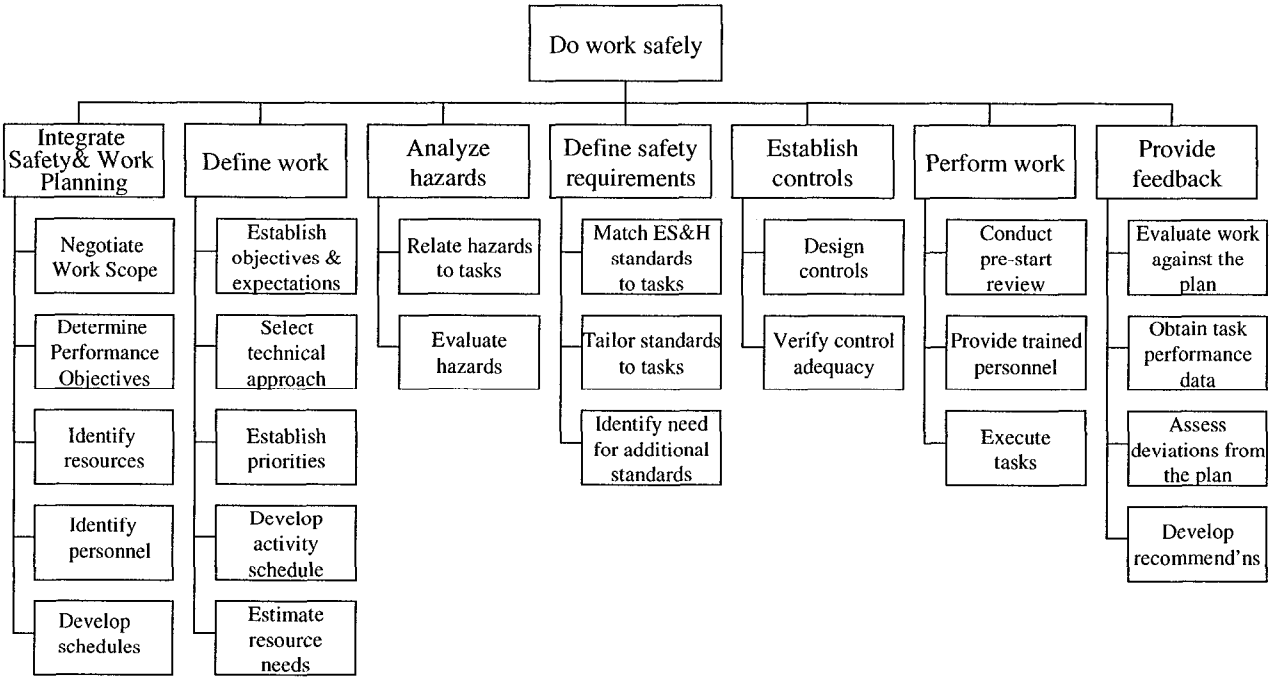


Figure 5.
Functional Decomposition for Doing Work safely

Operational Concepts. Another methodology was also used in this analysis. An operational concept definition was also developed for each of the FRAT descriptions. This approach was in recognition that the culture of the organization would be more receptive if there were guidelines that explained the rationale for the functions, requirements, the selected answer, and the tests that were part of the system definition for the ISMS.

These operational concepts also provided part of the decision criteria that helped to select the answers that would perform the functions and meet the requirements. In these descriptions, identified with an "O", the roles and responsibilities as well as authority were defined. An example of this is shown in Figure 6 and the text that follows.

