

SYSE 590 Integrative Workshop – Systems Engineering Study Plan

Learning Objectives and Study Plan	2
Elective Summaries	3
Professional Development and Continuing Education Course Summaries	5
Publication Summaries	8
Project Summary	9
Appendix I Systems Engineering Graduate Program Summary	44
Appendix II Integrative Workshop Summary	46
Appendix III Revision History	50

Learning Objectives & Study Plan

The early twentieth century British writer and critic George Orwell defended his advocacy of socialism, claiming he was less interested in how socialism could improve England, and more interested in how England could improve socialism. My study plan adopted similar language for my learning objective summary: not the application of risk analysis to systems engineering, but the application of systems engineering to improve risk analysis. Study emphasis has been on the application of applied risk analysis and safety engineering to support continued and uninterrupted operation of complex systems.

In addition to the required courses, summarized in the chronological table below, additional learning activities have included:

- Elective courses to support learning objectives (page 3)
- Non-credit professional development and continuing education courses (page 5)
- Submission of papers for publication (page 8)
- Project summary to support learning objectives (page 9)

Class	Term	Core	Elec	P/I	I/W
SYSE 510 Reducing Risk in Decision Making	01 Spr		4		
SYSE 591 Systems Engineering Approach	01 F	4			
SYSC 514 System Dynamics	02 W	4			
SYSE 573 Requirements Engineering	02 Spr		4		
SYSE 506 Project	02 Sum			4	
SYSE 506 Project	02 F			4	
SYSE 561 Logistics Engineering	03 W		4		
EMGT 565 Research Methods	03 Sum		4		
SYSE 510 Systems Security Engineering	03 F		4		
SYSE 595 Hardware / Software Integration	04 W	4			
EMGT 540 Operations Research	04 F	4			
SYSE 506 Project	04 F			1	
SYSE 590 Integrative Workshop	04 F				4
Subtotal		16	20	9	4

Electives

SYSE 510 Reducing Risk in Decision Making – Spring 2001

“Examine the concepts, techniques and tools for managing risk and making decision as key components of the systems engineering process. In this course, risk connotes a measure of the probability and severity of an undesired event. This course begins with an overview of the risk management (identifying, assessing, monitoring, and mitigating) and decision process. Differences between mission critical and non-mission critical programmatic risk will be emphasized. Other topics include the limits of expected value-based risk analysis, decision making strategies such as max/min, min/max and regrets. Formal methods in risk analysis, elementary decision analysis and decision trees, multi-objective decision making, pareto techniques, optimality, and trade-off analysis will be covered.”

Identifying and communicating decision criteria allows informed choices by all stakeholders. Documented decisions and risk management planning makes accountability clear and provides transparency. This allows repeatability and, if needed, retroactive analysis for feedback, learning, and improvement.

SYSE 573 Requirements Engineering – Spring 2002

“This course provides the knowledge and skills necessary to translate needs and priorities into system requirements, and develop derived requirements, which together form the starting point for engineering of complex . . . systems. The student will develop an understanding of the larger context in which requirements for a system are developed, and learn about trade-offs between developing mission needs or market opportunities first versus assessing available technology first. Techniques for translating needs and priorities into an operational concept and then into specific functional and performance requirements will be presented. The student will assess and improve the usefulness of requirements, including such aspects as correctness, completeness, consistency, measurability, testability, and clarity of documentation.”

Relevant to risk analysis and management because specifying system requirements is essential for successful implementation and operation. Poorly defined or communicated requirements may lead to omission or duplication, increasing probability of failure within the system.

SYSE 561 Logistics Engineering – Winter 2003

“This course will concentrate on logistics from a systems engineering perspective. Systems will include a mix of products and processes, materials, equipment, software, people, data, information, and services, within some form of hierarchy. The design for supportability/serviceability, the production and effective distribution of customer use, and the sustaining maintenance will be addressed on a total system life-cycle basis, with particular emphasis in the early phases of the development of new systems and/or reengineering of existing systems.”

Risk management identifies and mitigates variations from objective performance criteria. Logistics engineering defines input/output criteria and system support requirements for management during the life of the operation.

EMGT 565 Research Methods for Engineering & Technology Management – Summer 2003

“Research methods in Engineering and Technology Management; statistical techniques including proper selection, use, and interpretation of parametric and nonparametric tests along with factor and discriminant analysis. Design of experiments and model misspecification. The use of statistical software will be emphasized.”

Applied research and communication, with emphasis on data and literature reviews, case studies, and surveys. Systems engineering application through examination of practices and assumptions in an organizational setting that contribute to system design, analysis, operation, and performance.

SYSE 510 Systems Security Engineering & Integration – Fall 2003

“Interface management and integration engineering are two primary functions of Systems Engineers. These functions are becoming more and more important as the systems we design become more and more complex. This course covers the systems engineering approach to integration and interface management of complex systems. For application, this course concentrates its examples on the concerns of integration and interface management of human and automata security principals. While much the current concepts surrounding security apply to "information security" (ISEC) this course treats ISEC as only one of the vast application areas for security. Course goals include: Developing an understanding of system security issues, learning how to manage integration and interfacing of systems and system components, apply Systems Engineering Techniques to System Security Design, view Security Policy Development as a Systems Engineering Evolution, and learning techniques to manage risk inherent in system security issues.”

Security is a critical element of risk management. Analysis and development of controls on inputs/outputs in terms of malicious intent is complimentary to system safety engineering and its traditional focus on hardware/software failure or human error.

Professional Development and Continuing Education Courses

Fault Analysis for Systems Engineers – Spring 2002

“This introduction to fault analysis for systems engineers follows the new industry standard, ARP5580, which focuses on functional behavior and consequences rather than the more traditional piece-part analysis. The tutorial will carefully define terms used in the subject of fault analysis, describe the basis for functional failure, and describe the different kinds of fault analyses and when they should be applied. In addition, this tutorial will demonstrate how to integrate failure analysis into the requirements analysis process. ARP5580 will be reviewed in some detail. Finally, we will demonstrate how to conduct a functional failure modes and effects analysis on a communications system and integrate the results in requirements using the techniques described.”

Presented at Boeing in Seattle by Dr. Ron Carson, this tutorial introduced methods for fault analysis of integrated systems, and measures to ensure functional performance and detect and mitigate functional failure.

Applied Statistical Decision Theory – Summer 2002

“Systems engineering is a discipline that has at its heart processes for making near optimal technical decisions. Making good technical decisions in an environment of uncertainty with decision-maker risk aversion greatly enhances success in any endeavor. This tutorial addresses state of the art techniques for making good technical decisions, and provides attendees with both the theory and tools to apply the theory.”

Presented at the 2002 INCOSE Symposium in Las Vegas by Mark Powell of the University of Idaho, this tutorial introduced elements of decision theory, the difference between decision and outcome, and stakeholder risk tolerance as a factor in decision analysis.

Introduction to Fire Protection Engineering – Winter 2003

“Basics of fire science will be covered, including theory from related fields. Students will learn about room fire growth and spread mechanisms and the influence of fire properties of wall linings and combustible contents, and about the use of fire models to predict fire growth and fire conditions in rooms. Some topics will focus on the analysis and design of the systems that respond to the presence of fire such as fire detection and fire suppression systems. Another objective will be an understanding of the traditional practices of the prescriptive code approach as opposed to the performance (objective) based design. This will include the use of the main fire test methods in use today and how to analyze data from these tests. Some aspects of people interaction with fire will be covered as well. The emphasis will be on the current issues of importance to fire protection engineering.”

Taught by Dr. Joe Urbas of Pacific Fire Laboratory, this undergraduate course introduced fire protection engineering as part of a PSU degree program under

development. System engineering application through use of simulation software to model fire consequence and design appropriate protection systems.

Probabilistic Risk Analysis – Fall 2003

“The course is designed for professionals within academia, government, industry, consulting groups, trade associations, law firms, and other organizations who want to advance their knowledge of probabilistic risk analysis. The unique course will bring together nationally and internationally known experts from different disciplines to teach the common elements of probabilistic risk assessment, management, and communication. Using a practical and integrated approach that combines lectures with case examples, this program will teach the methods used to assess, manage, and communicate risks in a fully probabilistic framework. Upon completion of this course, you should be able to . . . critically review probabilistic risk assessments . . . distinguish variability and uncertainty, particularly in the context of risk management . . . understand the impacts of choices made to characterize information from data and experts . . . explore the use of Bayesian methods in risk assessments . . . communicate probabilistic risk assessment results.”

Taught at the Harvard School of Public Health in Boston by Dr. Kimberly Thompson and a team of international experts, this continuing education course covered methods of analyzing, communicating, and managing risk using probability concepts and related quantitative models.

System Safety and Reliability Analysis – Summer 2004

“Receive intensive training and expert guidance on fundamental methods to increase safety and ensure the reliability of complex systems. This working course taught by two leading experts enables you to practice what you learn. Understand and use Fault Tree Analysis and other quantitative methods to establish a basis for system safety requirements. Learn how to measure and test for reliability using methods such as Failure Mode & Effect Analysis (FMEA) and how to estimate a success level using a basic probability model. Learn how to reduce waste and to avoid critical system failures, false alarms and risky re-starts . . . These powerful methods originally developed and applied in the aerospace and nuclear power industries are increasingly relevant in a variety of business and industrial environments including manufacturing, consumer products, utilities and natural resource extraction. Continuous changes in technology, environmental regulation, public safety concerns and the need to do more with less all make the analysis of complex systems even more demanding. As the level of uncertainty surrounding probable outcomes increases, the safety professional's ability to accurately predict responses is integral to the design process.”

Taught at the University of Washington in Seattle by Dr. Kailash Kapur and David Haasl, this continuing education course provided a detailed framework for safety and reliability analysis of complex engineered systems.

Product Liability Workshop – Fall 2004

“Few manufacturers have a comprehensive program to minimize their product liability exposure. Many employees do not understand the breadth and severity of product liability laws. Frequently, they receive no training to make them sensitive to the implications of what they write and say. Typically, they do not fully appreciate the legal consequences of their actions. To help fill that void, we offer workshops to familiarize manufacturers' employees with the realities of product liability. These workshops are based on case studies that trace product problems from their beginnings and require the audience to decide, as the facts and events develop, what steps the manufacturer should take to protect itself from liability. This problem-solving method is never boring and is often challenging . . . the workshop is intended for senior managers and employees whose jobs require them to make decisions that can get manufacturers into product liability trouble. Among the people who will benefit from this workshop are those who make design decisions, those who draft instructions and warnings, and those who decide how to respond to product problems. The workshop is also intended for risk managers, in-house counsel and accident investigators.”

Presented in Portland by attorneys of Perkins Coie, this workshop illustrated case studies of decisions and communications early in the system life cycle with negative effects on operator safety and developer liability.

Hazard-Based Safety Engineering – Fall 2004

“As a product design/safety professional, or perhaps as a manager of your company's product engineering processes, you may have struggled at times balancing your product's safety requirements and guidelines against other important parameters, such as usability, cost, and customer satisfaction. Have you ever wondered why certain safety requirements exist, especially when they seem to impact your creativity or production schedule? Occasionally, you may propose a design not foreseen by current safety standards. Is your new design equivalently safe? What specific hazards does it anticipate? What safeguards can you incorporate to prevent those hazards from causing injury? HBSE is a process that gives you tools to answer those questions . . . in terms of fundamental engineering concepts. In this course you will learn the basic mechanisms by which products can cause injury to the human body. You will learn tools which can help you analyze those processes and determine how best to prevent the injury from occurring. You will put your skills to the test by participating in the hazard-based safety analysis of some familiar electrical products. And you will finish the workshop prepared to address difficult product safety issues in a team-oriented rather than an adversarial manner, supported by science as well as your own experience and engineering judgment.”

Presented at Underwriters Laboratories in Camas, Washington, this course reviewed safety design strategies to mitigate common sources of fire and personnel injury.

Publication Summaries

International Council on Systems Engineering Risk Management Working Group, et al., *Risk Management Maturity Level Model, RMRP-2002-02, Version 1.0*, Seattle, WA: INCOSE, 2002.

Credited as one of nine major contributors for work on this formal collaboration between the INCOSE Risk Management Working Group and other project risk management interest groups. This paper describes how to evaluate the degree of risk management maturity within an organization, based on work practices falling into one of four levels, identified as ad hoc, initial, repeatable, and managed. Determination of maturity level can be followed by initiatives to drive improvement in methods, communication, and consistency of risk management activities.

Gunderson, S., "Establishing and Auditing Measures for Hazardous Energy Isolation," *Journal of System Safety*, vol. 40, no. 2, 2004.

Systems extend across time through their life-cycle stages of concept, design, development, production, operation, and retirement. Within the stage of operation, maintenance represents a risk when hazardous energies may be present. Examples include chemical, electrical, or physical energy sources. The article proposes four metrics for control and isolation of hazardous energies during maintenance that may loosen system defenses, potentially threatening personnel or bystanders. The metrics may be established during system design, communicated in system documentation, and audited during the operation life cycle for verification of safe practices.

Gunderson, S., "Return to Sender: System Maintenance, Reverse Logistics, and Hazardous Materials Transportation," *Journal of System Safety*, vol. 40, no. 4, 2004.

Additionally, systems extend across space through their logistics functions of delivery and support. Within the stage of support, reverse logistics represents a risk when parts or components returned for service may be contaminated with hazardous materials. Examples range from minimally hazardous pump lubricants to significantly dangerous chemicals used for semiconductor processing. The article describes the risk of hazardous material leakage during transportation, and surveys the issues of design for transportation with residual chemicals or design for decontamination.

Project

Project work, drawing from the Portland State University systems engineering program and related student learning activities, documents and communicates the development of a system safety engineering course. Technical risk analysis and management has been emphasized over the project/program risks of schedule and cost. Student work and output have been designed to be complimentary with systems engineering approaches and methods, and congruent with the objectives of the graduate program. Overlap with existing core and elective courses, and emphasis on specialty or domain-specific subjects, have both been minimized. The primary goal of this project has been to contribute to the study goals summarized in page 2 above. The secondary goal of this project has been to develop material for possible inclusion in the systems engineering program as a future elective.

