

Conducting Safety Risk Management by Applying Systems Engineering Tools

W. Clifton Baldwin, PMP
System Engineering & Integration Group,
Federal Aviation Administration

October 2005

DOT/FAA/TC-TN06/1

Document is available to the public
through the National Technical Information
Service, Springfield, Virginia 22161



**U.S. Department of Transportation
Federal Aviation Administration**

William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: www.tc.faa.gov/its/act141/reportpage.html in Adobe Acrobat portable document format (PDF).

1. Report No. DOT/FAA/TC-TN06/1		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Conducting Safety Risk Management by Applying Systems Engineering Tools				5. Report Date October 2005	
				6. Performing Organization Code ACB-210	
7. Author(s) W. Clifton Baldwin				8. Performing Organization Report No. DOT/FAA/TC-TN06/1	
9. Performing Organization Name and Address U. S. Department of Transportation Federal Aviation Administration, William J. Hughes Technical Center Atlantic City International Airport, NJ 08405				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No.	
12. Sponsoring Agency Name and Address U. S. Department of Transportation Federal Aviation Administration, William J. Hughes Technical Center System Engineering & Safety Division, AJP-7131 Atlantic City International Airport, NJ 08405				13. Type of Report and Period Covered Technical Note	
				14. Sponsoring Agency Code ACB-200	
15. Supplementary Notes The author identified above represents the following organization: W. Clifton Baldwin with FAA System Engineering & Integration (ACB-210)					
16. Abstract The Federal Aviation Administration has developed the Safety Management System (SMS). The SMS states that all safety significant, new and modified systems, procedures, and operations must be evaluated for safety risk. Within the SMS, a framework process has been proposed for performing Safety Risk Management (SRM). Systems engineering is defined in part as the incorporation of all technical parameters to assure compatibility between physical and functional interfaces in a manner that optimizes system definition and design. The systems engineering tools include stakeholder analysis, context diagrams, use cases, functional architectures, and risk matrices, just to name a few examples. Systems engineering tools are proposed for certain stages of the SRM, which are not traditionally within the domain of safety engineering. The systems engineer's role in the SRM and the tools to conduct the process are explored. In order to test the concept, the En Route Automation Modernization (ERAM) system was passed through the first two stages of the SRM using systems engineering tools. The result was a hazard list at least as detailed as the existing documented system hazard list, which is used as a control. The identified safety risks are compared to the control list as a case study of the effectiveness of this proposal.					
17. Key Words Systems Engineering Risk Management Safety Engineering Safety Management System (SMS) Safety Risk Management (SRM) ERAM, En Route Automation Modernization				18. Distribution Statement This document is available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. A copy is retained for reference by the William J. Hughes Technical Center IRC.	
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 32	22. Price

Acknowledgements

I would like to thank the System Engineering and Safety Division (ACB-200) at the FAA's William J. Hughes Technical Center (WJHTC) for providing me with the time and encouragement to complete this technical note. I would especially like to acknowledge Christopher Reilly, Stephen Stratoti, John Chung, and Gerard Spanier for reviewing and commenting on various drafts of this paper.

Also I would like to acknowledge the FAA's ERAM Test Group at the WJHTC for providing me with the documentation needed to do the case study.

Finally I would like to thank the managers within the Office of Integrated Engineering Services (ACB) at the WJHTC who encouraged me to publish this paper.

Executive Summary

The Federal Aviation Administration's ATO Safety Service Unit has developed the Safety Management System (SMS). The SMS states that all safety significant, new and modified systems, procedures, and operations must be evaluated for safety risk. Within the SMS, a framework process has been proposed for performing Safety Risk Management (SRM). The SRM is a "systematic, explicit, and comprehensive approach for managing safety risk at all levels and throughout the entire scope of an operation and lifecycle of a system."¹ In order to stress the importance of the subject, the FAA has established metrics to monitor the progress of implementing safety risk management.

Systems engineering is defined in part as the incorporation of all technical parameters to assure compatibility between physical and functional interfaces, hardware and software interfaces, in a manner that optimizes system definition and design. In order to perform systems engineering, the systems engineer must employ tools of his or her trade. The products of these systems engineering tools are stakeholder analysis, context diagrams, use cases, functional architectures, and risk matrices, just to name a few examples.

This paper proposes the use of systems engineering tools for certain stages of the SRM, which are not traditionally within the domain of safety engineering. Although the Federal Aviation Administration's (FAA) Acquisition Management System (AMS) Policy states safety management shall be conducted and documented throughout the lifecycle of a system in accordance with the FAA's SMS², scheduling of the SRM is independent to the process of the SRM and outside of the scope of this paper. Basically the focus of this paper is on the systems engineer's role in the SRM and the tools to conduct the process.

In order to test the concept, the En Route Automation Modernization (ERAM) system was passed through the first two stages of the SRM using systems engineering tools. The resulting SRM is not complete as the goal of this paper is to test the concept and not necessarily perform a full safety analysis of ERAM. Nonetheless the systems engineering tools produced a hazard list at least as detailed as the existing documented system hazard list, which is used as a control. The identified safety risks are compared to the control list as a case study of the effectiveness of this proposal.

¹ Safety Management System Manual [9]

² <http://fast.faa.gov/index.htm>, Policy 4.12 System Safety Management

[This page left intentionally blank]

Table of Contents

1.	Introduction.....	1
1.1	Assumptions and Constraints.....	2
1.2	Definitions.....	2
1.3	Agency Requirements.....	3
2.	SRM Process with Systems Engineering.....	4
2.1	External Inputs.....	6
2.2	Describe System.....	7
2.3	Identify Hazards.....	9
2.4	Analyze Risk.....	10
2.5	Assess Risk.....	11
2.6	Treat Risk.....	12
2.7	External Outputs.....	13
3.	Proof of Concept Case Study.....	13
3.1	Case Study Describe System.....	13
3.2	Case Study Identify Hazards.....	14
3.3	Control Study.....	14
3.4	Analysis.....	14
4.	Conclusion.....	15
	References.....	16
	Acronym List.....	17
	Appendix A – Responsibilities within the SRM Process.....	18
	Appendix B – Case Study System Functions.....	19
	Appendix C – Case Study Identify Hazards.....	20
	Appendix D – Control Case.....	22
	Appendix E – Matching of Case Study to Control Case.....	23

List of Figures

Figure 1: SRM Process.....	5
Figure 2: N-Square Diagram of the Proposed SRM Process.....	6
Figure 3: Describe System.....	8
Figure 4: N-Square of the Describe System Stage.....	9
Figure 5: Analyze Risk.....	11
Figure 6: Risk Matrix.....	12
Figure 7: Treat Risk.....	13
Figure 8: Responsibilities within the SRM Process.....	18

1. Introduction

The Federal Aviation Administration's ATO Safety Service Unit has developed the Safety Management System (SMS). The SMS states that all safety significant, new and modified systems, procedures, and operations must be evaluated for safety risk. Within the SMS, a framework process has been proposed for performing Safety Risk Management (SRM). The SRM is a "systematic, explicit, and comprehensive approach for managing safety risk at all levels and throughout the entire scope of an operation and lifecycle of a system."³ In order to stress the importance of the subject, the FAA has established metrics to monitor the progress of implementing safety risk management (see [8]).

Systems engineering is defined in part as the incorporation of all technical parameters to assure compatibility between physical and functional interfaces, hardware and software interfaces, in a manner that optimizes system definition and design. In order to perform systems engineering, the systems engineer must employ tools of his or her trade. The products of these systems engineering tools are stakeholder analysis, context diagrams, use cases, functional architectures, and risk matrices, just to name a few examples.

This paper proposes the use of systems engineering tools for certain stages of the SRM, which are not traditionally within the domain of safety engineering. Therefore a competent systems engineer should be involved with the safety engineer in the conducting of safety risk management. Basically the focus of this technical note is on the systems engineer's role in the SRM and the tools to conduct the process. A graphical representation of the proposed responsibilities for the system engineer and the safety engineer is presented in Appendix A – Responsibilities within the SRM Process.

