DOT/FAA/AR-09/12

Air Traffic Organization
NextGen & Operations Planning
Office of Research and
Technology Development
Washington, DC 20591

Safety Risk Analysis of Unmanned Aircraft Systems Integration Into the National Airspace System: Phase 1

September 2009

Final Report

This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161.

U.S. Department of Transportation
Federal Aviation Administration

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: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/AR-09/12		

4. Title and Subtitle	5. Report Date
SAFETY RISK ANALYSIS OF UNMANNED AIRCRAFT SYSTEMS INTEGRATION INTO THE NATIONAL AIRSPACE SYSTEM: PHASE 1	September 2009
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
James T. Luxhøj, Ph.D., Principal Investigator	
9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Rutgers University Department of Industrial and Systems Engineering 96 Frelinghuysen Road Piscataway, NJ 08854-8018	
	11. Contract or Grant No. 06-G-008
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Aviation Administration Air Traffic Organization NextGen & Operations Planning Office of Research and Technology Development Washington, DC 20591	Final Report July 13, 2006 - August 31, 2007
	14. Sponsoring Agency Code AIR-160

15. Supplementary Notes

The Federal Aviation Administration Airport and Aircraft Safety R&D Division COTR was Dr. Xiaogong Lee.

16. Abstract

This report describes the system-level development of a hazard taxonomy for Unmanned Aircraft Systems (UAS). The taxonomy is termed the Hazard Classification and Analysis System (HCAS) and was developed by researchers at Rutgers University through a cooperative agreement with the Federal Aviation Administration (FAA). It was particularly emphasized that this study should remain focused at the systems level and not become operational in perspective. The Rutgers Phase 1 approach is based on the FAA regulatory perspective (i.e., Title 14 Code of Federal Regulations chapters on Aircraft, Airmen, Certification/Airworthiness, Flight Operations, and others). Such an approach uniquely distinguishes the HCAS taxonomy from all other UAS hazard analyses being performed by the Department of Defense, the RTCA-Special Committee 203, etc. The Phase 1 research goal was to develop a generalized taxonomy of system-level UAS hazards that would have broad applicability across FAA part types. The intent was that this Phase 1 study would lead to general research recommendations and guidelines in high-level support of the FAA UAS Program Office. The report describes the developmental steps leading to the HCAS taxonomy.

17. Key Words	18. Distribution Statement
Unmanned Aircraft System, Hazard and risk analysis	This document is available to the U.S. public through the National Technical Information Service (NTIS) Springfield, Virginia 22161.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	84	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

ACKNOWLEDGEMENTS

Dr. James T. Luxhøj, the Principal Investigator, acknowledges the contributions of Mr. Ahmet Oztekin, Ph.D. a student at Rutgers University, to this research and technical report. Dr. Luxhøj also acknowledges the support, participation, and guidance of Federal Aviation Administration staff, Dr. Xiaogong Lee, Mr. Michael Allocco, Mr. Steve Swartz, and Mr. Robert Anoll, to this Phase 1 research. Dr. Luxhøj is also appreciative of the technical expertise and comments by the FJ Leonelli Group, Inc. in their review of the draft of this Phase 1 technical report.

TABLE OF CONTENTS

			Page
EXECUTIVE SUMMARY			xi
1.	INTRODUCTION		1
	1.1	Purpose	1
	1.2	Background	1
	1.3	Related Documents	6
2.	DISCUSSION		7
	2.1	Methodology	7
	2.2	Generation of Hazard Scenarios	8
	2.3	Hazard Classification and Analysis System	9
	2.3.1	The HCAS Version 1.0	10
	2.3.2	The HCAS Version 2.0	11
3.	PRIORITIZATION APPROACH		14
	3.1	Methodology: Mapping Scenarios Into the HCAS Framework	15
	3.1.1	Hypothetical Scenarios	15
	3.1.2	Mapping Process	16
	3.2	The HCAS Prioritization	22
	3.3	The HCAS Results, Analysis, and Remarks	24
	3.3.1	The UAS System-Level Hazard Sources	24
	3.3.2	Airmen System-Level Hazard Sources	29
	3.3.3	Operations and NAS Interconnectivity System-Level Hazard Sources	31
	3.3.4	Environmental Hazard Sources	34
	3.3.5	Top 20 Hazard Sources	35
4.	CONCLUSIONS		36
5.	RESEARCH RECOMMENDATIONS		37
6.	BIBLIOGRAPHY		40
APPENDICES			
	A—Analytical Methods and Technology Reviews		
	B—The UAS e-Workbook		

LIST OF FIGURES

Figure		Page
1	Rutgers Phase 1 Multistep Research Approach	3
2	Representative Source Material	4
3	Positioning of Rutgers Phase 1 Research With the DO-264 Process	4
4	Safety Risk Management Process	5
5	Phase 1 Bottom-Up Approach	6
6	Relationship Among Hazard, Risk, and Mishap	7
7	Hammer's Hazard Modeling Approach	8
8	The HCAS Cube Model—Version 1.0	10
9	The FAA Regulatory Perspective	11
10	The HCAS Cube Model—Version 2.0	12
11	An Overview of UAS Hazard Prioritization	14
12	A Sample Scenario	16
13	The HCAS Outline	17
14	A Screen Capture of the Source File	22
15	Counting and Ranking Hazards	23
16	Ranking of Hazard Sources—UAS System-Level Hazard Source	26
17	Distribution of UAS System-Level Hazard Source Category	27
18	Distribution of Design Organization-Related Human Factors—UAS System-Level Hazard Source	28
19	Distribution of Design-Related Hazard Sources—UAS System-Level Hazard Source	28
20	Ranking of Subsystem-Level Hazard Sources—Airmen	30
21	Distribution of Human Factors in the Airmen System-Level Hazard Source	31

22 Ranking of Subsystem-Level Hazard Sources—Operations and NAS Interconnectivity 33

23 Distribution of Operations and NAS Interconnectivity System-Level Hazard Sources 33

24 Distribution of Hazard Sources—Environmental 34

25 Distribution of Top 20 UAS Hazard Sources According to the HCAS System-Level Categorization 36

LIST OF TABLES

Table		Page
1	Representative UAS Scenario Themes	9
2	Hazard Scenario Description for the First Scenario	18
3	Mapping of Scenario 1 Into the HCAS Framework	19
4	Narrative Text From Scenario 7	20
5	Key Text Identifying Hazards	21
6	Mapping of Scenario 7 Into the HCAS Framework	21
7	The UAS System-Level Hazard Sources	25
8	Airmen System-Level Hazard Sources	29
9	Operations and NAS Interconnectivity System-Level Hazard Sources	32
10	Environmental Hazard Sources	34
11	Top 20 UAS Hazard Sources for a Given Scenario Set	35

LIST OF ACRONYMS

ATC	Air traffic control
BBN	Bayesian Belief Network
CAMI	Civil Aerospace Medical Institute
CCA	Cause-consequence analysis
CFR	Code of Federal Regulations
CPD	Conditional probability distribution
CRM	Crew Resource Management
DAG	Directed acyclic graph
DoD	Department of Defense
ETA	Event tree analysis
FAA	Federal Aviation Administration
FMEA	Failure mode and effects analysis
FTA	Fault tree analysis
GAIN	Global Aviation Information Network
HALE	High-Altitude, Long-Endurance
HAZOP	Hazard and operability analysis
HCAS	Hazard Classification and Analysis System
HFACS	Human Factors Analysis and Classification System
HHM	Hierarchical Holographic Modeling
JPD	Joint probability distribution
LEDTools	Logic-Evolved Decision Tools
LTA	Less than adequate
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
PRA	Preliminary risk analysis
SC	Special Committee
SDHA	Scenario-Driven Hazard Analysis
SMS	Safety Management System
SRM	Safety Risk Management
UAS	Unmanned Aircraft System

EXECUTIVE SUMMARY

The National Airspace System (NAS) in the United States is becoming an increasingly complex array of commercial and general aviation aircraft, very light jets, unmanned aircraft systems, reusable launch vehicles, rotorcraft, airports, air traffic control, weather services, and maintenance operations, among others. This increased system complexity necessitates the application of systematic safety risk analysis methods to effectively manage the safety of the NAS.

As such, the Rutgers University Phase 1 Unmanned Aircraft Systems (UAS) research objectives may be summarized as

- to identify, categorize, and evaluate potential system-level hazards of UAS operations in the NAS.
- to coordinate the hazard identification and subsequent analysis with FAA offices.
- to focus on civil (i.e., public) applications.

This report describes the system-level development of a hazard taxonomy for UAS. The taxonomy is termed the Hazard Classification and Analysis System (HCAS) and was developed by researchers at Rutgers University in consultation with the Federal Aviation Administration (FAA). The research goal was to develop a generalized taxonomy of system-level UAS hazards that would have broad applicability across FAA part types. The intent was that this Phase 1 study would lead to general research recommendations and guidelines in high-level support of the FAA UAS Program Office. Moreover, it should be emphasized that the Rutgers Phase 1 approach is based on the FAA regulatory perspective (i.e., Title 14 Code of Federal Regulations) chapters on Aircraft, Airmen, Certification/Airworthiness, Flight Operations, and others). Such an approach uniquely distinguishes the HCAS taxonomy from all other UAS hazard analyses being performed by the Department of Defense, the RTCA-Special Committee 203, among others.

The five primary Rutgers Phase 1 research tasks involved:

1. Identifying UAS hazards and controls within the NAS.
2. Developing a system-level taxonomy for categorization of UAS hazards.
3. Developing a method for prioritization of UAS hazards.
4. Conducting analytical methods and supporting technology reviews to support the system-level analysis of UAS operations.

5. Formulating a long-term research plan to further support system-level analyses of UAS integration into the NAS.

This report describes the detailed integrated approach that was used to develop the taxonomy. This approach was based on system safety/risk analysis principles, and decision analytic methods for hazard categorization/prioritization, blended with inductive reasoning from hypothesized UAS scenarios to establish a systems-level framework to eventually assess the risks of emergent aeronautical operations into the NAS. The HCAS, or "cube" model, includes the four primary hazard sources or "cubes" of Airmen, Operations and NAS Interconnectivity, UAS, and Environment, and their corresponding subelements. This report presents the Phase 1 developmental steps leading to the taxonomy, definitions of the taxonomy elements, and representative analyses that could be performed with such a taxonomy. Finally, recommendations for a multiyear UAS safety risk research plan are also included.

1. INTRODUCTION.

1.1 PURPOSE.

The National Aerospace System (NAS) in the United States is becoming an increasingly complex array of commercial and general aviation aircraft, unmanned aerial system, reusable launch vehicles, rotorcraft, airports, air traffic control, weather services, and maintenance operations, among others. This increased system complexity necessitates the application of systematic safety risk analysis methods to understand, eliminate where possible, and reduce or mitigate risk factors. This study was performed to develop a generalized taxonomy of system-level UAS hazards that would have a broad applicability across Federal Aviation Administration (FAA) part types. In response to a research need communicated with the FAA Research and Technology Development Office, Airport and Aircraft Safety Group, researchers from Rutgers University, in a cooperative agreement with the FAA, developed a taxonomy known as the Hazard Classification and Analysis System (HCAS). Initial effort was to perform a system-level assessment that characterized Unmanned Aircraft System (UAS) hazards and risks. The research goal was to develop a generalized taxonomy of system-level UAS hazards that would have broad applicability across FAA part types. The intent was that this Phase 1 study would lead to general research recommendations and guidelines in high-level support of the FAA UAS Program Office. Thus, the Rutgers Phase 1 research objectives may be summarized as

- to identify, categorize, and evaluate potential system-level hazards of UAS operations in the NAS.
- to coordinate the hazard identification and subsequent analysis with FAA offices.
- to focus on civil (i.e., public) applications.

It should be emphasized that the resulting hazard taxonomy developed by the Rutgers Phase 1 research approach is based on the FAA regulatory perspective (i.e., Title 14 Code of Federal Regulations (CFR) chapters on Aircraft, Airmen, Certification/Airworthiness, Flight Operations, etc.). Such an approach uniquely distinguishes the developed taxonomy from all other UAS hazard analyses being performed by the Department of Defense (DoD), the RTCA-Special Committee (SC) 203, among others.

1.2 BACKGROUND.

The FAA's mission is to ensure the safe and efficient use of the navigable airspace in the United States; to regulate air commerce in such a manner as to best promote its development and safety; to promote a common system of air traffic and navigation for both military and civil aircraft; and to promote, encourage, and develop civil aeronautics. As such, a safety risk analysis of UAS integration into the NAS is highly aligned with the FAA's mission statement.

A UAS is defined as being comprised of the

> "…manufactured integrated system including the architecture, operations, procedures, and functions to support the Unmanned Aerial Vehicle (UAV), ground control, and command, communication, and control (C3) data links. The vehicle is comprised of airframe, mechanical, propulsion, and avionic subsystems. Ground control includes the pilot interface and support efforts: flight planning, maintenance, preparation and procedures. The C3 interface includes the data link between the vehicle or other vehicles and ground control. There is also communications between the vehicle and satellites concerning Global Positioning System (GPS)." (Allocco, 2006a, p. 10)

UAS applications are quite diverse. Applications include remote sensing, such as power line or pipeline monitoring, mapping, meteorology, geology, atmospheric monitoring, and agriculture. A UAS may also be used in security operations for threat detection, tracking, security monitoring, and possible mitigation (i.e., weapon disposal). Public safety applications include accessing hazardous areas, hazardous sites, firefighting, enforcement, search and rescue, disaster response, communication relay, visual recording and evaluation, and mitigation delivery. Commercial applications include weather monitoring and sensing, cargo transport, advertising, and broadcasting. Military applications involve remote weapon deployment, battlefield management, monitoring, target identification, detection, and communication. Research and development applications include high-altitude research, human factors research, flight endurance, fuel consumption, atmospheric monitoring and measurement, advanced flight dynamics, radiation monitoring, and materials science testing (Allocco, 2006a, p. 12).

Sponsored by the National Aeronautics and Space Administration (NASA) and industry, with participation by the FAA and the DoD, Access 5 was a national project to introduce High-Altitude, Long-Endurance (HALE) UAS for routine flights in the NAS. The stated goal of Access 5 is to foster the development of a robust civil and commercial market for HALE UAS. Thus, there is a national effort to promote the routine use of UAS applications in the NAS, thereby strengthening the need for a systematic approach to modeling the risks associated with the added complexity to the NAS. However, routine UAS operations in the NAS pose potentially new and different hazards and risks. The research need is to perform system safety risk analyses that characterize UAS hazards and risks with specific recommendations for safe operations in the NAS with guidelines for the eventual certification process.

The Rutgers Phase 1 safety risk analysis study focused on civil (i.e., public) applications of UAS integration into the NAS.

The Rutgers Phase 1 UAS/NAS Integration Safety Risk Study is concerned with a system-level assessment that characterizes UAS hazards and risks. Research outcomes include

recommendations and guidelines for long-term investigations and studies. In particular, the Phase 1 research objectives are described as:

- Identification of the UAS hazards and controls within the NAS.
- Development of a system-level taxonomy for categorization of UAS hazards.
- Development of a method for prioritization of UAS hazards.
- Administration of performance of analytical methods and supporting technology reviews to support the system-level analysis of UAS operations.
- Formulation of a long-term research plan to further support system-level analyses of UAS integration into the NAS.

As presented in figure 1, the Rutgers research team followed a systematic multistep approach in the performance of this UAS research study. To initiate the research, the Rutgers team reviewed a number of UAS-related documents. Representative documents are listed in figure 2. In particular, the RTCA-203 Guidance Material and Considerations for Unmanned Aircraft Systems (DO-304), Detect, Sense and Avoid Safety Metrics (2007), and Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications (DO-264) were reviewed. The suggested RTCA tripod model of NAS segments was studied and found to have an operational perspective that, while important, did not meet the Rutgers research objective of developing a system-level framework for characterizing UAS hazards. In addition, the Rutgers research team was requested to position its research with respect to the RTCA DO-264 methodology, which is shown in figure 3. Fundamentally, the Rutgers research team followed the Safety Risk Management (SRM) process as depicted in figure 4 that is consistent with guidelines included in Bahr (1997), as well as the FAA System Safety Handbook (2007). Note that the RTCA's tripod model included in figure 2 differs from the FAA SRM process.

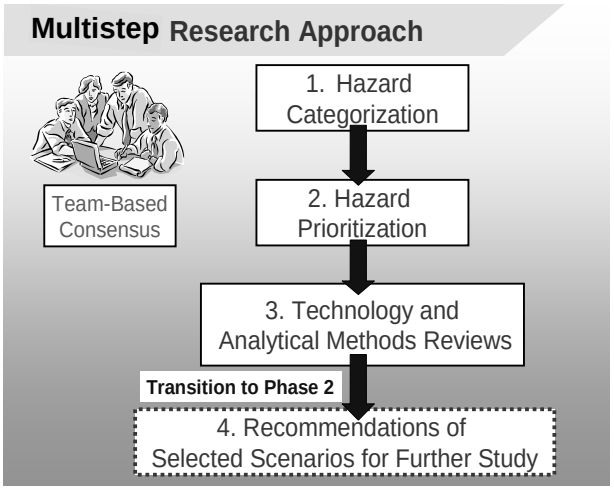


Figure 1. Rutgers Phase 1 Multistep Research Approach

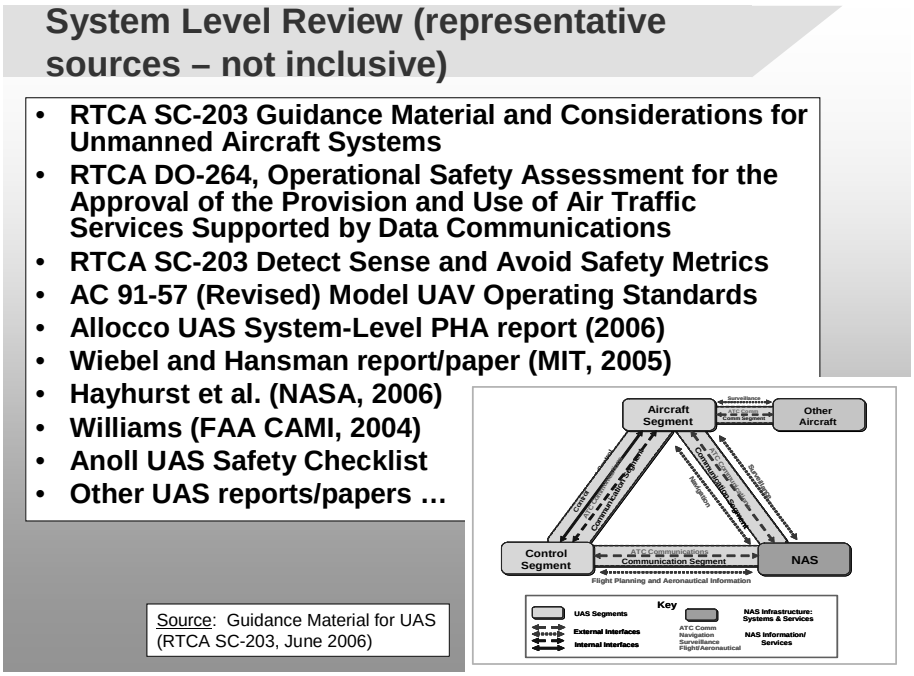


Figure 2. Representative Source Material

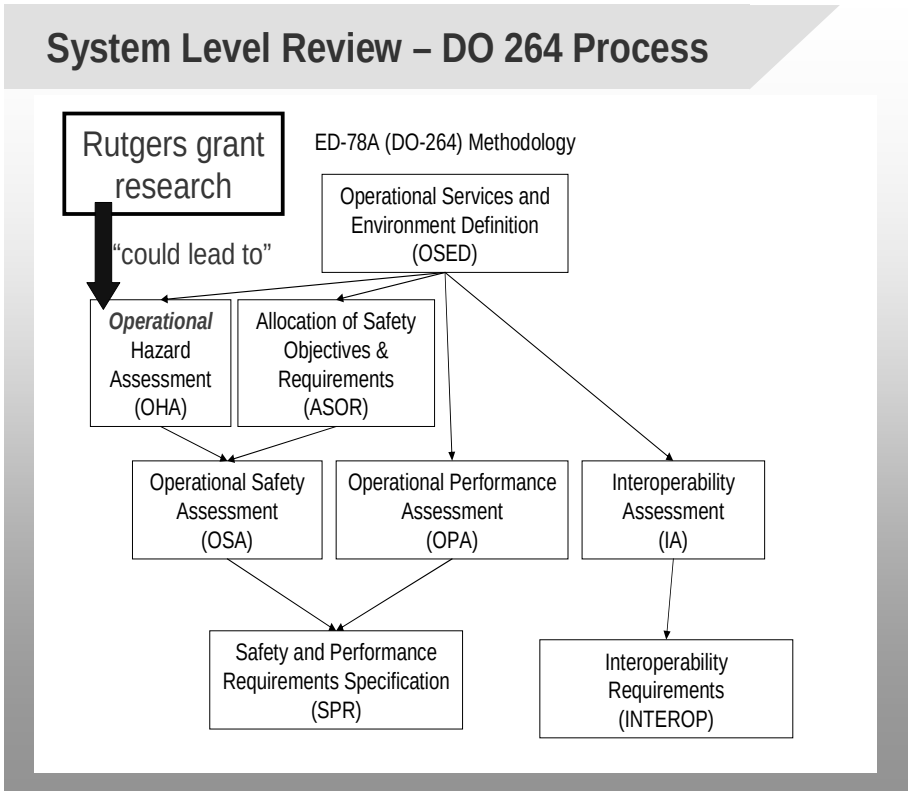


Figure 3. Positioning of Rutgers Phase 1 Research With the DO-264 Process

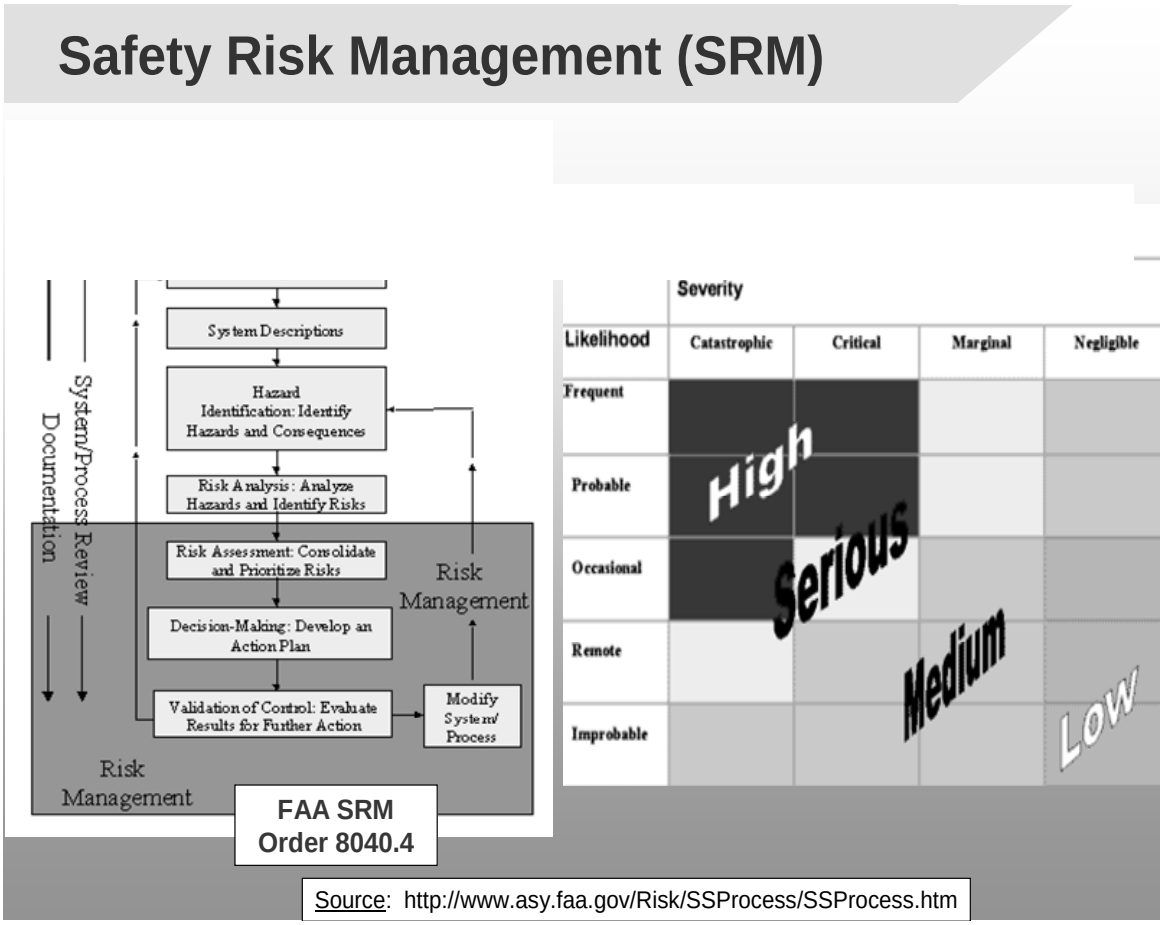


Figure 4. Safety Risk Management Process

Thus, the multistep research approach manifested into a more detailed, "bottom-up" systematic study, as shown in figure 5. The identification of UAS system-level hazards was based primarily upon a review of 208 hypothesized UAS scenarios (see Allocco, 2006a). This led to the development of a new taxonomy unique to the UAS domain. Based on this taxonomy, an implicit prioritization of UAS hazards was accomplished and is further described in section 3 of this report. As indicated in figure 5, the Phase 1 research hazard analysis forms the basis for subsequent risk analysis in a Phase 2 study. Additionally, the UAS system-safety Phase 1 study contributes, to some extent, to the overall development of a component of the higher-order, much larger scale Safety Management System (SMS) research that is underway.