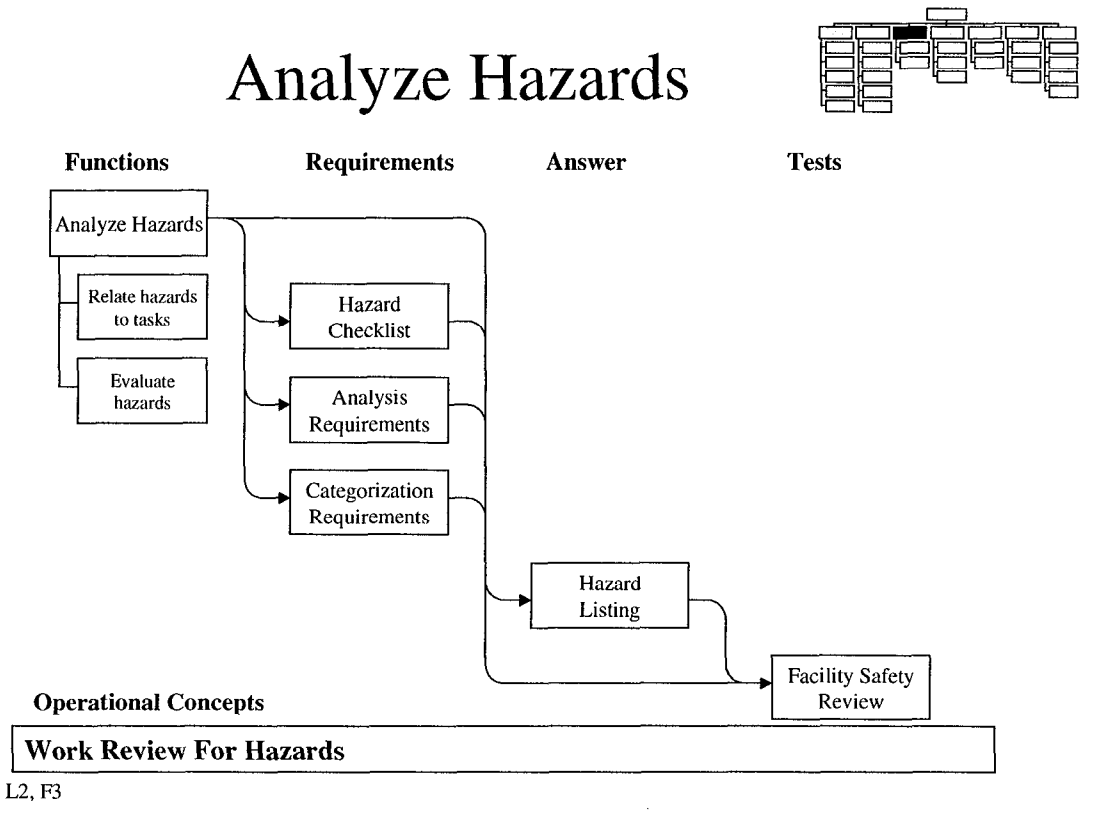


Figure 6.
Graphic Representation for Communicating Functions, Requirements, Answers, Tests, and Operational Concepts

Functions
ANALYZE HAZARDS (F)
The Activity Manager shall identify and analyze the hazards that are applicable to the work to be accomplished. Risk levels for each identified hazard shall be established. Each hazard shall be characterized as to type.

Requirements
HAZARD CHECK LIST (R)
Review the checklist of safety and environmental hazards that are cited in the Site ISMS for the work to be performed.

ANALYSIS REQUIREMENTS (R)
The hazards shall be analyzed in accordance with the Site ISMS.

CATEGORIZATION REQUIREMENTS (R)
All hazards shall be categorized as to type defined in the Site ISMS.

Operational Concepts
WORK REVIEW FOR HAZARDS (O)
The work to be performed is to be reviewed for hazards that are not covered by the existing safety documentation for the facility. Hazards identified shall have a method of control to eliminate or mitigate the consequences.

Answer
HAZARD LISTING (A)
A listing of hazards that are specific to the work to be done that are identified to risk level and type. This listing shall be abstracted from the generic listing of hazards that are relevant to the LLNL Site and are documented in the Site ISMS.

Tests
FACILITY SAFETY REVIEW (T)
The hazard listing should be reviewed and concurred in by a team comprised of the Environmental Safety & Health (ES&H) Team Leader, Facility Manager and the Activity Manager or their designees. This review should verify that the tasks are within the scope of work to be done in the facility.

This was an aid to establishing that Shared Vision between the Customer, the Stakeholders and the system Developers. It improved the communications and the understanding of what was required to establish an Integrated Safety Management System for hazardous operations.

PROCESS DATA

The first step in the engineering process was to extract requirements from the driver documents. While there was general agreement between the DOE and DNFSB requirements, both organizations interpreted the intent of ISM in slightly different ways.