Although the Acquisition Management System (AMS) Policy states safety management shall be conducted and documented throughout the lifecycle of a system in accordance with the FAA's SMS⁴, scheduling of the SRM is independent to the process of the SRM and outside of the scope of this paper.

Using the tools of systems engineering, a functional architecture is developed in order to describe a system. By analyzing the functional architecture, potential hazards can be identified by the systems engineer. After the hazards are known, safety engineers, who can develop appropriate responses, can analyze each of the risks. Working with the safety engineer, the systems engineer determines the impacts to the system of the safety engineer's responses.

In order to test the concept, the En Route Automation Modernization (ERAM) system was passed through the first two stages of the SRM using systems engineering tools. The resulting SRM is not complete as the goal of this paper is to test the concept and not necessarily perform a full safety analysis of ERAM. Nonetheless the systems engineering tools produced a hazard list at least as comprehensive as the existing documented system hazard list, which is used as a control. The identified safety risks are presented against the control list for comparison.

³ [Safety Management System Manual](#) [9]

⁴ <http://fast.faa.gov/index.htm>, Policy 4.12 System Safety Management

1.1 Assumptions and Constraints

In order to avoid confusion, the following assumptions and constraints apply throughout this technical note:

1. The systems engineer performs only the functions within the systems engineering domain and has the knowledge of systems engineering tools. For example, see [2] and [3] for descriptions of the systems engineering tools. For the purpose of this paper, safety engineering is outside the scope of systems engineering. It should be noted that the same individual could have both roles of systems engineer and safety engineer in practice.
2. The safety engineer performs only the functions within the safety engineering domain and has the knowledge of safety engineering tools. For the purpose of this paper, systems engineering is outside the scope of safety engineering. It should be noted that the same individual could have both roles of systems engineer and safety engineer in practice.
3. The systems engineer and the safety engineer are needed throughout the lifecycle of a system, but the complete lifecycle is outside of the scope of this paper. For the purposes of this paper, only the SRM process is within scope.
4. Formal and final documentation on ERAM is assumed correct and complete.
5. Testing and training elements of the ERAM system were not included in this study.
6. The control study performed by Lockheed Martin is assumed to adhere to the Safety Management System (SMS) or equivalent.
7. The concept was tested at the system level since that should be adequate to identify system hazards. If the safety engineer requests more details, the concept could be applied in theory at any level of detail by decomposing the architecture to the desired level.

1.2 Definitions

"One of the systems engineer's first jobs on a project is to establish nomenclature and terminology that support clear, unambiguous communication and definition of the system, its functions, components, operations, and associated processes⁵". The following terms are defined in order to support clear, unambiguous communications:

ERAM – En Route Automation Modernization: Within this study, ERAM is assumed to be the functional system, which is not necessarily the project to develop, test or train for ERAM.

Hazard – A hazard is defined as any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident (see [9]).

⁵ INCOSE Systems Engineering Handbook, Version 2a, Section 2.4

Risk – A risk is defined (see [10]) as a future event or situation with a realistic likelihood/probability ($0\% < \text{event} < 100\%$) of occurring and an unfavorable consequence/impact to the successful accomplishment of the well-defined program goals if it occurs. The specific instance of risk addressed by this white paper is the probability and severity of a hazard within a system.

Safety – Basically safety is a vague term, but for this paper it will be defined as freedom from unacceptable risk of hazards.

Systems Engineering – The translation of a need or deficiency into a system architecture through the iterative process of functional analysis, allocation, implementation, optimization, test, and evaluation; the incorporation of all technical parameters to assure compatibility between physical & functional interfaces, hardware & software interfaces, in a manner that optimizes system definition and design; and the integration of performance, manufacturing, reliability, maintainability, supportability, global flexibility, scalability, upgradeability, and other specialties into the overall engineering effort⁶.

For more information on systems engineering see [2], [3], [10] & [12].

Tools of Safety Engineering – As applied in this paper, tools of safety engineering are any tools, including but not limited to diagrams, templates, training, processes, and software unique to the safety engineer.

Tools of Systems Engineering – As applied in this paper, tools of systems engineering include but are not limited to stakeholder analysis, context diagrams, system use cases, functional architecture (IDEF0⁷) diagrams, risk matrices, systems documentation, and training which are unique to the systems engineer.

1.3 Agency Requirements

The FAA has outlined several high-level agency goals (see [8]). The first stated goal is “Increased Safety.” Within that goal, there are several objectives, of which Objective 7 is “enhance the safety of FAA’s air traffic systems.” For this objective, the stated strategy includes, “Design, develop, and implement a SMS that complies with the International Civil Aviation Organization’s (ICAO) requirements and applies a system safety approach to the FAA’s delivery of air traffic services.” The metric of this strategy is described as the performance target, which states, “Apply safety risk management to at least 30 significant changes in the NAS.” Hence the FAA is obligated to perform SRM to be in alignment with its own goals.

The necessity to perform an SRM is required by FAA Order 8040.4 (see [14]). The following excerpt extracted from ASD-100-SSE-1, REV 9.0, [1] provides an overview of the order:

FAA Order 8040.4 requires the FAA-wide implementation of safety risk management in a formalized, disciplined, and documented manner for all high-consequence decisions. Each program office and Line of Business (LOB) is required to establish and implement the policy contained within Order 8040.4 consistent with that program office and LOBs

⁶ Accepted definition of Stevens Institute of Technology’s SDOE Program

⁷ IDEF0 is a method derived from a graphical language designed to model the decisions, actions, and activities of an organization or system (see [11]).

role in the FAA. While the methods and documentation can be tailored with sufficient rationale, each program office and LOB is required to satisfy the following criteria:

Implement safety risk management by performing risk assessment and analysis and using the results to make decisions

Plan – the risk assessment and analysis must be predetermined, documented in a plan which must include the criteria for acceptable risk

Hazard identification – the hazard analyses and assessments required in the plan must identify the safety risks associated with the system or operations under evaluation

Analysis – the risks must be characterized in terms of severity of consequence and likelihood of occurrence

Risk Assessment – the risk assessment of the hazards examined must be compared to the acceptability criteria specified in the plan and the results provided in a manner and method easily adapted for decision making

Decision – the risk management decision must include the safety risk assessment and the risk assessments may be used to compare and contrast options

Based on the orders and agency goals, safety risk management is not an elective. The proposed process for performing safety risk management in the following section attempts to address the requirements while positively impacting the agency's metrics.

2. SRM Process with Systems Engineering

The SRM process includes five stages or steps (see Figure 1), which are continuously iterated throughout the development of the system. As defined in the SMS [9], the steps are titled Describe System, Identify Hazards, Analyze Risk, Assess Risk, and Treat Risk. The inclusion of systems engineering does not alter the process, but the responsible parties within each stage are modified. For a graphical description of who is responsible for each stage of this proposed process, see Appendix A – Responsibilities within the SRM Process at the end of this technical note. For use within this concept, major external inputs and outputs are identified in order to have the correct information available for the systems engineer to proceed and to describe what will be produced by the process (see Figure 2).