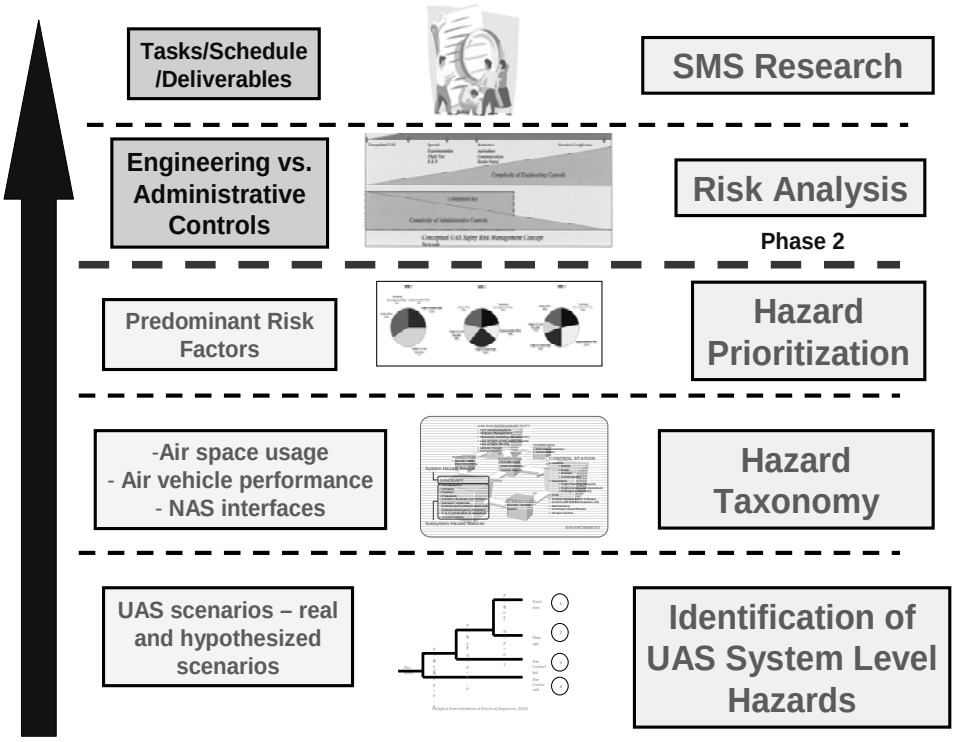


Figure 5. Phase 1 Bottom-Up Approach

1.3 RELATED DOCUMENTS.

The following documents relate directly to the issues addressed herein and were used as background references:

- RTCA SC-203 Guidance Material and Considerations for Unmanned Aircraft Systems
- RTCA DO-264, Operational Safety Assessment for the Approval of the Provision and Use of Air Traffic Services Supported by Data Communications
- RTCA SC-203 Detect, Sense and Avoid Safety Metrics
- Advisory Circular AC 91-57 (Revised) Model UAV Operating Standards
- Allocco UAS System-Level Preliminary Hazard Analysis report (2006a)
- Wiebel and Hansman report/paper (2005)
- Hayhurst, et al. (2006)
- Williams (2004)
- Anoll UAS Safety Checklist

In addition to these documents, other documents and research papers reviewed are listed in section 6.

2. DISCUSSION.

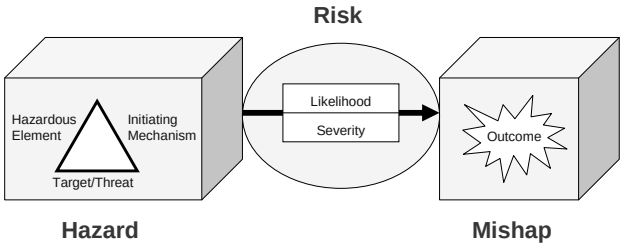
This section describes the methodology used to develop the systems-level taxonomy of UAS hazards.

2.1 METHODOLOGY.

Before proceeding with a description of the methodology used in UAS hazard categorization, it is important to establish some basic terminology. For the purpose of the Rutgers research, the following definition of a hazard is used:

> A hazard is a state or set of conditions of a system that, together with other conditions in the environment of the system, may lead to an unsafe event (adapted from Leveson, 1995).

Also, it is important to understand the relationship between hazard, risk, and mishap, as depicted in figure 6. Ericson (2005) describes a hazard triangle, portrayed in figure 6, which includes the hazardous element, initiating mechanism, and the target/threat. This notion of a hazard triangle influenced the Rutgers research team to think of hazard "sources." It should be noted that figure 6 is a simplification, and that mishap causation is not as linear as the figure suggests. Most likely, there will be multiple hazards acting in a nonlinear causative fashion. Further, this model can also be used to analyze a mishap outcome by showing the events leading to it. Although a mishap occurrence is rare, this model is still capable of identifying hazards (including hazardous elements, initiating mechanisms, and targets/threats) and associated risk, which may potentially result in a mishap outcome. The UAS hazard identification step involved identifying the components of the UAS and its NAS integration, treating the components as potential sources of system-level hazards, and decomposing the system further into its subcomponents. As such, the four primary hazard sources were initially identified as Aircraft, UAS-NAS Interconnectivity, Control Station, and Environment.



Source: Adapted from C.A. Ericson II, *Hazard Analysis Techniques for System Safety*, Hoboken, NJ: John Wiley & Sons, 2005.

Figure 6. Relationship Among Hazard, Risk, and Mishap

2.2 GENERATION OF HAZARD SCENARIOS.

The underlying system safety approach builds upon the concepts presented in Hammer (1972) and Raheja and Allocco (2006). In discussing hazard analysis, Hammer presents concepts of initiators, contributors, and primary hazards. For example, in figure 7, depicting the sequence of events leading to a rupture of a high-pressure air tank, the injury and/or damage resulting from the rupture of the tank are considered primary hazards. Moisture that causes the corrosion of the tank is considered the initiating hazard, and the corrosion, loss of strength, and pressure are viewed as contributory hazards. There is typically not a single hazard leading to an accident or incident, but rather multiple hazards activated by some triggering mechanism. This is especially true of system accidents that are the result of numerous initiators, contributors, and combinations of errors, failures, and malfunctions.

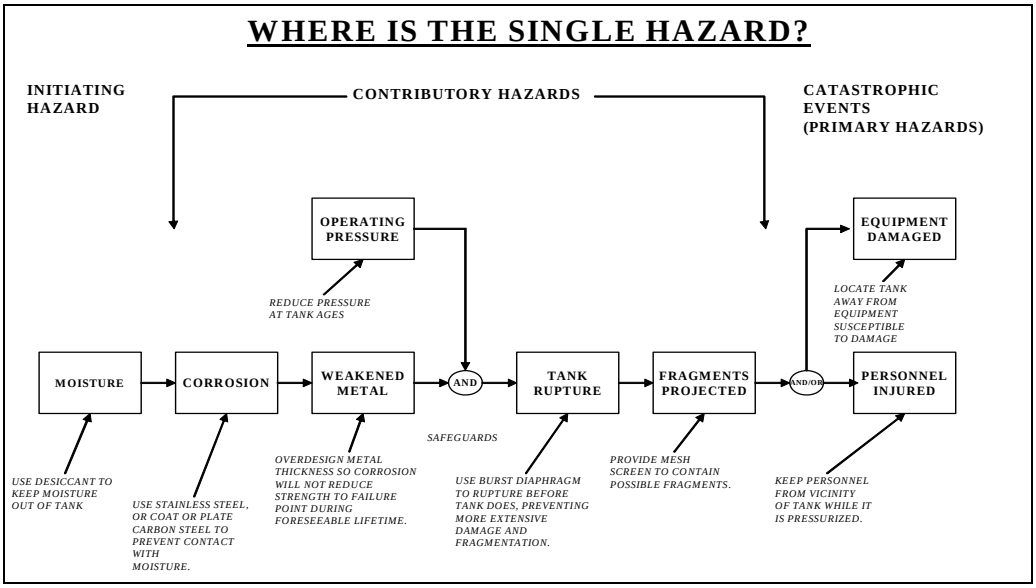


Figure 7. Hammer's Hazard Modeling Approach (Allocco, 2006a)

Allocco (2005) and Raheja and Allocco (2006) further extend Hammer's approach to develop the Scenario-Driven Hazard Analysis (SDHA) process. The SDHA may be used to understand the dynamics of either an actual or hypothesized accident. This report illustrates the results of an application of the SDHA process to the identification of hazard system and subsystem sources for emergent aeronautical operations, such as UAS.

The first step in the SDHA involves the generation of possible scenarios. Scenario development and characterization include the following: scenario description, initial contributors, subsequent contributors, life-cycle phase, possible effect, system state and exposure, recommendations, precautions, and controls. In a "conversation" or "dialogue" with subject matter experts, knowledge about accidents or possible accidents is elicited using "scenario themes" (see Raheja and Allocco, 2006), which are short, concise statements that describe the primary hazards and main contributory hazards. In the case of the scenario development for the UAS, 208 hazard scenario themes were identified in multiple sessions with experts. Representative scenario themes are presented in table 1. Scenario statements typically provide text as to how or why

potential accidents may occur. The accident life-cycle, including design, certification, surveillance by FAA Flight Standards, operations, maintenance, and training, should be considered. Luxhøj (2005a and 2005b), Lechner and Luxhøj (2005), and Andres, Luxhøj, and Coit (2005) also use induction from scenarios to develop risk models of commercial aircraft accidents for the assessment of a portfolio of new aeronautical products. In the situation of emergent aeronautical operations where actual accident or incident data is sparse, inductive reasoning from hypothesized scenarios is a plausible alternative. Fitzgerald (2007) also supports the use of reasoning from plausible scenarios in the case of human reliability assessment. It is recommended to use actual UAS incident or accident data if these are available.

Table 1. Representative UAS Scenario Themes (Allocco, 2006a)

List of Hazard Scenarios	
Seq. #	Hazard Scenario/ Description/Discussion
1	The transitional planning for UAS NAS integration is Less Than Adequate (LTA) and the planning does not allow for system design, development time, and maturity. Situation results in increased accident risks.
2	Assumptions concerning system reliability and availability maturity are LTA. There are transitional risks associated with UAS design, development time, system reliability, reliability growth, availability and maturity. Current situation results in vehicle not meeting expected NAS-level availability and reliability requirements associated with Catastrophic and Hazardous risks, consequently there may be increased accident risk.
3	Current DoD and contractor system safety and system reliability analyses and related data are not accessible to the FAA. As a result there are inappropriate assumptions made concerning knowledge of system safety and system reliability that may lead to increased risk.
4	Due to physical design limitations vehicles may not meet NAS-level availability and reliability requirements associated with Catastrophic and Hazardous risks, consequently there may be increased accident risk.

2.3 HAZARD CLASSIFICATION AND ANALYSIS SYSTEM.

Subsequent to the scenario development step, a more concise method for classifying and communicating the hazards was created. As is often the case, the “conversation” or “dialogue” with subject matter experts involved in the development of scenario themes sometimes included the use of vernacular statements or specialized language that may not necessarily be conducive to analysis. To facilitate the next step of classification and analysis, a new hazard taxonomy was developed termed the Hazard Classification and Analysis System (HCAS). The intent of this taxonomy was to facilitate the communication of the hazards as construed during the previous scenario development step.

2.3.1 The HCAS Version 1.0.

Using the definition, as adapted from Leveson (1995), that a hazard is a state or set of conditions of a system that, together with other conditions in the environment of the system, may lead to an accident (loss event), the taxonomy depicted in figure 8 was created. For UAS, the three primary hazard sources are identified as Aircraft, Control Station, and NAS Interconnectivity. These three hazard system sources form the three main HCAS "cubes." It is acknowledged that these three primary hazard sources are operative in a context, so "Environment" is included as the backdrop. For each of the system hazard source potentials, subsystem elements are also identified in figure 8. For example, for the system hazard source of "Aircraft," the subsystem hazard sources of aerodynamics, airframe, payload, propulsion, avionics hardware and software, sensors/antennas, control and communication link, onboard emergency recovery, verification and validation, and human factors are included. Note also that the interactions among the three system hazard sources are depicted in figure 8. The notion of a "hazard source" is consistent with hazardous element of Ericson's "hazard triangle" and recognizes that a hazard needs a trigger or initiator to move it from a dormant to an active state, thus focusing on the hazard's "potential" to do harm. A summary paper on HCAS Version 1 is presented in Oztekin, Luxhøj, and Allocco (2007).

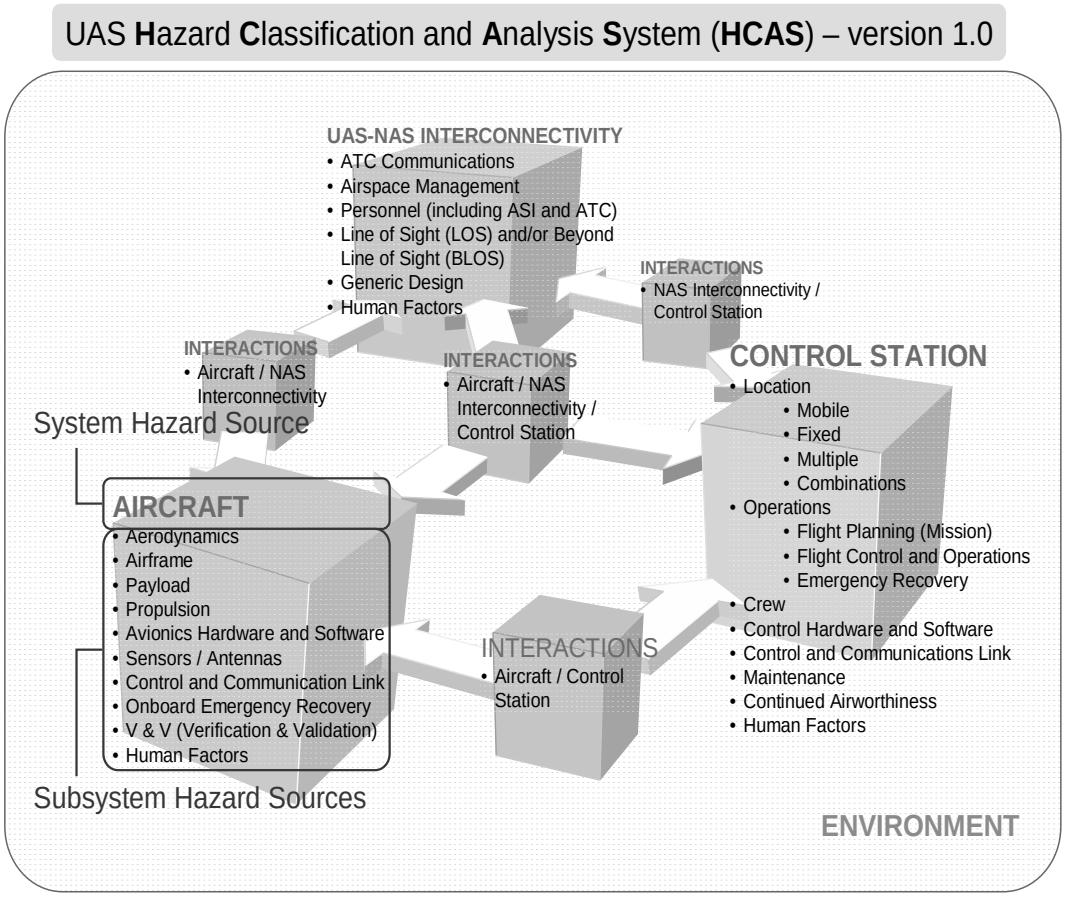


Figure 8. The HCAS Cube Model—Version 1.0

2.3.2 The HCAS Version 2.0.

In subsequent discussions with the FAA UAS Program Office, there was a recommendation that the proposed Rutgers UAS hazard framework needs to consider, to some extent, alignment with the FAA's regulatory perspective dealing with 14 CFR on Aircraft, Airmen, Certification/Airworthiness, Flight Operations, etc., as noted in figure 9. Post meeting, an attempt by the Rutgers research team to move their proposed taxonomy closer to alignment with the 14 CFR Parts 121 and 91 was developed and is presented in figure 10. This alignment is consistent, to some extent, with the FAA document "UAS in the US NAS—Interim Operational Approval Guidance" (2005).

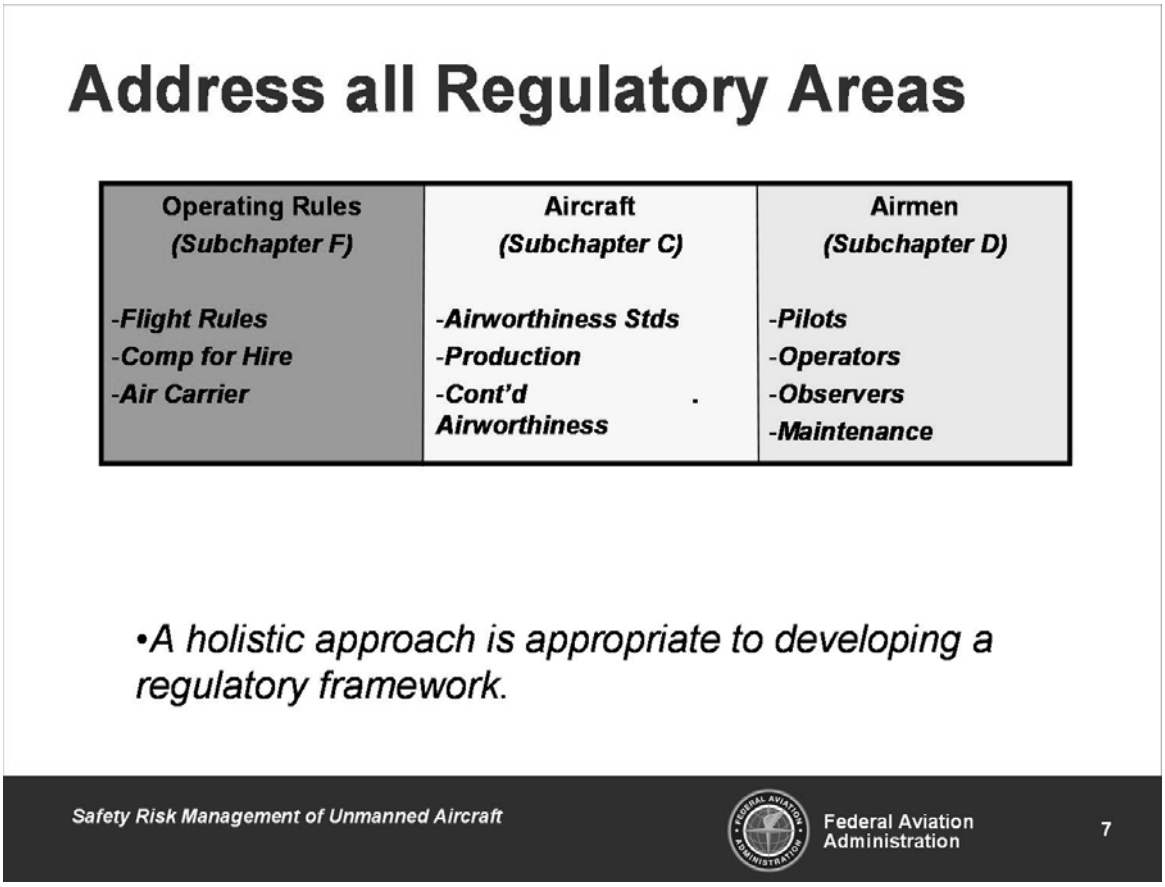


Figure 9. The FAA Regulatory Perspective (Anoll, 2007)

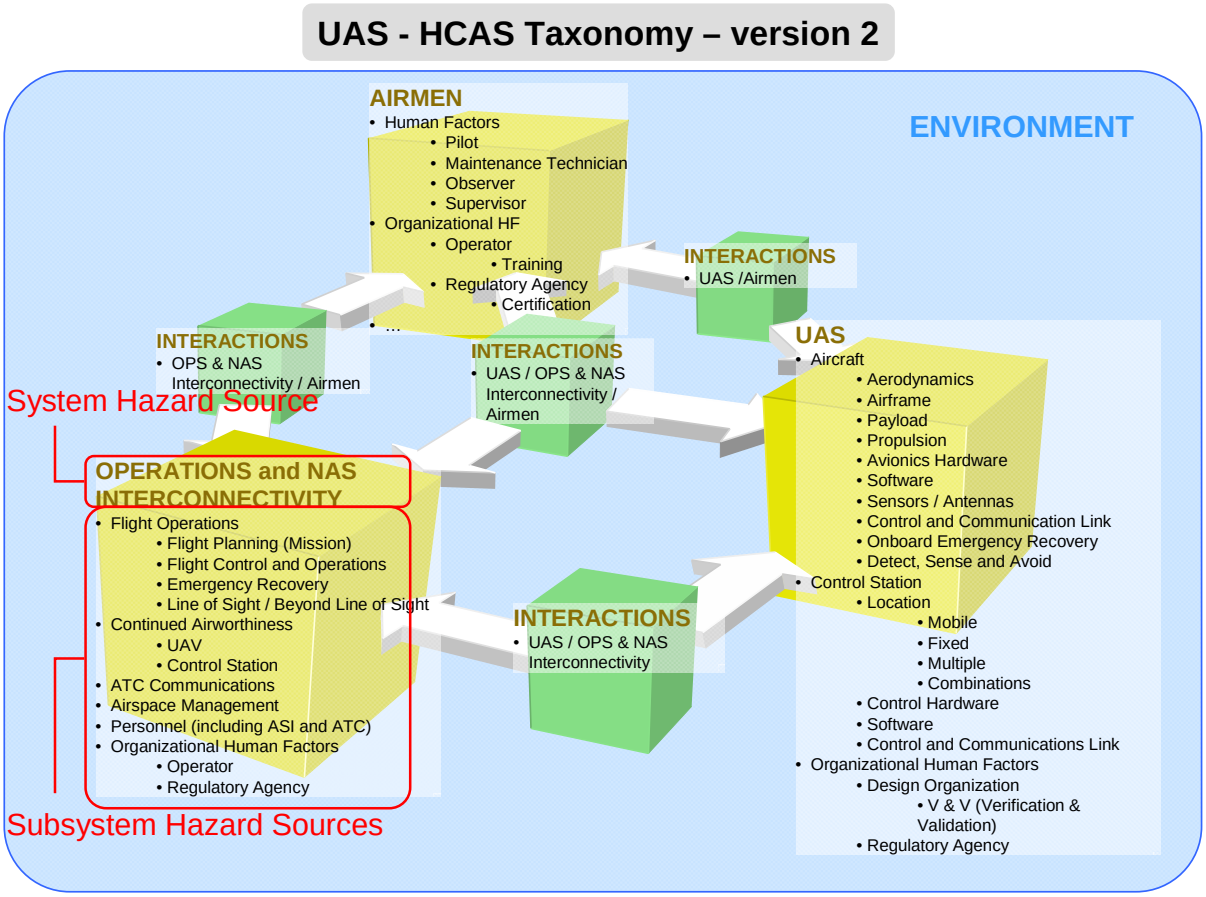


Figure 10. The HCAS Cube Model—Version 2.0

Note that in the HCAS Version 2, the system source of Control Station is now subsumed by a system hazard source termed UAS. Also, the system source of Aircraft from HCAS Version 1 is subsumed under UAS in version 2. Airmen is extracted from HCAS Version 1 into a separate system hazard source in HCAS Version 2. A new system hazard source termed Operations and NAS Interconnectivity is created in version 2. The Environment still forms a system hazard source as a backdrop in HCAS Version 2. Elements of Human Factors now appear in the three main HCAS system hazard sources. An excellent overview of UAS human factors issues is presented in Willams (2004). The HCAS Version 2 cube model is now more aligned, to some extent, with the FAA's 14 CFR chapters. It is recommended that additional reviews be conducted with knowledgeable members from the aviation community during a Phase 2 study to develop a more detailed regulatory alignment. Hayhurst, et al. (2006) provides excellent reflections on the potential hazards of the integration of UAS into the NAS and the implications for regulations. AeroVations (2004), Clothier and Walker (2006), Marsters (2003), Marsters and Sinclair (2003), Weibel and Hansman (2004), Wikland (2003), and Anoll (2006) provide additional insights on safety issues associated with UAS operations.