Project Outline

1.0) Introduction

- 1.1) Risk Management
- 1.2) Exclusions
- 1.3) Limitations

2.0) System Safety Design and Analysis

- 2.1) Design
- 2.2) Life Cycle Analysis
- 2.3) Functional Analysis
- 2.4) Configuration Analysis
 - 2.4.1) Hardware
 - 2.4.2) Software
 - 2.4.3) Human Factors
 - 2.4.4) Organizational Factors

3.0) Metrics

- 3.1) Systems Engineering Metrics
- 3.2) Measures for Risk
- 3.3) Measures for Reliability
- 3.4) Integrated Measures for Risk and Reliability Analysis

4.0) Conclusion

1.0) Introduction

Risk is an inherent part of engineering and managing any system, and as system complexity increases, so do the sources and consequences of risk. The discipline of systems engineering provides a framework to identify and mitigate both the requirements and the risks of complex systems.

Blanchard and Fabrycky define systems engineering as “good engineering with special areas of emphasis.” [9] This emphasis includes a top-down approach that views the system as a whole instead of the bottom-up approach of championing components or sub-systems by specialty disciplines or engineering groups potentially in conflict with each other. Systems engineering is interdisciplinary in nature, with attention to requirements definition and recognition of life-cycle stages to address all functional and design objectives.

The formal definition of systems engineering, according to the International Council on Systems Engineering, (INCOSE) is “an interdisciplinary approach and means to enable the realization of successful systems.” [45] This follows the *systems engineering process*, which is “a logical, systematic, comprehensive, iterative problem solving set of processes selectively used to accomplish systems engineering tasks.” Systems engineers translate customer or end-user needs into integrated lower-level functions and solutions. Such tasks as traceability of design decisions and resource allocations, control of process and material changes, and definition of interfaces are crucial to systems engineering success.

But the systems engineering process does not make use of uniform checklists or process maps. As risk changes with system complexity, so does the degree of formal system engineering methodology. INCOSE identifies this flexibility as *tailoring*, and the *Systems Engineering Handbook* devotes an entire section to this important concept for achieving system completion while reducing risk with effective use of engineering resources. (Fig. 1)

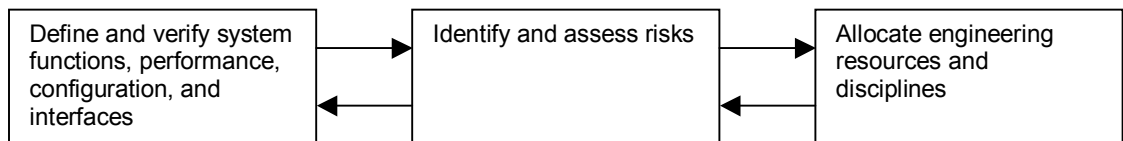


Fig. 1 Tailoring the Systems Engineering Process to the System

Calvano and John summarize tailoring the systems engineering process, and the importance of first understanding the nature and the complexity of the system to be engineered. [16] System complexity drives tailoring of the systems engineering process towards completion with a high degree of confidence that “emergent” and “synergistic” behaviors have been addressed. Until an “acceptable level of confidence is achievable,” Calvano and John recommend conservative systems engineering strategies. This recommendation for approaching complexity is directly related to analytical limitations described in further detail below.

In addition to system complexity as an individual concept, Dvir et al. introduce the UCP model for addressing the combined risks posed by uncertainty, complexity, and pace. [28] Uncertainty refers to the level of innovation needed for system completion, from integration of commercially available products to significant materials science engineering. Complexity, as described above, refers to interactions between system interfaces. And pace refers to the speed of system development. Each of these factors represents different risks and the various possible combinations each require different approaches or tailoring of systems engineering efforts. Such combinations for analysis and resolution demonstrate the broad nature of risks to be managed by the system engineer.

1.1) Risk Management

Risk management comprises a four-stage effort of identification, analysis, communication, and control. But a definition of risk must occur prior to its management. The definition of risk depends on the perspective of an observer or group of observers evaluating relative threats to expected benefits. Molak describes this as “a probability of an adverse effect . . . [but] definition of an ‘adverse effect’ is a value judgement.” [60] Kumamoto and Henley acknowledge the perception of risk as based on individual or group subjectivity, but expand the point estimate of Molak with description of risk as a distribution of outcomes and likelihoods. [54]

According to INCOSE, risk represents an undesired consequence and is specifically mentioned in the *Systems Engineering Handbook* in three of the four phases of the systems engineering program life cycle. “Technology and risk assessment” occurs at the earliest phase of concept exploration. Risk is part of the title of the second phase of program definition and risk reduction. And risk management is a formal element of the third phase of engineering and manufacturing development. Risk management tasks include balancing requirements, resolving conflicts between specialty engineers, and assigning an appropriate level of formality to engineering processes. As part of tailoring, the degree of formality of any process, including risk management, is driven by the level of acceptable risk, a concept related to analytical limitations described in further detail below.

In the event system complexity and risk tolerance demands a formal systems engineering management plan, INCOSE provides an outline for integration of risk management into the systems engineering process:

“Describe the technical risk management program including the approach, methods, procedures, and criteria for risk identification, quantification sensitivity assessment, handling, and risk impact integration into decision processes . . . describe plans to minimize technical risk (e.g., additional prototyping, technology and integration verification, back up development). Identify risk control and monitoring measures including special verifications, technical performance measurement parameters, and critical milestones.”

Specific risks merit identification in the *Systems Engineering Handbook* beyond the general concept of “undesired consequences.” Of special concern to systems engineers in the development of a complex system are risks posed to cost, schedule, performance, and environmental impacts. (Fig. 2)

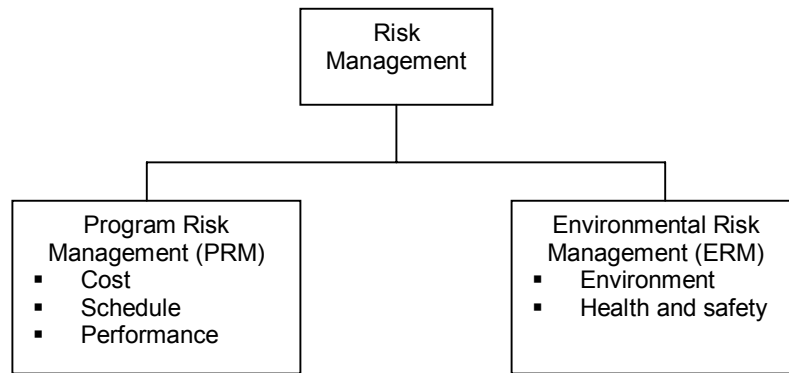


Fig. 2 Risk Management in the Systems Engineering Process

Although divided in the illustration above and identified by unique acronyms, the risk concepts each influence the other, and much of the handbook section on risk management reinforces the interrelationship of these risks and consequences. In serial publications on program risk management, Kujawski first concentrates on cost, but follows up with a method for risk response action (RRA) for an “efficient RRA set” to balance cost, schedule, and performance. [52, 53] However, cost, schedule, and performance dominate the discussion at the expense of the sibling risks of environment, health, and safety. This is emphasized in the handbook with placement of environmental risk at a lower rank: “ERM should be considered an integral part of system development, and therefore is incorporated into PRM.”

But ERM, or the hazards representing physical threats to the system, its operators, and the surrounding environment, participate equally in the success or failure of a system. Too much attention to safety may represent increased cost, schedule delay, or complexity interfering with performance. Too little attention to safety, with cost savings or accelerated schedules as examples, may lead to catastrophic events, potentially beyond the capability of the organization to recover. As noted above, both tailoring and balancing are required for all requirements and all risks.

ERM is an equal part of the performance risks inherent in technical systems, in spite of minimal coverage in the systems engineering literature. Sproles adopts a wide, contextual view in his discussion of effectiveness and performance measures, without specific mention of safety or environmental hazards and their potential effects. [85] Similarly, the handbook limits its discussion of technical risk as failure to achieve measurable performance requirements. Smith concurs with his definition of failure as non-conformance to a defined performance criterion. [83] However, failure of a safety-critical component, or failure propagation leading to loss of control or hazardous operating conditions, crosses the line from an abstract performance measurement to a real hazard. At this point, the safety analyses of ERM merge with the reliability and performance analyses of PRM for a categorical review of technical risks. (Fig. 3)

Although the various risks influence each other, technical risks represent a separate category in terms of analysis and physical hazards from the program risks of cost and schedule. Pennock and Haimes propose a similar argument with their relocation of performance under technical risks, while keeping cost and schedule under program risks. [65] Abadi and Bahill, on the other hand, warn about the difficulty and potential

confusion of program implementation versus system analysis. [1] This warning reflects a similar tension in this paper on integrating systems engineering (i.e., process) and systems safety engineering (i.e., product).

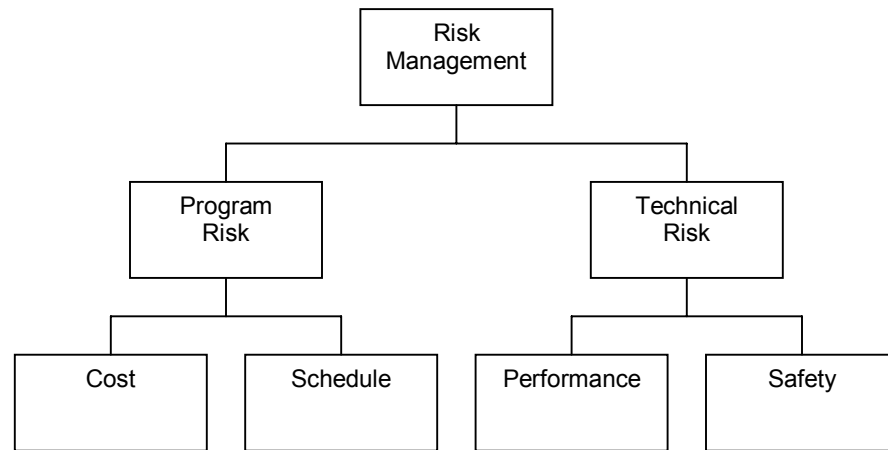


Fig. 3 Management of Program versus Technical Risks

The first objective of this paper is to argue the validity of the above illustration and the role of system safety engineering as a key element of the systems engineering process. If the goal of risk assessment and communication is to support informed decisions, then systems engineering and system safety engineering provide a necessary compliment to each other. Systems engineers, starting from the top, drive requirements to specialty engineers and engineering teams. System safety engineers approach integrated hazards that influence technical risks, but communicate analytical results up for approval of solutions or risk acceptance. Given these roles, the second objective of this paper is to provide a model for improved assessment of value of information as system safety engineers communicate risk in the context of the systems engineering process. In other words, each should be a more informed consumer of the methods and perspectives of the other.

1.2) Exclusions

Technical risk separated from program risk excludes cost and schedule as noted above. Additional exclusions are necessary to provide focus. Security and defense against malicious system damage is a significant exclusion. [4, 37] Traditional risk management concerns such as legal risks, financial risks, market share loss, and supply chain interruption are also excluded. [38]

1.3) Limitations

Any discussion of the value of information of technical risk analysis calls for acknowledgement of limitations as well as exclusions. Primary limitations for consideration include analytical completeness, subjectivity, and uncertainty. Each of these limitations influences the materials in this paper.

Analytical completeness, using the language of probability theory, deals with exclusions and the feasibility of mapping a collectively exhaustive sample space. Petroski denies

this is even possible in considering the risks of complex system: “absolute certainty about the fail-proofness of a design can never be attained, for we can never be certain that we have been exhaustive in asking questions about its future.” [67] Such inability to consider all manifestations of system behavior is the foundation of normal accident theory by Perrow, who defines a system accident in terms of multiple, emergent failures interacting in unanticipated ways by designers and operators. [66, 16] The “normality” of such accidents derives its name from the growth of system complexity and increases in hardware-software coupling in both commercial and military applications.

Analytical completeness refers not only to the inability to *begin* comprehensive analysis as described above, but also the inability to *close* an analysis. In the introduction of the *System Safety Analysis Handbook*, the editors caution about an analytical process that is “open-ended and not well defined. Each step is fraught with difficulties that do not easily lend themselves to a pre-defined or consistent solution.” [86] Clemens and Simmons add that no closed-formed solutions are available to the system safety practitioner, who must acknowledge both art and science as aspects of the profession. [21] Cox and Tait, in more damning language, debunk any definitive opportunity for closure:

“By generating numerical values for the consequences and probabilities of adverse events, QRA [quantified risk assessment] can bring objectivity to the decision-making process. However, QRA is not, and never will be, a precise scientific method, and should not be seen as a mechanistic or automatic means of making risk management decisions.” [24]

Given this inability to assure analytical closure, the Department of Defense system safety standard introduces the critical term of residual mishap risk, which is the risk remaining following analysis and implementation of risk mitigation techniques. [92] Ultimately, residual mishap risk depends on reduction to levels acceptable to program or jurisdictional authorities.

Although the final decision of an authority figure may appear objective due to possible references to legal or contractual sources, the underlying sources may be arbitrary or subjective. If subjectivity can be a factor in an authority figure, then it can also be a factor in the analytical process. Redmill cites judgement, bias, and inaccuracy as undermining objective analysis: “the results obtained by one risk analysis are unlikely to be obtained by others starting with the same information,” and “hazards not identified are neither analyzed nor mitigated.” [72, 73] Wilson and Shlyakhter concur in their assessment and additional argument that analyst overconfidence is a factor in analytical accuracy, or, garbage in, garbage out. [97]

Finally, uncertainty in risk analysis is a subject with much published research. Uncertainty, not to be confused with stochastic variability, refers to many issues such as the knowledge of the analyst and his/her selection of model data, boundaries, and construction. [39] Thompson separates uncertainty from variability by explaining that sample variability will not disappear with measurement, but uncertainty will with adequate data collection that recognizes uncertainty and consideration of information value. [88] Recognizing this potential effect on analytical quality, Vose differentiates between first-order and second-order analysis; the former considers only variability, the latter accounts for effect of uncertainty. [96] The subject of uncertainty also includes

significant research on evaluating expert opinion as sources of analytical information. [5, 7, 23, 75, 94]

The limitations of analytical completeness, subjectivity, and uncertainty each emphasizes that risk analysis and risk management, traditionally focusing on outcomes and decisions, requires equal attention to the inputs and analyses that make such decisions possible.