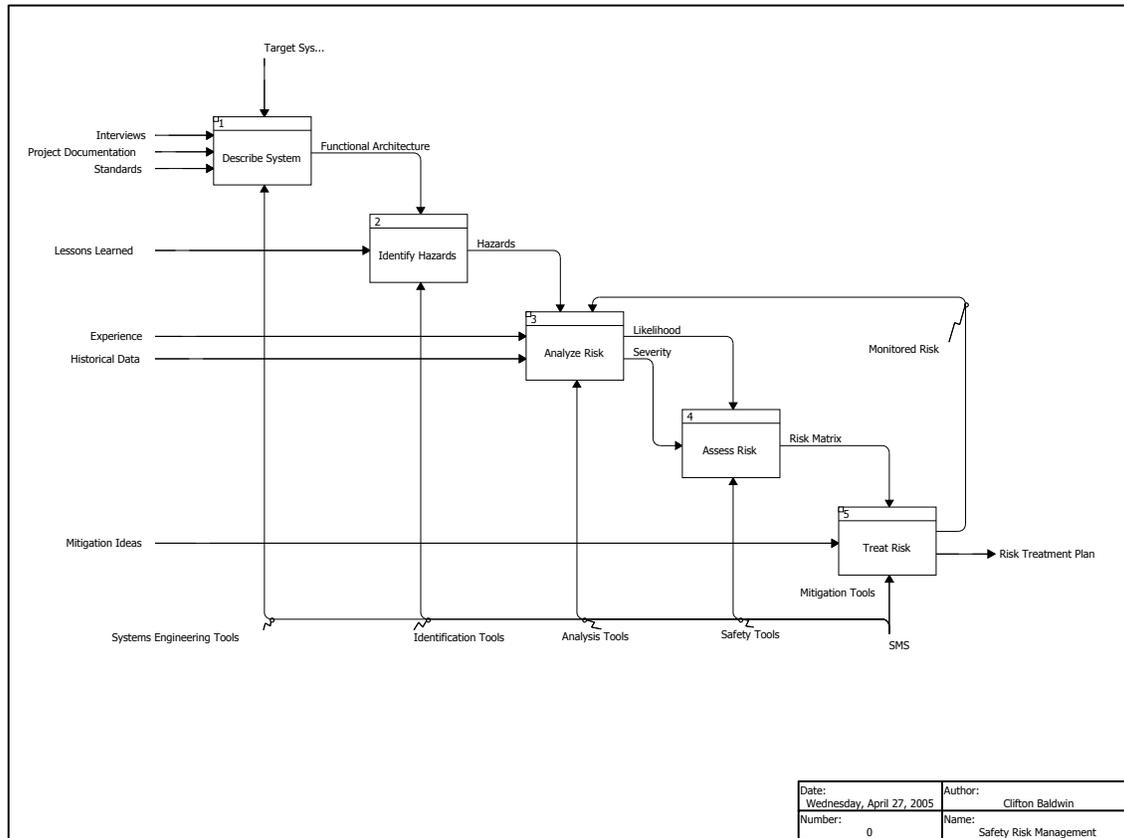


Figure 1: SRM Process⁸.

⁸ Functional architecture IDEF0 diagrams are produced by the Vitech Corporation's Core 5.1 systems engineering tool.

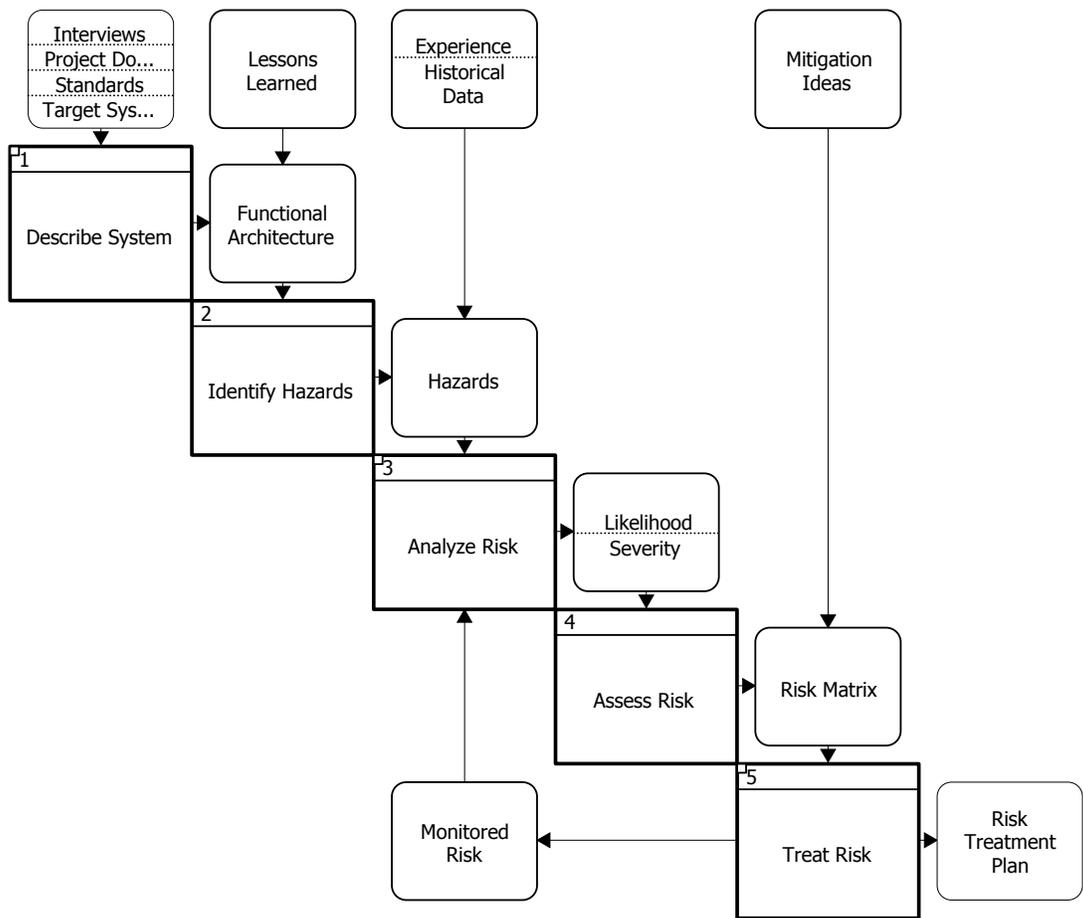


Figure 2: N-Square Diagram of the Proposed SRM Process.

2.1 External Inputs

The SRM process is triggered by the system. The AMS states safety management shall be conducted and documented throughout the lifecycle of a system and is the policy for the triggering of the SRM process. Nonetheless a target system is needed to activate the process for obvious reasons.

Project documentation is the most important input to the process from the systems engineer’s perspective. Unfortunately project documentation is often lacking in the needed details. Ideally project documentation should include the stakeholder list, the context diagram, the system’s use cases, and a true functional architecture. Lacking this information, the systems engineer may need to conduct research to fill in any gaps. In any case, the project documentation should include requirement documents, any system architecture documents, high-level interface documents, and high-level design documents. For an example of insufficient documentation, it appears that many existing “functional architectures” are just altered physical architectures. A true functional architecture would define what the system will do, and not the pieces that will actually do it. For instance, the functional architecture may have an item called “track aircraft” and the details of what will do the tracking are outside the scope of the functional

architecture. A functional architecture with an item called “use radar” or just “radar” is not a functional architecture item since the goal of the system is to track aircrafts and not use radar. Radar is the physical tool to track the aircrafts.

In order to fill any undesirable gaps, research including interviews with various stakeholders and examination of the existing documentation is needed.

An often-overlooked yet important set of passive stakeholders is the set of standards of which a system must adhere. The systems engineer makes a list of all active and passive stakeholders as part of his or her research. When important stakeholders, such as standards, have not been identified, the systems engineer can add it to the stakeholder list. An easily identified safety risk is the absence of the proper safety standards for a system.

Lessons learned, including checklists developed from previous projects, are important tools of the systems engineer. There is no reason to repeat any safety risks from previous projects. Even in the case when a previous project is not similar to the existing system, lessons learned may lead the systems engineer to identifying new potential hazards.

After the potential hazards list has been identified, the safety engineer needs to input his or her experiences as well as any historical data that has been collected on similar hazards. Upon completion of the analysis, mitigation ideas are fed into the process from the safety engineer, systems engineer, or any person on the project with a good idea on how to handle the hazard.