2.3.2.1 The HCAS Taxonomy Element Definitions.

At the crux of the HCAS mapping methodology, the definitions of the HCAS taxonomy elements exist. However, the mechanics of the mapping process, whose details are presented in section 3, call for examples, rather than conventional generic definitions. Therefore, the following list provides some helpful examples in addition to the definitions of the subsystem-level hazard sources, which may facilitate the replication of the mapping process on different scenario sets than the one used throughout the current research. The examples entail text fragments, in most cases just a single word, from the narrative of the actual scenarios mapped into the HCAS taxonomy. These examples can be used for a second party, such as another group of analysts, to map another set of UAS scenarios into the HCAS taxonomy and to perform subsequent risk and safety analysis.

Some basic terms frequently used throughout this section are repeated here to aid this discussion.

- Hazard

  A hazard is a state or set of conditions of a system that, together with other conditions in the environment of the system, may lead to an accident (loss event) (adapted from Leveson, 1995).

- Hazard Sources

  Four main hazard source categories encompassing the UAS domain are identified, as shown in figure 10. Each one of these four categories corresponds to a key component of the domains of interest. However, these components do not represent categories of hazards. They are categories of hazard sources and do not represent individual hazards for the UAS domain. They are primarily components of the UAS domain.

Almost each main system-level category of the HCAS taxonomy includes a human factors subsystem-level category. The handling of human factors in the UAS domain as separate subgroups facilitates the mapping process significantly and makes the distinction between human factors and nonhuman factors hazard sources much easier at the final analysis. Due to past experience with building human factors risk models for aviation accidents, it was decided to make use of a taxonomy specifically designed for aviation-related human factors for the purpose of mapping subsystem-level UAS human factors under the HCAS hierarchy. Therefore, elements of the "Human Factors Analysis and Classification System (HFACS)" are used for mapping the human factors subsystem-level hazard sources into the HCAS taxonomy. For an extensive discussion on HFACS, the reader is referred to the text by Wiegmann and Shappell (2003).

HCAS is meant to be used as a framework to categorize UAS-related hazards. Hence, each encounter with a new scenario set adds to its existing structure, thereby improving it.

3. PRIORITIZATION APPROACH.

This section presents how the HCAS may be used to develop an implicit prioritization of system-level UAS hazards. As previously mentioned, the primary objective of the current research is to develop a system-level hazard source taxonomy for the specific purpose of risk analysis of UAS. HCAS has an intuitive structure. It represents a promising tool to categorize hazard sources for aviation leading to a unique way to perform risk and safety analysis of the problem domain. However, the applicability of the HCAS taxonomy to the UAS domain still requires a demonstration.

For the purpose of demonstration, the HCAS taxonomy was applied to a set of hypothetical UAS hazard scenarios provided by the FAA. By applying the HCAS taxonomy, individual hazard sources were identified for each specific hypothetical scenario. Ultimately, within the context of the provided set of scenarios, the goal is to identify a set of hazard sources that exemplify a prominent portion of the risk associated with UAS operations. In other words, the goal is to rank UAS hazards given the hypothetical scenario set at hand.

In the next section, the methodology employed to identify and rank-order individual hazard sources using the HCAS framework is discussed in detail. When the mapping of the 208 scenarios to create the HCAS framework is complete, hazard "counts" may be obtained. These counts lead to implicit proportions or percentages of the hazard system and subsystem sources, as derived from the 208 hypothesized scenarios. It should be noted that these hypothesized scenarios were developed with the assistance of subject matter experts. These hazard percentages should not be considered absolute values but as "relative" proportions suggesting an implied rank ordering of hazards to assist, to some extent, in hazard prioritization. Figure 11 graphically depicts how SDHA contributes to an implicit prioritization of UAS hazards.

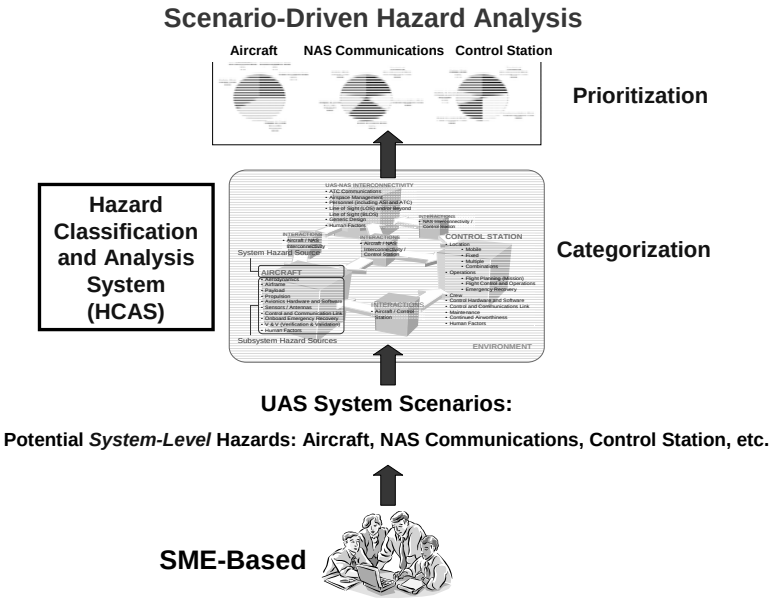


Figure 11. An Overview of UAS Hazard Prioritization

3.1 METHODOLOGY: MAPPING SCENARIOS INTO THE HCAS FRAMEWORK.

The identification of individual hazard sources within the narrative text of an individual scenario is referred to as mapping. More specifically, during the mapping process, each scenario is scrutinized to determine specific parts of its narrative text that correspond to a particular category in the HCAS hierarchy. Matching narrative fragments to a hazard source identified by the HCAS taxonomy constitutes, in a sense, a mapping of the hypothetical scenario using the HCAS framework.

Before illustrating the details of the mapping with some examples, it is essential to understand what the hypothetical scenarios entail. One should also note that the mapping methodology introduced in this report is developed independently of any particular set of scenarios. As a generic methodology, it is applicable to any scenario set across the aviation domain.

3.1.1 Hypothetical Scenarios.

There were 208 scenarios analyzed. In broad terms, each scenario describes a hypothetical hazard and a list of causal or contributing factors leading to this hazard. The narrative text for each hypothetical scenario consists of a single page and is presented in table format. Figure 12 depicts a typical scenario. For the purpose of this research, there are two columns of interest: Hazard Scenario/Description/Discussion and Initial/Contributors Hazards (Causes). These two columns contain all the information needed to identify the set of individual hazards and map them into the HCAS framework.

System Hazard Analysis:
(Risk Management Decisions, Design, Test, Operational, and other Life Cycle Risks)
UAS Integration into the NAS
Appendix A, Table A

POC: Mike Allocco, AFS-430

DRAFT DOCUMENT in Work

Version 2, Updated March 2006

Possible Initiating Hazard	Seq. # 82,91	Hazard Scenario/ Description/ Discussion	Initial /Contributory Hazards (Causes)	Mission/Phase/ System State (See note at footer)	Possible Effect	Vehicle KE < Risk: Initial/ Current/ Residual	Vehicle KE > Risk: Initial/ Current/ Residual	Vehicle W/Weapon Risk: Initial/ Current/ Residual	Recommended Precautions, Requirements, and Mitigations
LTA Design (LD)	7	The autonomous UAS functions, architecture, and operations, and not adequately understood, designed, or evaluated against potential Catastrophic and Hazardous risks, consequently there may be increased accident risk.	The autonomous UAS system is not adequately evaluated due to: Lack of resources Lack of knowledge associated with integrated risks Incomplete design details integrating functions, architecture, and operations Poor assumptions of risk Oversight Omissions Political influence Risk perception Additional risk control is not successfully applied. Vehicles may not meet NAS-level requirements, consequently failures and hazards can occur which could result in collision, loss of controlled flight, deviation from flight plan, or CFIT.	System risk adversely affects vehicles during worst case situations Vehicle is in motion: taxi, takeoff, climb, cruise, descending, landing when contingency occurs	Collision (OR) CFIT	IR = 2B	IR = 1B	IR = 1+C	12. In order to conduct systematic design and to identify and evaluate system risks a representation c the UAS/NAS integrated system is required. Develc an integrated diagram and/or model which details integrated functional, physical (architectural), proce and operational domains. Include discussions involving automated functions, processing, sensing, and detection. Describe both ground and avionics built-in-test capabilities, warnings, and cautions. De the pilot, operator, and controller interfaces, monito displays, and controls. Include information on proficiency and training. 13. Validate the UAS/NAS integrated system diagram/model and show evidence that the diagram/model has been used to conduct system saf engineering analyses, studies, and assessments; provide documentation to assure that the system risk have been eliminated or controlled to an acceptable level, in accordance with best practices, (e.g., Mil-S 882, FAA SSHB, FAR's, SSMP, and SMS, current versions.)

A-7

Limiting Assumptions and Notes: This analysis reflects worst case potential accidents; actual risks may be of lower severity or likelihood. Consider the worst case system states: poor operator visibility, minimal experience and training, minimal requirements, NAS traffic is present during vehicle flight path transition. Loss of controlled flight occurs over high density populated areas. Advanced technology may not be robust from a reliability or availability view. Fail-safe devices, backups, recovery, contingencies, and redundancy has just been verified. Airports or airstrips and not totally isolated or segregated. The engineering statistics may not have been proven and the UAS system is still under a reliability growth dynamic. The risks presented are general and will vary on a specific flight plan, operational evaluation, test, or mission. Specific phase, test, task, mission, contingency, or operational hazard analyses are required.

This analysis is not all inclusive. The analysis will be refined and updated as specific information is acquired. Recommended precautions, requirements, and mitigations are developed as the analysis progresses. These system-level recommendations are interrelated and consequently will enhance system mitigation. Not all interrelated recommendations are shown within these worksheets.

Figure 12. A Sample Scenario

3.1.2 Mapping Process.

In broad terms, the mapping process involves reading the narrative text of each scenario, identifying individual hazard sources, and matching them with the corresponding hazards source category of the HCAS.

The following examples of an actual scenario mapped into the HCAS framework illustrate the details of the mapping process. The HCAS framework is provided in figure 13 as quick reference.

OUTLINE – HCAS Taxonomy

1. **UAS (Systems Level)**
   - **1.1. Aircraft (Subsystems Level)**
     - 1.1.1. Aerodynamics
     - 1.1.2. Airframe
     - 1.1.3. Payload
     - 1.1.4. Propulsion
     - 1.1.5. Avionics Hardware and Software
     - 1.1.6. Sensors / Antennas
     - 1.1.7. Control and Communication Link
     - 1.1.8. Onboard Emergency Recovery
     - 1.1.9. Detect, Sense and Avoid
   - **1.2. Control Station**
     - 1.2.1. Location
       - 1.2.1.1. Mobile
       - 1.2.1.2. Fixed
       - 1.2.1.3. Multiple
       - 1.2.1.4. Combinations
     - 1.2.2. Control Hardware and Software
     - 1.2.3. Control and Communications Link
   - **1.3. Organizational Human Factors**
     - 1.3.1. Aircraft Design Organization
     - 1.3.2. Control Station Design Organization
     - 1.3.3. Regulatory Agency

2. **AIRMEN**
   - **2.1. Individual Human Factors (HF)**
     - 2.1.1. Pilot
     - 2.1.2. Maintenance Technician
     - 2.1.3. Observer
     - 2.1.4. Supervisor
   - **2.2. Organizational HF**
     - 2.2.1. Operator
       - 2.2.1.1. Training
     - 2.2.2. Regulatory Agency
       - 2.2.2.1. Certification

3. **OPERATIONS and NAS INTERCONNECTIVITY**
   - **3.1. Flight Operations**
     - 3.1.1. Flight Planning (Mission)
     - 3.1.2. Flight Control and Operations
     - 3.1.3. Emergency Recovery
     - 3.1.4. Line of Sight / Beyond Line of Sight
   - **3.2. Continued Airworthiness**
     - 3.2.1. UAV
     - 3.2.2. Control Station
   - **3.3. ATC Communications**
   - **3.4. Airspace Management**
   - **3.5. Personnel (including ASI and ATC)**
   - **3.6. Organizational Human Factors**
     - 3.6.1. Operator
     - 3.6.2. Regulatory Agency
     - 3.6.3. Design Organization

4. **ENVIRONMENTAL FACTORS**

5. **INTERACTIONS**
   - **5.1. UAS / Interconnectivity**
   - **5.2. UAS / Airmen**
   - **5.3. Interconnectivity / Airmen**
   - 5.4. **UAS / Interconnectivity / Airmen**

Figure 13. The HCAS Outline

During the mapping process, the most important parts of the narrative are found in the Hazard Scenario and Initial/Contributory Hazards columns. The Hazard Scenario column provides a brief description for the scenario at hand, as shown in table 2.

Table 2. Hazard Scenario Description for the First Scenario

Seq. # 82,91	Hazard Scenario/ Description/ Discussion
1	The transitional planning for UAS NAS integration is LTA and the planning does not allow for system design, development time, and maturity. Situation results in increased accident risks.

The description of the hypothetical scenario serves multiple purposes. For example, when performing future in-depth analysis on the mapped data, rather than referring to a particular scenario by an abstract number, the description, albeit a brief one, provides a context to the reference. In table 2, the extracted description is "transitional planning for the UAS NAS integration is Less Than Adequate (LTA)." Along with this brief description, for the purpose of mapping, this particular scenario is referenced by its number—in this case "1"—as assigned by the Allocco list of scenarios in the "Seq." column. The actual mapping of the scenario happens at the next step. This step focuses on the information provided in the "Initial/Contributory Hazards" column.

The initial and contributory hazards are associated with a particular scenario. The next task is to identify them explicitly. Even a cursory look at the scenario indicates that each line corresponds to a specific hazard.

Once individual hazards are identified, they are matched with their corresponding HCAS category, thereby creating a mapping of that particular scenario in terms of the HCAS framework. The final mapping for the first scenario is provided in table 3.

Table 3. Mapping of Scenario 1 Into the HCAS Framework

<table>
<tr><th></th><th colspan="4">HCAS Framework</th></tr>
<tr><th>Scenario Narrative Text</th><th>Hazard</th><th colspan="2">Subsystem-Level Hazard Source</th><th>System-Level Hazard Source</th></tr>
<tr><td>Inadequate knowledge</td><td>Inadequate knowledge</td><td rowspan="4">3.6.3. Design Organization</td><td rowspan="4">3.6. Organizational Human Factors</td><td rowspan="4">3. Operations and NAS Interconnectivity</td></tr>
<tr><td>Overconfidence, assumption of success</td><td>Overconfidence/ overreliance</td></tr>
<tr><td>Oversight</td><td>Oversight</td></tr>
<tr><td>Omission</td><td>Omission</td></tr>
<tr><td>Design immature, risk control not successful</td><td>Verification and validation</td><td>1.3.3. Design Organization</td><td>1.3. Organizational Human Factors</td><td rowspan="2">1. UAS</td></tr>
<tr><td>Design robustness, reliability, availability</td><td>Design reliability and availability</td><td colspan="2">1.1. Aircraft</td></tr>
</table>

The first column in table 3 contains the text fragments extracted from the original narrative of the scenario, which represent the individual hazards identified by the scenario. Although the identification and extraction of individual hazards were performed by the Rutgers research team and have not been validated or vetted by any outside expertise, it is clear that the original narrative text leaves little room for interpretation and, in most cases, it is quite straightforward to find a representative HCAS hazard close enough to the intended meaning of the scenario. On the other hand, it should be noted that the UAS scenarios examined are basically conjectures on the UAS domain and represent a hypothetical set of potential hazards in that particular domain. Furthermore, as indicated earlier, the 208 hypothetical scenarios are generated with the help of at least one contributing subject matter expert. Since this whole research is, in fact, a proof of concept of the applicability of the proposed HCAS framework to the UAS domain, it was decided intentionally to forego the validation of the mapping, which would require another set of subject matter experts, at this phase of the research. Hence, the focus is only to see whether the HCAS is suitable for use in conjunction with a set of UAS scenarios, in this case, specifically the 208 hypothetical scenarios at hand.

Next, to further clarify the process, another example of the methodology used for mapping UAS scenarios into the HCAS framework is presented. In table 4, the “Hazard Scenario Description” and “Initial/Contributory Hazards” columns for scenario 7 are presented to facilitate the discussion.

Table 4. Narrative Text From Scenario 7

Possible Initiating Hazard	Seq. # 82,91	Hazard Scenario/ Description/ Discussion	Initial/Contributory Hazards (Causes)
Design	7	The autonomous UAS functions, architecture, and operations, and not adequately understood, designed, or evaluated against potential Catastrophic and Hazardous risks, consequently there may be increased accident risk.	The autonomous UAS system is not adequately evaluated due to: Lack of resources Lack of knowledge associated with integrated risks Incomplete design details integrating functions, architecture, and operations Poor assumptions of risk Oversight Omissions

In this example, the text fragment extracted from the original narrative of the scenario is:

"The autonomous UAS system is not adequately evaluated"

This text fragment is used to identify and refer to the original scenario in the mapping, along with its "sequence (seq.) #" number (i.e., 7). In terms of identifying individual hazards and mapping them into the HCAS, the process starts by determining the key language in the narrative text. The key language corresponding to individual hazards appears highlighted in table 5.

Table 5. Key Text Identifying Hazards

Possible Initiating Hazard	Seq. # 82,91	Hazard Scenario/ Description/ Discussion	Initial/Contributory Hazards (Causes)
Design	7	The autonomous UAS functions, architecture, and operations, and not adequately understood, designed, or evaluated against potential Catastrophic and Hazardous risks, consequently there may be increased accident risk.	The autonomous UAS system is not adequately evaluated due to: Lack of resources Lack of knowledge associated with integrated risks Incomplete design details integrating functions, architecture, and operations Poor assumptions of risk Oversight Omissions

Next, the hazards identified in table 5 are mapped into their corresponding categories in the HCAS framework. The resulting mapping is presented in table 6.

Table 6. Mapping of Scenario 7 Into the HCAS Framework

	HCAS Framework			
Scenario Narrative Text	Hazards	Subsystem-Level Hazard Source		System-Level Hazard Source
Lack of knowledge	Inadequate knowledge	1.3.1. Aircraft Design	1.3. Organizational Human Factors	1. UAS
Poor assumption of risk	Poor assumption of risk			
Oversight	Oversight			
Omission	Omission			
Lack of resources	Lack of resources			

By identifying individual hazards and mapping them into the HCAS framework for each particular scenario, a hazard set is determined, which is generated in accordance to a

predetermined framework (in this case, HCAS framework). At the end of the mapping process, an attribute, or hazard, list is created for each scenario.

The raw data of the results of the mapping process for this study were collected in a Microsoft® Excel® spreadsheet. The spreadsheet provided an intuitive representation of the outcome of the mapping process where the first column listed the brief descriptions of all 208 scenarios, and the header was comprised of the HCAS taxonomy. Then, across a row representing each scenario, check marks indicated the individual HCAS hazards identified earlier during the mapping process. Figure 14 shows the source file from this spreadsheet.

		AIRCRAFT											CONTROL STATION								
													Location				Operations				
Scenario #	Hazard Definition	Propulsion (incl. Fuel Source)	Flight Management and Aviaonics Hardware / Software	Sensors / Antennas	Onboard Power	Control & Communications Link	Onboard Conflict Avoidance Subsystem (incl. DSA)	Onboard Health Monitoring & Emergency Recovery	Verification & Validation	Design Reliability & Availability	Generic Design	Generic Redundancy	Mobile	Fixed	Multiple	Combinations or not defined	Flight Planning (Mission)	Flight Control and Operations	Emergency Recovery	Crew	Control H and Sc
1	The transitional planning for UAS NAS integration is LTA								1	1											
2	Assumptions concerning reliability and availability maturity are LTA								1	1											
3	Current DoD and contractor system safety and system reliability analyses and related data are																				
4	vehicles may not meet NAS-level availability and reliability requirements associated with Cata									1		1									
5	UAS designs do not meet quantitative levels for Catastrophic and Hazardous risks	1	1	1	1																
6	The allocation of risk control is LTA										1										
7	The autonomous UAS system is not adequately evaluated																				
8	Initial airspace exposure Special Use Airspace or Access Areas may not be adequate																				
9	Advanced designs take time to mature																				
10	Transitional risks associated with the "build a little, test a little" approach occur									1											
11	LTA planning or procedures development																				
12	unique risks associated with UAS high altitude (TBD) operations																				
13	coordination, communication (between UAS operator/pilot, observer, or vehicle and/or ATC)																				
14	LTA Contingency Procedures and Planning																				
15	Vehicle sensors provide limited field of view			1																1	
16	Vehicle video/IR sensors provide limited field of view			1																1	
17	Vehicle video/IR sensors provide limited field of view			1																1	
18	Vehicle video/IR sensors provide limited field of view			1																1	
19	Vehicle video/IR sensors provide limited field of view			1																1	
20	Vehicle video/IR sensors provide limited field of view			1																1	
21	Airport/airstrip selection is LTA																1				
22	Communication (VHF, UHF, data link, radio) is lost		1			1														1	
23	UAS onboard autonomous conflict avoidance subsystem fails		1				1													1	
24	Semi- autonomous conflict avoidance subsystem fails		1				1													1	
25	LTA design UAS autonomous or semi-autonomous weather detection/sensor subsystem oc		1	1																1	
26	Conflict avoidance subsystem fails at a critical time		1				1													1	
27	LTA input data/information		1																		
28	Unsuccessful go-around occurs		1			1	1														
29	Unsuccessful go-around occurs		1																	1	
30	Autonomous UAS identifies hazard and must deviate from flight plan and deviation is not detected, comm		1																		
31	Loss of surveillance occurs		1																	1	
32	LOC due to icing																			1	
33	LTA real-time video communicated to pilot/operator																				
34	undetected HMI resulting in confusion or loses situational awareness																			1	
36	Vehicle is unable to maintain an extended loiter		1		1															1	
37	Vehicle is unable to maintain an extended loiter	1																			
38	Special vehicles are unable to successfully take off, land, or transition from or to flight config	1			1																
39	Special vehicles are unable to successfully take off, land, or transition from or to flight config	1	1	1	1																
40	autonomous UAS flight is attempted at high altitude and vehicle sensors are unable to enable									1											
41	(non composite) UAS airframes/structures may have latent damage/hazards																				
42	(composite) UAS airframes/structures may have latent damage/hazards																				
43	Intruder jams communication or UAS system																				
44	Intruder spoofs UAS control.																				
45	On board UAS processing capability is LTA																				
46	On board UAS processing limitations are limited		1																	1	
47	the use of SV, COTS or NDI or GFE is not specifically intended for UAS use		1			1														1	
48	loss of communication between (UAS, Control, and/or ATC) occurs due to frequency conges									1										1	