2.0) System Safety Design and Analysis

Given analytical completeness as a limitation, system safety design and analysis requires multiple iterations and reviews to close potential omissions as much as is feasible. Haimes refers to these iterations in his description of hierarchical holographic modeling. [35] The term holographic describes the multifaceted nature of system risks and their necessary analyses, while the term hierarchical describes the process of viewing systems both from microscopic and macroscopic perspectives.

“The HHM philosophy is grounded on the premise that complex systems . . . should be studied and modeled in more than one way. Because such complexities cannot be adequately modeled or represented through a planar or single model or vision, overlapping of these visions is unavoidable. This can actually be helpful in providing a holistic appreciation of the interconnectedness among the various components, aspects, objectives, and decision-makers associated with a system.”

If performed to an appropriate level of detail, Haimes argues “the hierarchy would approach a ‘complete set’” of risk scenarios, exposures, and controls. Although not exhaustive, the perspectives of life cycle, functional, and configuration analysis in this section support design from a systems engineering perspective to discover and mitigate technical risks. (Fig. 4)

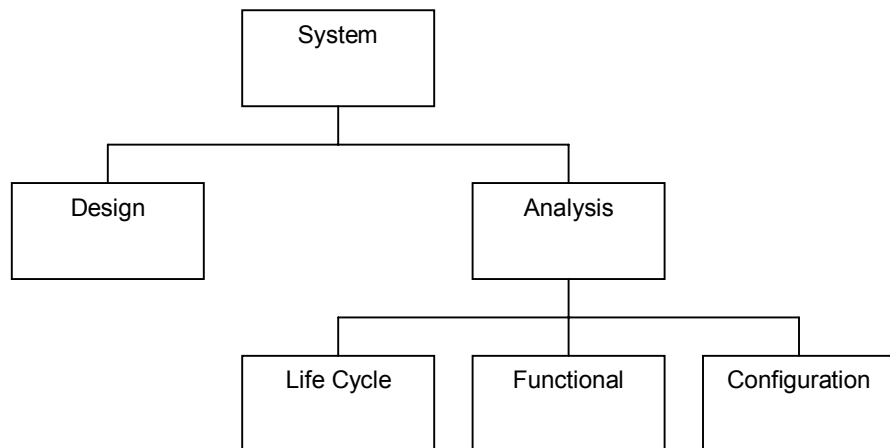


Fig. 4 System Design and Analysis for Technical Risk Reduction

These perspectives indicate a systematic framework meeting the letter and the intent of the INCOSE definition of a system: “an integrated set of elements . . . that accomplish a

defined objective.” In other words, both the design and analysis require logical integration similar to that of the system.

In his description of a systems approach to design and operation for safety, Hessami includes seven necessary principles: proactivity, prevention, protection, response, recovery, organizational learning, and continual enhancement. [40] Optimization of these principles poses a significant challenge to duty holders and decision-makers. Achieving these principles requires early attention at every level of the organization, and the life cycle, functional, and configuration analyses drive recognition and management of technical risks as a systems engineering activity with support from system safety and other engineering disciplines. Compartmentalization, according to Hessami, will degrade risk management and effective system engineering results:

“Safety and security are emergent properties of a product, service, process, system, or mission. Consideration of these important properties must be an integral aspect of decision making at all levels in any organization. Their attainment is not and should not be left as the sole prerogative of a specialist department. It is a matter of culture, nurtured and supported by organizational policies, making it everyone’s concern.”

Following discussions of design and analytical issues, the subject of culture will be revisited at the end of this section, demonstrating the role culture plays in inquiry and communication as a critical element of comprehensive technical risk management.

2.1) Design

In *MIL-STD-882D Standard Practice for System Safety*, design for system safety adopts a set of best practices to identify and reduce risks to levels acceptable to system managers while meeting system and mission objectives. Among these best practices the most important include a safety design hierarchy, safety design elements, and recognition of both acceptable and unacceptable conditions for system configuration.

The design hierarchy for system safety begins at the lowest possible hazard and is based on “expected effectiveness” in the final system. (Table 1) The first preference involves hazard elimination through design, which rules out hazard exposure, or the need for engineered safety systems or human response. As hazard elimination loses feasibility, need for intervention rises, and potential for hardware/software failures, human error, or both, increases.

With the hierarchy providing guidance, safety design requirements can bring more precision to hazard mitigation efforts. (Table 2) The requirements are general in nature, but can be incorporated into final system test and acceptance following reference to applicable codes or contracts, and defined in quantitative and measurable terms.

Finally, acceptable and unacceptable conditions provide further guidance for system design. (Table 3) Although optional depending on system mission and objectives, these conditions may be used to communicate upper and lower bounds for hazard acceptance and control.

Rank	Hazard Mitigation
1	Eliminate hazards through design selection
2	Incorporate safety devices
3	Provide warning devices
4	Develop procedures and training

Table 1 MIL-STD-882 System Safety Design Hierarchy

Requirement
Eliminate or reduce hazardous materials, or select based on minimal risk if necessary
Isolate hazardous materials or operations from operators or other operations
Locate equipment for operational and maintenance access with minimal exposure to hazards
Isolate energy sources through physical separation or shielding
Install safety devices where necessary; plan periodic functional tests
Define safe disposal procedures
Install warning signals; minimize probability of incorrect operator response
Install warning labels and instructions; standardize within system
Define safe operating procedures and operator training
Minimize severity/propagation in the event of system damage
Eliminate overly restrictive procedures that will be disregarded
Define change review/control procedures

Table 2 MIL-STD-882 System Safety Design Requirements

Acceptable	Unacceptable
Two or more independent failures or human errors for a non-safety critical function	Single component or common mode failure resulting in catastrophic or critical mishap
Three or more independent failures or human errors for a safety critical function	Dual independent failures resulting in catastrophic or critical mishap
Design for error prevention in assembly, installation, or connection	Generation of hazardous energy without protection of personnel or sensitive subsystems
Design for prevention of damage propagation from one component to another	Packaging or handling characteristics or procedures resulting in mishap
Design for limited operation, interaction, or sequencing leading to mishap	Hazard categories otherwise specified as unacceptable
Design for failure or fault tolerance; i.e., safety factor	
Design for failure or fault tolerance; i.e., alternate operating path(s) or safe energy release	
Design for limited or controlled use of hazardous materials	
Design for failure alerting and recovery	

Table 3 MIL-STD-882 Acceptable/Unacceptable Conditions

2.2) Life Cycle Analysis

System safety engineering is most effective when introduced at the earliest design stages, where safety elements can share equal consideration with other design elements, and analysis and verification can proceed during development. Roland and Moriarty describe this as “systematic, forward-looking identification and control of hazards throughout the life-cycle of a project, program, or activity.” [74] This statement integrates well into the concept of the life cycle in the *Systems Engineering Handbook*. Although design dominates the first three stages, the last stage is where the system realizes physical manifestation, and where hazards pose real versus theoretical threats. (Table 4)

Phase	Activity
0	Concept exploration
I	Program definition and risk reduction
II	Engineering and manufacturing development
III	Production, fielding/deployment, operational support, and retirement/disposal

Table 4 INCOSE Systems Engineering Process and Life Cycle Phases

The transition from design activities to physical realities emphasizes that just as the systems engineering process has a life cycle, so does the system being developed. Blanchard categorizes this as logistics engineering, including not just transportation and delivery, but also support functions such as maintenance: “logistics and the *design for supportability* must be inherent within early system design and development process if the results are to be cost-effective.” [8] Typically, front-end efforts such as research, design, acquisition, and production have higher visibility than downstream activities such as operations and support. However, the highest potential for reducing the downstream costs occurs at the earliest stages prior to freezing the requirements or building into the system, when changes may be too disruptive or cost-prohibitive. Blanchard identifies this as “total cost visibility” potentially effecting cost and performance, including safety-critical measures.

Life cycle analysis includes supportability considerations such as design for reliability, maintainability, and disposal. In terms of reliability and maintainability, systems will extend across time, requiring safe failure prevention or correction at the material, component, or subsystem level. [42, 89] Safe maintenance involves designing systems and procedures that do not cause damage during access, disassembly, or re-assembly. [55] Safe maintenance also involves design of systems and procedures that do not cause harm to maintenance personnel or other personnel in the immediate area. [33] Finally, as systems extend across time, they may also extend across space with reverse logistics for material return, service, or disposal. [30, 34]

2.3) Functional Analysis

At the earliest stages of the systems engineering process, functional analysis defines system tasks and activities that characterize system behavior. The objective of functional analysis, according to INCOSE, is to “provide the foundation for defining the system architecture through the allocation of functions and subfunctions to hardware/software and operations . . . functional analysis/allocation describes what the system will do, not

how it will do it.” Mar and Morais reinforce a similar argument that functional analysis is the beginning of the systems engineering process, driving requirements and the solutions or architectures that will be realized in the final system. [57]

Functional analysis may be conducted and presented in a number of forms, including control flow diagrams, data flow diagrams, state transition diagrams, and functional block diagrams. According to INCOSE, the specific format is less important than the complete identification and sequence of functions needed to satisfy system and mission objectives. In fact, multiple formats developed in parallel “allows for a ‘check and balance’ of the analysis process and will also aid in the communication across the system design team.” This recommendation echoes Haimes and hierarchical holographic modeling for multiple perspectives to adequately capture system functions and risks.

If functions characterize system objectives, then faults and failures characterize system risks. The opposite of functions, faults and failures are closely related and frequently used as synonyms in the engineering literature. A fault is defined as an anomaly or unacceptable variation in required functional operation, and a failure is defined as the inability to perform a function. [80] Given these definitions, Carson identifies fault analysis as a necessary compliment to functional analysis. [17] Recognition of functional performance deviations drives design changes to eliminate such risks, or addition of detection, compensation, and recovery systems to tolerate such risks. Finally, Carson argues that fault analysis performed in response to functional analysis drives analytical completeness: “the union of all possible conditions is the universal set . . . having defined responses for all conditions leaves nothing to chance.”

Rausand and Høyland have classified both functions and their deviations leading to faults and failures for reference and use in analysis. [69] (Table 5) Such failures may be used for state categories for Markov analysis to model possible system operating transitions. [68] The level of analytical detail is characterized both by system complexity and recognized risks, and analysis may range from “black-box” modeling accounting for two states (working/failed), or account for further state variables and details on components or sub-systems necessary for “white-box” modeling. [12] The *Systems Engineering Handbook* addresses this issue for both functional and fault/failure analysis as an element of tailoring:

“In establishing the stop criteria, recognize that the objective of pushing the decomposition to greater detail is to reduce the program risk. At some point, the incremental risk reduction becomes smaller than the cost in time or money of the effort to further decompose. Each program will be different, so it is impossible to set forth all-purpose stop criteria.”

Functions	Failures
Essential	Primary
Auxiliary	Secondary
Protective	Command
Information	Intermittent
Interface	Extended
Superfluous	Complete
On-line	Partial
Off-line	Sudden
	Gradual
	Catastrophic
	Degraded

Table 5 Functional and Failure Mode Categories

2.4) Configuration Analysis

As functional analysis reviews system behaviors and actions, configuration analysis reviews the architectural building blocks of the physical system. Haimes describes these elements as deeply interactive and each influencing the other. Their contributions and interfaces form the subjects for analysis of hardware, software, human, and organizational factors of technical risk. [35] (Fig. 5) Excluded from this relationship are socio-cultural factors such as location of high-risk operations in poor regions where decision-makers and other stakeholders are not affected by legal and physical consequences. [29]

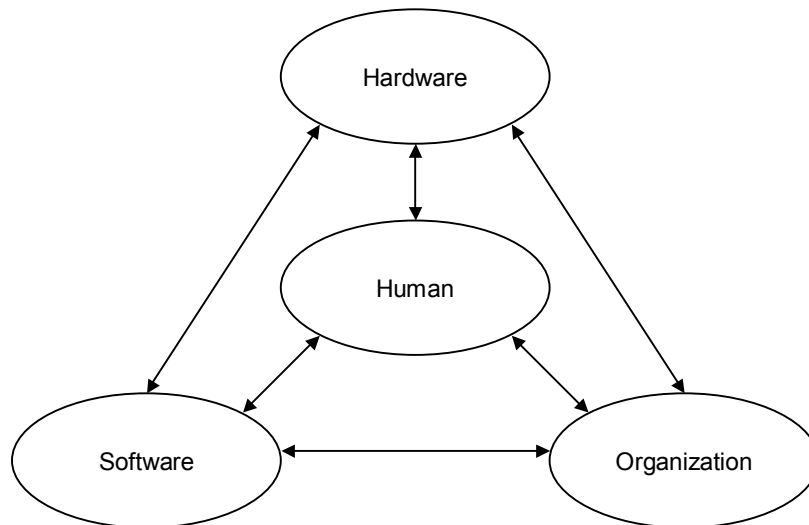


Fig. 5 System Elements [35]

2.4.1) Hardware

Hardware assemblies can be reviewed using strength/stress and physics of failure (POF) analyses that identify the physical processes and mechanisms of hardware breakdown. Blischke and Murthy identify deterioration as an underlying cause of physical failure, aggravated by manufacturing flaws, weaknesses in design, or aging, misuse, or mishandling. [12] Adding detail to the general concept of deterioration, Blischke and Murthy follow up with the specific failure mechanisms of overstress and wearout to provide further precision. (Table 6)

Overstress Failures	Wearout Failures
Brittle fracture	Wear
Ductile fracture	Corrosion
Yield	Dendritic growth
Buckling	Interdiffusion
Large elastic deformation	Fatigue crack propagation
Interfacial deadhesion	Diffusion
	Radiation
	Fatigue crack initiation
	Creep

Table 6 Physical Failure Mechanisms

Hardware failure prevention is closely related to maintainability, which is discussed in further detail in multiple sources. [8, 10, 26, 89, 98]

2.4.2) Software

Software, unlike hardware, is not subject to deterioration or other forms of physical wear, but its potential contributions to system risks are no less significant. Following partition of hardware versus software functions, the issue of control versus safety functions must be addressed. (Fig. 6) Kletz argues that safety-critical software systems should be independent of control software systems, and hard-wired where practical. [51] Multiple industry standards support this argument for safety, monitoring, and emergency shutdown systems. [2, 3, 47] However, this division is biased towards the process industries, where shutdown to a safe non-operating condition is feasible and can be designed into the system. [32] Other applications, such as aerospace, automotive, and medical systems may not permit such clear partitioning when loss of control and shutdown could represent a catastrophic scenario.