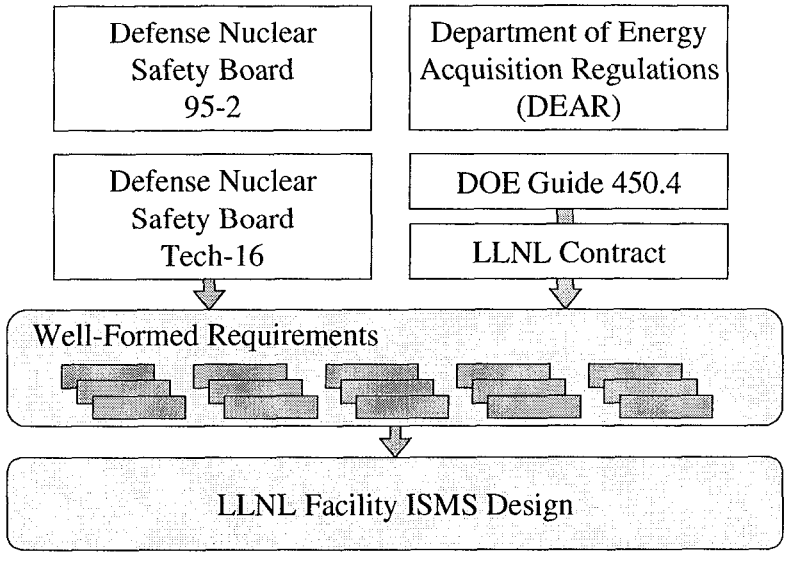


Figure 7.
DNFSB and DOE Requirements

The ISM requirements can be summarized as a set of principles and a set of functions.

Principles

- Line Management Responsibility for Safety
- Clear Roles and Responsibilities
- Competence Commensurate With Responsibility
- Balanced Priorities
- Identification of Safety Standards and Requirements
- Hazard Controls Tailored to Work Being Performed

Functions

- Define the Scope of Work
- Analyze Hazards
- Develop/Implement Controls
- Perform Work
- Feedback/Improvement

Level 0 of the FRAT hierarchy; set the top level expectations for the ISMS:

DO WORK SAFELY (F)

Accomplish work safely in facilities that perform High Consequence Operations. High Consequence Operations are those that have the potential to threaten the safety of the workers, the public or the environment. This work shall be within the safety envelope for the LLNL Site and shall meet the requirements of the Site ISMS that have been established for a Facility and that protects the public, the workers and the environment for all work process activities

MEET REGULATIONS (R)

Structure the tasks to meet DOE requirements as defined in the LLNL contract and statutes and regulations established by National, State and Local agencies as applicable to the facility.

MEET TASK NEEDS (R)

Meet the requirements established by the researchers and engineers for the tasks that have to be accomplished to satisfy the research objectives.

HIGH CONSEQUENCE OPERATIONS(O)

High consequence operations are tasks that have a plausible possibility of causing significant damage to a worker, the public, the facility or the environment in the event of an accident.

LINE MANAGEMENT RESPONSIBILITY(O)

Line management is responsible for ensuring that work is performed safely. At LLNL, Engineering is responsible for doing work safely, Programs are responsible for what work is performed.

CLEAR ROLES AND RESPONSIBILITIES(O)

Clear and unambiguous lines of authority and responsibility are defined for all organizational levels. A facility may be operated on one of three modes: landlord/tenant, line, or matrix. A landlord/tenant facility will have a strong (landlord) facility organization that is responsible for safety of the facility and the (tenant) operations within the facility. The landlord organization approves all activities within the facility. A line facility has one organizational structure that is responsible for both the facility and the operations within the facility. A matrix facility has a split organizational structure with responsibility for safety shared among two or more organizations. Top level management and safety functions are the same for each type of facility, however the authority and accountability paths are different.

COMPETENCE COMMENSURATE WITH RESPONSIBILITIES(O)

Personnel possess the experience, knowledge, skills, and abilities that are necessary to discharge their responsibilities.

FACILITY ISMS (A)

A facility oriented safety management system was selected as the choice over the continuation of the current approaches that have been followed. This management system will emphasize worker, public and environmental safety in an integrated approach with the work planning.

APPROVAL OF FACILITY ISMS (T)

Obtain approval of the Facility Integrated Safety Management System by LLNL management.

EVOLUTION OF SYSTEM CONCEPTS

It is interesting to note the evolution of system concepts that took place during the course of the project. At the beginning of the project it became clear that there was a great deal of similarity between the ISM "cycle" and any self-correcting feedback control system.