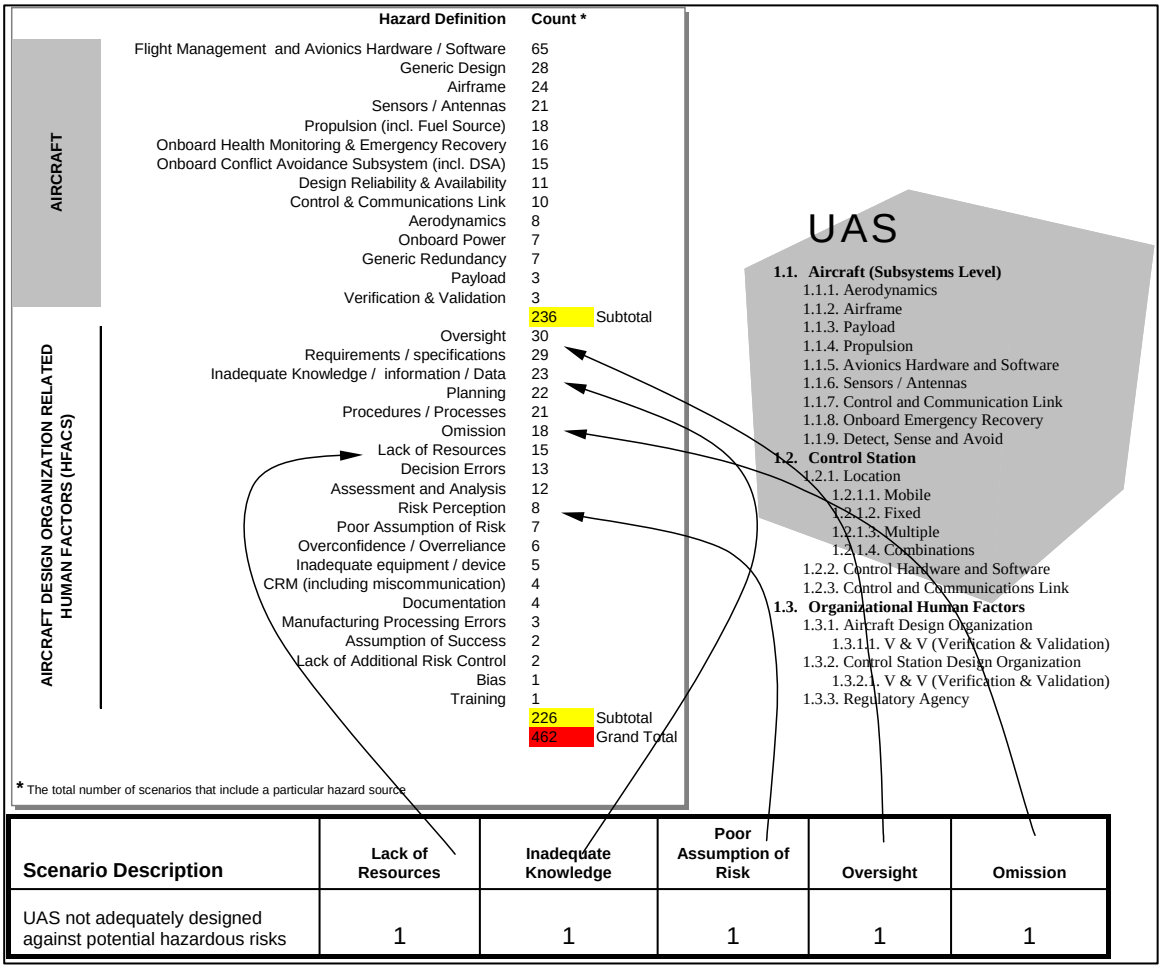
Figure 14. A Screen Capture of the Source File

3.2 THE HCAS PRIORITIZATION.

Prioritization or ranking of hazards is done in accordance with the hierarchical framework of the HCAS taxonomy. Therefore, a prioritization analysis of hazards is performed for each one of the

four categories of the HCAS taxonomy, resulting in a different ranking for each HCAS hazard source category.

With regard to the methodology used to prioritize UAS hazards, a very basic, yet intuitive, approach is applied to the results of the mapping process. In the previous section, it was stated that the results of the mapping were formatted as a spreadsheet, referred to as the "source" file. The source file contains the counts of each individual hazard along with information regarding its association to the HCAS framework. When the hazards are sorted with respect to their counts within a particular HCAS category, a prioritization is obtained for that category based simply on frequency. This concept is illustrated in figure 15. The arrows show the links from the example scenario hazard counts to the total hazard numerical counts.



Scenario Description	Lack of Resources	Inadequate Knowledge	Poor Assumption of Risk	Oversight	Omission
UAS not adequately designed against potential hazardous risks	1	1	1	1	1

Figure 15. Counting and Ranking Hazards

Since any sort of prioritization analysis performed on the results of the mapping would be based on a hypothetical UAS scenario set, a more complicated approach to hazards prioritization was not performed at this phase of the research. Hence, the frequency-based prioritization of UAS hazards performed here represents a proof of concept, which underlines the fact that the results

of the scenario mapping process can be processed by various formal prioritization methods, including frequency count, among many others.

3.3 THE HCAS RESULTS, ANALYSIS, AND REMARKS.

This section presents the results of the UAS hazard prioritization analysis based on the outcome of the HCAS mapping process previously described. The results of the prioritization for each system-level hazard source (i.e., for each of the four main system-level categories of HCAS) are presented separately in related sections.

In the following sections, a ranking of the individual hazards are presented followed by detailed graphs analyzing the distribution of subsystem-level hazard sources and individual hazards within that particular category. An analysis pertaining to the ranking and graphs presented are provided to conclude each section.

The ranking and subsequent analyses are presented in a manner that emphasizes the distinction between the design- and human factor-oriented hazard source groups for each main HCAS category. It should be noted that, in the HCAS taxonomy presented in figure 2, human factors elements of the taxonomy are grouped under three separate subsystem-level hazard source groups, each titled "Organizational Human Factors," for all three system-level hazard sources, namely UAS, Airmen, and Operations and NAS Interconnectivity. However, that distinction is made in the analyses to emphasize the difference between design- and human factors-related hazard sources. Hence, all the results presented here carry this undertone and are introduced to underline the distinction between UAS hazards originated from the hardware or software design and UAS hazards stemming from organizational and individual human factors.

This distinction is important, especially because the UAS domain and its interaction with the NAS is of an emerging nature. Neither the regulatory body, with its various components and programs, nor the design organizations and operators, with different sizes and objectives, have been able to develop a common understanding about the risks associated with an emerging technology coupled with its virtually unlimited application, namely the risks associated with design and human factors.

3.3.1 The UAS System-Level Hazard Sources.

Table 7 presents the complete list of individual hazards under the UAS system-level hazard source group identified by the mapping process of the HCAS taxonomy into the UAS scenario set at hand (i.e., 208 UAS scenarios). It is a complete enumeration of individual hazards under the UAS system-level hazard source category and includes total counts for individual hazards rank-ordered from highest to lowest counts in the particular scenario set used.

UAS design- and human factors-related hazard sources are presented in separate groups due to the reasons elaborated in the previous section. Additionally, within these two groups, the hazards are ranked with respect to their individual counts.

Table 7. The UAS System-Level Hazard Sources

System Level Hazard Source	Subsystem Level Hazard Sources	Individual Hazard Sources	Count
UAS - Design	Aircraft	Flight Management and Avionics Hardware / Software	65
	Control Station	Control Hardware and Software	54
	Aircraft	Generic Design	28
	Aircraft	Airframe	24
	Aircraft	Sensors / Antennas	21
	Control Station	Control & Communications Link	19
	Aircraft	Propulsion (incl. Fuel Source)	18
	Control Station	Generic Design	17
	Aircraft	Onboard Health Monitoring & Emergency Recovery	16
	Aircraft	Onboard Conflict Avoidance Subsystem (incl. DSA)	15
	Aircraft	Design Reliability & Availability	11
	Aircraft	Control & Communications Link	10
	Aircraft	Aerodynamics	8
	Aircraft	Onboard Power	7
	Aircraft	Generic Redundancy	7
	Aircraft	Payload	3
	Control Station	Location / Combinations or not defined	2
	Control Station	Location / Mobile	1
	Control Station	Location / Fixed	0
	Control Station	Location / Multiple	0
UAS - Human Factors	Aircraft Design Org related HF	Oversight	30
	Aircraft Design Org related HF	LTA Requirements / specifications	29
	Aircraft Design Org related HF	Inadequate Knowledge / information / Data	23
	Aircraft Design Org related HF	LTA Planning	22
	Aircraft Design Org related HF	LTA Procedures / Processes	21
	Aircraft Design Org related HF	Omission	18
	Aircraft Design Org related HF	Human Factors - General	15
	Aircraft Design Org related HF	Lack of Resources	15
	Aircraft Design Org related HF	Decision Errors	13
	Aircraft Design Org related HF	LTA Assessment and Analysis	12
	Control Station Design Org HF	LTA Requirements / specifications	12
	Aircraft Design Org related HF	Risk Perception	8
	Control Station Design Org HF	Inadequate Knowledge / information / Data	8
	Control Station Design Org HF	Decision Errors	8
	Aircraft Design Org related HF	Poor Assumption of Risk	7
	Control Station Design Org HF	LTA Procedures / Processes	7
	Aircraft Design Org related HF	Overconfidence / Overreliance	6
	Control Station Design Org HF	Lack of Resources	6
	Aircraft Design Org related HF	Inadequate equipment / device	5
	Aircraft Design Org related HF	CRM (incld. miscommunication)	4
	Aircraft Design Org related HF	LTA Documentation	4
	Generic Org. Related HF	Verification & Validation	3
	Aircraft Design Org related HF	Manufacturing Processing Errors	3
	Control Station Design Org HF	Oversight	3
	Aircraft Design Org related HF	Assumption of Success	2
	Aircraft Design Org related HF	Visual Limitations	2
	Aircraft Design Org related HF	Lack of Additional Risk Control	2
	Control Station Design Org HF	Human Factors - General	2
	Control Station Design Org HF	Omission	2
	Control Station Design Org HF	LTA Planning	2
	Aircraft Design Org related HF	Skill Based	1
	Aircraft Design Org related HF	Loss of Situational Awareness	1
	Aircraft Design Org related HF	Bias	1
	Aircraft Design Org related HF	LTA Training	1
	Control Station Design Org HF	Skill Based	1
	Control Station Design Org HF	Risk Perception	1
	Control Station Design Org HF	LTA Assessment and Analysis	1
	Control Station Design Org HF	Inadequate equipment / device	1
	Control Station Design Org HF	Manufacturing Processing Errors	1

In figure 16, the distinction between human factors-related hazards and design-related hazards is removed and an overall ranking or prioritization of individual hazards within the UAS system-level hazard source category is presented. In addition to that ranking based on frequency count of particular hazard source, figure 16 provides information with regard to the subsystem-level attribute of individual hazard source. In other words, along with the hazard's ranking order, its subsystem-level affiliation can also be deduced.

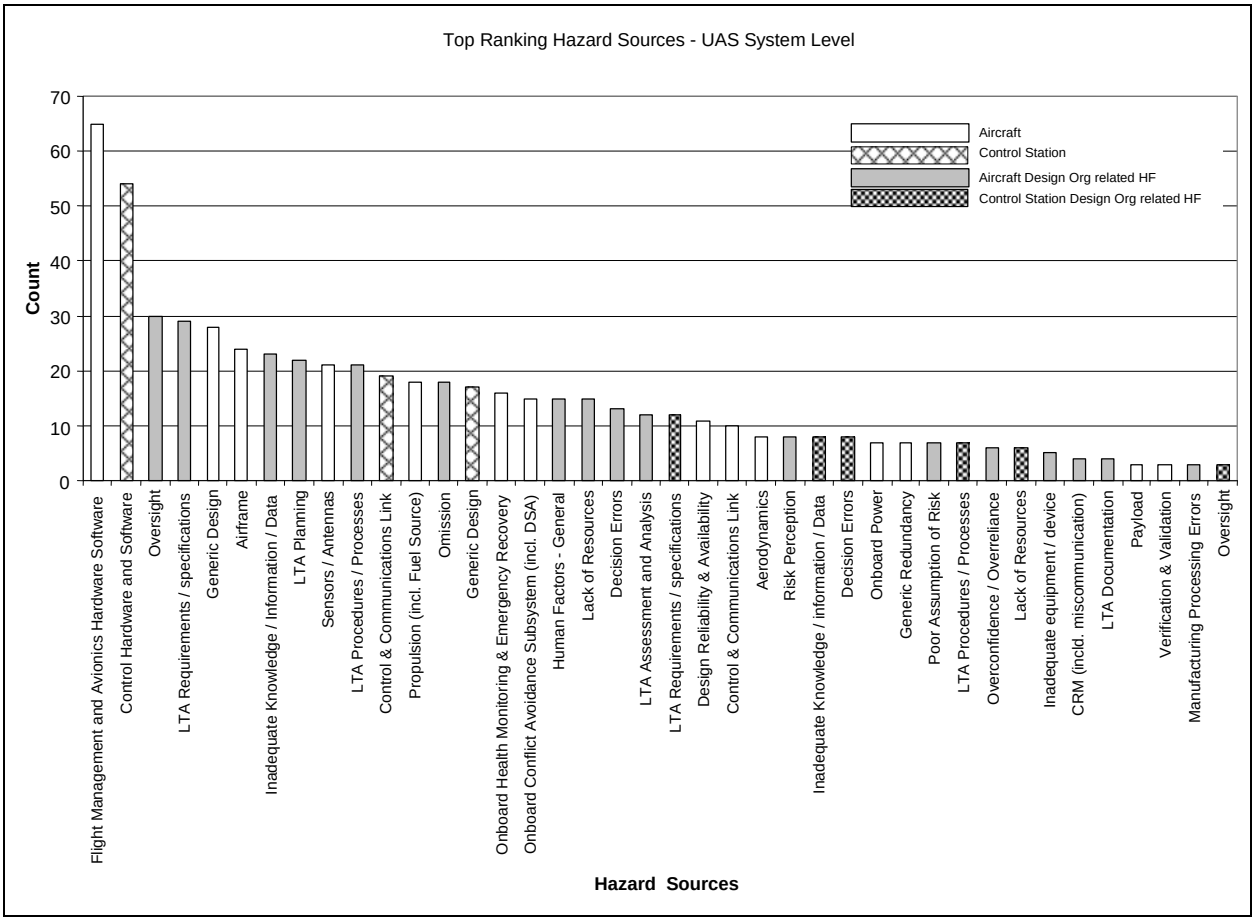


Figure 16. Ranking of Hazard Sources—UAS System-Level Hazard Source

From figure 16, it is clear the top ranking hazard in the UAS system-level hazard source group is "Flight Management and Avionics Hardware/Software," which is a hazard source associated with aircraft design and appears in 65 scenarios from within the given scenario set (specific information for the count can be found in table 7). The second hazard source in the ranking is "Control Hardware and Software," which is a hazard source associated with control station design and is mentioned in 54 scenarios out a set of 208 scenarios. Finally, the third hazard source on the ranking list is "Oversight," which is a human factor associated with an aircraft design organization. It appears in 30 scenarios.

The next issue that arises is how these individual hazard sources are distributed with respect to their association to human factors or design. This distribution issue of hazard sources of the UAS system-level category is presented in figure 17.

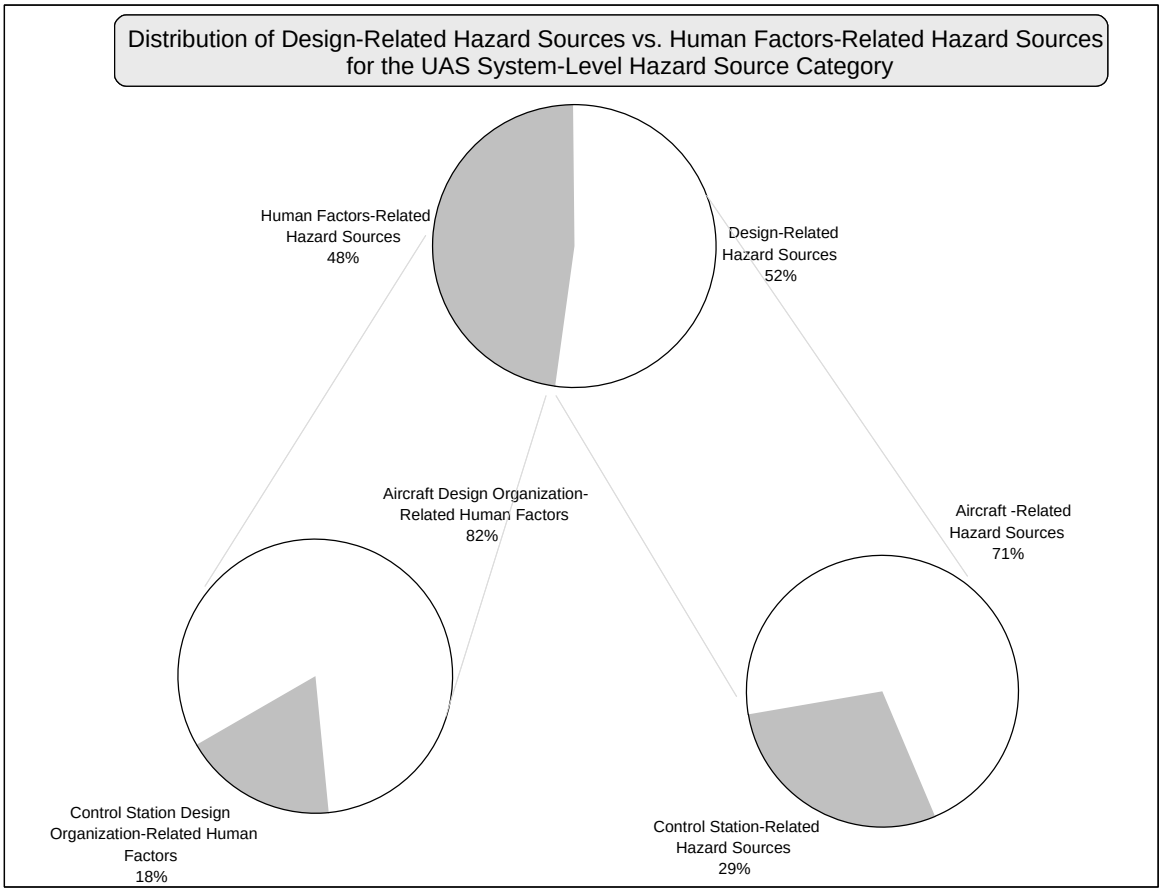
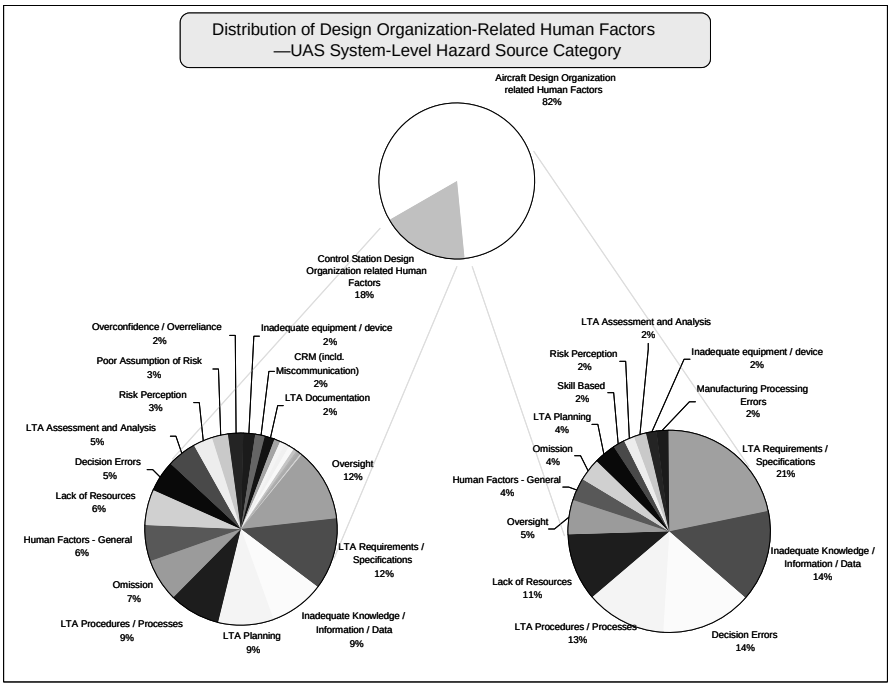


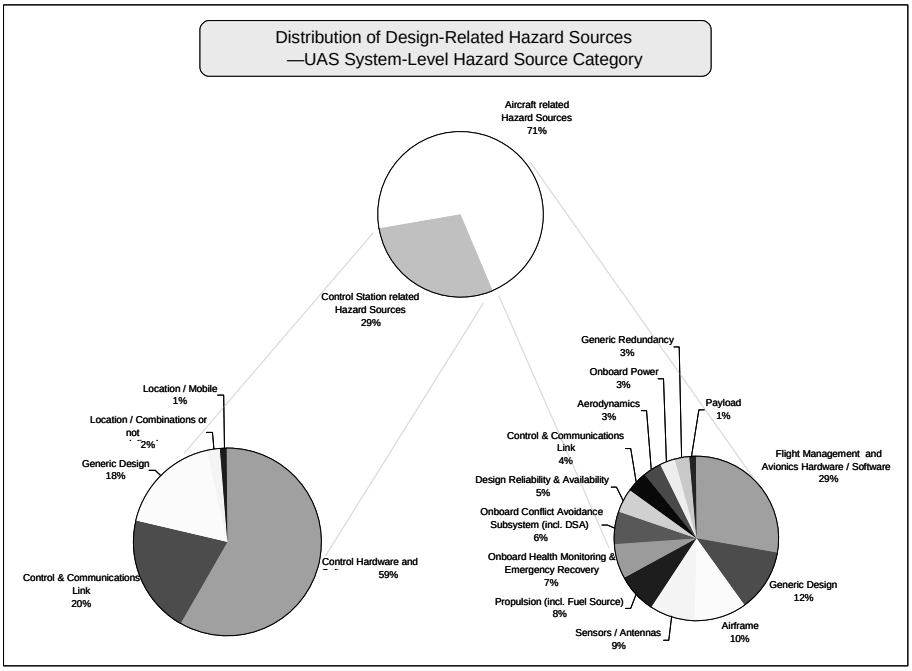
Figure 17. Distribution of UAS System-Level Hazard Source Category

Figures 18 and 19 provide further detailed information on distribution for design organization-related human factors and design organization-related hazard sources, respectively.



CRM = Crew Resource Management

Figure 18. Distribution of Design Organization-Related Human Factors—UAS System-Level Hazard Source



DSA = Detect, sense and avoid

Figure 19. Distribution of Design-Related Hazard Sources—UAS System-Level Hazard Source

3.3.2 Airmen System-Level Hazard Sources.

In table 8, the list of all the individual hazard sources associated with the airmen system-level HCAS category identified during the mapping process are presented.

Table 8. Airmen System-Level Hazard Sources

System Level Hazard Source	Subsystem Level Hazard Source	Hazard Source	Count
AIRMEN	Individual Human Factors	Loss of Situational Awareness	30
		CRM (incld. miscommunication)	13
		Decision Errors	13
		Distraction	6
		wrong response to emergency	6
		Omission	5
		Oversight	5
		Skill Based	5
		Channelized Attention	3
		Complacency	3
		Poor Assumption of Risk	3
		Risk Perception	3
	Organizational Human Factors	Human Factors - General	31
		LTA Training	9
		Inadequate Knowledge / information / Data	7
		LTA Procedures / Processes	5
		LTA Requirements / specifications	5
		Lack of Resources	4
		LTA Planning	4
		LTA Assessment and Analysis	3
		Human Learning Curve	2
		LTA needs analysis	2
		Medical Condition	2
		Excessive tasking/ workload	1
		Experience knowledge transfer	1
		Omission	1
		Oversight	1
		Risk Perception	1
		Safety Culture	1
		Undefined	1
		Total	176

In table 8, the Count column provides the number of scenarios where the subject hazard source is determined relevant during the mapping process. The counts represent frequencies of occurrences for individual hazard sources. These frequencies are then used to rank-order the individual hazard sources within two subsystem-level hazard sources under the airmen system-level category.