2.2 Describe System

The Describe System step is principally a systems engineering procedure. According to the SMS as documented in [9], this stage involves the definition of the stakeholders, the definition of scope and objectives of the target system, the planned uses of the target system, and the intended functions of the target system. Ideally a systems engineer performs this step using the accepted tools of systems engineering (see Figure 3). The safety engineer is not needed to describe the system, but he or she creates a safety risk management plan at this stage if one has not already been produced.

First the systems engineer must determine all the stakeholders of the system. In order to be comprehensive, all active and passive stakeholders need to be recorded. The list of stakeholders would include any human interaction, any non-human (system) interaction, applicable policies and laws, and any other entities that have any relationship with the intended system.

Using the complete list of stakeholders along with appropriate documentation, the systems engineer can create a context diagram for the system. The context diagram graphically illustrates all the stakeholders and displays any interfaces. By knowing the interfaces, dependencies that may be potential hazards can be identified in the next stage.

The context diagram along with project documentation and interviews with stakeholders should provide the systems engineer with the information necessary to describe the use cases of the system. Use cases describe scenarios that the system is designed to perform. They will be helpful in playing out potential hazardous situations to determine consequences later on.

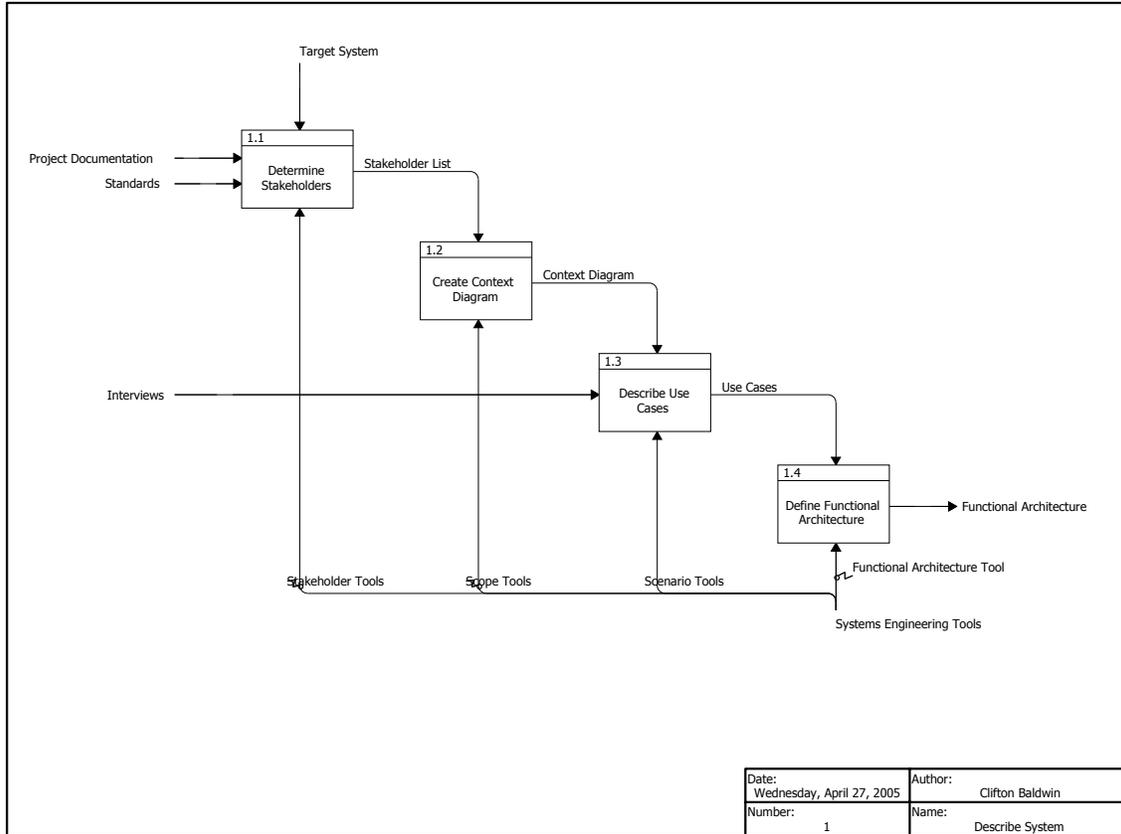


Figure 3: Describe System.

Using the use cases and context diagram, the systems engineer will define the functional architecture, the primary output of this stage. The functional architecture describes what the system does as well as any interfaces (see Figure 4). According to appendix B of the Safety Management System Manual [9], identification of the functions of a system is a primary tool to identify hazards of the system. It should be noted that the systems engineering process to develop a functional architecture is iterative as more details are discovered. Therefore the systems engineer may cycle several times within this stage before completing his or her functional architecture.

Although outside of the scope of the SRM process, the by-products of this step are the system's stakeholder list, context diagram, use cases, and functional architecture diagrams. These systems engineering artifacts can be saved for use elsewhere within the development of the system. For one instance, any decisions regarding changes to the system can be based in part on information found within these documented items.

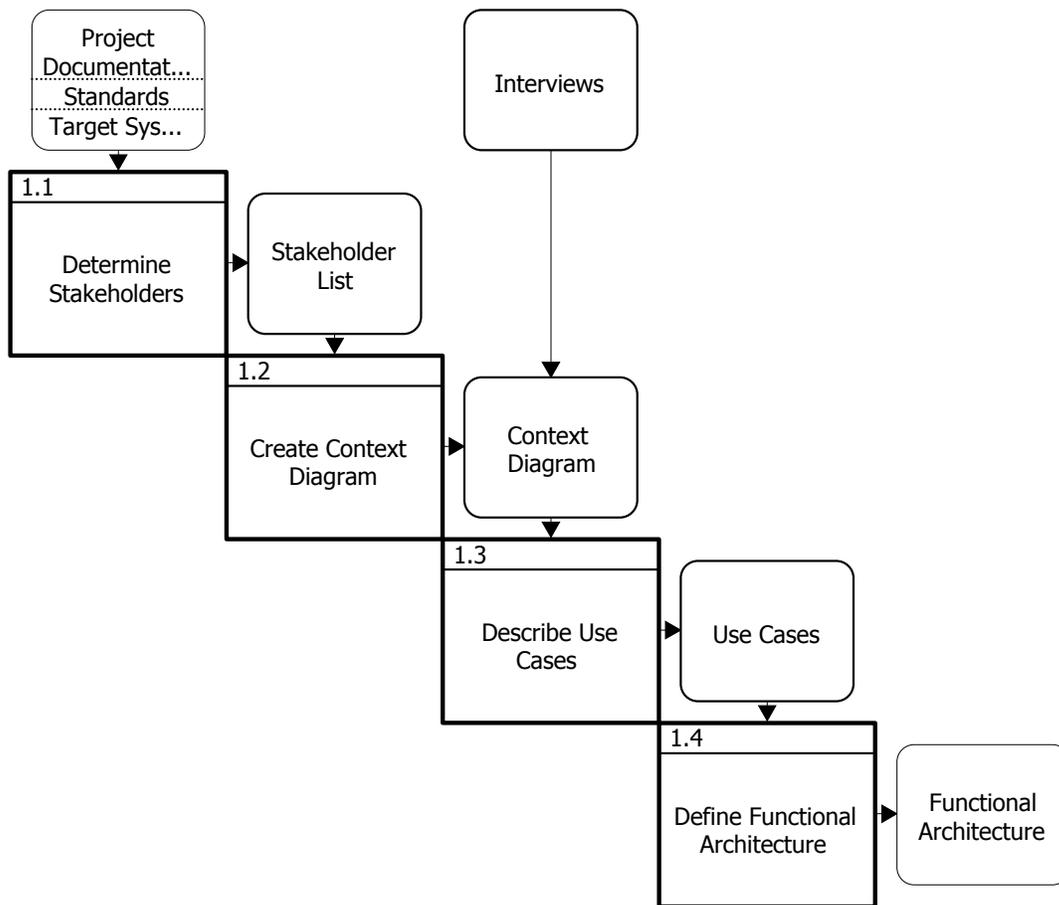


Figure 4: N-Square of the Describe System Stage.