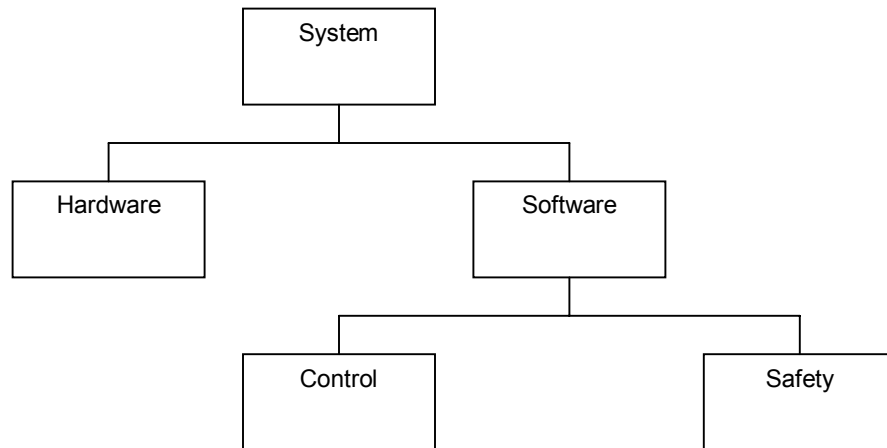


Fig. 6 Partitioning Illustration

In the hierarchy of safety devices, Dunn places software last: physical, mechanical, electromechanical power cutoff, analog/digital, and finally computer logic subsystem. [27] Reasons for this include reliability, potential errors in development, and potential difficulty of evaluation. One significant hazard involves latent faults that lie undetected until needed; this is known as a failure upon demand. Another hazard involves unexpected outputs following combinations not revealed during system validation; this represents a sneak circuit. Simpler is better. Given this, Dunn has classified software characteristics with greater potential for “fault-free” or “fault-burdened” operations. (Table 7)

“Fault-Free”	“Fault-Burdened”
Small	Large
Simple	Complex
Single CPU	Multiple CPUs
Discrete variables	Discrete and analog variables
“Soft” real-time operation	Real-time operation
No interrupts	Interrupts
Exhaustive testing possible	Exhaustive testing impossible

Table 7 Software Fault-Potential Characteristics

2.4.3) Human Factors

Human intervention plays a role in almost all systems, with exceptions such as orbital satellites and unmanned aircraft as examples if one excludes communication. The three primary considerations for human factors in systems include an environment that is survivable, ergonomic features for safe and effective physical interaction, and signals intelligible to the cognitive abilities of the intended operators. (Fig. 7) These considerations are derived from functional analysis, with emphasis per INCOSE on *interface*: “points of human interface may be thought of as the content and the location

(origin and destination) of information that may be conveyed between humans or between a human and a machine.”

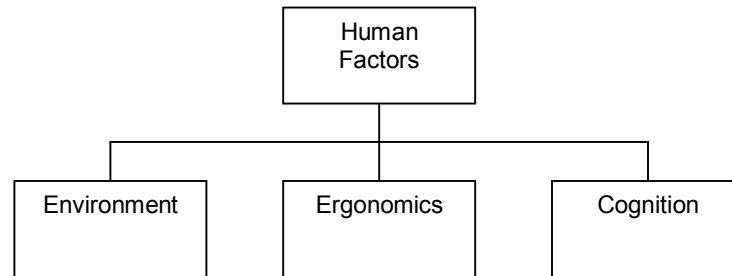


Fig. 7 Human Factors Considerations

Environmental considerations include elements such as breathable air and other life support requirements such as tolerable temperature ranges. There is some blur between environmental and ergonomic considerations, which are discussed below. The critical difference in this paper is that ergonomics covers active interaction such as manipulation of controls where both safety and effectiveness may be an issue, while environmental covers basic life support and survivability. In an aerospace application, cabin pressure and oxygen content is an environmental issue, while ease of operation is an ergonomic issue. In an industrial application, exhaust of toxic fumes is an environmental issue, while access to control buttons is an ergonomic issue.

Ergonomic considerations cover a wide range of sensory issues for the intended operators. Typically discussed in ergonomic references is the sense of touch and its effect on both operator and the system. Chapanis covers the human body and interaction with system operations with descriptions of dimensional requirements, static postures such as sitting and standing, active work such as maintenance and movement of controls, and relationship of strength/fatigue to work/rest cycles. [20] Aside from touch, sight and sound also play a role in human safety and performance. One issue is adequate light, control of noise, and design of signals for interpretation in these environments. Meister and Enderwick cover this subject of appropriate signal design, and potential for multiple interpretive pathways for unsanctioned use or response. [58]

Finally, design of interpretation and communication tasks calls for recognition of human cognitive abilities and limitations. Reason outlines a classification system for human performance issues including skill-based, rule-based, and knowledge-based errors. [70] Skill-based errors include inattention, omission following interruption, over-attention, and repetition. Rule-based errors include misapplication, information overload, and use of incorrect rule. Knowledge-based errors include bias, overconfidence, illusory correlation, and false causality. This classification provides system designers with tools for design of controls, tasks, instructions, training, and information exchange to prevent errors with harmful potential.

2.4.4) Organizational Factors

Human factors cover the domain of the individual, while organizational factors cover the working and reporting relationships established and sustained by management. There is much overlap between these subject areas, and each contributes to the other. [48]

Primary considerations for review of organizational factors include effects on conduct and analysis, with additional subcategories for each. (Fig. 8)

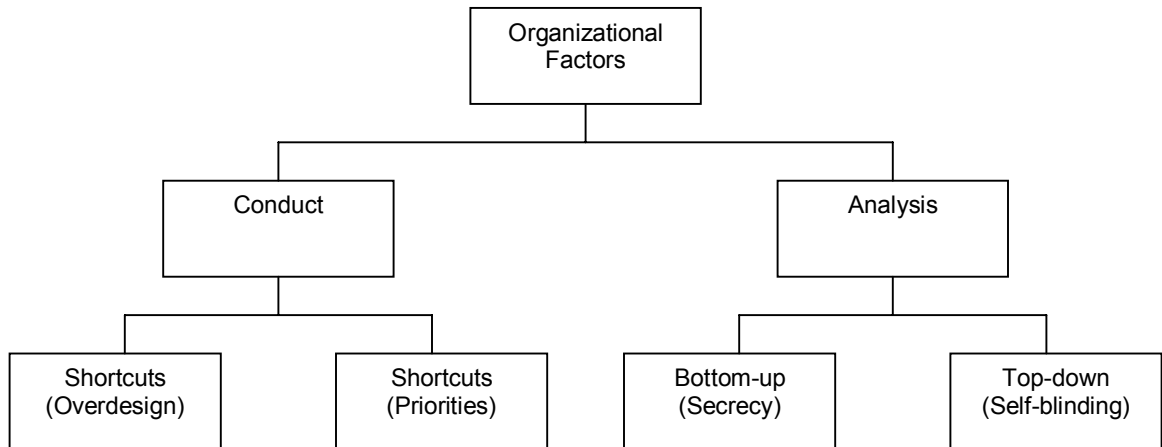


Fig. 8 Organizational Factors Considerations

Conduct within an organization is a product of the management system, which influences “values, attitudes and *patterns of behavior*.” [44, emphasis added] Conduct can be both designed into an operation, or influenced during ongoing operations. In terms of design, systems engineers can encourage safe operation with realistic task and response analysis. Reason cites overdesign as a strong factor in unsafe operation, when the bandwidth for “necessary” actions is wider than the scope of “permissible” actions. [71] From ignoring warnings and deviating from written procedures, to actively bypassing safety interlocks for maintenance access, overdesign may lead to hazardous shortcuts.

While systems engineers make design decisions effecting future conduct expected to occur following system start-up and operation, they have much less to do with management priorities influencing conduct during operation. Paté-Cornell outlines the organizational contributions to the individual and group behaviors within technical systems in her systems-actions-management (SAM) model. [63] Management policies, both written and implied, such as pay scales, time pressure, and internal competition for resources drive work practices that may undermine both human safety and technical performance. An observation during a case study on space shuttle maintenance revealed a significant problem with lean scheduling: “in one case, the bond [of the adhesive fastening heat-resistant tiles to the shuttle body] had been altered by an employee who had spit in the glue to make it cure faster.” Although ultimately a management responsibility, the systems engineer may have to anticipate self-serving individual response to unrealistic time or resource allocations.

Conduct during operation requires the forward-looking perspective of the systems engineer, but similar organizational dynamics during the design process may interfere with analytical integrity and directly influence the quality of the engineering results. In these cases, it is not the operator but the designer of the system who may be the victim of organizational factors, with potential influence on bottom-up flow of information or top-down reception of information. Both can significantly undermine system safety and effectiveness.

The bottom-up flow of information involves the behavior and communication of individual engineers or groups of engineers. Secrecy may inhibit appropriate flow of information, and may be either willful or unconscious. Rouhiainen and Soukas describe bias, preferred solutions, and strong personal identification with work products as sources of unconscious barriers to communication and analysis. An environment of peer review and supervisory controls provide constructive avenues for discovery and correction of design flaws: “it is essential that the appropriate level of authority is present . . . and that the analysis is carefully controlled to prevent the natural ‘ownership’ of the design from inhibiting a thorough, objective examination.” [76] Willful secrecy represents a far more malicious strain of bottom-up obstructionism. Davenport and Prusak cite information hoarding as a symptom of a dysfunctional organization: “employees may feel that their knowledge is critical to their unique value as an employee, and thus their continued tenure in the organization. Under these circumstances they may be reluctant to share that knowledge.” [25] An environment where knowledge sharing is rewarded more than knowledge hoarding is critical to preventing willful secrecy that may hide detection of system risks. “A genuinely open knowledge market will test official beliefs and expose the flaws of the faulty ones before they can do much damage.”

In addition to the bottom-up issues of secrecy and information hoarding, top-down signals from management may inhibit communication due to intolerance of non-conforming perspectives. Whether willful ignorance or unconscious reflection of organizational values, the result is a form of self-blinding that does not permit complete due diligence of risks. Managerial bias and pressures for a preferred outcome can influence both how information is received and how it is solicited. In terms of receipt of information, burden of proof may be skewed towards an unspoken but predetermined decision. In her case study of the analysis leading to the launch and loss of the space shuttle *Challenger*, Vaughan cited that “instead of proving that it was safe to fly, they had to prove it was unsafe.” [95] In terms of solicitation of information, the loss of the space shuttle *Columbia* provides an additional case study on managerial boundaries of acceptable analysis out of line with system risks. [22] Cabbage and Harwood interviewed NASA engineers describing “the flow of information as typically going from the top down, with managers above not always interested in having data flow up.” [15] The chair of the *Columbia* accident investigation panel, Hal Gehman, described a similar bottleneck:

“They say all the right things. ‘We have open doors and e-mails, and anybody who sees a problem can raise his hand, blow a whistle, and stop the whole process.’ But then when you look at how it really works, it’s an incestuous, hierarchical system, with invisible rankings and a very strict informal chain of command . . . if a person brings an issue up, what caste he’s in makes all the difference.” [56]

Such self-blinding may be active, as described in the social pressures above, or passive, as summarized in the exchange below between the *Columbia* accident investigation panel and Linda Ham, chair of the *Columbia* mission management team:

Panel: “As a manager, how do you seek out dissenting opinions?”

Ham: “Well, when I hear about them.”

Panel: “Linda, by their very nature you may not hear about them.”

Ham: “Well, when somebody comes forward and tells me about them.”

Panel: “But Linda, what techniques do you use to *get* them?” [56]

No answer followed the last question above, revealing an ineffective risk identification and management system. On this subject, Hillson describes a capability maturity assessment tool for rating both an organizational culture in terms of top-down risk inquiry and the bottom-up risk management work products of analysis, prioritization, and mitigation. [43, 46, 82] Based on the case studies and disasters above, NASA did not demonstrate advanced maturity on either top-down or bottom-up approach. This support for analysis and demand for analytical quality characteristic of a mature risk management organization is necessary for due diligence to defend system safety engineering resources and efforts appropriate for complex systems. This is directly related to the proposed metric in the next section.

3.0) Metrics

A metric is an established method of conducting and communicating a measurement of a system element. Metrics can be used to evaluate system performance against target criteria, and drive behaviors toward achieving conditions that satisfy these criteria. Kaydos emphasizes objective metrics, and provides examples for engineering environments such as design or process cycle time, mean time to failure, and defects per million. [50] According to Kaydos, one of largest challenges does not involve measuring data, but deciding which metrics qualify as *key performance factors*:

“While excellent performance is obviously desirable in all areas of a business, the KPFs define where it must be achieved, even at the expense of other performance factors. In many respects, the difficulty in determining a company’s key performance factors lies not in identifying things to measure, but in deciding what are the critical few items that will drive a company’s strategy and its success . . . determining key performance factors requires making choices and tradeoffs, because it is impossible to maximize everything. Making these choices is not easy, but it must be done. No company has the resources to be all things to all possible customers.”