The overall ranking of airmen-related hazard sources is presented in figure 20. The top hazard in the above ranking appears as Human Factors—General and due to its relatively nondescript nature it may require some additional remarks. “Human Factors—General” refers to generic organizational human factors that are related to the airmen category.

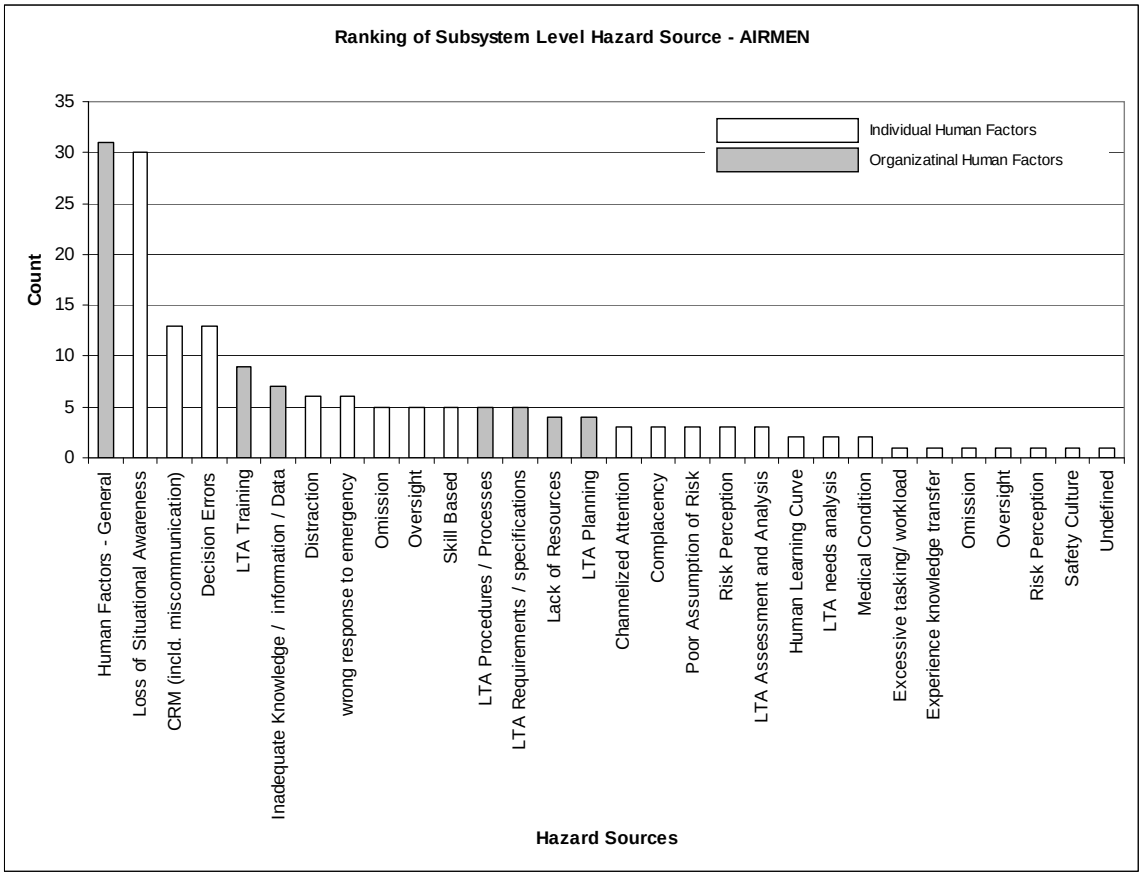
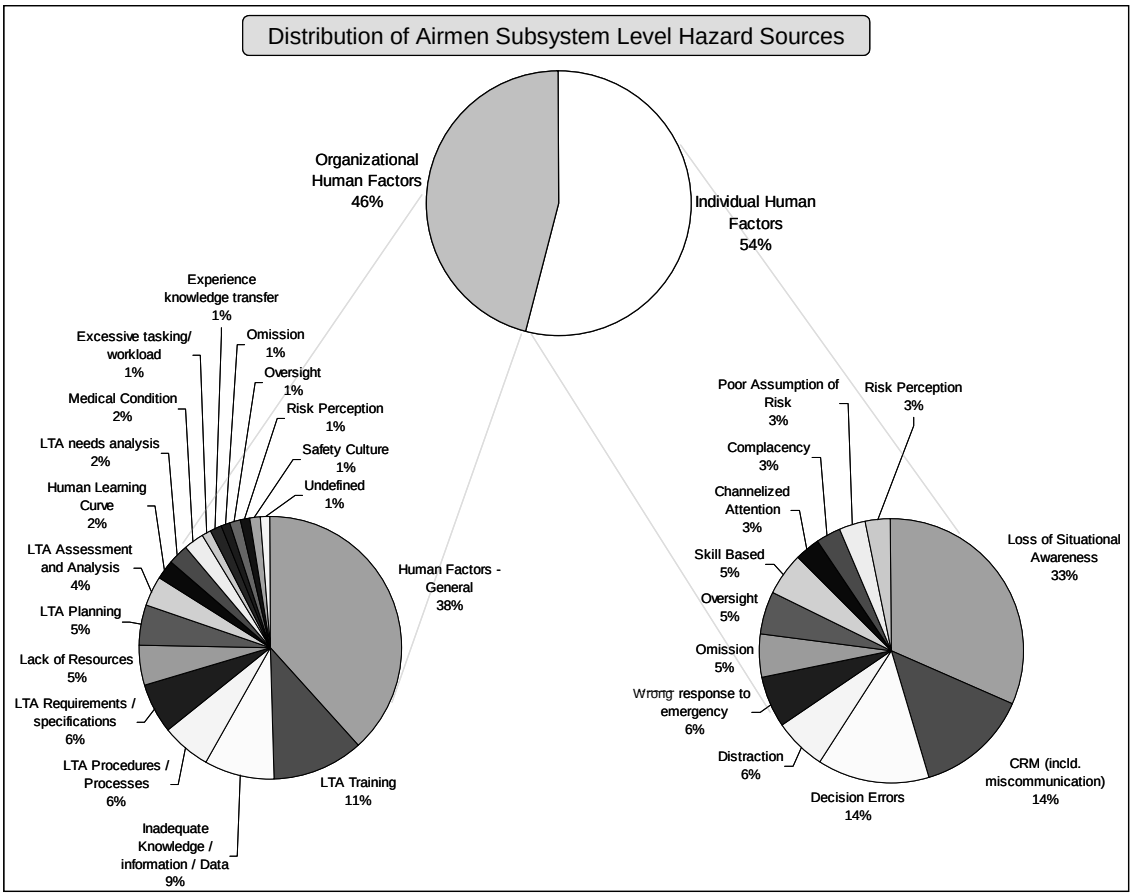


Figure 20. Ranking of Subsystem-Level Hazard Sources—Airmen

The distributions and further deconstruction of individual and organizational human factors for the airmen system-level hazard source group are presented in figure 21. The detailed distribution in figure 21 indicates that "less than adequate training" appears to be the second most common theme in the organizational human factors after the nondescript generic human factors. Another important observation from the distribution graphs is that "loss of situational awareness" emerges as the most important individual human factor with a distribution of 33% in the Airmen subsystem-level hazard source group. However, it should be noted that the ranking of hazard sources and their distribution is based on the scenario set used throughout this research, and, therefore, the results are only representative of that particular UAS scenario set. Notwithstanding the dependency on the scenario set used, the mere existence of structured results is indicative of the potential applicability of the proposed HCAS taxonomy and the mapping methodology.



CRM = Crew Resource Management

Figure 21. Distribution of Human Factors in the Airmen System-Level Hazard Source

3.3.3 Operations and NAS Interconnectivity System-Level Hazard Sources.

The results regarding the ranking of individual hazard sources mapped as related to the "Operations and NAS Interconnectivity" system-level hazard source group are presented in table 9 and figures 22 and 23, respectively.

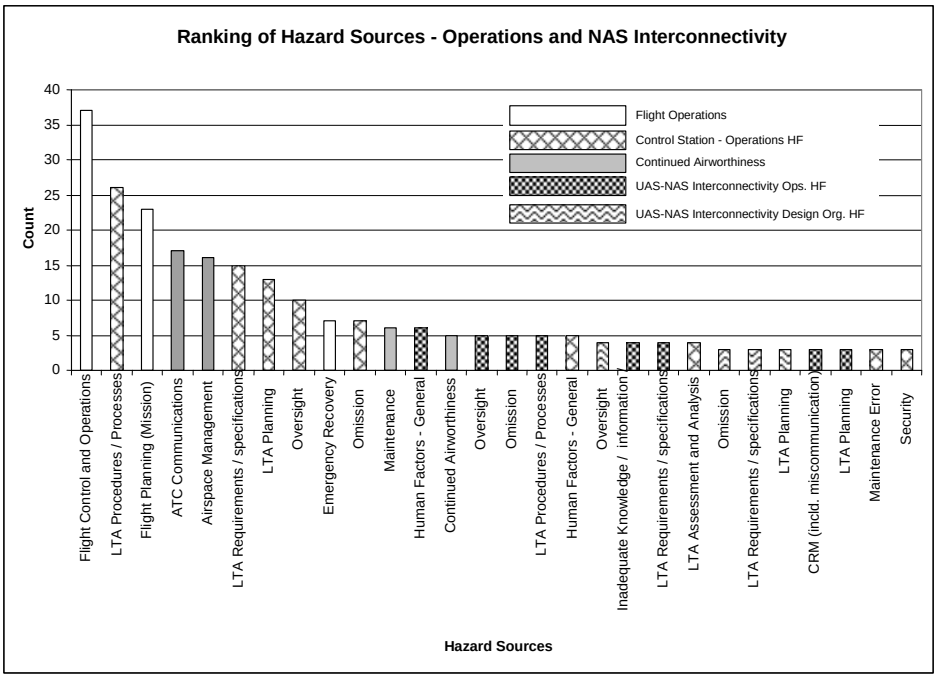
As with previous result sections for the UAS and Airmen system-level categories, the complete list of individual hazards identified by the HCAS mapping process related to "Operations and NAS Interconnectivity" system-level hazard source group is provided in table 9. Again, the list is organized so that individual hazard sources are rank-ordered and grouped under their respective subsystem-level hazard source groups. In figure 22, individual "Operations and NAS Interconnectivity" hazard sources are rank-ordered without taking their hierarchical HCAS associations into consideration. As with the earlier rankings, the individual hazard sources are rank-ordered according to their frequency counts. Note that in figure 22, "ATC Communications" and "Airspace Management" represent two major hazard source categories at the same level and importance as the other five hazards source categories listed in the legend field of the figure. However, since no individual hazard source has been identified as pertinent to their subcategory during the mapping process, they are not listed in the legend but included in

the overall ranking and shaded dark gray to distinguish them from the individual hazard sources. Figure 23, on the other hand, presents the subsystem-level distribution of the individual hazards sources.

Table 9. Operations and NAS Interconnectivity System-Level Hazard Sources

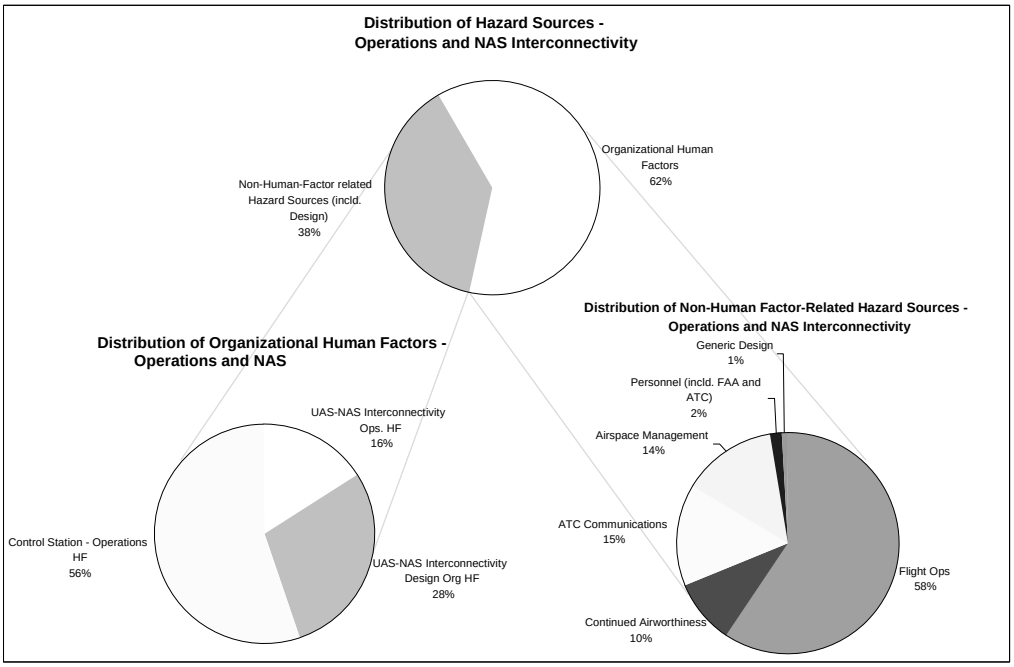
	Subsystem Level Hazard Sources		Individual Hazard Source	Count
	Flight Ops		Flight Control and Operations	37
	Flight Ops		Flight Planning (Mission)	23
	Flight Ops		Emergency Recovery	7
	Flight Ops		Line Of Sight (LOS) and/or Beyond Line of Sight	1
	Continued Airworthiness		Maintenance	6
	Continued Airworthiness		Continued Airworthiness	5
	ATC Communications			17
	Airspace Management			16
	Personnel (incld. FAA and ATC)			2
	Generic Design			1
Organizational Human Factors	Organizational Human Factors	UAS-NAS Interconnectivity Design Org HF	Oversight	4
			Omission	3
			LTA Requirements / specifications	3
			LTA Planning	3
			Inadequate Knowledge / information / Data	2
			Decision Errors	2
			LTA Training	2
			Lack of Resources	2
			Human Factors - General	1
			Overconfidence / Overreliance	1
			Risk Perception	1
			Loss of Situational Awareness	1
			Bias	1
			CRM (incld. miscommunication)	1
			Poor Assumption of Risk	1
			LTA Procedures / Processes	1
			LTA Assessment and Analysis	1
		UAS-NAS Interconnectivity Ops. HF	Human Factors - General	6
			Oversight	5
			Omission	5
			LTA Procedures / Processes	5
			Inadequate Knowledge / information / Data	4
			LTA Requirements / specifications	4
			CRM (incld. miscommunication)	3
			LTA Planning	3
			Decision Errors	2
			Skill Based	2
			Poor Assumption of Risk	2
			LTA Assessment and Analysis	2
			LTA Documentation	2
			Lack of Resources	2
			Risk Perception	1
			Loss of Situational Awareness	1
			LTA Training	1
			Lack of Additional Risk Control	1
			Lack of Contingency Analysis	1
			LTA cross-cueing	1
		Control Station - Operations HF	LTA Procedures / Processes	26
			LTA Requirements / specifications	15
			LTA Planning	13
			Oversight	10
			Omission	7
			Human Factors - General	5
			LTA Assessment and Analysis	4
			Maintenance Error	3
			Security	3
			Decision Errors	2
			wrong response to emergency	2
			Poor Assumption of Risk	2
			Lack of Resources	2
			Lack of Additional Risk Control	2
			Inadequate Knowledge / information / Data	1
			Risk Perception	1
			Over-extended mission duration	1
			LTA Documentation	1
			LTA weather data / information	1
			Inadequate equipment / device	1
			Lack of Contingency Analysis	1

ATC = Air traffic control
HF = Human factors



ATC = Air traffic control
CRM = Crew Resource Management

Figure 22. Ranking of Subsystem-Level Hazard Sources—Operations and NAS Interconnectivity



ATC = Air traffic control
HF = Human Factors
Ops = Operations

Figure 23. Distribution of Operations and NAS Interconnectivity System-Level Hazard Sources

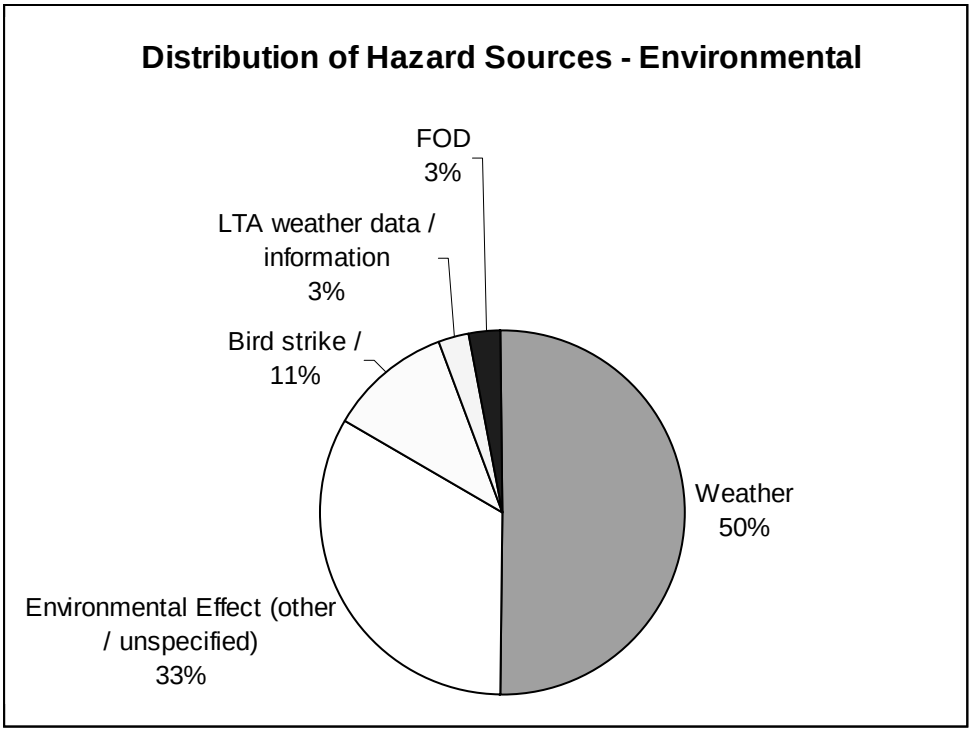
3.3.4 Environmental Hazard Sources.

The final system-level hazard source category in the proposed HCAS taxonomy deals with the environmental condition. Compared to the other three system-level groups, it presents a more restricted fidelity, as far as subsystem-level hierarchy is concerned. The complete list of environmental factors according to the HCAS mapping process is presented in table 10.

Table 10. Environmental Hazard Sources

Hazard Sources	Count
Weather	18
Environmental effect (other)	12
Bird strike	4
LTA weather data/information	1
Foreign object damage	1

Figure 24 illustrates the distribution of the environmental factors identified. Weather-related generic environmental factors comprise half of the identified potential hazard sources.



FOD = Foreign object damage

Figure 24. Distribution of Hazard Sources—Environmental

3.3.5 Top 20 Hazard Sources.

In the previous section, the results of the HCAS hazard prioritization process are presented hierarchically. Separate rankings of individual hazard sources and their distribution is provided for each of the four main HCAS system-level hazard source categories. Although this approach makes detailed analysis possible, it may lead to somewhat insufficient interpretation of the overall picture as far as the whole domain is concerned.

A consolidated list of individual hazard sources for the top 20 HCAS hazards is presented in table 11. Along with their frequency count, their taxonomical associations, such as system- and subsystem-level groupings, are also provided. According to the results of the HCAS mapping process, 8 of the top 20 hazard sources are related to potential hardware/software design issues, 9 are related to human factors, 2 are related to operations, and 1 is associated with environmental factors, making up 45%, 39%, 12%, and 4% of the total frequency count, respectively. A more detailed analysis of the top 20 HCAS hazard sources is provided in figure 25.

Table 11. Top 20 UAS Hazard Sources for a Given Scenario Set

Ranking	System-Level Hazard Sources	Subsystem-Level Hazard Sources	Hazard Source	Count
1	UAS	Aircraft	Flight Management and Avionics Hardware / Software	65
2	UAS	Control Station	Control Hardware and Software	54
3	Ops & NAS Interconnectivity	Flight Ops	Flight Control and Operations	37
4	Airmen	Organizational Human Factors	Human Factors - General	31
5	UAS	Aircraft Design Org related HF	Oversight	30
6	Airmen	Individual Human Factors	Loss of Situational Awareness	30
7	UAS	Aircraft Design Org related HF	LTA Requirements / specifications	29
8	UAS	Aircraft	Generic Design	28
9	Ops & NAS Interconnectivity	Control Station - Operations HF	LTA Procedures / Processes	26
10	UAS	Aircraft	Airframe	24
11	UAS	Aircraft Design Org related HF	Inadequate Knowledge / information / Data	23
12	Ops & NAS Interconnectivity	Flight Ops	Flight Planning (Mission)	23
13	UAS	Aircraft Design Org related HF	LTA Planning	22
14	UAS	Aircraft	Sensors / Antennas	21
15	UAS	Aircraft Design Org related HF	LTA Procedures / Processes	21
16	UAS	Control Station	Control & Communications Link	19
17	UAS	Aircraft	Propulsion (incl. Fuel Source)	18
18	UAS	Aircraft Design Org related HF	Omission	18
19	Environment		Weather	18
20	UAS	Control Station	Generic Design	17

HF = Human factors
Ops = Operations

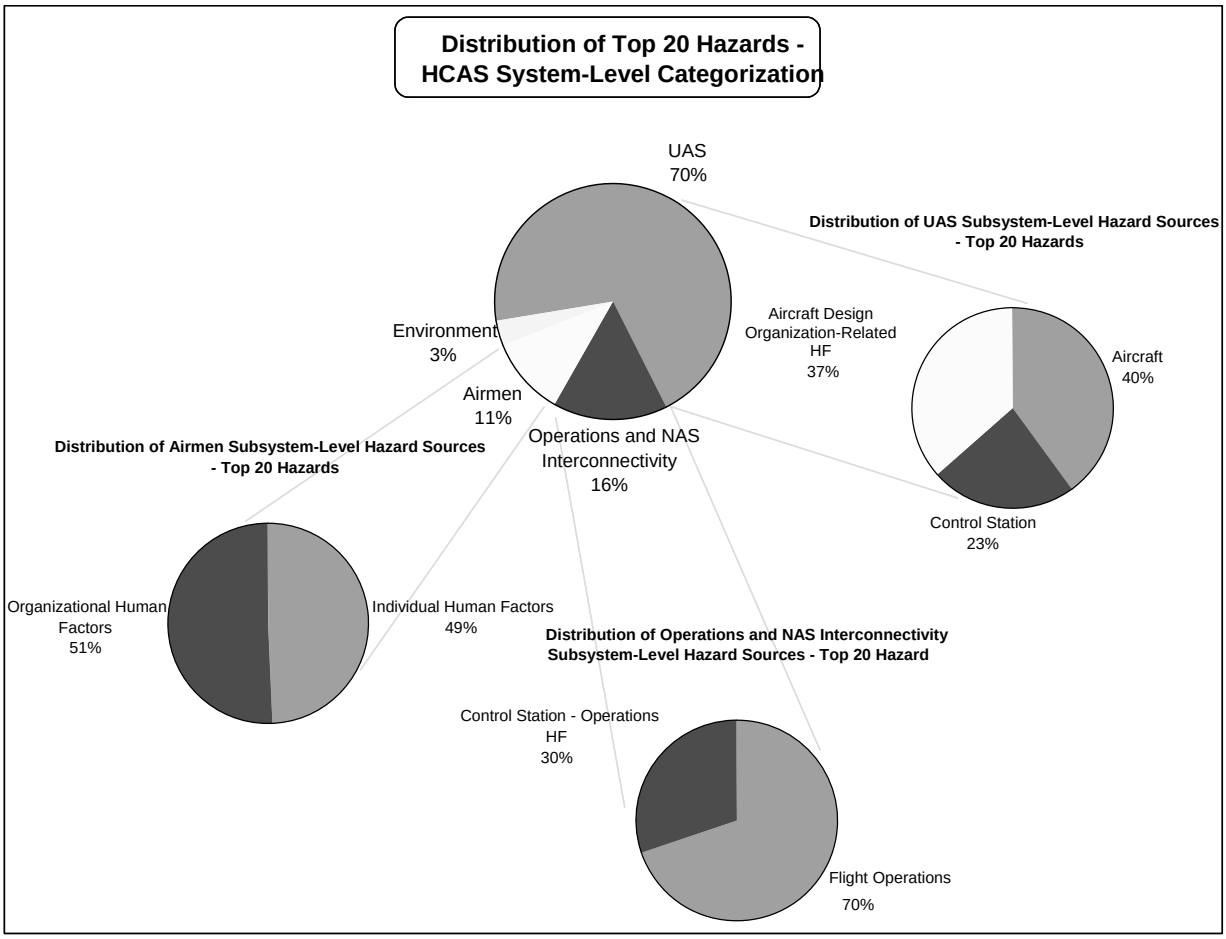


Figure 25. Distribution of Top 20 UAS Hazard Sources According to the HCAS System-Level Categorization

4. CONCLUSIONS.

This section of the report provides brief reviews of analytical methods and technology that may be used to support hazard and safety risk analysis. The completion of the Rutgers Phase 1 unmanned aircraft systems (UAS) safety risk research project resulted in the following conclusions:

- The Scenario-Driven Hazard Analysis (SDHA) process appears to be a productive method to generate plausible scenarios for subsequent analysis. Since the Rutgers research team was not involved in the scenario generation phase, to some extent, the use of the UAS scenarios by the Rutgers research team served as a vetting of the SDHA process. Coupled with the experience of the Rutgers team in using scenarios to assist with probabilistic risk assessments for commercial aviation, the UAS research added further support for the use of scenarios in hazard and risk analysis.