2.3 Identify Hazards

The Identify Hazards step has the primary responsibility of determining all the potential hazards of a system. The identification uses a structured approach including lessons learned from similar systems and any available agency-specific checklists. The functions and interactions of the system from the previous step's functional architecture are the input to this step. The goal of this part is to create a comprehensive list of hazards regardless of their practicality. Improbable and unrealistic hazards can be dismissed after they are analyzed appropriately, which demonstrates that they were properly considered. The safety engineer may work with the systems engineer to identify the hazards, but the systems engineer is better prepared to analyze the documentation from the preceding step. In addition, project team members may contribute some identified risks based on their knowledge of the system.

For each of the identified functions of the system, there are basically five questions that should be addressed. These questions are documented in the Appendix B of the Safety Management System Manual [9]. The questions are the following:

1. What can fail?
2. How can it fail?
3. How frequently will it fail?
4. What are the effects of the failure?
5. How important, from a safety viewpoint, are the effects of the failure?

The first four questions are ideally suited to the systems engineer as well as other technical experts of the system. Both the safety engineer and the systems engineer should address the fifth question. Each of the engineers can deal with this question using “what if” scenarios, such as “What if the component fails?” or “What if the data is corrupted?” The systems engineer can identify “what if” situations based on the functioning and interactions of the system, and the safety engineer can approach the same question from a safety point of view. Therefore in an ideal situation, both engineers would work together in order to create the most comprehensive list of potential safety hazards possible.

2.4 Analyze Risk

For the Analyze Risk stage, the safety engineer has a comprehensive list of hazards to analyze (see Figure 5). The systems engineer does not have any systems engineering tools that can analyze the safety hazards, and primarily the safety engineer conducts the work at this stage. Due to the broad identification work, some of the hazards may be quickly dismissed during analysis. Yet if everything is not initially considered, some valid hazards may go undetected. Furthermore the safety engineer has the expertise to dismiss a potential hazard, while the systems engineer may not be qualified to do so. The analyze risk step applies the system’s functions determined earlier to decide how the hazard may impact the system. Utilizing the use cases produced by the systems engineer, the hazards can be tracked through a full scenario to determine all consequences of the hazard if the safety engineer deems it necessary. Based on the impact of the hazard, the severity is determined as well as a likelihood of each hazard occurring.

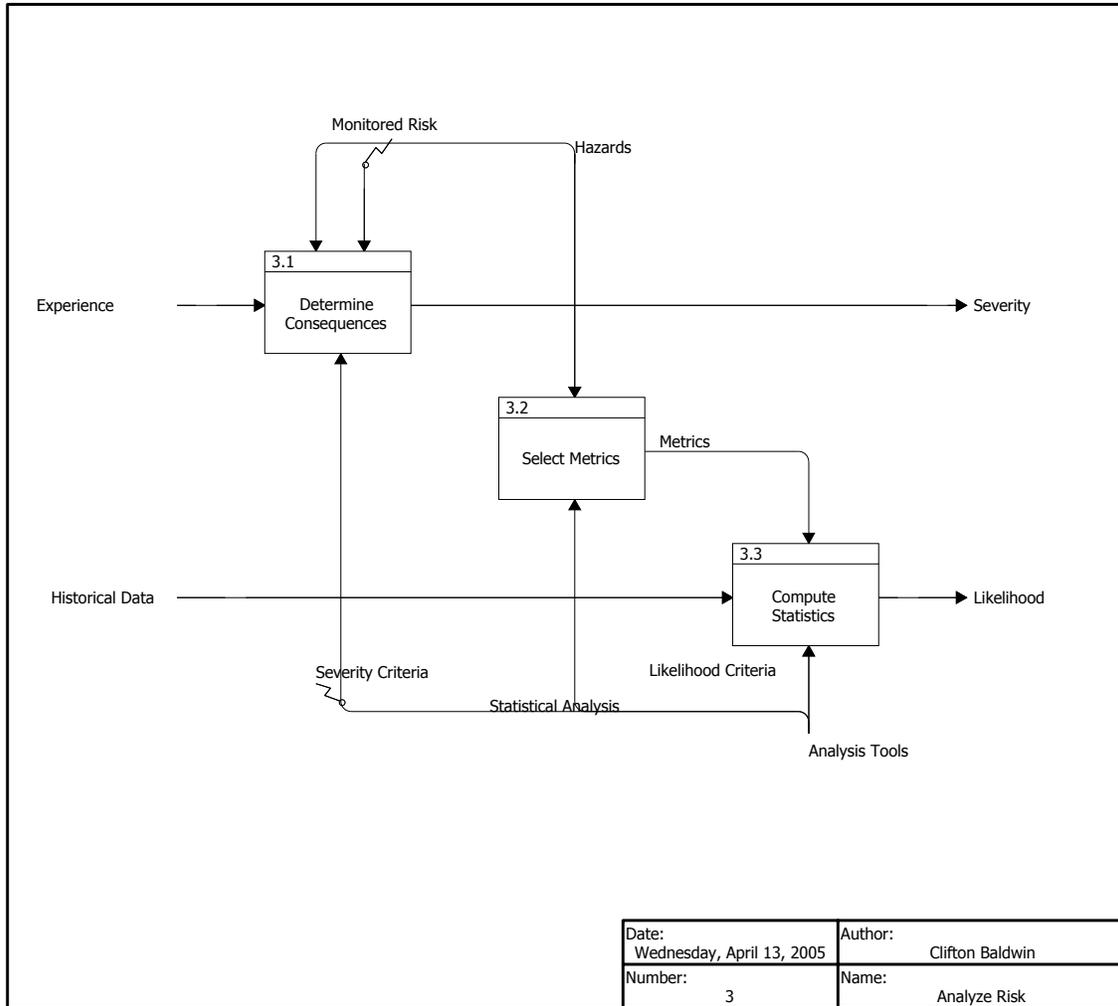


Figure 5: Analyze Risk.

2.5 Assess Risk

For the Assess Risk step, the safety engineer has a list of all analyzed hazards. Based on the analysis results, the safety engineer ranks the hazards appropriately. The safety engineer or the project manager uses safety tools to determine a minimum threshold for hazards. Any hazard falling below the threshold, which would include any improbable or unrealistic hazards, can be accepted with accompanying documentation. The remaining hazards above the threshold are categorized into the risk matrix (see Figure 6 and [7]). If a hazard is assessed below the threshold mark but the safety engineer believes the hazard may change in the future, the hazard may be included in the matrix for tracking purposes.