This selection process for implementation of system metrics recalls the issue of tailoring methods against resources, risks, customer requirements, and organizational strategy.

3.1) Systems Engineering Metrics

The *Systems Engineering Handbook* does not directly address measurement of system elements other than cost and schedule. This is consistent with the program risk management emphasis of INCOSE previously discussed. Receiving the highest level of attention is earned value measurement system (EVMS), “an excellent project management tool,” along with brief descriptions of other control techniques such as run charts and control charts.

However, other metrics in the systems engineering community address the issue of capability and maturity. [14, 31] The CMMI-SE/SW capability maturity model and its EIA/IS-731.1 predecessor include scales with six levels for measurement of systems engineering effectiveness. The six levels, in ascending order of quality, start at the lowest level of zero and end at an optimal level of five. (Table 8) These levels, as observable and verifiable performance characteristics, provide the criteria for evaluation

of an organization structuring its systems engineering management program, developing quality improvement plans, or preparing for third-party audits.

Level	Capability	Description
0	Not performed	Not performed or performed without verifiable work products; no assurance of success
1	Performed	Informal; minimal planning/tracking; no assurance of process stability; dependence on individuals or “heroes;” verifiable work products
2	Managed	Defined by policy; planning and tracking; defects controlled and removed; key information managed
3	Defined	Standardized; formal change control; customer feedback reviewed; consistent program success
4	Quantitatively managed	Metrics and targets drive activity; performance can be quantitatively/statistically modeled and predicted
5	Optimizing	Quantitative improvements; cause/effect can be modeled and predicted; sub-functions/organizations tailored for optimal system performance

Table 8 CMMI-SE/SW Capability Maturity Levels

Nothing prohibits use of the CMMI-SE/SW capability maturity levels or related scaling systems specifically for risk management. As described above, Hillson has developed an assessment method for rating risk management capability and maturity. This scale has four levels instead of five, starting at the lowest level of one for “ad hoc” and ending at the highest level of four for “managed.” Each level describes increasing attention to risk management formality. However, the four levels do not directly translate to the six levels of CMMI-SE/SW. This problem raises the last two of the four classifications of uncertainty in risk analysis according to Rowe. [78] The first two classifications of temporality (i.e., past and forward states) and structure (i.e., complexity) do not apply. But the last two classifications of metrics (i.e., measurement) and translation (i.e., ability to explain and interpret) illustrate this misalignment with the four-level risk management capability maturity scale and the six-level CMMI-SE/SW model.

Others have developed models for measuring system safety and risk management effectiveness, but with similar misalignment issues. Bofinger et al. propose an extension of capability and maturity assessment for suppliers of safety-related systems, but do not provide scaling for side-by-side comparison with and translation to CMMI-SE/SW. [13] Caseley et al. propose measurement of more common resource impacts such time spent for analysis and improvement of safety processes. [18] Finally, Saad and Hsu integrate project risks with both program and business risks, but do not provide a scale for integration with CMMI-SE/SW. [79]

Given these scaling issues interfering with translation into systems engineering environments using the CMMI-SE/SW capability maturity model, the challenge of integrating system safety engineering into a systems engineering framework involves adequate measurement permitting consistent risk communication across disciplines. This challenge provides an opportunity for a metric that aligns the systems engineering and system safety engineering concepts of risk. The proposed metric involves a multidimensional scale for technological risk and reliability analysis that directly corresponds to the CMMI-SE/SW scale.

3.2) Measures for Risk

In its simplest form, risk analyses may take the form of hazard identification, worst-case scenarios, or estimates of probability and severity entered into a matrix. The MIL-STD-882D matrix provides an example of comparative probability and severity rankings and their associated values for prioritization. (Table 9) This is a standard risk management tool used with a number of variations. [21, 35]

Severity → Probability ↓	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Table 9 MIL-STD-882 Risk Assessment Matrix with Values

But the ubiquitous nature of this tool requires inquiry, each time it is used, on the underlying method used to arrive at each value. The values provide a quantitative output, but the analytical inputs may be from expert opinion or judgement, instead of objective measures such as historical or test data. Given this potential for uncontrolled, subjective, and potentially arbitrary input, Hessami dismisses the matrix as valuable for anything other than ranking and prioritization: “once regarded the state-of-the-art in pseudoquantified assessment, [matrices] are essentially outmoded and inapt for today’s complex systems and standards of best practice.” [41]

Criticism of the risk assessment matrix illustrates its nature as an output-based tool without regard to controlled or consistent input or process, where the analytical quality and precision is or is not driven. Theofanous argues that risk analysis should be approached as a research question, with a methodical frame of assessment for obtaining resolutions in a clear, consistent, and complete manner. [87] MIL-STD-882D suggests output values with standardized upper and lower bounds on severity and frequency values, but does not strictly define analytical quality or process. (Fig. 9)

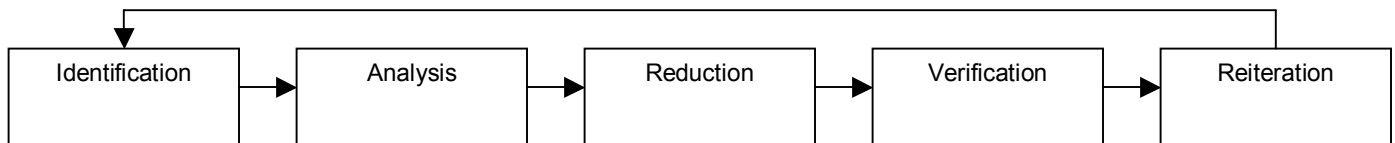


Fig. 9 MIL-STD-882 Risk Analysis Process

Absent a well-defined process and objectives, the analysis may be at higher risk of leading to inconclusive, erratic, or incorrect results, rendering the matrix irrelevant. “If the objectives and purpose are unclear, then the assessment will be unclear.” [6] A tighter definition of the analytical sequence provides a “formal groundwork” for repeatable conduct and traceable results. (Fig. 10) This formality draws from the WASH-1400 study on nuclear power safety. [93]

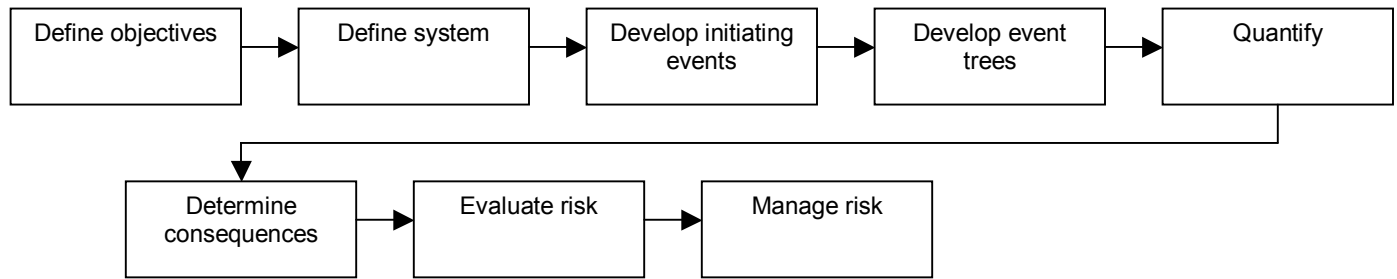


Fig. 10 Expanded Risk Analysis Process [6]

Soukas takes the issue of risk analysis as a process and adds four specific questions for ongoing evaluation of quality. [84] The questions include: have hazards been identified, have remedial measures been introduced, have risks been accurately estimated, and do analytical results correspond to resources? These questions, reiterated during the analytical process, provide a feedback loop for practitioners and managers to review quality and appropriateness for the system requirements and resources. (Fig. 11) Finally, Soukas describes in the strongest terms that quality of analytical input drives the validity of its output: “safety analysis resembles a production system having its own information and management systems. The indirect assessment of the quality of safety analysis is based on the assumption that the quality of an analysis depends on the adequacy of the process behind the analysis.”

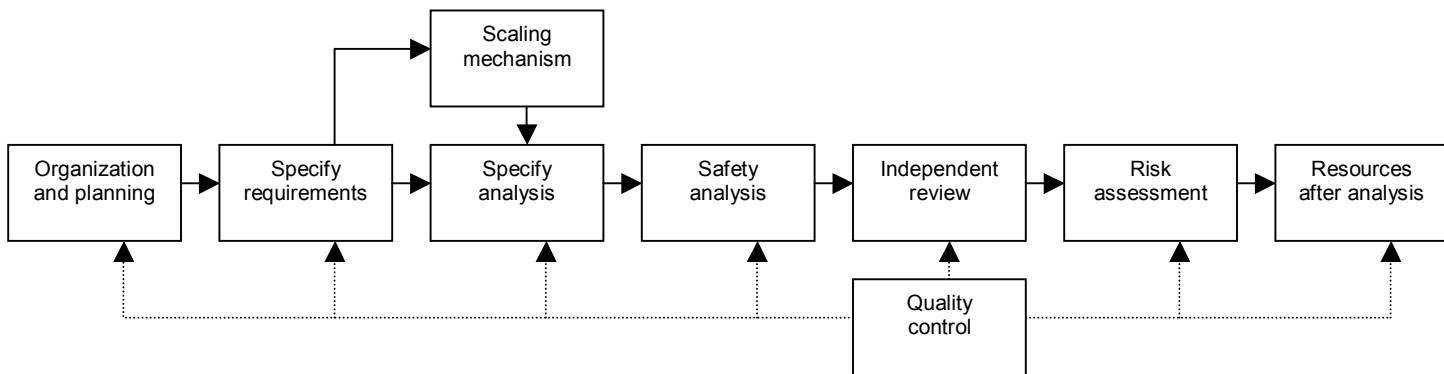


Fig. 11 Expanded Risk Analysis Process with Quality Control [84]

But process flows, even with quality control, do not by themselves permit translation to the CMMI-SE/SW capability maturity model. To meet the challenge of integrating risk analysis with capability maturity measures, the flow diagram must be converted to a scale. Paté-Cornell identifies six ascending levels of risk analysis, beginning at identification at the lowest level, and accounting for uncertainty at the highest level. [64] (Table 10) Inclusion of uncertainty (i.e., limited analyst knowledge) as it relates to variability (i.e., stochastic processes) provides a higher degree of confidence in the use of data. [96] Additionally, higher levels of quantification can generate documentation to begin system reliability predictions. [77]

Level	Description
1	Identification of hazard
2	Worst-case approach
3	Quasi-worst cases and plausible upper bounds
4	Best estimate; maximum credible probability or loss severity
5	First-order probabilistic risk analysis; mean probabilities or frequencies
6	Second-order probabilistic risk analysis; inclusion of risk uncertainties

Table 10 Six Levels of Risk Analysis [64]

Paté-Cornell's six levels do not directly correspond to the six capability maturity levels of CMMI-SE/SW, but they are close enough in number and ascending levels of precision to begin a metric that aligns system safety engineering within a systems engineering context. (Table 11)

Level	Capability	Description
0	Not performed	Not performed or performed without verifiable work products; unsystematic hazard identification
1	Performed	Informal, partially documented hazard identification up to worst-case scenario
2	Managed	Formal, documented hazard identification method up to worst-credible scenario
3	Defined	Standardized, consistent hazard identification method to maximum-credible probability or loss severity
4	Quantitatively managed	Risk modeling method to include first-order probabilistic analysis; probability density functions to include likelihood/severity
5	Optimizing	Advanced risk modeling to include second-order probabilistic analysis; probability density functions to include uncertainties

Table 11 Risk Analysis Maturity Measures

3.3) Measures for Reliability

Risk implies a *negative* or unwanted outcome, and the probability and severity ratings of the MIL-STD-882D risk assessment matrix adopt this perspective. (Table 9) Reliability, on the other hand, implies a *positive* or wanted outcome. Its definition as the probability of specified performance over a specified time frame reinforces this positive connotation. [11] In terms of reliability as related to safety, the IEC 61508 standard uses specified performance criteria for rating elements with significant impact on system safety. (Table 12)

Level	P (Dangerous Failure / Year)	P (Failure / Demand)
1	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-5}$ to $< 10^{-4}$
2	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-4}$ to $< 10^{-3}$
3	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-3}$ to $< 10^{-2}$
4	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-2}$ to $< 10^{-1}$

Table 12 IEC 61508 Safety Integrity Levels [47]

Although the IEC 61508 scale is ordinal like the CMMI-SE/SW capability maturity levels, direct conversion to six levels for use in a multidimensional scale integrating risk and reliability analysis is not appropriate. Like the MIL-STD-882D risk assessment matrix, the levels reflect output instead of process.

Reliability predictions are important factors for system development, acquisition, and operation. For systems engineers, reliability drives life cycle plans, from preventative and corrective maintenance to system retirement determination. For system safety engineers, reliability drives failure detection, isolation, and compensation plans. Metrics such as the IEC 61508 levels are critical drivers for system requirements, design, test, and acceptance. However, reliability predictions, whether derived from tests, models, handbooks, randomized samples, non-random observations, vendor claims, subjective expert opinion, or other sources must be viewed with scrutiny. [62] Chan and Tortorella advise that reliability predictions should be provided consistently, systematically, accurately, and precisely. [19] The first two are standardized, but the latter two may be suspect: “information usually does not include the details of the experiments or data analyses that led to the published parameter estimates.” Given this, a reliability analysis scale based on process instead of output will provide a range consistent with the risk analysis maturity measures.