- A system-level hazard taxonomy for UAS integration into the National Airspace System (NAS) is possible to develop from scenarios. The proposed Hazard Classification and

Analysis System (HCAS) taxonomy is novel and presents a robust and resilient way not only to capture the four major system-level sources of hazards (i.e., Airmen, Operations and NAS Interconnectivity, UAS, and Environment), but also to serve as a tool for ensuring that the interdependencies among hazards are modeled. It is demonstrated with a proof of concept that the HCAS framework presented in this report assists with UAS hazard categorization and prioritization. A regulatory perspective based on the Federal Aviation Administration (FAA) Title 14 Code of Federal Regulations (CFR) chapters provided a strong foundation for building such a hazard classification and analysis framework for unmanned aircraft.

- While the HCAS was developed using a certain scenario set, it was concluded that the HCAS is essentially independent of any particular scenario set and could easily be updated given access to any UAS data set using the systematic process mapping strategy outlined in this report. It should be noted that the UAS hazard percentages presented in this report are based on a given scenario set and are not generalizable but are provided as examples of proof of concept. While it is acknowledged that the scenario set used in the initial development is not exhaustive, it is contended that the scenarios form a plausible representative set. de Jong present an approach to pushing the boundary between imaginable and unimaginable hazards that keeps the performance of the hazard identification process separate from the hazard analysis and hazard mitigation processes. A future research task could involve the use of the method to see what impact, if any, the use of their suggested methods would have on UAS hazard identification.

- Some vetting of the HCAS taxonomy occurred by representatives from the FAA UAS Program Office and the analysts and program staff at the FAA William J. Hughes Technical Center and during a presentation at a System Safety Society Conference; however, it is suggested that additional industry reviews of the HCAS taxonomy be performed. This will ensure that a robust, resilient system framework has indeed been developed for UAS system-level hazard identification and prioritization.

5. RESEARCH RECOMMENDATIONS.

Phase I of the UAS safety risk research, as documented herein, proposes a novel approach, HCAS taxonomy, to analyze hazards derived from specific scenarios (actual or hypothesized) by classifying UAS hazards with linkages to the FAA 14 CFR regulatory requirements. Although initial results of this research demonstrate the capabilities of the proposed approach and proof of concept, it requires further research to capture potential hazards in reference to the FAA 14 CFR requirements while operating UAS in the NAS and apply it to UAS safety risk analysis. Furthermore, modeling risks and assessing their controls can pose additional technical challenges, particularly for the risks that are unfamiliar with the current manned aviation.

To implement the proposed HCAS taxonomy to perform UAS safety risk analysis, it is recommended that the following tasks be considered to establish a systematic approach to study

safety issues of integrating UAS in the NAS. These proposed research tasks are briefly described below.

- Continue the development of HCAS taxonomy to ensure that its applications encompass all potential UAS hazards. To support its applications, a reference manual of the HCAS taxonomy needs to be developed to provide the end-user with necessary instructions to use it in specific UAS hazard analyses.

- Review risk modeling methods for UAS applications. There are a variety of risk modeling methods available to the analyst, such as fault trees, event trees, multi-event sequence models, Bayesian Belief Networks (BBNs), fuzzy sets, among others. Each of these methods has certain technical advantages and requires specific input data sets. Detailed reviews of these analytical methods may be necessary to provide recommendations on their potentials and/or shortfalls while being applied for UAS risk analysis.

- Decomposition of the hazards in the proposed UAS taxonomy into a framework of causal factors. The decomposition of hazards into their constituent causal factors is an essential part of safety risk analysis. To determine mishap risk and hazard mitigations, detailed root causes of the hazards need to be identified and properly described. This research task will investigate and develop a framework of causal factors consistent with the proposed system- and subsystem-hazard sources in the UAS hazard taxonomy.

- Develop influence diagrams that graphically describe the complex interrelations of various hazard causal factors. The influence diagram is necessary in support of safety risk analysis. An influence diagram depicts interrelations and/or interdependencies of different hazard "clusters" that lead to potential mishaps. These influence diagrams can be used to facilitate discussions in the UAS hazard analysis process and its subsequent identification of causal factors. The resulting influence diagrams will serve as an essential step to initiate the development of risk models that will require likelihood and severity assessments with available data as well as subject matter expertise.

- Develop methods and algorithms for uncertainty analyses, which will be required to study the sensitivities of the risk models developed. Since UAS operating in the NAS are relatively new and emergent, mishap data are not readily available. It is recommended that the proposed UAS hazard taxonomy be transformed into influence diagrams for select UAS mishap scenarios. These influence diagrams will display specific hazard causal factors and their interactions. However, uncertainties will exist in likelihood and severity assessments, and the impact of these uncertainties on UAS scenario risk evaluations need to be studied. This research task will lead to the development of new analytical methods and corresponding prototype software tools for assessing the uncertainties associated with the construction of the influence diagrams of hazard causal factors for selected UAS scenarios. Such a research task will lead to more robust and defensible risk modeling and facilitate exploration of the sensitivities and impacts of both single- and multifactor perturbations on the risk values.

- Develop a reference manual for the HCAS causal factors. It is recommended that the causal factors underlying the system and subsystem hazard sources be identified and categorized. The reference manual will describe the proper approach to describe and provide general procedures to derive causal factors from hazards. It can be included in the final HCAS reference manual once the UAS safety risk analysis methods are fully developed.

- Apply the influence diagrams to selected UAS hazards. As mentioned above, influence diagrams are constructed to depict the complex interactions of UAS hazard causal factors in support of the subsequent safety risk analyses. While applying these influence diagrams to identify and describe hazard causal factors, likelihood and severity assessments of these causal factors will be studied for selected UAS hazards. These assessments will be conducted by using a complementary approach of knowledge elicitations from subject matter experts and available mishap data.

- Map existing risk controls/mitigations to the UAS hazards/causal factors and perform a "gap analysis." After the UAS hazards and their concomitant causal factors are identified, a mitigation matrix needs to be developed to map available risk controls/mitigations to the hazard causal factors. Effectiveness of these risk controls/mitigations will be analyzed in reference to current NAS safety standards to identify gaps and shortfalls. Results of these analyses will identify the areas that new and/or enhanced risk controls/mitigations are required. A mitigation portfolio can be developed. For example, some mitigation options include eliminating the hazard, reducing the hazard's occurrence, reducing the likelihood that the hazard leads to the consequence, and/or reduce the consequence severity.

- Develop text mining tools to apply the proposed HCAS taxonomy approach to automatically analyze UAS scenarios, which are often documented in textual files, to categorize hazards for a safety risk analysis. Currently, the reading of scenarios and mapping of keywords into the HCAS taxonomy elements is a manual process conducted by an experienced analyst. It is not only a time consuming process, but also hinders the HCAS applications, particularly when a scenario with associated hazards is updated as event-data become available. Once the tools are developed, they will serve as a substitute for this time-intensive manual process.

- Develop a prototype data system that is consistent with the refined UAS hazard taxonomy. Further development and refinement of the proposed UAS taxonomy of hazards with causal factors could be used to create the framework of a prototype UAS mishap data system. It will support both UAS safety risk analyses and event-driven hazard assessments. This research task will lead to the creation of a prototype software shell consistent with the UAS hazard taxonomy.

These recommendations are derived from the results of the Phase I study of the UAS safety risk analysis documented in this report. They form a systematic approach to develop procedures and methods of analyzing safety risks while integrating UAS in the NAS based on the FAA 14 CFR regulatory framework.

6. BIBLIOGRAPHY.

AeroVations Associates (2004), "Priorities for Canadian UAV Research and Technology Development: A Limited Survey of Stakeholders," Report AVA 04-02.

Ale, B.J.M., L.J. Bellamy, R.M. Cooke, L.H.J. Goossens, A.R. Hale, D. Kurowicks, A.L.C. Roelen, and E. Smith (2005), "Development of a Causal Model for Air Transport Safety," *Proceedings of the European Safety and Reliability Conference*, Tri City, Poland, pp. 37-44.

Allocco, M. (2005), "Hazards in Context with System Risks," *Proceedings of the International System Safety Conference*, San Diego, California.

Allocco, M. (2006a), "Present Status of System-Level Preliminary Hazard Analysis, UAS Integration into the NAS," Draft Technical Report, Federal Aviation Administration.

Allocco, M. (2006b), *System Safety Engineering and Management Guidebook*, Federal Aviation Administration.

American Society for Quality (2006), "Failure Mode and Effects Analysis," retrieved June 12, 2006, from http://www.asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

Andersen, S.K., K.G. Olesen, F.V. Jensen, and F. Jensen (1989), "HUGIN—A Shell for Building Bayesian Belief Universes for Expert Systems," in *Proceedings of the Eleventh International Joint Conference on Artificial Intelligence*, Detroit, Michigan, pp. 1080-1085.

Andres, D. (2005), *Development of a Post-Consequence Model for Aircraft Accident Severity Assessment*, M.S. Thesis, Department of Industrial and Systems Engineering, Rutgers University, Piscataway, New Jersey.

Andres, D.M., J.T. Luxhøj, and D.W. Coit (2005), "Modeling of Human-System Risk and Safety: Aviation Case Studies as Exemplars," *Human Factors and Aerospace Safety*, Vol. 5, No. 2, pp. 137-167.

Anoll, R. (2007), "UAS Program Office: System Safety Program Plan, FAA, May 16.

Anoll, R. (2006), "Safety Checklist," Federal Aviation Administration, Unmanned Aircraft System (UAS) Program Office, Washington, DC.

Aven, T. (2003), *Foundations of Risk Analysis*, England: John Wiley & Sons, Ltd.

Ayyub, B.M. (2003), *Risk Analysis in Engineering and Economics*, New York: Chapman & Hall/CRC.

Bahr, N.J. (1997), *System Safety Engineering and Risk Assessment: A Practical Approach*, New York: Taylor & Francis.

Bareither, C. and J.T. Luxhøj (2007), "Uncertainty and Sensitivity Analysis in Bayesian Belief Networks: Applications to Aviation Safety Risk Assessment," *International Journal of Industrial and Systems Engineering*, Vol. 2, No. 2, pp. 137-158.

Benner, L. (1975), "Accident Investigation: Multilinear Events Sequencing Methods," *Journal of Safety Research*, Vol. 7, No. 2, pp. 67-73.

Benner, L. (1977), "Accident Theory and Accident Investigation," *Hazard Prevention*, Vol. 13, pp. 18-21.

Blackman, H.S. and D.I. Gertman (1994), *Human Reliability and Safety Analysis Data Handbook*, 1st ed., New York: John Wiley & Sons, Inc.

Bott, T., S. Eisenhawer, J. Kingson, and B. Key (2003), "A New Graphical Tool for Building Logic-Gate Trees," LA-UR-03-134, Los Alamos National Laboratory, *Proceedings of the American Society of Mechanical Engineers–Pressure Vessels and Piping Annual Meeting*, Cleveland, Ohio.

Burdick, G.R. and J.B. Fussell (1983), "On the Adaptation of Cause-Consequence Analysis to U.S. Nuclear Power Systems, Reliability and Risk Assessment," *System Reliability and Risk Assessment*, JBF Associtates, Inc., Knoxville, Tennessee.

Buys, J.R. and J.L. Clark (1995), Revision 1A, SCIE-DOE-01-TRAC-14-95, Technical Research and Analysis Center, SCIENTECH, Inc.

Castillo, E., J.M. Gutierrez, and A.S. Hadi (1997), *Expert Systems and Probabilistic Network Models*, New York: Springer-Verlag.

Clemens, P.L. (2002), *Human Factors and Operator Errors*, 2nd ed., Jacobs Sverdrup.

Clothier, R.A. and R.A. Walker (2006), "Determination and Evaluation of UAV Safety Objectives," *Proceedings of 21st International Unmanned Air Vehicle Conferenc*e, Bristol, United Kingdom, pp. 18.1-18.16.

Crow, K. (2002), "Failure Modes and Effects Analysis," retrieved June 29, 2006, from http://www.npd-solutions.com/fmea.html

de Jong, H.H., H. Blom, and S.H. Stroeve (2007), "How to Identify Unimaginable Hazards?" *Proceedings of the 25th International System Safety Conference*, Baltimore, Maryland.

Donald, S., T. Bott, and S. Eisenhawer (2004), "Representing Subjective Knowledge in Engineering Systems Using Possibility Trees," Los Alamos National Laboratory, *8th World Multi-Conference on Systemics, Cybernetics and Informatics*, Orlando, Florida.

Ericson, II, C.A. (2005), *Hazard Analysis Techniques for System Safety*, New York: Wiley-Interscience.

EuroControl (2004), "Review of Techniques to Support the EATMP Safety Assessment Methodology," Volume 1, EuroControl Experimental Center, EEC Note No. 01/04.

FAA System Safety Handbook (2000), "Chapter 7: Integrated System Hazard Analysis," pp. 7-1 to 7-18.

FAA (2005), "Unmanned Aircraft System Operations in the U.S. National Airspace System—Interim Operational Approval Guidance (2005)," Federal Aviation Administration, AFS-400 UAS Policy 05-01, September 16.

Fam, C.F. and U.C. Yu (2004), "BBN-Based Software Project Risk Management," *The Journal of Systems and Software,* Vol. 73, pp. 193-203.

Ferry, T.S. (1988), *Modern Accident Investigation and Analysis*, 2nd ed., New York: John Wiley & Sons, Inc.

Fitzgerald, R.E. (2007), "Can Human Error in Aviation be Reduced Using ASHRAM?" *Proceedings of the 25th International System Safety Conference*, Baltimore, Maryland, August 13-17.

Haimes, Y. (2004), *Risk Modeling, Assessment, and Management*, New York: John Wiley & Sons, Inc.

Hammer, W. (1972), *Handbook of System and Product Safety*, Englewood Cliffs, NJ: Prentice-Hall.

Hayhurst, K.J., J.M. Maddalon, P.S. Miner, M.P. DeEalt, and G.F. McCormick (2006), "Unmanned Aircraft Hazards and Their Implications for Regulation," *25th Digital Avionics Systems Conference*, October 15, pp. 5B1-1 - 5B1-12.

Heinrich, H.W. (1936), *Industrial Accident Prevention*, New York: McGraw-Hill.

Institute of Engineering and Technology (2004), "Quantified Risk Assessment Techniques, Failure Mode and Effects Analysis," *Health and Safety Briefings*, September, Nos. 26 a,b,c.

Jensen, F.V. (1995), *Introduction to Bayesian Networks*, United Kingdom: University-College London Press.

Jensen, F.V. (1996), *Introduction to Bayesian Networks*, New York: Springer Verlag.

Jones, P.L., J. Jorgens, A.R. Taylor, Jr., and M. Weber (2002), M.S. Thesis, *Risk Management in the Design of Medical Device Software Systems,* Center for Devices and Radiological Health, Food and Drug Administration, Rockville, Maryland.

Kaplan, S., Y. Haimes, and B. Garrick (2001), "Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk," *Risk Analysis*, Vol. 21, No. 5.

Keller, F. (2006), "Is There Hope for Quantitative Risk Analysis in Commercial Aviation?" *Proceedings of the 24th International System Safety Conference*, Albuquerque, New Mexico.

Lechner, K. (2007), *Security Risk Assessment Using Bayesian Belief Networks and Logic-Evolved Decision Models*, M.S. Thesis, Department of Industrial and Systems Engineering, Rutgers University, Piscataway, New Jersey.

Lechner, K.W. and J.T. Luxhøj (2005), "Probabilistic Causal Modeling of Risk Factors Contributing to Runway Collisions: Case Studies," *Human Factors and Aerospace Safety*, Vol. 5, No. 3, pp. 185-216.

Leveson, N.G. (1995), *Safeware: System Safety and Computers*, New York: Addison-Wesley Publishing Company.

Luxhøj, J.T. (2003), "Probabilistic Causal Analysis for System Safety Risk Assessments in Commercial Air Transport," *Proceedings of the Workshop on Investigating and Reporting of Incidents and Accidents (IRIA)*, Williamsburg, Virginia, pp. 17-38.

Luxhøj, J.T. (2005a), "Model-Based Reasoning for Aviation Safety Risk Assessments," *SAE World Aerospace Congress*, Dallas/Fort Worth, Texas.

Luxhøj, J.T. (2005b), "Aviation Safety in Practice: Applying Principles and Tools to Measure Risk Reduction," *Safety Across High-Consequence Industries*, Saint Louis University, St. Louis, Missouri.

Luxhøj, J.T., A. Choopavang, and D.N. Arendt (2001), "Risk Assessment of Organizational Factors in Aviation Systems," *Air Traffic Control Quarterly*, Vol. 9, No. 3, pp. 135-174. *(Special Issue on Flight Safety)*.

Luxhøj, J.T., M. Jalil, and S.M. Jones (2003), "A Risk-Based Decision Support Tool for Evaluating Aviation Technology Integration in the National Airspace System," *Proceedings of the AIAA's 3rd Annual Aviation Technology, Integration, and Operations (ATIO) Technical Forum*, Denver, Colorado.

Marsters, G.F. (2003), "Ummmm…So Where Does the Pilot Sit?" The W. Rupert Turnbull Lecture, *50th Annual General Meeting of the Canadian Aeronautics and Space Institute*, Montreal, Canada.

Marsters, G.F. and M. Sinclair (2003), "Integrating UAVs With Conventional Operations: Some Regulatory Issues," retrieved from http://www.aerovations.ca September 2007.

Mercaldi, G.A., S.R. Hosner, and D.B. Fay (2006), "Generating Aviation System Safety and Safety Engineering Requirements from Federal Aviation Administration Regulations and Guidance," *Proceedings of the 24th International System Safety Conference*, Albuquerque, New Mexico.

Modarres, M. (2006), *Risk Analysis in Engineering: Techniques, Tools, and Trends*, New York: Taylor & Francis/CRC.

Moriaty, B. and H.E. Roland (1990), *System Safety Engineering and Management*, 2nd ed., New York: John Wiley & Sons, Inc.

Oztekin, A., J.T. Luxhøj, and M. Allocco (2007), "A General Framework for Risk-Based System Safety Analysis of the Introduction of Emergent Aeronautical Operations into the National Airspace System," *Proceedings of the 25th International System Safety Conference*, Baltimore, Maryland, August 13-17.

Pate-Cornell, M.E. (1984), "Fault-Tree vs. Event Trees in Reliability Analysis," *Risk Analysis*, Vol. 4, No. 3, pp. 177-186.

Pearl, J. (1988), *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, San Francisco, California: Morgan Kaufmann.

Raheja, D.G. and M. Allocco (2006), *Assurance Technologies Principles and Practices: A Product, Process, and System Safety Perspective*, 2nd ed., New York: Wiley-Interscience.

Rausand, M., and A. Høyland (2003), *System Reliability Theory*, New York: Wiley.

Roelen, A.L.C., R. Weaver, R.M. Cooke, R. Lopuhaa, A.R. Hale, and L.H.J. Goosens (2003a), "Aviation Causal Modeling Using Bayesian Belief Nets to Quantify Management Influence," *Safety and Reliability*, Bedford and van Gelder, Swets and Zeitlinger, eds., Lisse, pp. 1315-1320.

Roelen, A.L.C., R. Weaver, A.R. Hale, L.H.J. Goosens. R.M. Cooke, R. Lopuhaa, M. Simons, and P.J.L. Valk (2003b), "Causal Modeling for Integrated Safety at Airports," in *Safety and Reliability*, eds. Bedford and van Gelder, Swets and Zeitlinger, Lisse, pp. 1321-1327.

RTCA Special Committee (SC) 203 Working Group 3, RTCA, (2007), "Detect, Sense and Avoid Safety Metrics," Washington, DC.

RTCA, "Guidance Material and Considerations for Unmanned Aircraft Systems" (2007), DO-304, RTCA Special Committee (SC) 203, RTCA, Inc., Washington, DC.

RTCA, "Guide to Methods and Tools for Airline Flight Safety Analysis (2001)," GAIN Working Group B: Analytical Methods and Tools.

RTCA, "Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications" (2000), DO-264, RTCA Special Committee (SC) 189, RTCA, Inc., Washington, DC.

Safety Management Services (2002), HAZOP Basis, retrieved June 12, 2006, from http://www.sms-ink.com/services_pha_hazop.html

Vick, S.G. (2002), *Degrees of Belief*, Reston, Virginia: American Society of Civil Engineers.

Weibel, R.E. and R.J. Hansman (2004), "Safety Considerations for Operations of Different Classes of UAVs in the NAS," *AIAA's 4th Aviation Technology, Integration and Operations (ATIO) Forum*, Chicago, Illinois.

Wiegmann, D.A. and S.A. Shappell (2003), *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*, England: Ashgate Publishing Limited.

Wiklund, E. (2003), "Flying with Unmanned Aircraft (UAVs) in Airspace Involving Civil Aviation Activity: Air Safety and the Approvals Procedure," The Swedish Aviation Safety Authority.

Williams, K.W. (2004), "A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications," CAMI report DOT/FAA/AM-04/24, Civil Aerospace Medical Institute, Federal Aviation Administration, Oklahoma City, Oklahoma.

APPENDIX A—ANALYTICAL METHODS AND TECHNOLOGY REVIEWS

A.1 ANALYTICAL METHODS REVIEW.

This appendix presents some background information on the available literature related to hazard/accident analysis techniques, qualitative methods used in risk analysis, and quantitative approaches in risk management. The material in this appendix is excerpted and adapted with permission from M.S. theses by Andres (2005) and Lechner (2007) written under the guidance of Dr. James T. Luxhøj during his role as principal investigator on a National Aeronautics Space Administration-sponsored research project on aviation safety risk analysis. Qualitative risk analysis methodologies attempt only to prioritize the various risk elements in subjective terms, while quantitative methods provide a more objective and visible support for decision making in risk management. Common practice is to employ several of the following complementary methodologies in a disciplined manner to detect hazards and assess risk (Jones, et al., 2002). In addition to this material, Ericson (2005) provides explanations with examples of 22 commonly used hazard analysis methods in the discipline of system safety. The EuroControl Experimental Centre (2004) provides detailed evaluations of 19 safety assessment techniques down-selected from a list of 500 different techniques. A summary of methods for system safety/risk analysis by Allocco (2006b) is also provided.

A.1.1 HAZARD ANALYSIS TECHNIQUES.