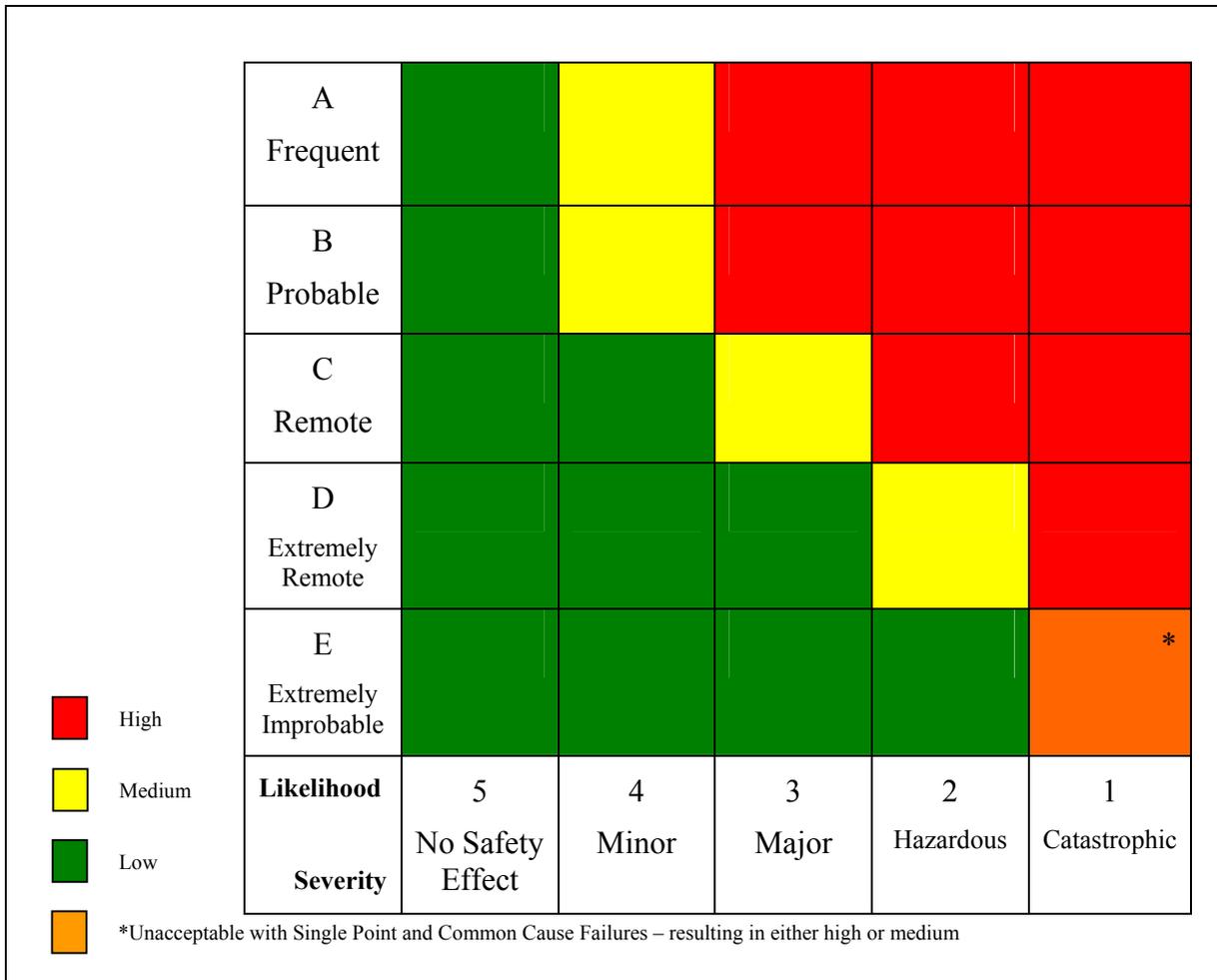


Figure 6: Risk Matrix.

2.6 Treat Risk

The Treat Risk step is the final stage in the process. The result of this step is to respond to the risks, which is the ultimate goal of the SRM. At this stage, the systems engineer should assist the safety engineer. The systems engineer brings knowledge of the system including how any changes may affect it, while the safety engineer brings the knowledge of what can be done to mitigate each hazard risk. Feasible mitigation options are identified and the best response is chosen for each risk. A risk treatment plan is developed to execute the mitigation response. The project manager will be given the plan in order to implement it, and the safety engineer monitors the hazard to ensure the mitigation options are effective (see Figure 7). If further mitigations or changes are needed for the existing risks, the safety engineer may consult with the systems engineer again and as many times as needed to make the system safer.

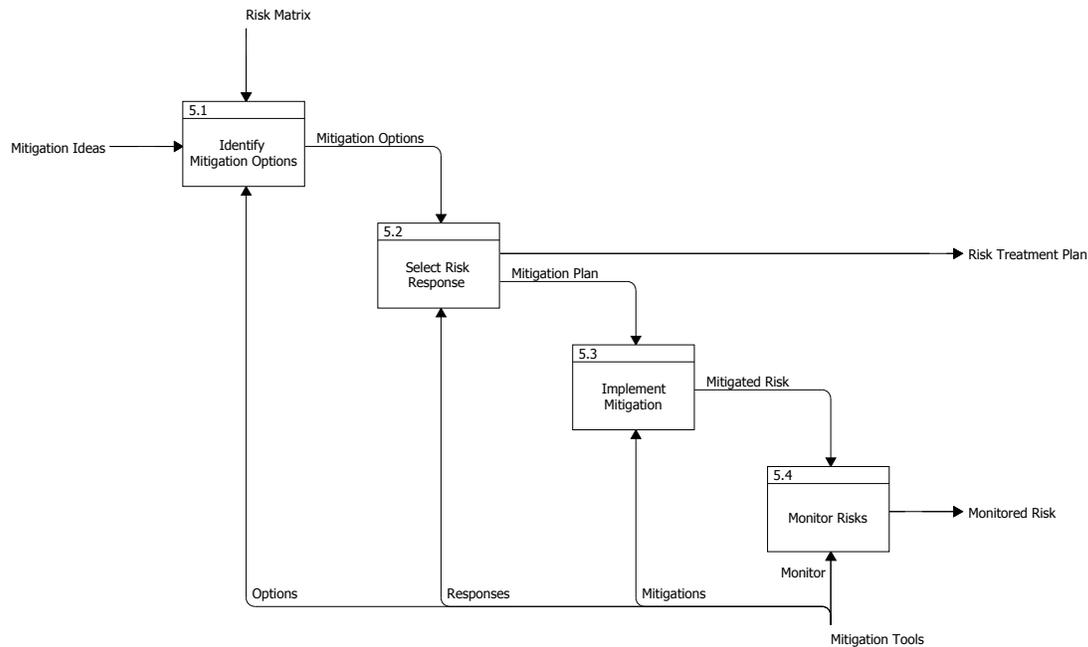


Figure 7: Treat Risk.

2.7 External Outputs

The primary output of the process is the risk treatment plan. Monitored risks are a secondary output. Existing risks continue to feed back into the process until one of three events occurs: 1) the risk is mitigated to the extent that it cannot cause harm, 2) the risk becomes obsolete, or the worst case, 3) the risk materializes and causes a safety issue.

Although the existing known safety risks should be under control at this point, new or undiscovered safety risks may yet be present. The SRM process must continuously cycle in order to detect the safety risks before a hazard materializes.

3. Proof of Concept Case Study

In order to test the concept of applying systems engineering tools to an SRM, a case study was conducted. Due to familiarity of the system by the author and the accessibility of documentation, the En Route Automation Modernization (ERAM) system was chosen as the system. The study was not rigorous as its objective was to prove the concept and not necessarily do a complete SRM analysis of ERAM.

Using the tools and practices of formal systems engineering, the first two stages of the SRM process were performed. The results of these two stages follow.

3.1 Case Study Describe System

In order to obtain an initial list of potential safety hazards of ERAM, several existing documents were examined (see [5], [6] and [13])

Following the procedure outlined in section 2.2 for the Describe System step, an initial functional architecture of ERAM was developed. For the purpose of this case study, the process outlined in Figure 3 was performed only once with no further iterations. One pass was sufficient to develop a functional architecture for this purpose, but a full analysis of ERAM may require several more iterations. It should be noted that the ERAM documentation did include some versions of the systems engineering artifacts, but they were incomplete in their current state for this purpose. See Appendix B – Case Study System Functions for the resulting list of functions.

3.2 Case Study Identify Hazards

For each function or dependency of ERAM, a hazard may occur if the function or dependency is lost or corrupted. If ERAM adversely affects any other system during its normal operations, it would be identified as a hazard also. By design, ERAM does not interfere with other systems but rather uses other systems where appropriate.