Michaels describes a product maturity scale that combines both output and process. [59] Nouns such as “first-article,” “prototype,” and “design” cover physical or functional outputs instead of the quantitative predictions of IEC 61508, while phrases such as “validated by analysis” cover processes. (Table 13)

Risk Multiplier	Event
0.0	Similar production first-article product tested successfully
0.1	Similar production first-article product produced
0.2	Similar prototype tested successfully
0.3	Similar prototype fabricated
0.4	Similar brassboard tested successfully
0.5	Similar brassboard fabricated
0.6	Similar breadboard tested successfully
0.7	Similar breadboard fabricated
0.8	Similar functional design completed
0.9	Similar functional design validated by analysis
1.0	Similar functional design not validated by analysis

Table 13 Product Maturity Scale [59]

The combined output and process scale of Michaels illustrates that just as system development follows a standard path from design to construction, so do various analytical and test activities. Blischke and Murthy concur in their review of the need for structured data collection required to successfully present valid reliability predictions. [11] This is acknowledged in the MIL-STD-781D and MIL-STD-785B standards for system reliability engineering. [90, 91] Both standards outline this development flow with the added quality element of a closed-loop failure reporting, analysis, and corrective action system (FRACAS). (Fig. 12)

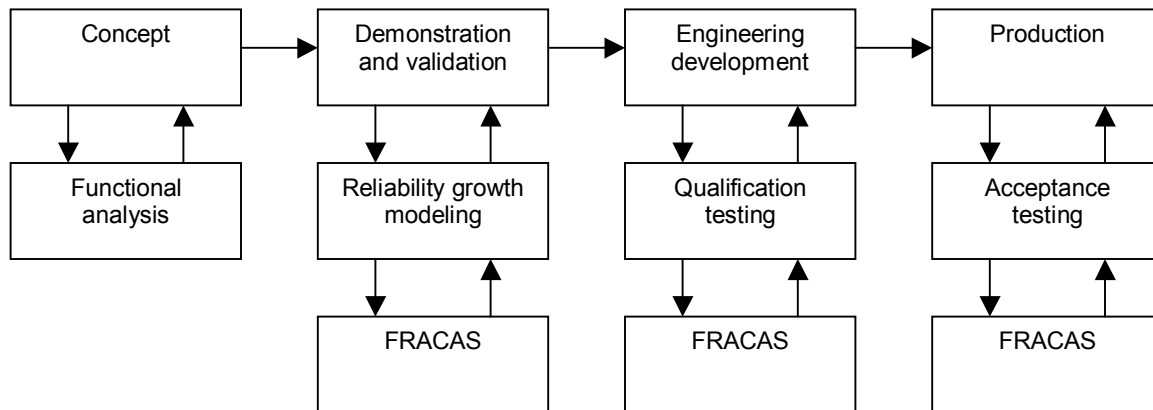


Fig. 12 MIL-STD-781D and MIL-STD-785B Reliability Engineering Process

Adopting this process and the logic of the risk analysis maturity measures, a scale for reliability analysis can be framed for integration with CMMI-SE/SW capability maturity modeling. (Table 14)

Level	Capability	Description
0	Not performed	Not performed or performed without verifiable work products; unsystematic reliability analysis/prediction
1	Performed	Informal, partially documented reliability analysis/prediction
2	Managed	Formal, documented reliability analysis/prediction
3	Defined	Standardized, consistent reliability analysis/prediction; formal change management with controlled system/analysis revisions
4	Quantitatively managed	Reliability modeling method to include first-order probabilistic analysis; probability density functions for survival predictions
5	Optimizing	Advanced reliability modeling to include second-order probabilistic analysis; probability density functions to include uncertainties

Table 14 Reliability Analysis Maturity Measures

3.4) Integrated Measures for Risk and Reliability Analysis

By themselves the risk analysis and reliability analysis maturity measures may not add significant value to systems engineering activities beyond other measures already discussed. It is their shared number of levels, consistent with the CMMI-SE/SW maturity model, which permit location without conversion on a two-level multidimensional scale, representing relative distance for comparison of analytical processes and outputs within the life-cycle stages of a system. (Fig. 13) The placement at relative distances, known as perceptual mapping, permits this comparison on the same unit of measure. [36] Geometric representation of risk is not new, as the MIL-STD-882D risk assessment matrix of probability and severity demonstrates. Jones describes other configurations using probability and severity, such as coordinate and quadrant maps. [49] What the scale below permits is representation and communication of both dimensions of maturity for risk and reliability analysis within a CMMI-SE/SW context.

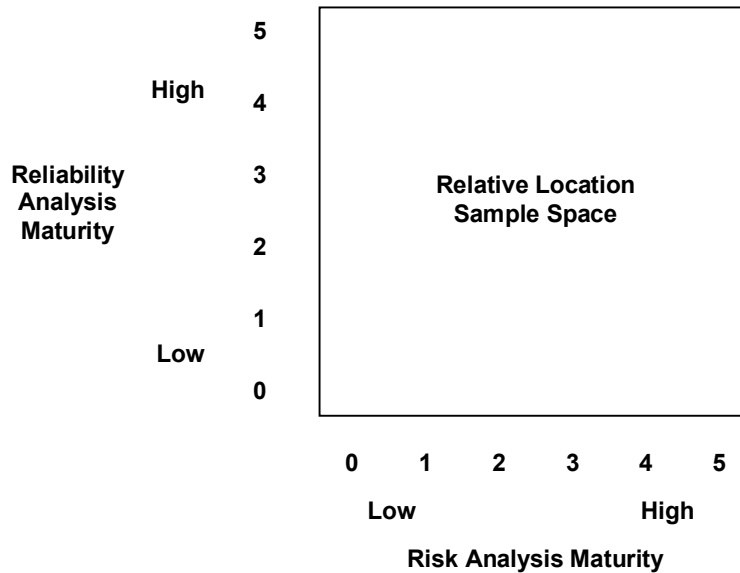


Fig. 13 Multidimensional Maturity Scale for Technical Risk and Reliability Analysis

Although not explicitly divided into quadrants, relative locations at high and/or low ratings indicate degrees of technical risk that may influence system safety. Additionally, the consequences of technical risk may not only affect system performance, but also system cost and schedule. A summary of possible high versus low combinations illustrates the effect of maturity levels on performance and technical risk potential. (Table 15)

Risk	Reliability	Summary
High	High	Very mature process; established system development with corresponding analysis of technical risks and prediction of reliability ranges
High	Low	Immature process; risk analyses occurring with incomplete data on system reliability, but acknowledgement of uncertainty may inform decisions
Low	High	Immature process; reliability analyses occurring with incomplete data on system safety and failure consequences
Low	Low	Very immature process; incomplete risk and reliability analyses; safety and reliability functions/organizations performing below mature capabilities

Table 15 Relative Risk and Reliability Analysis Maturity Levels

The relative levels of the multidimensional maturity scale can contribute to the systems engineering process in a number of ways. First, the systems engineer can use the levels to initiate and communicate the scope of work at a targeted capability maturity level. This can be tailored as appropriate for the organization and the system under development, with risk and reliability resources balanced to prevent sub-optimization or appearance of favoritism. Second, the systems engineer can review progress and work products during the development life cycle to verify safety and reliability teams have not drifted from each other in terms of parallel pacing or cooperative positions. In the event of mismatched levels, resolution through realignment can return the teams to a shared vision of system development and risk management. Finally, the systems engineer communicating, reviewing, and verifying capability maturity levels of safety and reliability teams will have higher assurance of a safe and successful system than one treating either or both engineering domains as secondary concerns.

4.0) Conclusion

Given the scope of this project was to conduct the research to complete a system safety engineering course, drawing from systems engineering references and related academic/professional activities, the concluding section of this paper includes an outline for development of an elective for future students. Students would approach such a course with a prior background and undergraduate education in engineering, followed by the introductory course in systems engineering approach, to add to their portfolio of requirements and electives. (Fig. 14) The purpose of the course would be to develop technical risk analysis and management skills within a systems engineering context.

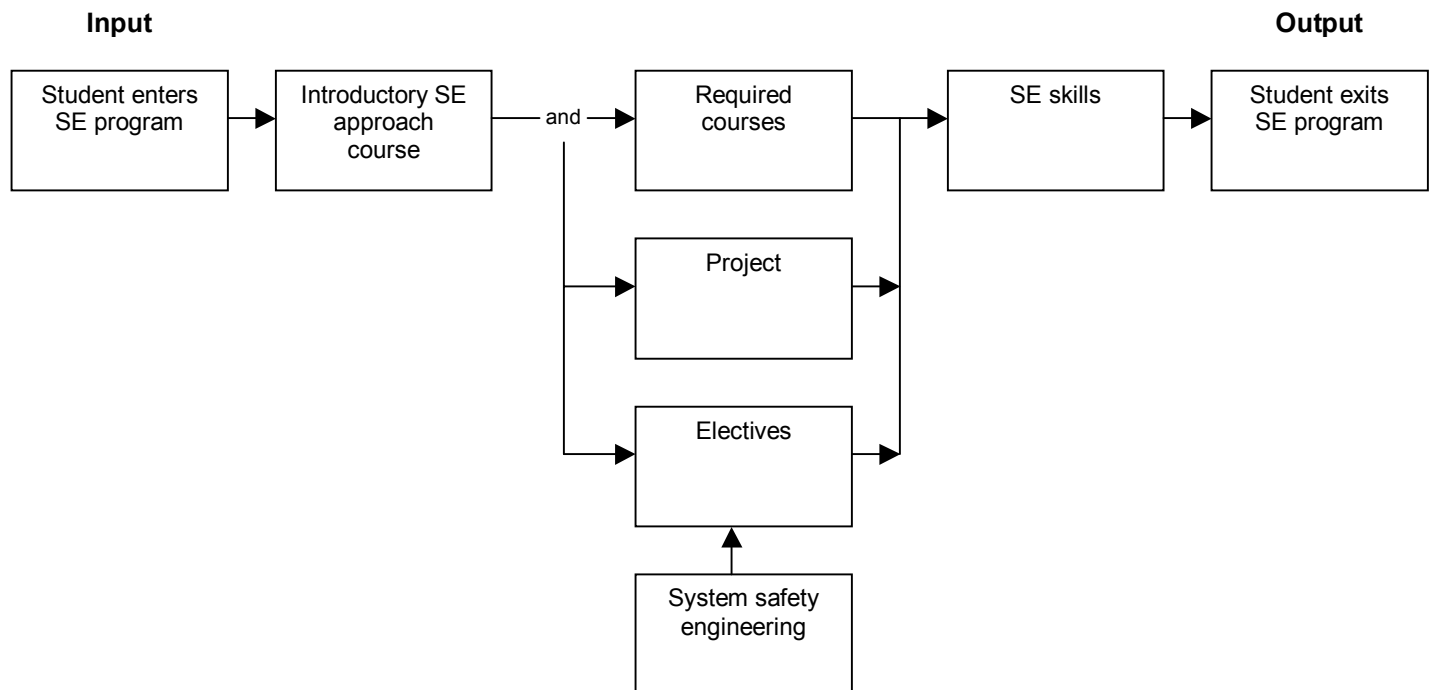


Fig. 14 Systems Engineering Study Path with System Safety Engineering

The course contents either presented in the form of a traditional class or through internet delivery would draw from materials and references in this paper. (Table 16) Reading assignments from the five selected texts would provide the foundation for assignments and tests to evaluate student performance. The five texts include one book that would have to be purchased, and four soft copies available from the internet. Blischke's and Murthy's *Reliability: Modeling, Prediction, and Optimization* is the one book, selected for its discussion of both safety and reliability, and its additional statistical materials allowing for future use as a reference. [12] Readings from the *Systems Engineering Handbook* can be provided to the students at no charge pending approval from INCOSE, or purchased for a fee. [45] All three of the final texts, Clemmons's and Simmons's *System Safety and Risk Management: A Guide for Engineering Educators*, *MIL-STD-882D Standard Practice for System Safety*, and the CMMI – SE/SW capability maturity model are available at no cost for download from the internet. [21, 92, 14]

Week	Presentation Subject(s)	Reading(s)
1	Risk management and the SE process; tailoring; technical risk	INCOSE pp. 9-19, 61-77, 107-112, 163-165
2	Risk and the system life cycle	Clemmons and Simmons chapter I ; Blischke and Murthy pp. 19-24
3	Design for system safety	MIL-STD-882D
4	System safety analysis part 1; hardware and software factors	Blischke and Murthy pp. 169-175, 287-299
5	System safety analysis part 2; human and organization factors	INCOSE pp. 197-216, 79-98
6	Functional and fault analysis	Blischke and Murthy pp. 12-18; INCOSE pp. 123-138
7	Fault tree analysis; failure modes and effects analysis	Blischke and Murthy pp. 201-219, Clemmons and Simmons chapters VI and VII
8	Risk analysis	Clemmons and Simmons chapters II and III
9	Reliability analysis	Blischke and Murthy pp. 467-488, 511-534
10	Management of risk and reliability analysis; capability maturity modeling	Blischke and Murthy pp. 427-459; CMMI – SE/SW pp. 11-20, 33-54

Table 16 Sample System Safety Engineering Course Content

Of the many risks that can threaten a system, the technical elements of safety and performance can directly influence the program or project elements of cost and schedule. Additionally, failure propagation such as fire, physical breakdown, loss of control, or compounding human error can bring significant harm to the system and its operators. The specialty domains of system safety and reliability engineering provide methods to review and correct these risks. However, it is the system safety engineer who has responsibility to integrate these concerns for the development of a safe and effective system. Integration of organizational as well as technical concerns prevents the compartmentalization that permits isolated specialists to say “not my problem:”

“Most engineers are employed and conditioned to work in large organizations where division of labor also results in division of responsibility . . . if assigned to act on safety, engineers will do so. If not, they might consider it a waste of their organization’s time to busy themselves with matters outside their immediate sphere of operation.” [81]

In the traditional business or government organization, tension and disconnection exists where the technical personnel conducting analyses and the managers making decisions may not share educational or professional backgrounds; “success or failure (of risk decisions) rests upon the adequacy of communication.” [61] The strength of the systems engineering environment relative to traditional organizations is the integration of technical concerns for professional conduct that drives top-down communication of functions and requirements, with congruent demand for bottom-up communication of analytical results. A multidimensional maturity scale for technical risk and reliability analysis permits this top-down and bottom-up risk communication in a framework consistent with CMMI – SE/SW capability maturity modeling.