Experience has shown that accidents are rarely simple and almost never result from a single cause. Rather, they usually have multiple factors and develop from clearly defined sequences of events, which involve perform ance errors, changes, oversights, and omissions (Buys and Clark, 1995). Accident investigators need to identify and document not only the events themselves, but also the relevant pre-accident, accident sequence, and post-accident conditions (Ferry, 1988). To accomplish this, a straightforward approach can be used that decomposes the entire sequence into a logical flow of events from the beginning of accident development. This flow of events need not lie in a single event chain but may involve confluent and branching chains (Benner, 1975). The analyst/investigator often has the choice of expressing the accident sequence as a group of event chains, which merge at a common key event, or as a primary chain of sequential events into which causative factors feed as conditions that contribute to event occurrence, or as a combination of the two. Traditional analytical techniques mainly deal with the identification of accident sequences and seek unsafe acts or conditions leading to a loss. Such techniques include sequence of events, change analysis, and multilinear events sequencing (MES), all of which are described in the following sections.

A.1.1.1 Hazard Operability Analysis.

A hazard and operability analysis (HAZOP) is a structured process in which a multidisciplinary team performs a systematic study of a process using guide words to discover how deviations from the design intent can occur in equipment, actions, or materials, and whether the consequences of these deviations can result in a hazard (Safety Management Services, 2002). The HAZOP team members focus on specific parts of the process being studied called nodes. HAZOP is applicable to any system or procedure and produces qualitative results.

The HAZOP methodology includes several steps. After a thorough understanding of the process is gained, the process is broken into nodes. Next, guidewords, which are simple words, are used to qualify or quantify the intention to discover system deviations. While there are generic lists of guidewords available, sometimes it is important to generate an appropriate guideword set for a specific process being studied. The guidewords in table A-1 is an example of a general list that can apply to many systems.

Table A-1. Guidewords and Meanings for HAZOP
(http://pie.che.ufl.edu/guides/hazop/)

Guidewords	Meaning
No	Negation of the design intent
Less	Quantitative decrease
More	Quantitative increase
Part of	Qualitative decrease
As well as	Qualitative increase
Reverse	Logical opposite of the intent
Other than	Complete substitution

Each node is examined for deviations from normal conditions, and all causes for these deviations are listed along with all consequences. After this, safeguards and/or controls are evaluated and actions are recommended. HAZOP requires a well-defined system or activity and the team must have access to detailed design and operational information. The HAZOP process systematically reviews credible deviations, identifies potential accidents that can result from the deviations, investigates engineering and administrative controls to protect against the deviations, and generates recommendations for system improvements. This detailed analysis process requires a substantial commitment of time from both the analysis facilitator and other subject matter experts. The HAZOP process focuses on identifying single failures that can result in accidents of interest. If the objective of the analysis is to identify all combinations of events that can lead to accidents of interest, more detailed techniques should be used.

A.1.1.2 Sequence of Events.

Heinrich (1936) suggested the “domino” theory of accidents. Five dominos—social environment and ancestry, undesirable traits (e.g., recklessness, violent temper, lack of knowledge, etc.), unsafe acts or behaviors, accident, and injury—formed the basis of the domino effect techniques. Figure A-1 is a pictorial of Heinrich’s theory. His idea was that accidents are a sequence of events in a predetermined proceed/follow relationship, like a row of falling dominos. This view changes the focus of accident investigations toward the events involved, rather than the conditions surrounding the accident environment. The objective is for analysts and investigators to understand the accident phenomenon on the basis of the chain of events that had occurred. His theory was that if a set of unsafe conditions set up a row of vulnerable dominos, an “unsafe act” would start them toppling. However, should a domino in the sequence

be removed, no injury or loss would be incurred. Under this concept, the investigator looks for information that will help reconstruct the chain of events that constituted the accident.

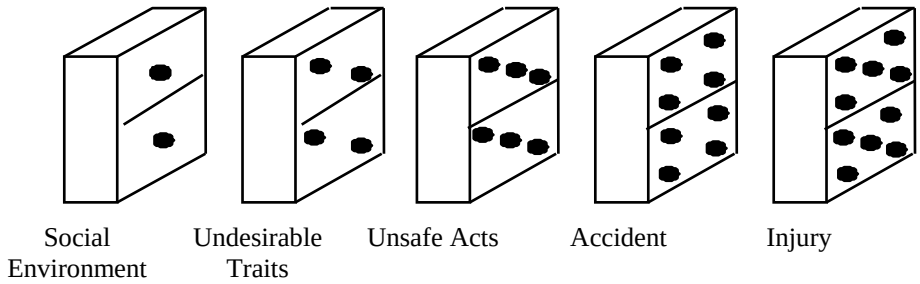


Figure A-1. Heinrich's Theory of Accidents

A.1.1.3 Change Analysis.

The origins of change analysis can be traced back to before World War II, as performed by W.G. Johnson. The RAND Corporation (Ferry, 1988) further developed the concept of change analysis for the U.S. Air Force. Their concept was to identify change in a system that would normally operate without mishap. Something had to have changed to make the mishap possible. That is, a disturbance to a homeostatic process is the catalyst initiating the accident sequence. By comparing what changes occurred that resulted in a mishap to the normal accident-free task, causal factors might be identified. Such change could be directional or exponential. Once a directional change is initiated, it would continue to proceed until another change occurred. If an exponential change is initiated, the changes would interact to compound the effects of mishaps.

The classic change analysis process involves six steps, as shown in figure A-2. Note how the process compares the pre-accident situation to the post-accident consequence. The process aids in determining the changes to the system that had to occur for an accident to be initiated. It is considered to be a relatively quick process for detecting obscure causes.

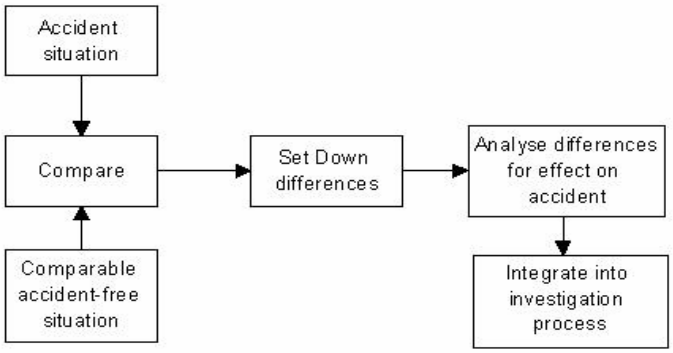


Figure A-2. Change Analysis Diagram

A.1.1.4 Multilinear Events Sequencing.

Multilinear Events Sequencing is an analytical technique initially developed by Benner (1975) while working with the National Transportation Safety Board. In 1987, Hendrick and Benner

developed a systems-based multilinear sequence method for accident investigations. For accident investigation purposes, an event is a significant happening logically ensuing from or giving rise to another happening. For something—termed an action—to happen, someone or something—termed an actor—must bring it about. Both the actor and the action must be described precisely, and an event must be described in terms of a single actor and action. It is further assumed that an activity is occurring when an accident begins. An activity is defined as a set of successive events toward some anticipated or intended outcome. An activity proceeds toward its outcome in a relatively stable progression of events involving interacting elements. This dynamic equilibrium of successive events progresses in a state of homeostasis, requiring adaptive behavior or adaptive learning by the actors involved in maintaining the stable flow of events.

When external influences—termed perturbations—vary or deviate from what is usual or expected, they disturb the activity and initiate the possibility of injury or damage. As long as the actors adapt to the perturbations encountered without being stressed beyond their capability to adapt or recover (Benner, 1977), homeostasis is maintained, and an accident does not occur. If one of the actors fails to adapt, the perturbation initiates an events sequence that ends homeostasis and begins the accident sequence. From that event onward, the events sequence may overstress one of the actors, causing injury or damage. These injurious events may initiate other changes that overstress subsequent actors with cascading injury or damage. Until the subsequently stressed actors are able to accommodate the stresses without further harm, the accident continues toward its outcome. Thus, the accident can be seen to begin with a perturbation and end with the last injurious or damaging event in the continuing accidental events sequence. If the actors adapt to the perturbation at any time before injury occurs, a no-accident outcome is achieved, even though the activity may be disordered.

This explanation provides a basis for defining the beginning and end of any accident under investigation and for developing and ordering the events sequence of the accident. Identifying chronological events helps structure the search for the relevant factors and events involved in the accident and provides a method for testing the relevancy of additional events or conditions encountered by the investigator.

Since each actor is involved in sequential events, the events for each are displayed in a linear chain of events. Arrows depicting the flow of the events in a logical sequence link each entry and show the relationship of events to one another. Adding the conditions that must exist for the events to occur and linking them to the events with arrows can show the full explanation of the events for any actor involved in the accident. Furthermore, by arraying the events associated with each actor in parallel horizontal lines across the chart, with the timing of each event maintained relative to the other events, the relationship of each event to every other event in terms of both its timing and its proceed/follow logic can be seen. When two or more actors produce the outcome, the events are displayed as in figure A-3. Note that the spacing of each event is used to show the timing of the event in relation to the other events.

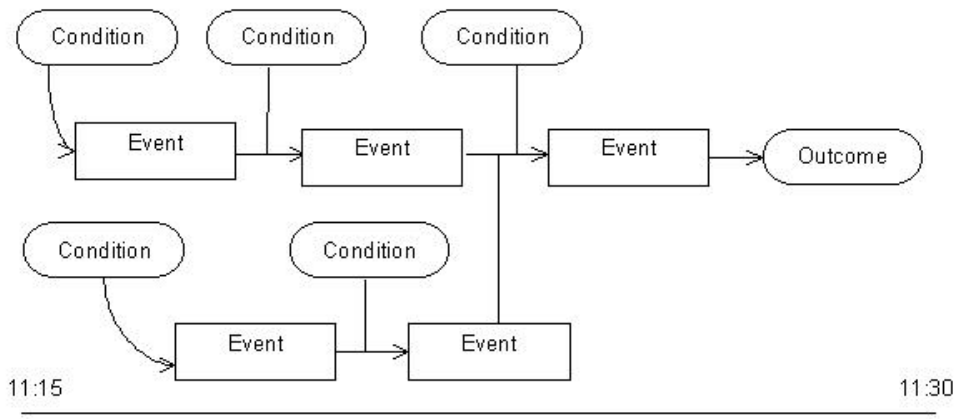


Figure A-3. Multilinear Events Sequence Diagram

This MES charting method provides a way for the investigator of any accident to identify, order, and display the explanation of the relevant factors in the accident. When combined with the generalized explanation of accidents and the criteria for investigative decisions arising from that explanation, the tools for answering the investigator's questions are available.

A.1.1.5 Summary of Hazard Analysis Techniques.

These analysis methods provide noteworthy contributions by requiring the documentation of the factors used in the analysis. By systematically displaying the events and conditions analyzed, these methods give visibility to the relationships involved among the factors, thus, greatly facilitating the communication of the findings to other analysts. Table A-2 compares the three methodologies discussed.

Table A-2. Hazard Analysis Techniques

Analysis Technique	Limitations	Applications
HAZOP	• Requires a well-defined system • Team must have access to detailed information • Tedious • Time intensive • Costly	• Very systematic yet simple approach • Examines interactions between critical components of system • Multidisciplinary team used to identify more problems • Investigates controls to protect against the deviations

Table A-2. Hazard Analysis Techniques (Continued)

Analysis Technique	Limitations	Applications
Sequence of events	• Popular among safety community	• Linear progression characteristic of the model—events must occur in exact sequencing • Interactions among events, contributing causes, and the duration and timing of each event limit the identification of all causal factors
Change analysis	• Used by various private accident investigators as well as with U.S. Air Force	• Expert knowledge of systems operation essential to determination of changes • Very involved when applied to complex processes (Ferry, 1988)
MES	• National Transportation Safety Board uses a similar concept as part of a hybrid approach	• Perceived complexity in developing framework to process all information gathered • Difficulty in identifying human factors with limited work experience

Among the traditional methodologies for the analysis of accidents discussed above, the domino effect and change analysis are the most widely used methods. However, the sequence of events methodology excels because of its simplicity in application. The user simply identifies the accident and deduces the other dominos that led to the undesired event. Change analysis is widely used in the analysis of accidents or failures in a system when change is the suspected causal factor. The MES approach involves a quantitative assessment of engineering structures, the environment, and the timeline analysis (Blackman and Gertman, 1994). The model encourages a complete description of the accident event and successfully avoids introducing investigator bias.

Hazard analysis is the identification of hazards and their causes. However, risk analysis is a systems-safety approach that investigates a system for causal factors and remedies that may exist in personnel, equipment, and environment. Representative risk analysis methodologies are presented in the following sections.

A.1.2 QUALITATIVE RISK ANALYSIS METHODOLOGIES.

In this section, preliminary risk analysis, hazard operability study, and failure mode and effects analysis are discussed. Excellent overviews of risk analysis methods are provided in Aven (2003), Ayyub (2003), and Modarres (2006).

A.1.2.1 Preliminary Risk Analysis.

Preliminary risk analysis (PRA) is a top-down approach that postulates unplanned and undesired events, and determines which components of the system may have contributed to the mishap. It is referred to as top-down methodology because the point of initiation is a hypothesized system-level outcome, which is then dissected into more detailed events.

PRA investigates the event sequence that transforms a potential hazard into an undesired event. First, a list of all the possible hazards related to the system is developed. Next, the hazardous events are analyzed separately. Finally, possible improvements, preventive measures, and mitigation strategies are devised for each hazard. The result of PRA is to provide a basis for determining which hazardous events require more attention and which analysis methods are most appropriate. When PRA is used with a frequency and/or consequence diagrams, identified hazards can be categorized according to risk, prioritized, and then analyzed to determine preventive measures (Moriaty and Roland, 1990).

A.1.2.2 Failure Mode and Effects Analysis.

Failure mode and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service (American Society for Quality, 2006). FMEA examines potential failures by analyzing the parts of a system and listing the corresponding consequences should a specific failure occur. After understanding the purpose of a process, a flow diagram is constructed to establish structure. Next, failure modes are identified and effects of the modes listed are enumerated. These effects are ranked by severity, and the causes for each failure mode are determined. Then, a simple scoring methodology is applied, in which a numerical weight or probability factor is assigned to each cause. A common industry standard uses a scale where 1 indicates not likely and 10 indicates inevitable (Crow, 2002). Mechanisms currently in place to prevent a failure from occurring need to be analyzed for effectiveness. The likelihood of detecting the cause and ultimately averting a failure is resolved through the risk priority number (*RPN*) that is established by the following:

$$(RPN) = Severity(S) \times Occurrence(O) \times Detection(D)$$

Using this approach, an appropriate set of actions is recommended. FMEA is a laborious process that requires the analysis of each subcomponent of the system. A typical FMEA addresses potential human errors only to the extent that human errors produce equipment failures of interest. Misuse of equipment that does not cause an equipment failure is often overlooked in an FMEA. A typical FMEA addresses potential external influences (environmental conditions, system contamination, external impacts, etc.) only to the extent that these events produce equipment failures of interest. Results are dependent on the mode of operation.

A.1.2.3 Hierarchical Holographic Modeling.

As described in Haimes (2004), Hierarchical Holographic Modeling (HHM) has been effectively applied to identify risk and to aid in decision making in widespread domains. This technique is named after holography, a photography technique in which no lens is used. Because many

organizations share an inherent hierarchical structure, HHM is an appropriate technique for many areas. HHM is particularly suited to large-scale, hierarchical, multilevel systems in which it attempts to deal with the inescapable multifarious nature of such systems (Kaplan, et al., 2001). In this procedure, a complex system is decomposed into a series of subsystems. The underlying idea is that the risks associated with these subsystems contribute to and ultimately determine the risk of the overall system (Kaplan, et al., 2001). Interactions between the components and processes of these subsystems are evaluated to identify risks.

Accounting for all or most of the important elements of uncertainty within a system, applying HHM offers a more comprehensive risk analysis. Among the many benefits of using HHM is the ability to model relationships among subsystems while ensuring model traceability. Using HHM adds robustness and resilience in capturing various system aspects and societal elements. Furthermore, the approach of addressing specific aspects of a system is responsive to multiple objectives and decision makers that may be apparent in complex systems. Often, attempting to encompass all the crucial aspects of a system within a single model provides inaccurate results. Administering an HHM analysis provides several different perspectives and a more representative depiction of the infrastructure of a system.

A.1.2.4 Summary of Qualitative Risk Analysis Methodologies.

Qualitative techniques greatly rely on the intuition, insights, and experience of the analyst. They provide a structured approach to guide the analyst's thought process. The most significant advantage of these techniques is that they can be performed at the system level and effectively identify potential hazards and failures within a system. Table A-3 summarizes the characteristics of the three methods discussed. Qualitative methods alone cannot encapsulate risk analysis; accordingly, representative quantitative methods are presented next.

Table A-3. Qualitative Risk Analysis Methodologies

Methodology	Advantages	Limitations
PRA	• Activities lacking safety measures can be readily identified • Quickly identifies hazardous events resulting in most severe loss	• Inability to account for common cause failures • Does not capture time and rate dependant events • Interactions between components of complex system cannot be portrayed
FMEA	• Can uncover a multitude of subtle failure modes • Provides useful documentation of system • Requires less intuitive skill • Every component systematically examined	• Rigorous technical detail • Overlooks multiple fault scenarios • For large systems, results are voluminous

Table A-3. Qualitative Risk Analysis Methodologies (Continued)

Methodology	Advantages	Limitations
HHM	• Accounts for all or most of the important elements of uncertainty within a system • Interactions among components of subsystems and between subsystem and environment are evaluated • Consideration for multiple objectives decision makers	• Incorporates different decomposition approaches and may be confusing • Less systematic • Laborious, time-consuming process

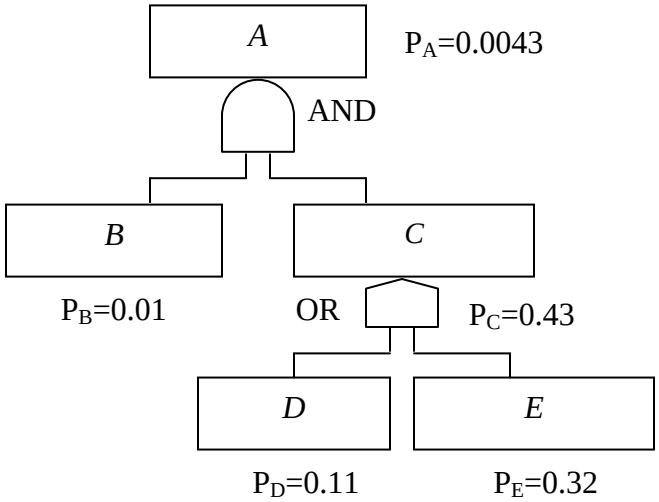
A.1.3 QUANTITATIVE RISK ANALYSIS TOOLS.

In this section, fault tree analysis (FTA), event tree analysis (ETA), cause-consequence analysis (CCA), and Bayesian Belief Networks (BBN) are described.

A.1.3.1 Fault Tree Analysis.

FTA was derived by Bell Telephone Laboratories in 1962 as a method for performing safety evaluations of the Minutemen Intercontinental Ballistic Missile Launch Control System. FTA is a top-down approach, which may be used as a tool to extend PRA in a methodical manner, based on the principle that most failures are caused by a combination of circumstances (Pate-Cornell, 1984). FTA first defines the single most serious outcome or system-level fault. A fault tree is then constructed by establishing the combination and sequence of factors and events that might lead to the top event. It uses a graphic model of the pathways within a system that can lead to an undesirable loss event. The pathways interconnect contributory events and conditions, using standard logic symbols (AND, OR etc). The result is a cause-and-effect diagram, which is based on deductive logic.

Figure A-4 is an example of a fault tree for the event *A*. The top event is event *A*, which is caused by events *B* AND *C*. Event *C* is due to either event *D* OR event *E*. The relations denoted by AND and OR gates are not probabilistic, but by assigning probabilities to each event, the probability of the top event can be calculated. This requires knowledge of the probable failure rates. At an OR gate the probabilities must be added to yield the probability of the succeeding, whereas at an AND gate, the probabilities are multiplied. Assuming that the events *B* and *C* are independent and events *D* and *E* are mutually exclusive, the probability of *A*, can be calculated.



$$P\{\text{Event } A \text{ occurs}\} = P\{\text{Event } B \text{ occurs}\} \text{ AND } P\{\text{Event } D \text{ occurs OR Event } E \text{ occurs}\}$$
$$= P(B)P(D \cup E) = P_B\,(P_D + P_E) = P_B\,P_D + P_B\,P_E$$
$$= (0.01)\,(0.11) + (0.01)\,(0.32) = 0.0043$$

Figure A-4. Fault Tree Example

This is a powerful technique for identifying events that have the greatest influence on the top event. Clearly, FTA can be used in qualitative or quantitative risk analysis. The difference is that the qualitative FTA is not as structured and does not require logic as robust as the formal fault tree. This method is used in various industries and there is vast amount of literature and software packages that support the methodology.

A.1.3.2 Event Tree Analysis.

ETA is an inductive procedure that shows all possible outcomes resulting from an initiating event, taking into account additional events and factors and whether installed safety barriers are functioning or not (Rausand and Høyland, 2003). Table A-4 contains information about event tree terminology.

Table A-4. Event Tree Terminology
(http://www.uscg.mil/hq/gm/risk/E-Guidelines/rbdm.htm)

Initiating Event	The occurrence of some failure with the potential to produce an undesired consequence. An initiating event is sometimes called an incident.
LOA	A protective system or human action that may respond to the initiating event.

Table A-4. Event Tree Terminology (Continued)
(http://www.uscg.mil/hq/gm/risk/E-Guidelines/rbdm.htm)

Branch Point	Graphical illustration of (usually) two potential outcomes when a line of assurance is challenged; physical phenomena, such as ignition, may also be represented as branch points.
Accident Sequence or Scenario	One specific pathway through the event tree from the initiating event to an undesired consequence.

The first steps in building an event tree are to identify and define an initiating event that may give rise to unwanted consequences. Then, potential resulting accident sequences are described and an event tree is constructed. After this, the frequency of the initiating event and the conditional probabilities of the branches in the event tree are determined. Finally, the probabilities for the identified consequences can be calculated (Rausland and Høyland, 2005). The example event tree shown in figure A-5 captures the initiating event of a fire and details several different scenarios. The probability of the individual scenarios can be calculated using the following approach.

Scenario 1: *P* {Resultant Event: Multiple Fatalities}
= *P* {Event: Fire Spreads Out Quickly = Yes}x *P* {Event: Sprinkler Fails to Work = Yes} x
P {Event: People Cannot Escape = Yes}
= (0.9) (0.3) (0.5) = 0.135.

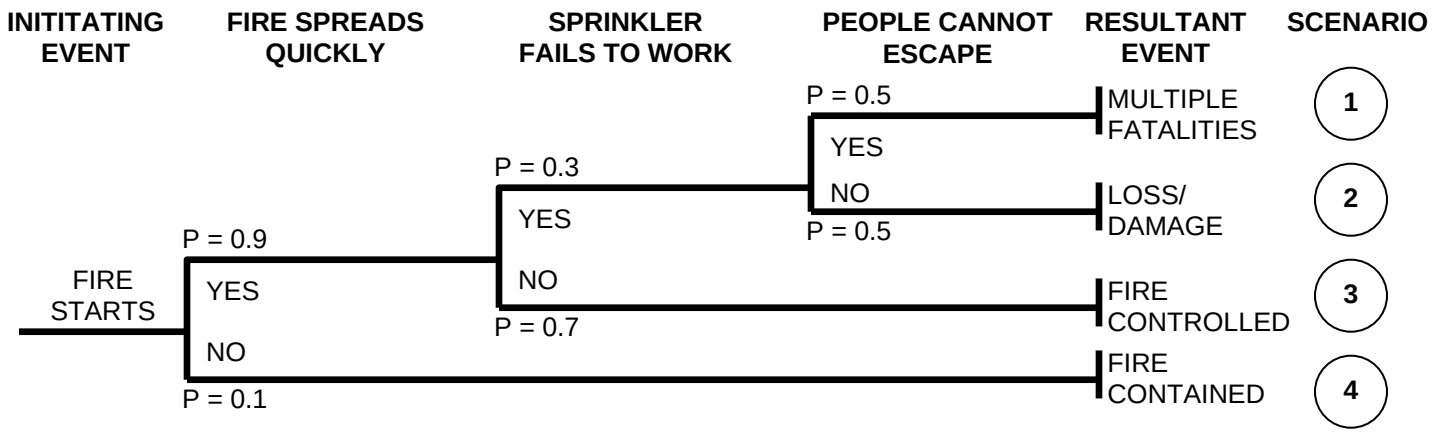


Figure A-5. Simplified Event Tree
(The Institute of Engineering and Technology, 2004)

A.1.3.3 Cause-Consequence Analysis.