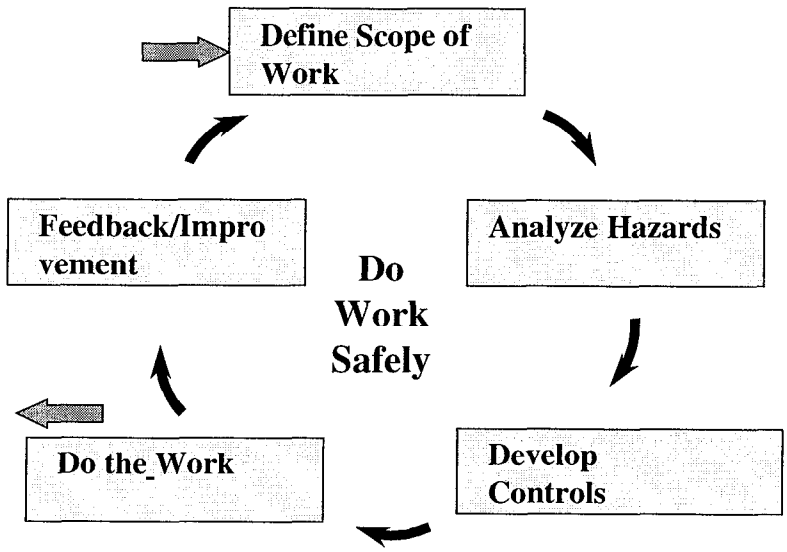


Figure 8.
ISMS Cycle

The user community quickly pointed out a fundamental flaw in the ISMS cycle as contained in the driver documents. If taken literally, the feedback only occurs after the work has been done. A more accurate design yielded the diagram in figure 9 that could still be mapped back to the original requirements.

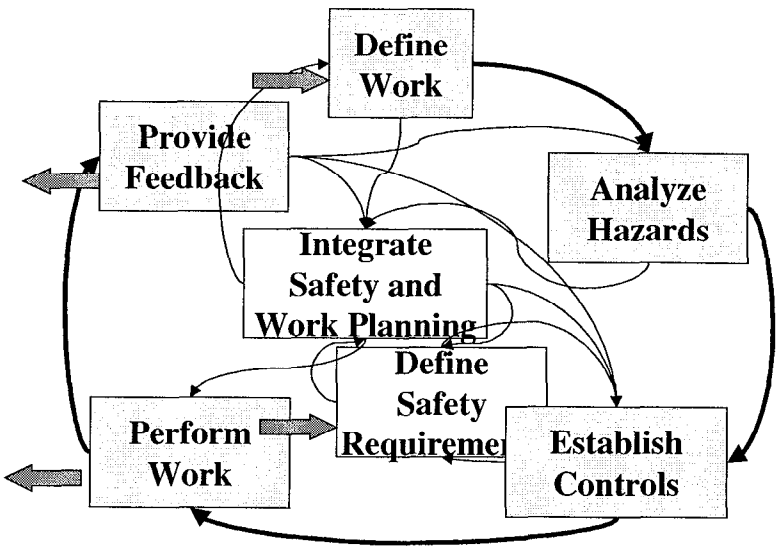


Figure 9.
"Improved" ISMS Cycle

The "improved" diagram included functions to "Integrate Safety and Work Planning" and to "Define Safety Requirements". The diagram in figure 10 shows a process that begins to look more like a control system

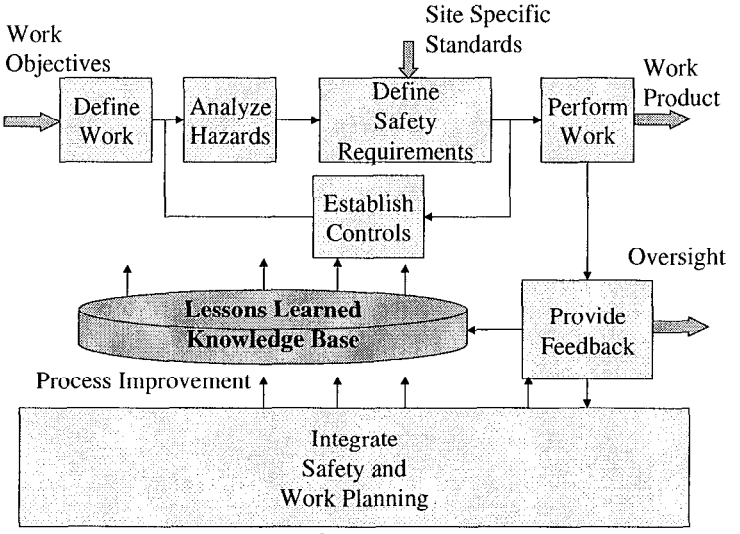


Figure 10.
ISMS With Feedback

The final evolution of the ISMS was achieved when it was realized that work planning and safety planning are mirror images of each other. Work and safety planning needed to function in a coordinated way in order to achieve the goals set forth at the beginning of the project. Figure 11 shows the balanced ISMS. In the figure below, Program and Project Requirements form the basis for analyzing work processes and defining operational constraints. Site and Facility Requirements form the basis for analyzing hazards and defining safety constraints.