References

- [1] Abadi, C.D., and Bahill, T., "The Difficulty in Distinguishing Product from Process," *Systems Engineering*, vol. 6, no. 2, pp. 106 – 115, 2003.
- [2] American Institute of Chemical Engineers, *Guidelines for Safe Automation of Chemical Processes*, New York, NY: AIChE, 1993
- [3] American National Standards Institute, *ANSI/ISA S84.01-1996 Application of Safety Instrumented Systems for the Process Industries*, Washington, DC: ANSI, 1996.
- [4] Anderson, R., *Security Engineering: A Guide to Building Dependable Distributed Systems*, New York, NY: Wiley, 2001.
- [5] Ayyub, B.M., *Elicitation of Expert Opinions for Uncertainty and Risks*, Boca Raton, FL: CRC Press, 2001.
- [6] Bahr, N.J., *System Safety Engineering and Risk Assessment: A Practical Approach*, Washington, DC: Taylor & Francis, 1997.
- [7] Bedford, T., and Cooke, R., *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge, UK: Cambridge, 2001.
- [8] Blanchard, B.S., *Logistics Engineering and Management*, 5th ed., Upper Saddle River, NJ: Prentice Hall, 1998.
- [9] Blanchard, B.S., and Fabrycky, W.J., *Systems Engineering and Analysis*, 3rd ed., Upper Saddle River, NJ: Prentice Hall, 1998.
- [10] Blanchard, B.S., Verma, D., and Peterson, E.L., *Maintainability: A Key to Effective Serviceability and Maintenance Management*, New York, NY: Wiley, 1995.
- [11] Blischke, W.R., and Murthy, D.N.P., "Introduction and Overview," *Case Studies in Reliability and Maintenance*, W.R. Blischke and D.N.P. Murthy, Ed., Hoboken, NJ: Wiley, 2003.
- [12] Blischke, W.R., and Murthy, D.N.P., *Reliability: Modeling, Prediction, and Optimization*, New York, NY: Wiley, 2000.
- [13] Bofinger, M., Robinson, N., Lindsay, P., Spiers, M., Ashford, M., and Pitman, A., "Experience with Extending CMMISM for Safety Related Applications," International Council on Systems Engineering, 12th Annual Symposium, Las Vegas, NV, July 28 – August 1, 2002.
- [14] CMMI Product Team, *Capability Maturity Model Integration (CMMISM), Version 1.1 CMMISM for Systems Engineering and Software Engineering (CMMI – SE/SW, V.1.1) Continuous Representation*, Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute, 2001.

- [15] Cabbage, M., and Harwood, W., *Comm Check . . . The Final Flight of Shuttle Columbia*, New York, NY: Free Press, 2004.
- [16] Calvano, C.N., and John, P., "Systems Engineering in an Age of Complexity," *Systems Engineering*, vol. 7, no. 1, pp. 25 – 34, 2004.
- [17] Carson, R., "Fault Analysis for Systems Engineers," International Council on Systems Engineering, 12th Annual Symposium, Las Vegas, NV, July 28 – August 1, 2002.
- [18] Caseley, P., Clark, G., Murdoch, J., and Powell, A., "Measurement of System Safety Processes," International Council on Systems Engineering, 13th Annual Symposium, Arlington, VA, June 29 – July 3, 2003.
- [19] Chan, C.K., and Tortorella, M., "Confidence Intervals for Hardware Reliability Predictions," *Case Studies in Reliability and Maintenance*, W.R. Blischke and D.N.P. Murthy, Ed., Hoboken, NJ: Wiley, 2003.
- [20] Chapanis, A., *Human Factors in Systems Engineering*, New York, NY: Wiley, 1996.
- [21] Clemens, P.L., and Simmons, R.J., *System Safety and Risk Management: A Guide for Engineering Educators*, Cincinnati, OH: U.S. Department of Health and Human Services, 1998.
- [22] Columbia Accident Investigation Board, *Report Volume I: August 2003*, accessed online 4 June 2004 at www.nasa.gov/columbia/home/index.html.
- [23] Cooke, R.M., *Experts in Uncertainty: Opinion and Subjective Probability in Science*, Oxford, UK: Oxford University Press, 1991.
- [24] Cox, S.J., and Tait, N.R.S., *Reliability, Safety and Risk Management: An Integrated Approach*, Oxford, UK: Butterworth-Heinemann, 1991.
- [25] Davenport, T.H., and Prusak, L., *Working Knowledge: How Organizations Manage What They Know*, Boston, MA: Harvard, 1998.
- [26] Dhillon, B.S., *Engineering Maintainability: How to Design for Reliability and Easy Maintenance*, Houston, TX: Gulf, 1999.
- [27] Dunn, W.R., *Practical Design of Safety-Critical Computer Systems*, Solvang, CA: Reliability Press, 2002.
- [28] Dvir, D., Shenhar, A.J., and Alkahr, S., "From a Single Discipline Product to a Multidisciplinary System: Adapting the Right Style to the Right Project," *Systems Engineering*, vol. 6, no. 3, pp. 123 – 134, 2003.
- [29] Evan, W.M., and Manion, M., *Minding the Machines: Preventing Technological Disasters*, Upper Saddle River, NJ: Prentice Hall, 2002.

- [30] Fleischmann, M, *Quantitative Models for Reverse Logistics*, Berlin, Germany: Springer, 2001.
- [31] Government Electronics and Information Technology Association, *EIA/IS-731.1 Systems Engineering Capability Model*, Washington, DC: GEIA, 2001.
- [32] Gruhn, P., and Cheddie, H., *Safety Shutdown Systems: Design, Analysis, and Justification*, Research Triangle Park, NC: ISA, 1998.
- [33] Gunderson, S., "Establishing and Auditing Measures for Hazardous Energy Isolation," *Journal of System Safety*, vol. 40, no. 2, pp. 11 – 13, 2004.
- [34] Gunderson, S., "Return to Sender: System Maintenance, Reverse Logistics, and Hazardous Materials Transportation," *Journal of System Safety*, vol. 40, no. 4, 2004 accessed online 10 August 2004 at www.system-safety.org/index.htm.
- [35] Haimes, Y.Y., *Risk Modeling, Assessment, and Management*, 2nd ed., Hoboken, NJ: Wiley, 2004.
- [36] Hair, J.F., Anderson, R.E., Tatham, R.L., and Black, W.C., *Multivariate Data Analysis*, 5th ed., Upper Saddle River, NJ: Prentice Hall, 1998.
- [37] Head, G.L., *Essentials of Risk Control, Volume II*, 3rd ed., Malvern, PA: Insurance Institute of America, 1995.
- [38] Head, G.L., and Horn, S., *Essentials of Risk Management, Volume I*, 3rd ed., Malvern, PA: Insurance Institute of America, 1997.
- [39] Helton, J.C., "Treatment of Uncertainty in Performance Assessments for Complex Systems," *Risk Analysis*, vol. 14, no. 4, pp. 483 – 511, 1994.
- [40] Hessami, A.G., "A Systems Framework for Safety and Security: The Holistic Paradigm," *Systems Engineering*, vol. 7, no. 2, pp. 99 – 112, 2004.
- [41] Hessami, A.G., "Risk Management: A Systems Paradigm," *Systems Engineering*, vol. 2, no. 3, pp. 156 – 167, 1999.
- [42] Hill, R.S., and Nutt, M.W., "Risk Informed Design for System Life Cycle," International Council on Systems Engineering, 13th Annual Symposium, Arlington, VA, June 29 – July 3, 2003.
- [43] Hillson, D.A., "Towards a Risk Maturity Model," *The International Journal of Project and Business Risk Management*, vol. 1, no. 1, pp. 35 – 45, 1997.
- [44] Hurst, N.W., *Risk Assessment: The Human Dimension*, Cambridge, UK: Royal Society of Chemistry, 1998.
- [45] International Council on Systems Engineering, *Systems Engineering Handbook Version 2a*, Seattle, WA: INCOSE, 2004.

- [46] International Council on Systems Engineering Risk Management Working Group, et al., *Risk Management Maturity Level Model, RMRP-2002-02, Version 1.0*, Seattle, WA: INCOSE, 2002.
- [47] International Electrotechnical Commission, *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, Geneva, Switzerland: IEC, 1998.
- [48] Jackson, S., "Organizational Safety: A Systems Engineering Perspective," International Council on Systems Engineering, 12th Annual Symposium, Las Vegas, NV, July 28 – August 1, 2002.
- [49] Jones, R.B., *Risk-Based Management: A Reliability-Centered Approach*, Houston, TX: Gulf, 1995.
- [50] Kaydos, W., *Operational Performance Measurement: Increasing Total Productivity*, Boca Raton, FL: St. Lucie Press, 1999.
- [51] Kletz, T.A., *Computer Control and Human Error*, Houston, TX: Gulf, 1995.
- [52] Kujawski, E., "Selection of Technical Risk Responses for Efficient Contingencies," *Systems Engineering*, vol. 5, no. 3, pp. 194 – 212, 2002.
- [53] Kujawski, E., "Why Projects Often Fail, Even with High Cost-Contingencies," *Systems Engineering*, vol. 5, no. 2, pp. 151 – 155, 2002.
- [54] Kumamoto, H., and Henley, E.J., *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed., New York, NY: IEEE Press, 1996.
- [55] Kumar, U.D., and Crocker, J., "Maintainability and Maintenance – A Case Study on Mission Critical Aircraft and Engine Components," *Case Studies in Reliability and Maintenance*, W.R. Blischke and D.N.P. Murthy, Ed., Hoboken, NJ: Wiley, 2003.
- [56] Langewiesche, W., "Columbia's Last Flight: The Inside Story of the Investigation – and the Catastrophe it Laid Bare," *The Atlantic Monthly*, vol. 292, no. 4, pp. 58 – 87, 2003.
- [57] Mar, B.W., and Morais, B.G., "FRAT – A Basic Framework for Systems Engineering," International Council on Systems Engineering, 12th Annual Symposium, Las Vegas, NV, July 28 – August 1, 2002.
- [58] Meister, D., and Enderwick, T.P., *Human Factors in System Design, Development, and Testing*, Mahwah, NJ: Lawrence Erlbaum, 2002.
- [59] Michaels, J.V., *Technical Risk Management*, Upper Saddle River, NJ: Prentice Hall, 1996.
- [60] Molak, V., "Introduction and Overview," *Fundamentals of Risk Analysis and Risk Management*, V. Molak, Ed., Boca Raton, FL: CRC Press, 1997.

- [61] Morison, R., and Anderson, J.J., "Risk Assessment – Risk Management: The Need for a Synthesis," *The Analysis, Communication, and Perception of Risk*, B.J. Garrik and W.C. Gekler, Ed., New York, NY: Plenum Press, 1991.
- [62] O'Connor, P.T., *Practical Reliability Engineering*, 4th ed., West Sussex, UK: Wiley, 2002.
- [63] Paté-Cornell, E., "Finding and Fixing Systems Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis," *Risk Analysis*, vol. 22, no. 2, pp. 319 – 334, 2002.
- [64] Paté-Cornell, M. E., "Uncertainties in risk analysis: Six levels of treatment," *Reliability Engineering and System Safety*, vol. 54, no. 2 – 3, pp. 95 – 111, 1996.
- [65] Pennock, M.J., and Haimes, Y.Y., "Principles and Guidelines for Project Risk Management," *Systems Engineering*, vol. 5, no. 2, pp. 89 – 108, 2002.
- [66] Perrow, C., *Normal Accidents: Living with High-Risk Technologies*, Princeton, NJ: Princeton University Press, 1999.
- [67] Petroski, H., *To Engineer is Human: The Role of Failure in Successful Design*, New York, NY: Vintage, 1992.
- [68] Pukite, J., and Pukite, P., *Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety, and Supportability Analyses of Complex Computer Systems*, New York, NY: IEEE Press, 1998.
- [69] Rausand, M., and Høyland, A., *System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd ed., Hoboken, NJ: Wiley, 2004.
- [70] Reason, J., *Human Error*, Cambridge, UK: Cambridge, 1990.
- [71] Reason, J., *Managing the Risks of Organizational Accidents*, Aldershot, UK: Ashgate, 1997.
- [72] Redmill, F., "Risk Analysis – A Subjective Process," *Journal of System Safety*, vol. 39, no. 2, 2003, accessed online 30 April 2004 at www.system-safety.org/index.htm.
- [73] Redmill, F., "Subjectivity in Hazard Analysis," *Journal of System Safety*, vol. 40, no. 1, 2004, accessed online 30 April 2004 at www.system-safety.org/index.htm.
- [74] Roland, H.E., and Moriarty, B., *System Safety Engineering and Management*, 2nd ed., New York, NY: Wiley, 1990.
- [75] Rosqvist, T., "Bayesian aggregation of experts' judgements on failure intensity," *Reliability Engineering and System Safety*, vol. 70, no. 3, pp. 283 – 289, 2000.