After studying what ERAM is proposed to do, a list of potential safety hazards was created. These potential hazards would be the result of a faulty ERAM. By design, ERAM is not planning to incorporate any safety hazards into the National Airspace System (NAS). Unfortunately systems do not always work as planned. For the resulting list of potential hazards, see Appendix C – Case Study Identify Hazards.

3.3 Control Study

During the course of executing the SRM process, a documented study was discovered that attempts to cover the subject of ERAM safety. In February 2005 Lockheed Martin completed a system hazard analysis [7]. In the study, fifteen (15) potential hazards were identified. This document is used as a control to test the proposed concept. See Appendix D – Control Case for the findings of the control study.

The process of using systems engineering tools aided the identification of 36 potential hazards for this case study. Thirty-four (34) of the 36 potential hazards can be consolidated and grouped into the fifteen (15) control hazards identified in [7]. The remaining two (2) potential hazards coincide with control hazards identified in [4]. For a side-by-side comparison of the case study to the control case, see Appendix E – Matching of Case Study to Control Case.

3.4 Analysis

The case study identified a list of hazard risks, which are more detailed than the control hazard risks from [7]. If desired, the risks obtained in the case study could be consolidated into the more general list quite easily. In addition, two additional hazard risks were identified that can be grouped into a “system dependencies” risk, which is identified in some detail in [4]. These two system dependency items are necessary since any dependency is a potential risk to the system regardless of the quality of the external system. External systems are outside of the scope of ERAM by definition, and therefore any dependency is outside of the control of ERAM. This creates a potential risk. It is not easily apparent why the system dependencies would be identified for subsystems in [4] but not the entire system in [7].

4. Conclusion

This paper attempts to outline responsibilities of a systems engineer during the SRM process as well as the need for systems engineering tools. This paper documents a proof of concept case study for using the tools of systems engineering to perform the first two stages of the SRM process on the ERAM system. It was not the intent of this paper to do a full safety risk analysis of ERAM or outline the timeline for doing the SRM process. The results of the case study indicate that the use of systems engineering tools does produce an appropriate list of hazard risks that can be further analyzed by a safety engineer. Hence there appears to be a need for a competent systems engineer to complete the full SRM on a system.

References

1. ASD-100-SSE-1, REV 9.0, NAS Modernization, System Safety Management Program, FAA Acquisition Management System, U.S. Department of Transportation, Federal Aviation Administration, Acquisition, Research and Other Procurement Parties.
2. Blanchard, Benjamin S. & Wolter J. Fabrycky, Systems Engineering and Analysis, 3rd ed., Prentice-Hall, Inc., 1998.
3. Buede, Dennis M., The Engineering Design of Systems, Models and Methods, John Wiley & Sons, 2000.
4. En Route Automation Modernization (ERAM), Subsystem Hazard Analysis (SSHA), Draft, Document Number FAA-ERAM-2004-0450, October 8, 2004, CDRL Item: B018
5. En Route Automation Modernization (ERAM), System Safety Program Plan (SSPP), Document Number FAA-ERAM-2003-0247, September 29, 2003, CDRL Item: B017
6. En Route Automation Modernization (ERAM), System/Segment Specification, Volume II: System Architecture Design Document (SADD), October 14, 2003, CDRL: B002
7. En Route Automation Modernization (ERAM), System Hazard Analysis (SHA), Document Number FAA-ERAM-2005-0078, February 10, 2005, CDRL Item: B023
8. Federal Aviation Administration, Flight Plan 2005 – 2009, February 2005.
9. Federal Aviation Administration, Safety Management System Manual, version 1.1, May 21, 2004.
10. Federal Aviation Administration, National Airspace System, System Engineering Manual, version 3.0, September 30, 2004.
11. Federal Information Processing Standards (Draft) Publication 183, Integration Definition for Function Modeling (IDEF0), December 21, 1993.
12. International Council on Systems Engineering, Systems Engineering Handbook, ver. 2a, Technical Board of INCOSE, June 2004.
13. Requirements Document for En Route Automation Modernization, Approved April 21, 2003
14. U.S. Department of Transportation, Federal Aviation Administration, Order 8040.4, Safety Risk Management.

Acronym List

ACB-200	System Engineering & Safety Division, WJHTC, FAA
ACB-210	System Engineering & Integration Group, WJHTC, FAA
AMS	Acquisition Management System
ARTCC	Air Route Traffic Control Center
ATC	Air Traffic Control
ATCBI	Air Traffic Control Beacon Interrogator
ATCRBS	Air Traffic Control Radar Beacon System
CP	Conflict Probe
ERAM	En Route Automation Modernization
FAA	Federal Aviation Administration
ICAO	International Civil Aviation Organization
IDEF0	Integration Definition for Function Modeling
INCOSE	International Council on Systems Engineering
M&C	Monitor and Control
NAS	National Airspace System
PMP	Project Management Professional (Certified credentialing program of the Project Management Institute)
SDOE	System Design and Operational Effectiveness (Graduate program from Stevens Institute of Technology's Charles V. Schaefer, Jr. School of Engineering)
SEM	System Engineering Manual
SMS	Safety Management System
SOC	Systems Operations Center
SRM	Safety Risk Management
TFM	Traffic Flow Management
URET	User Request Evaluation Tool
WJHTC	William J. Hughes Technical Center