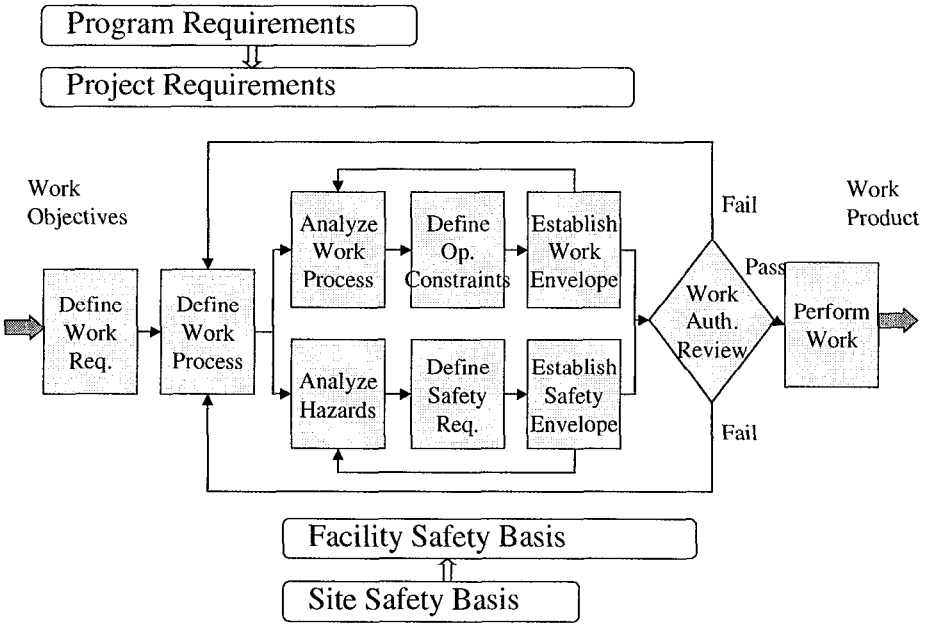


Figure 11.
Balanced Work and Safety Planning

Proper integration of operational and safety constraints (work and safety envelopes) is assured during the Work Authorization Review.

CONCLUSION

Safety Professionals have long recognized the need to balance safety against the need to accomplish useful work. Managers have long recognized that safe working conditions are essential for high productivity. However, both groups tend to sub-optimize their respective systems.

We have shown how basic systems engineering techniques can be applied to "the total system" to meet the needs of Safety Professionals and Managers alike. The FRAT methodology proved to be an effective tool for developing the Integrated Safety Management System.

References:

Mar, Brian W., "Systems Engineering Basics," *NCOSE Journal*, Vol. 1, No. 1, Sept 1994

Morais, B. G. and Grygiel, M. L, "Application of Systems Engineering into an Ongoing Operation:, *Proceedings of the Fourth Annual NCOSE Symposium*, 1994

Mar, B. W. and Morais, B. G., "*The Engineering of Complex Systems*", SYNERGISTIC APPLICTIONS, Inc., 1997

Robert Barter has 25 years experience in electronic engineering, software development, project management, safety, and systems engineering on Department of Defense and Department of Energy (DOE) projects. He has experience developing control systems, performing underground nuclear testing, software development for high reliability systems, and hazardous waste management. Bob received his Bachelor of Science degree in Electronic Engineering from Northrop University in 1970. Bob is a member of the DOE, Life Cycle Asset Management, Systems Engineering Implementation Team. He is on the chapter's Board of Directors and ambassador to Lawrence Livermore National Laboratory (LLNL) where he is currently the principal systems engineer on two projects.

MR. BERNARD G. MORAIS is the President of Synergistic Applications, Inc. and has over thirty five years of Program management and Systems Engineering experience in industry. He has a BSEE and M.S. in Systems Management. One of the more significant achievements in his career was leading the development of the first Systems Engineering Management Guide for the Defense Systems Management College when he was Director of Space Systems Division Systems Engineering for the Lockheed Missiles and Space Company. He has provided consulting support and training for National and International government agencies as well as communications and energy companies. He is a founding member of INCOSE, has been an Adjunct Professor at San Jose State University and has lectured in Systems Engineering at many other universities.