- [76] Rouhiainen, V., and Soukas, J., "Performance of the Analysis," *Quality and Management of Safety and Risk Analysis*, J. Soukas and V. Rouhiainen, Ed., Amsterdam, Netherlands: Elsevier, 1993.
- [77] Rouvroye, J.L., and van den Bliet, E.G., "Comparing safety analysis techniques," *Reliability Engineering and System Safety*, vol. 75, no. 3, pp. 289 – 294, 2002.
- [78] Rowe, W.D., "Understanding Uncertainty," *Risk Analysis*, vol. 14, no. 5, pp. 743 – 750, 1994.
- [79] Saad, J., Hsu, J.C., "An Integrated Risk Management Process," International Council on Systems Engineering, 13th Annual Symposium, Arlington, VA, June 29 – July 3, 2003.
- [80] SAE International, *ARP 5580 Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications*, Warrendale, PA: SAE International, 2001.
- [81] Schinzinger, R., "Technological Hazards and the Engineer," *Ethics and Risk Management in Engineering*, A. Flores, Ed., Lanham, MD: University Press, 1989.
- [82] Shoultz, J., "Risk Management Capability Maturity Quantitative Assessment Tool," Council on Systems Engineering, 13th Annual Symposium, Arlington, VA, June 29 – July 3, 2003.
- [83] Smith, D.J., *Reliability, Maintainability, and Risk: Practical Methods for Engineers*, 6th ed., Oxford, UK: Butterworth Heinemann, 2001.
- [84] Soukas, J., "Quality of Safety Analysis," *Quality and Management of Safety and Risk Analysis*, J. Soukas and V. Rouhiainen, Ed., Amsterdam, Netherlands: Elsevier, 1993.
- [85] Sproles, N., "Formulating Measures of Effectiveness," *Systems Engineering*, vol. 5, no. 4, pp. 253 – 263, 2002.
- [86] Stephens, R.A., and Talso, W.W., Ed., *System Safety Analysis Handbook*, 2nd ed., Albuquerque, NM: New Mexico Chapter, System Safety Society, 1997.
- [87] Theofanous, T.G., "On the proper formulation of safety goals and assessment of safety margins for rare and high-consequence hazards," *Reliability Engineering and System Safety*, vol. 54, no. 2 – 3, pp. 243 – 257, 1996.
- [88] Thompson, K.M., "Variability and Uncertainty Meet Risk Management and Risk Communication," *Risk Analysis*, vol. 22, no. 3, pp. 647 – 654, 2002.
- [89] Timmins, P.F., *Solutions to Equipment Failures*, Materials Park, OH: ASM International, 1999.
- [90] U.S. Department of Defense, *MIL-STD-781D Reliability Testing for Engineering Development, Qualification, and Production*, 1986.

- [91] U.S. Department of Defense, *MIL-STD-785B Reliability Program for Systems and Equipment Development and Production*, 1980.
- [92] U.S. Department of Defense, *MIL-STD-882D Standard Practice for System Safety*, 2000.
- [93] U.S. Nuclear Regulatory Commission, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, 1975.
- [94] Uckun, S., Dawant, B.M., and Kawamura, K., "Uncertainty Management in Engineering Risk Assessment," *The Analysis, Communication, and Perception of Risk*, B.J. Garrik and W.C. Gekler, Ed., New York, NY: Plenum Press, 1991.
- [95] Vaughan, D., *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, Chicago, IL: University of Chicago, 1996.
- [96] Vose, D., *Risk Analysis: A Quantitative Guide*, 2nd ed., Chichester, UK: Wiley, 2000.
- [97] Wilson, R., and Shlyakhter, A., "Uncertainty and Variability in Risk Analysis," *Fundamentals of Risk Analysis and Risk Management*, V. Molak, Ed. Boca Raton, FL: CRC, 1997.
- [98] Wulpi, D.J., *Understanding How Components Fail*, 2nd ed., Materials Park, OH: ASM International, 1999.

Appendix I Systems Engineering Graduate Program Summary

Background

Systems Engineering focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then continuing with design synthesis and system validation while considering the complete problem: Operations--Performance--Test--Manufacturing--Cost & Schedule--Support--Disposal. Systems Engineering integrates all the disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation. Many of us already practice systems engineering, but call it something else: design or development of product, process, and service. This course of study will enable the engineering to function in an interdisciplinary team and apply their area of engineering specialty toward the development of a product, process, or service.

Learning Objectives

Improve students' ability to engineer complex products, processes, or services.

Develop students' understanding of basic systems concepts and their application to the engineering life cycle.

Develop students' understanding of key systems engineering skills, including team building, communication, synthesis & creativity, problem solving, management of time and resources, database management, and life-cycle viewpoints.

Build on students' existing knowledge and project experiences by providing additional domain specialization or project management tied to systems engineering skills.

General Requirements

The course of study requires 45 credits all taken at the graduate level. The student will be under the supervision of the Director of Systems Engineering, and a faculty advisor from his department of specialty, and an industry advisor knowledgeable with the student's internship/project experience. Core courses will introduce the student to systems methods and its tools. Elective courses will provide advanced domain knowledge mostly in the student's area of specialty. Courses from other departments will enable the student to apply this domain knowledge in an interdisciplinary, integrated manner. The internship/project will be a capstone experience combining both systems engineering and domain-specific approaches in the engineering of a complex system.

Core Courses (16 Credits)

SYSE 591 Systems Engineering Approach (4 Credits)

EMGT 540 Operations Research (4 Credits)

SYSE 595 Hardware-Software Integration (4 Credits)

One of 3 modeling classes (4 credits):

SYSC 514 System Dynamics
SYSC 527 Discrete System Simulation
SYSC 529 Process Modeling and Simulation

Elective Courses (16 Credits)

Each student will be under the advisement of the Director of Systems Engineering and a faculty advisor from one of the following departments: Civil Engineering, Computer Science, Electrical & Computer Engineering, Engineering Management, Mechanical Engineering, and System Science. Elective courses will come from any one of these PSU departments based on a plan of study agreed upon by both advisors and the student. Courses from other universities may be acceptable, as evaluated on a case by case basis, and up to a limit of 15 credits. Systems Engineering courses are also available as electives.

Projects & Internships (9 Credits)

Each student will participate in an industrial experience either as part of a formal internship (SYSE 504) or as part of an industrial project (SYSE 506). These industrial experiences will involve the student, faculty advisors and an industrial advisor. The internship may be full time or part time with nine months of full time employment earning 9 credits. The internship/project must encompass systems level considerations as applied to a product, process or service requiring knowledge from multiple engineering disciplines.

Integrative Workshop (4 Credits)

A total of four credits of interactive workshop between faculty advisor and student are required. The student will be guided to consolidate their project experience and knowledge from elective courses with concepts from their systems engineering core courses. This interaction could be conducted on-line the Internet in SYSE 590 Integrative Workshop (IW). Two important concepts in Systems Engineering are integration and management of interfaces, related to both physical components and product development process. The objective of IW is for the student to exercise these concepts as applied to their course work and project work. The workshop will span the student's entire program under the guidance of an advisor, thus giving the time to achieve several goals. One, the student is given feedback as they apply discipline skills in systems settings. Two, the student will be asked to reflect on past approaches as it relates to newer more advanced systems skills. Third, the IW will review systems topics over several terms, thus reinforcing their use. In this way, behavioral change, from engineering specialty thinking to systems engineering thinking, will be achieved. The program also benefits because students continuously assess how well all courses INTEGRATE to achieve Systems Engineering education goals. Workshops will culminate in a student portfolio summarizing the academic knowledge and practical experience students gained while in the Systems Engineering program.

The summary above is from the PSU systems engineering web page at <http://www.cecs.pdx.edu/Systems/program/masters.html>.

Appendix II Integrative Workshop Summary

Systems Engineering is an acquired behavior to be developed throughout the Masters degree program. Students and faculty advisors will engage in creative workshop activities integrating technical specialty skills and project experience invoking systems engineering applications of communication, synthesis and creativity, team building, problem solving, management of time and resources, and system life-cycle thinking. A student portfolio will document the program plan and document that the desired behavioral change is taking place.

Students are expected to devote a total of 120-160 hours to develop a portfolio. Students will be graded on an on-going basis, and then recorded depending on which terms they enroll in course. The portfolio will summarize the courses taken, relate course topics to each other, summarize discussions with peers and advisors, and document the student's reflection on the relation of course and discussion topics to Systems Engineering.

Advisors are expected to devote at least 100 hours to each student throughout their degree program by providing assistance in the development of study plans, guidance in the integration of course topics, help in the selection of creative exercises, insight regarding systems engineering concepts, and feedback on portfolio progress.

Place in development of department's total program

The program will be enhanced due to:

- 1) assessment of student progress in meeting learning objectives;
- 2) coupling of specialty disciplines to SYSE skills;
- 3) reinforcement of SYSE behavior;
- 4) assessment of objectives and assessment of progress toward meeting them;
- 5) an open forum for discussing program changes;
- 6) formal planning of student study plans

Educational purposes to be served by this course

The objective of SYSE 590 is to provide an interactive workshop between faculty advisor and Masters student. The student will be challenged to consolidate their project experience and knowledge from elective courses with concepts from the required systems engineering core courses. SYSE concepts of integration, synthesis, and interface management will be continually exercised based on Masters program components.

Methods of evaluation to be used in this course

Student:

Monitoring student input to Internet discussions, performance on project reports, and development of student portfolio. With guidance from the advisor, the student will define the objectives of their portfolio along with performance criteria, and then reflect on how well their portfolio meets the objectives. The advisor will grade this reflection with special emphasis on the utilization of SYSE concepts.

Course:

Because of its nontraditional nature, course assessment is given a high priority.

Examples include:

Monitoring of weekly email, chat, and Bulletin Board discussions,

Reflection on cumulative Bulletin Board discussions,

Surveys of student impressions,

Review of entries in each student portfolio.

Meeting Program Goals

The learning objectives for the Master of Engineering in Systems Engineering are to improve students' ability to engineer complex products and processes as a consequence of using the systems engineering concepts presented in the Core Courses. The Elective Courses build on students' existing knowledge and project experiences by providing additional domain specialization or project management exposure. Two important concepts presented in the systems engineering core are integration and management of interfaces as related to both physical components and product development processes. In SYSE 590, the student exercises these concepts, using their program of study. Elective course work and project work must couple to systems core courses. Course components must logically interface and build to meet the program objectives. In addition to exercising the concepts of integration for the student, SYSE 590 will provide assessment of student's progress and program integrity, available to other students, faculty and industry partners.

Course Goals

SYSE 590 - Integrative Workshop (IW) is a distance learning seminar series, spanning the student's entire program under the guidance of an advisor, thus allowing time to achieve several goals. First, the student is given feedback as discipline skills are applied in a systems settings. Second, the student will be asked to reflect on past approaches as they relate to newer more advanced systems skills. Third, the IW will review systems topics over several academic terms, thus reinforcing their use. In these ways, behavioral change from engineering specialty thinking to systems engineering thinking will be developed. Because of the difficulty of achieving these types of goals, the program must be continuously assessed. Specifically, course modules and groups of courses must integrate to achieve these goals, and if not, corrective changes must be incorporated early in the student's program.

Portfolio Contents

The workshops will culminate in a student portfolio that: a) formatively records their studies, b) applies systems principles to their program planning and evaluation, and c) summarizes the academic knowledge and practical experience students gained while in the systems engineering program. The portfolio must contain at least three components.

1. Study plan and record of courses actually taken:
 - a. a well thought out study plan,
 - b. evaluate progress achieved through this study plan,
 - c. assess beneficial changes that occur in study plan.

2. Reflection on coupling of technical specialties and SYSE fundamentals:
 - a. connection between the fundamentals learned in past with newly learned advanced systems topics,
 - b. relationship of the domain knowledge gained in electives to systems concepts,
 - c. use of systems concepts in projects and their impact on the development environment.

3. Exemplify systems engineering applied to review of student's program:
 - a. defining the specific objectives of compiling their own portfolio, given that their advisor and employer are customers/stakeholders such as,
 - 1) evidence of competencies
 - 2) additional work in integration and interface management
 - 3) assessment of student's program
 - 4) comparison of student's program to past portfolios

 - b. measuring how well these objectives were met,
 - 1) advisor interaction
 - 2) student peer interaction
 - 3) engineering peer interaction
 - 4) supervisor interaction
 - 5) outside studies and case studies

 - c. evaluating process at end of their program.

Web Archival

Most of the student-to-student and student-to-faculty interaction will be conducted on-line via the Internet using email and bulletin boards. As inexpensive new technology becomes available (such as Internet TV) additional forms of communication will be incorporated.

Students will be encouraged to archive their portfolio on the Systems Engineering web site as a model for future student use and for program evaluation. Personal or proprietary entries in the portfolio will be restricted to student and advisor, but this restriction is not expected to detract from the value of making these portfolios public.

Students will also be encouraged to compile their portfolios on a continuous basis and to make available on the web after some reasonable student-faculty interaction. A portfolio template will be suggested to students to make their documentation process easier and foster consistency in the web site design.

Academic Integrity

IW will serve as a window for stakeholders and evaluators to view individual student performance and how well the program aids students to attain this performance. Such a safeguard is an imperative when considering the web nature of the program. Two other demands are placed on the IW and the portfolio. Students will not be in a position to give a personal presentation as part of an on-campus graduate seminar, which is traditionally used as a significant component in exit evaluation. The portfolio may serve as the Exit Document. In addition the student will be encouraged to include their project report in the web archives and link it from the portfolio. (As technology permits, the student may also include a presentation video on web, linked from their portfolio). The other demand is the application of original and significant Systems Engineering concepts as part of the project work. The project should demonstrate 9 credits of scholarly work in Systems Engineering. Maintenance of the portfolio on an on-going basis will give formative assessment, and the final document will give summative assessment of the application of Systems Engineering concepts in project work.

The summary above is from the PSU systems engineering web page at <http://www.cecs.pdx.edu/Systems/program/masters.html>.

Appendix III Revision History

Revision	Date	Description
A	02 Mar 2002	Original documentation.
B	04 Apr 2002	Update student learning objectives. Update project summaries. Add PSU course descriptions to elective summaries. Divide annotated bibliography into system (general) and risk (specific) subject areas.
C	04 May 2002	Change summer 2002 elective due to schedule conflict. Update scheduled courses in study plan. Update project summaries.
D	13 Aug 2002	Update scheduled courses in study plan. Update project summary; add concept map and summaries of completed project work. Update annotated bibliography.
E	22 Aug 2002	Change fall 2002 elective due to continued project opportunities.
F	11 Nov 2002	Major revision. Update and consolidate project summary. Delete annotated bibliography. Add resources links.
G	03 Mar 2003	Update scheduled courses in study plan. Update resources links.
H	28 May 2003	Delete spring 2003 elective due to schedule conflict. Add summer 2003 elective. Update scheduled courses in study plan. Add professional/academic development summary.
I	06 Oct 2003	Update scheduled courses in study plan. Update professional/academic development summary. Delete resources links.
J	15 Dec 2003	Update scheduled courses in study plan. Update project summary. Revise study plan concept map.
K	09 May 2004	Update scheduled courses in study plan.
L	09 Sep 2004	Major revision. Add table of contents, publication summaries, and project text.
M	08 Dec 2004	Final revision.