Appendix A – Responsibilities within the SRM Process

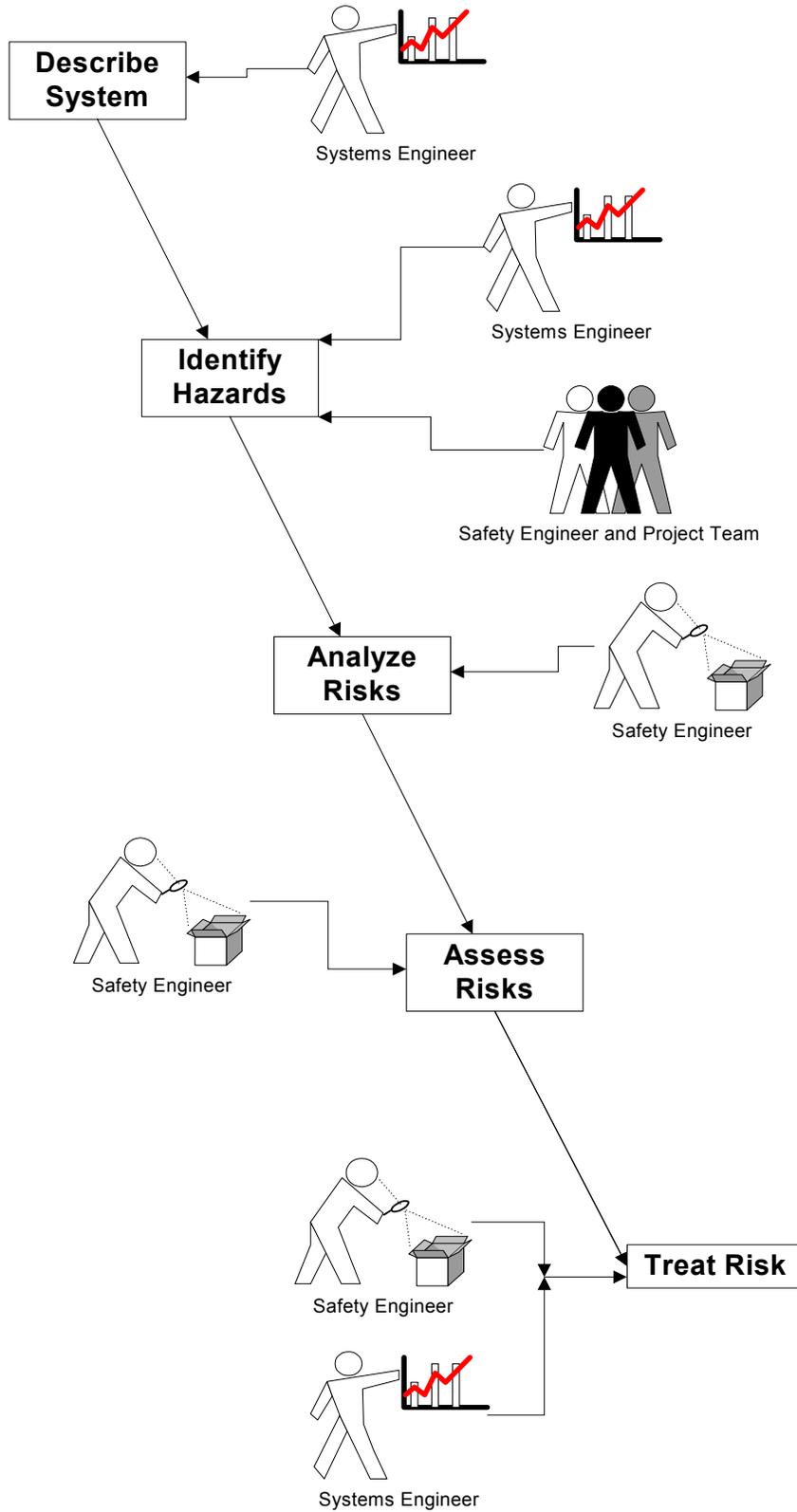


Figure 8: Responsibilities within the SRM Process

Appendix B – Case Study System Functions

The following list of ERAM functions is the result of the describe system step:

- Support tactical surveillance capabilities
- Support strategic surveillance capabilities
- Perform surveillance data processing
- Perform flight data automation
- Track aircraft
- Perform trajectory modeling capabilities
- Support collaborative processing, flexible airspace structures, and dynamic routes
- Provide information on NAS status, traffic management initiatives, and other ATC constraints and flight progress.
- Process flight plan positions
- Provide meteorological information
- Provide aeronautical information
- Support for routine and special military aircraft operations
- Perform traffic flow management
- Provide decision tools
- Process and monitor conflict alerts
- Perform system recording and playback that support error processing and operational response to time-critical search and rescue operations, incidents, and accidents
- Provide air-ground communications including data messages and communications among systems
- Support subsystems, such as ETMS, CPDLC, CTAS, URET, Conflict Probe (CP), and NIMS
- Provide the ability to monitor, reconfigure, and restore the system and certify the service from the ARTCC SOC
- Perform Monitor and Control (M&C) capabilities, such as correlating and managing events, monitoring network health, gathering performance data, performing diagnostics on sub-system errors; downloading and using support tools from the SOC; and configuring, re-configuring, and verifying proper hardware operation.
- Support other systems, such as ASR, ARSR, FPS, Air Traffic Control Beacon Interrogator (ATCBI), Mode S, and Air Traffic Control Radar Beacon System (ATCRBS) surveillance sources.

Appendix C – Case Study Identify Hazards

Based on the functions identified in Appendix B – Case Study System Functions, the following potential hazards were identified:

- Loss of tactical surveillance capabilities
- False tactical surveillance
- Loss of strategic surveillance capabilities
- False strategic surveillance
- Loss of surveillance data processing capabilities
- Loss of flight data automation capabilities
- Loss of tracking capabilities
- Inaccurate tracking
- Loss of trajectory modeling capabilities
- False trajectory models
- Loss of flight plan position processing
- Inaccurate flight plan position
- Loss of meteorological information
- False meteorological information
- Loss of aeronautical information
- Loss of support for routine and special military aircraft operations
- Loss of decision tools
- Missed conflict alert
- False conflict alerts
- Conflict alert sounds too many "false alarms"
- Loss of traffic flow management (TFM)
- Incorrect TFM metering
- Incorrect TFM sequencing
- Loss of system recording and playback that support error processing and operational response to time-critical search and rescue operations, incidents, and accidents
- Corrupted system recording
- Loss of communications
- Security breach of communications – unauthorized access
- Corrupted data messages.

- Unauthorized disclosure of confidentially sensitive data
- Losses of the ability to monitor, reconfigure, and restore the system and certify the service from the ARTCC SOC
- Loss of Monitor and Control capabilities, such as correlating and managing events, monitoring network health, gathering performance data, performing diagnostics on sub-system errors; downloading and using support tools from the SOC; and configuring, re-configuring, and verifying proper hardware operation.
- False network health, false performance data, false performance diagnostics, and incorrectly verified hardware operation
- Loss of information on NAS status, traffic management initiatives, and other ATC constraints and flight progress.
- Corrupted information on NAS status, traffic management initiatives, and other ATC constraints and flight progress.
- Dependency on other systems, such as ETMS, CPDLC, CTAS, URET, CP, and NIMS.
- Loss of support for other systems, such as ASR, ARSR, FPS, ATCBI, Mode S, and ATCRBS surveillance sources.

Appendix D – Control Case

In February 2005 Lockheed Martin completed a system hazard analysis [7]. In the study, fifteen (15) potential hazards were identified. They are the following:

- Loss of Surveillance Data
- Corruption of Surveillance Data
- Loss of Flight Data
- Corruption of Flight Data
- Loss of Alert Data
- Corruption of Alert Data
- Excessive Alerts
- Loss of Communications
- Corruption of Communications
- Loss of Weather Data
- Corruption of Weather Data
- Loss of M&C Capabilities
- Corruption of M&C Data
- Loss of Storage
- Corruption of Storage

Appendix E – Matching of Case Study to Control Case

The following lists each control hazard with the experimentally identified hazards underneath:

- Loss of surveillance data
 - Loss of tactical surveillance capabilities
 - Loss of strategic surveillance capabilities
 - Loss of surveillance data processing capabilities
 - Loss of tracking capabilities
- Corruption of surveillance data
 - False tactical surveillance
 - False strategic surveillance
 - Inaccurate tracking
- Loss of flight data
 - Loss of flight data automation capabilities
 - Loss of trajectory modeling capabilities
 - Loss of flight plan position processing
 - Loss of TFM
- Corruption of flight data
 - False trajectory models
 - Inaccurate flight plan position
 - Incorrect TFM metering
 - Incorrect TFM sequencing
 - Loss of support for routine and special military aircraft operations
 - Loss of decision tools
- Loss of alert data
 - Missed conflict alert
- Corruption of alert data
 - False conflict alerts
- Excessive alerts
 - Conflict alert sounds too many "false alarms"
- Loss of communications
 - Loss of communications

- Corruption of communications
 - Security breach of communications – unauthorized access
 - Corrupted data messages.
 - Unauthorized disclosure of confidentially sensitive data
- Loss of weather data
 - Loss of meteorological information
 - Loss of aeronautical information
- Corruption of weather data
 - False meteorological information
- Loss of M&C Capabilities
 - Loss of system recording and playback that support error processing and operational response to time-critical search and rescue operations, incidents, and accidents
 - Losses of the ability to monitor, reconfigure, and restore the system and certify the service from the ARTCC SOC
 - Loss of Monitor and Control capabilities, such as correlating and managing events, monitoring network health, gathering performance data, performing diagnostics on sub-system errors; downloading and using support tools from the SOC; and configuring, re-configuring, and verifying proper hardware operation.
- Corruption of M&C data
 - Corrupted system recording
 - False network health, false performance data, false performance diagnostics, and incorrectly verified hardware operation
- Loss of storage
 - Loss of information on NAS status, traffic management initiatives, and other ATC constraints and flight progress.
- Corruption of storage
 - Corrupted information on NAS status, traffic management initiatives, and other ATC constraints and flight progress.
- System dependencies (from [4])
 - Dependency on other systems, such as ETMS, CPDLC, CTAS, URET, CP, and NIMS
- Loss of support for other systems, such as ASR, ARSR, FPS, ATCBI, Mode S, and ATCRBS surveillance sources.