One of the methods used by the nuclear industry is CCA, which is used to analyze the risks associated with nuclear power stations. It is complementary to FTA and ETA because it combines cause analysis from FTA and consequence analysis from ETA. First, by using FTA, sources of potential hazard and the events that could initiate such hazard are identified. Then, by using ETA, the possible sequence of events that could result from such occurrences is

established. Event chains are identified in relation to the probability of the individual events occurring; thus, the probabilities of each consequence can be calculated. The overall risk level of the initiating event is determined by aggregating all the known hazards (Burdick and Fussell, 1983). Figure A-6 is an example of a format for CCA. With the exception of the Branching Operator and Consequence Descriptor, the symbols are similar to those used in FTA. Given that the initiating event occurred with probability P_0, consequence 1 occurs when the branching operator indicates that the union of event *A* with event *B* has occurred with probability P_1. Assuming that events *A* and *B* are mutually exclusive, the probability of consequence one can be stated as: P {Consequence 1} = $P_0 P_1$ where $P_1 = P_A + P_B$. Consequences 2 and 3 can be derived similarly. The analysis is exhaustive, $P_0 = (P_0 P_1) + (P_0 (1- P_1) P_0 (1- P_2)) + (P_0 (1- P_1) P_2)$. Once the consequences are aggregated, the appropriate risk level is determined. This method has the ability to analyze multiple outcomes, treat the time sequences of events, and identify single-point successes/failures and the nuances associated with the success/failure.

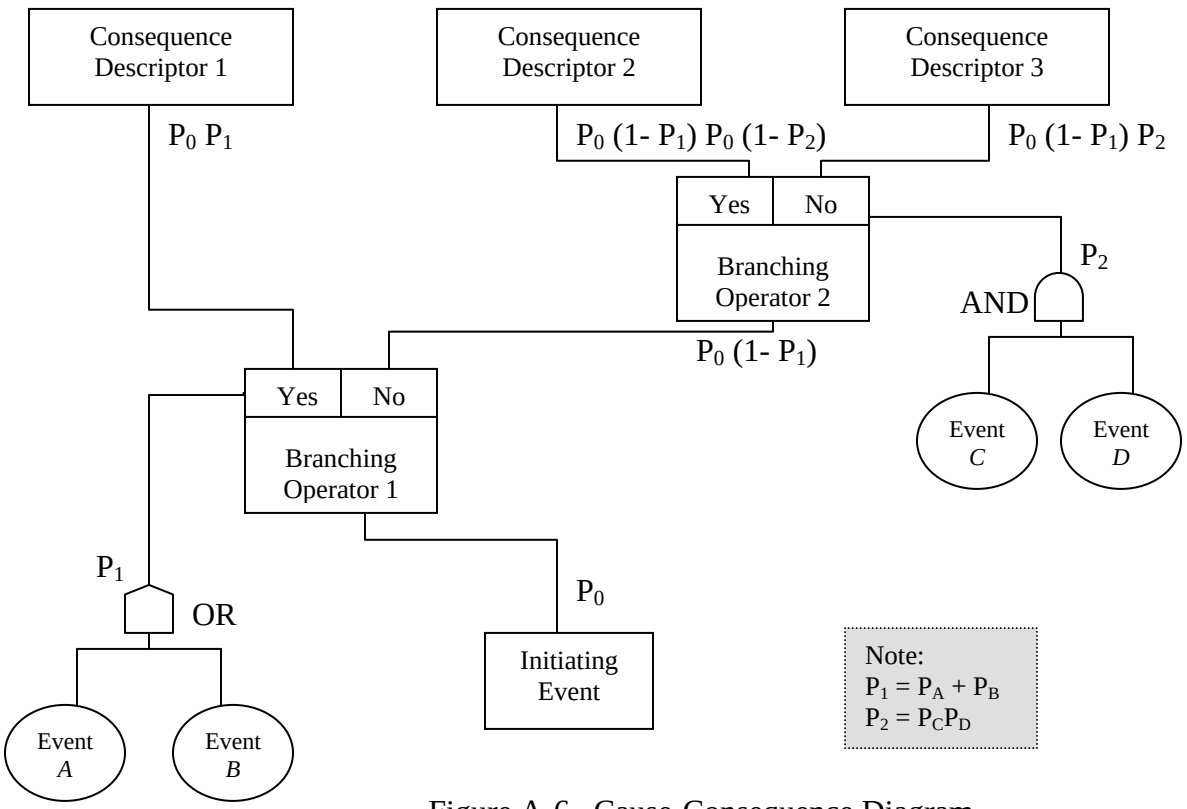


Figure A-6. Cause-Consequence Diagram
(Adapted from Clemens, 2002)

A.1.3.4 Bayesian Belief Networks.

BBN, also known as casual probabilistic networks, have recently gained popularity in industry to support decision making in risk management (Pearl, 1988; Andersen, et al., 1989; Jensen, 1995 and 1996; Fam and Yu, 2004). BBNs originated from the challenges in representing expert knowledge in domains where expert knowledge is uncertain, ambiguous, and incomplete (Jensen, 1995 and 1996). Similar to previous methodologies, a BBN is represented at two levels: qualitative and quantitative. Qualitatively, causal networks are used to graphically represent the

relationships among variables of interest. Quantitatively, Bayesian calculus, known as classical probability calculus, is employed to discover the intricacies underlying the interrelationships among the variables.

A causal network is a diagram comprised of a set of variables and a set of directed links connecting the variables. This diagram is mathematically termed a directed graph and the concepts associated with directed graphs arise from graph theory. Each variable represents a single event and is denoted by a node. The directed links, also termed directed edges, are denoted by arrows. Figure A-7 is an example of a directed graph that is comprised of a set of six nodes and a set of five links. The links signify the direct/causal dependencies and influences between the variables. For example, the link $X_1 \rightarrow X_2$, denoted as L_{12} represents the direct dependence between variables X_1 and X_2. Missing links between variables encode independencies (Castillo, et al., 1997).

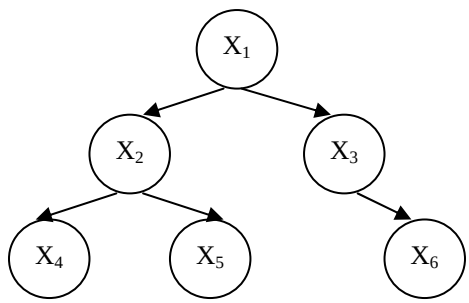


Figure A-7. An Example of a Directed Acyclic Graph

A formal definition of directed graph is given as follows:

- Directed Graph. A graph G = (X, L) is defined as two sets X and L, where X is a finite set of n nodes denoted by $X = \{X_1, X_2, \ldots, X_n\}$ and L is the set of directed links denoted by $L = \{L_{ij} | X_i \text{ and } X_j \text{ are linked}\}$.

  In this simple, directed-graph example, X_1 is the parent node of X_2 and X_3, and X_2 and X_3 are children of X_1. The example represents a directed acyclic graph.

- Parents and Children. When there is a direct link $X_i \rightarrow X_j$ (i.e, from X_i to X_j), then X_i is called the parent of X_j, and X_j is called the child of X_i.

- Directed Acyclic Graph. A directed graph is termed cyclic if it has at least one cycle in the diagram. Otherwise, it is termed a directed acyclic graph (DAG). DAGs are an integral characteristic of BBNs.

As stated by graph theory, influence diagrams have three basic independence structures:

- Serial connections
- Diverging connections
- Converging connections

Figure A-8 is a diagram of a serial connection. Variable *A* has a direct influence on its child, *B*, which has a direct influence on its child, *C*. Variable *A* also has an indirect influence on *C*, meaning that information on *A* influences the certainty of *C* through variable *B*. However, if knowledge of the state of *B* exists, variable *C* is independent of variable *A*. When the state of a variable is explicitly given, it is termed instantiated. The variable *B* is blocked, so information from *A* cannot be transmitted to *C* through variable *B*.

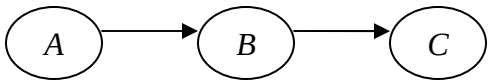


Figure A-8. Serial Connection

FigureA-9 represents a diverging connection. Variable *A* directly influences all of its children. In other words, the certainty of events *B*, *C*, and *D* are dependent on evidence of *A*. If *A* is instantiated, variables *B*, *C*, and *D* are all independent of each other and cannot communicate with each other.

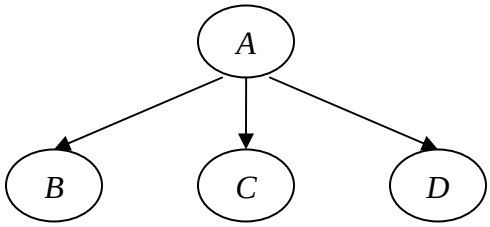


Figure A-9. Diverging Connection

A description of a converging connection is displayed in figure A-10. All the parent nodes, *A*, *B*, and *C*, directly influence variable *D*. Unlike serial and diverging connections, if the states of *D* are empty (unknown), the parent nodes are independent. Yet, if any type of evidence affects the certainty of *D*, then the parents become dependent. Variable *D* may be instantiated from direct knowledge on *D* or from evidence acquired from a child of *D*.

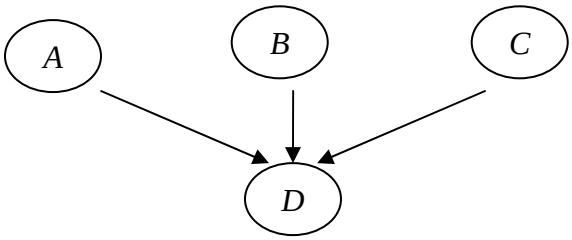


Figure A-10. Converging Connection

Numerous approaches exist to numerically deal with uncertainty, such as Dempster-Shafer calculus and fuzzy logic (Pearl, 1988). In BBNs, the random variables (nodes) can be discrete, continuous, or mixed; however, to measure uncertainty in causal networks, the states or sample space of the variables must be mutually exclusive and collectively exhaustive. Two important types of BBNs are multinomial BBNs and normal, or Gaussian, BBNs. All variables in multinomial BBNs are discrete random variables that have a finite set of possible values.

The goal is to assign every state of a variable a real value measuring the degree of uncertainty for its occurrence. To obtain measures with physical and practical significance, Bayesian calculus, which is based on conditional probability, is used.

An example of a conditional statement is, "the probability of event A given B is x," which is mathematically written as $P(A|B) = x$.

The fundamental rule of probability calculus is as follows:

$$\begin{aligned} P(A,B) &= P(A|B)\,P(B) \\ &= P(B|A)\,P(A) \end{aligned}$$

Thus, yielding Baye's Rule:

$$P(B|A) = \frac{P(A\,|\,B)P(B)}{P(A)}$$

If the variable B has mutually exclusive and exhaustive states, $b_1, b_2, \ldots, b_m$, then $P(A|B)$ is an n x m matrix consisting of nm entries of the configuration $P(a_i|b_j)$ where m column sums are all equal to one, or $\sum_{i=1}^{n} \mathrm{P}(\mathrm{a_i}\,|\,\mathrm{b_j}) = 1$ for j=1, …, m. This matrix is termed the conditional probability distribution (CPD) of variable A. Applying the fundamental rule to the nm entries yields,

$$P(a_i|b_j)P(b_j) = P(a_i, b_j).$$

Thus, a new $P(A,B)$ matrix of size n x m is obtained by multiplying each $P(a_i|b_j)$ entry of the CPD to the corresponding $P(b_j)$. The sum of all the entries in this matrix is equal to 1, or $\sum_{i,j} P(a_i\,|\,b_j) = 1\ \forall i, j$. This matrix is termed the joint probability distribution (JPD) or probability mass function for variables A and B. From the JPD, the probability distribution $P(A)$ can readily be calculated. There are exactly m mutually exclusive events, $(a_i, b_1),\ldots,(a_i, b_m)$, for which A is in state a_i. Thus,

$$P(a_i) = \sum_{i=1}^{n} P(a_i, b_j) \forall j\ .$$

This computation is referred to as marginalization. The variable B, is marginalized out of the JPD, yielding the probability distribution of A.

The blocking of information demonstrates the Bayesian calculus concept of conditional independence. The formal definition is given as:

- Conditional Dependence and Independence. Let the variables *A*, *B*, and *C* be three sets of disjoint variables. *A* is said to be conditionally independent of *C* given the variable *B* if and only if

$$P(a_i|b_j) = P(a_i|b_j, c_k) \ \forall i, j, k$$

  Otherwise, *A* and *C* are conditionally dependent given *B*. Conditional independence occurs in serial and diverging connections (see figures A-8 and A-9). Conditional dependence occurs in converging connections (see figure A-10).

What conditional independence indicates is that once *B* is known, knowledge of *C* has no influence on *A*, or knowledge of *C* does not add any new information to *A*.

The significance of the causal relations is demonstrated by quantifying the links. For example, if *B* is a child of *A*, then probability calculus designates $P(B|A)$ as the strength of the link. Now, if *C* is also a parent to *B*, then $P(B|A)$ and $P(B|C)$ does not provide any information on how the interaction of *A* and *C* may influence *C*; therefore, $P(B|A,C)$ must be measured. Some causal relations may be cyclic, but cannot be modeled quantitatively because no calculus exists that can handle cycles. In summary, a BBN must have the following:

- A set of nodes and a set of links connecting the nodes
- Each node has a finite number of mutually exclusive states
- The nodes together with the links form a DAG
- Each node with a parent has a corresponding CPD

Applications of BBNs to aviation safety appear in Ale, et al. (2005), Roelen, et al. (2003a and 2003b) and Luxhøj (2003, 2005a, and 2005b) and Luxhøj, et al. (2001), and Luxhøj, et al. (2003).

A.1.3.5 Logic-Evolved Decision Tools.

Logic-Evolved Decision Tools (LEDTools) is a decision analysis software package that has been developed for experts with extensive knowledge about a particular system to build visual graphs easily to depict what is taking place (Donald, et al., 2004). LEDTools is particularly useful because those with the ability to interact with experts and translate knowledge into process tree logic are often unavailable. The aim of LEDTools is to make model building a simple task for experts, thereby reducing the need for logic model-building specialists. The software provides a user-friendly interface that draws upon the formation of tree structures with logic gates. Process trees are constructed to develop a comprehensive set of scenarios. Then, LEDTools evaluates these scenarios in a consistent and traceable manner. A heavy emphasis is placed on the visual characteristics of logic trees to make their development well organized and efficient for subject

matter experts. This approach is based on the fact that experts have detailed knowledge about systems, not the logic modelers.

One fundamental structure used in LEDTools is the process tree, which is a deductive logic tree. This structure provides a framework for deductively generating possible causes of a final state or possible outcomes of an initial state. In doing this, the tree allows the analyst to draw conclusions based on input data. The basic gates used in an LED tree are outlined in table A-5.

Table A-5. Basic LEDTools Gates

GATE	TYPE
	Terminal Node
	Inclusive OR
	Exclusive OR
	Taxonomy
	AND
	Priority AND
	Causal
	Cycle
	Inferential AND

Included in the LEDTools, another utility capability of LEDTools software package is the path solver. The path solver can be used to assemble the "story" of the problem. The tree is a set of logical equations that can be enumerated to arrive at various scenarios. "Conceptually, the paths are found by successively substituting into the logical equations and preserving the partial results at each step" (Bott, et al., 2003). A digraph is a directed visual graph that can be constructed using LEDTools software. The digraph is formed using the paths previously outlined by the path solver. This allows users to view a clear representation of the situation in graphical form.

A.1.3.6 Summary of Quantitative Risk Analysis Tools.

Quantitative techniques provide a means to logically calculate safety measures. The tools discussed are based on mathematical analysis using certain models, which can be highly uncertain. Table A-6 provides an overview of the quantitative techniques presented.

Table A-6. Quantitative Risk Analysis Tools

Analysis Tool	Advantages	Limitations
FTA	• Great for working overall probability of undesired event • Probabilities easily determined	• Does not account for dependencies between events • Linear causality emphasized
ETA	• Multiple resulting events analyzed • Probabilities easily calculated	• Does not account for dependencies between events • Confined to binary logic modeling • Difficult to incorporate nonlinear relationships
CCA	• Multiple outcomes analyzed • End events need not be foreseen • Explores time-sequenced systems	• Pathways must be anticipated • Analyzes for only a single challenge/failure/loss
BBN	• Readily handles situations where data is limited or inaccessible • Models causal relationships • Allows for robust probabilistic inference • Strengths of relationships between elements readily represented • Allows for combination of • subjectivity and objectivity	• Combinatorial explosion if not modeled carefully • All assessments must be well documented to avoid becoming nontraceable
LEDTools	• Easily interpreted by layperson • Efficient, systematic method • Process tree methodology emphasizes visual approach • Wide spectrum of applications	• Need to develop a comprehensive set of scenarios to maximize effectiveness • Time intensive when used in a complex system

A.2 CONCLUSIONS.

It is evident that the process of identifying hazards and their causes involves many aspects of a system. The more intricate a system, the more likely it is to overlook potential hazards. Attempting to identify all possible hazards and their causes is imperative. Potential hazards

should not be excluded because their occurrence probability at the time of the analysis seems abstract. No single methodology exists that ensures the identification of all potential sources of harm. The results of hazard analysis should give a complete and unbiased picture of all potential hazards and their causes. It is ideal to apply several of the discussed methodologies in a structured manner to detect hazards and assess risk.

Two different procedures can be used to estimate the risk associated with each hazard occurring: qualitative and quantitative. Both procedures have their strengths and weaknesses. Qualitative techniques compare and classify safety based on the experience of the analysts. They are subjective in nature as levels for the severity and likelihood of a hazardous event are assigned with discretion. A weakness of this method is that the assignment of levels may be arbitrary without underlying detailed knowledge. Quantitative techniques compare and classify safety based on calculations from mathematical models. Quantitative methods use occurrence probabilities together with a severity rating. Many of these probabilities must be calculated from statistical methods. The weakness of these methods is that reliable statistical data may not be accessible and that using uncertain data may erroneously represent a high level of precision.

Of all the methodologies discussed, Bayesian Belief Networks (BBN) have shown to provide the most significant insights in risk management. BBNs are a marriage between Bayesian probability theory and graph theory. They provide a natural tool for dealing with two problems that occur throughout applied mathematics and engineering: uncertainty and complexity. BBNs provide an objective and visible support for decision-making in risk management. BBN's influence diagrams visually model cause-consequence relations, therefore, facilitating risk identification. They also provide probabilistic assessments and model uncertainties using expert judgment. Subjectivity reflects the expert's intimate knowledge of the system, elements in the scenario, and the exact dynamics behind the scenarios, and the expert's ability to intelligently simplify, compute, or aggregate these situations. When new knowledge or evidence is presented, the new information is considered and the BBN is updated.

A.2 TECHNOLOGY REVIEW.

As Co-Chair of the Global Aviation Information Network (GAIN) Working Group B: Analytical Methods and Tools from March 1999 to June 2000, Dr. Luxhøj co-led a team of government, industry, and academia members to perform intensive reviews of a number of software tools to support risk analysis and other methods. The *GAIN Guide to Methods and Tools for Airline Flight Safety Analysis* is a valuable resource that contains reviews and critiques of supporting technology. While the supporting tools were reviewed in the context of aviation safety, the reviews extend to and have applicability to the UAS domain. In particular, section 3.1 on Tools for Event Analysis and section 3.2 on Methods for Event Analysis are relevant to the UAS domain in that tools and methods for risk analysis, trend analysis, text mining, and human factors analysis are reviewed and critiqued. While it is acknowledged that there are most likely software updates to these tools since the time of the GAIN review, the basic structure and analysis capabilities of the tools remain unchanged.

A.3 BIBLIOGRAPHY.

Ale, B.J.M., L.J. Bellamy, R.M. Cooke, L.H.J. Goossens, A.R. Hale, D. Kurowicks, A.L.C. Roelen, and E. Smith (2005), "Development of a Causal Model for Air Transport Safety," *Proceedings of the European Safety and Reliability Conference*, Tri City, Poland, pp. 37-44.

Allocco, M. (2006b), *System Safety Engineering and Management Guidebook*, Federal Aviation Administration.

American Society for Quality (2006), "Failure Mode and Effects Analysis," Retrieved June 12, 2006, from http://www.asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

Andersen, S.K., K.G. Olesen, F.V. Jensen, and F. Jensen (1989), "HUGIN—A Shell for Building Bayesian Belief Universes for Expert Systems," in *Proceedings of the Eleventh International Joint Conference on Artificial Intelligence*, Detroit, Michigan, pp. 1080-1085.

Andres, D. (2005), *Development of a Post-Consequence Model for Aircraft Accident Severity Assessment*, M.S. Thesis, Department of Industrial and Systems Engineering, Rutgers University, Piscataway, New Jersey.

Aven, T. (2003), *Foundations of Risk Analysis*, England: John Wiley & Sons, Ltd.

Ayyub, B.M. (2003), *Risk Analysis in Engineering and Economics*, New York: Chapman & Hall/CRC.

Benner, L. (1975), "Accident Investigation: Multilinear Events Sequencing Methods," *Journal of Safety Research*, Vol. 7, No. 2, pp. 67-73.

Benner, L. (1977), "Accident Theory and Accident Investigation," *Hazard Prevention*, Vol. 13, pp. 18-21.

Blackman, H.S. and D.I. Gertman (1994), *Human Reliability and Safety Analysis Data Handbook*, 1st ed., New York: John Wiley & Sons, Inc.

Bott, T., S. Eisenhawer, J. Kingson, and B. Key (2003), "A New Graphical Tool for Building Logic-Gate Trees," LA-UR-03-134, Los Alamos National Laboratory, *Proceedings of the American Society of Mechanical Engineers–Pressure Vessels and Piping Annual Meeting*, Cleveland, Ohio.

Burdick, G.R. and J.B. Fussell (1983), "On the Adaptation of Cause-Consequence Analysis to U.S. Nuclear Power Systems, Reliability and Risk Assessment," *System Reliability and Risk Assessment*, JBF Associtates, Inc., Knoxville, Tennessee.

Buys, J.R. and J.L. Clark (1995), Revision 1A, SCIE-DOE-01-TRAC-14-95, Technical Research and Analysis Center, SCIENTECH, Inc.

Castillo, E., J.M. Gutierrez, and A.S. Hadi (1997), *Expert Systems and Probabilistic Network Models*, New York: Springer-Verlag.

Crow, K. (2002), "Failure Modes and Effects Analysis," retrieved June 29, 2006, from http://www.npd-solutions.com/fmea.html

Donald, S., T. Bott, and S. Eisenhawer (2004), "Representing Subjective Knowledge in Engineering Systems Using Possibility Trees," Los Alamos National Laboratory, *8th World Multi-Conference on Systemics, Cybernetics and Informatics*, Orlando, Florida.

EuroControl (2004), "Review of Techniques to Support the EATMP Safety Assessment Methodology," Volume 1, EuroControl Experimental Center, EEC Note No. 01/04.

Fam, C.F. and U.C. Yu (2004), "BBN-Based Software Project Risk Management," *The Journal of Systems and Software*, Vol. 73, pp. 193-203.

Ferry, T.S. (1988), *Modern Accident Investigation and Analysis*, 2nd ed., New York: John Wiley & Sons, Inc.

Haimes, Y. (2004), *Risk Modeling, Assessment, and Management*, New York: John Wiley & Sons, Inc.

Heinrich, H.W. (1936), *Industrial Accident Prevention*, New York: McGraw-Hill.

Jensen, F.V. (1995), *Introduction to Bayesian Networks*, United Kingdom: University-College London Press.

Jensen, F.V. (1996), *Introduction to Bayesian Networks*, New York: Springer-Verlag.

Jones, P.L., J. Jorgens, A.R. Taylor, Jr., and M. Weber (2002), M.S. Thesis, *Risk Management in the Design of Medical Device Software Systems*, Center for Devices and Radiological Health, Food and Drug Administration, Rockville, Maryland.

Kaplan, S., Y. Haimes, and B. Garrick (2001), "Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk," *Risk Analysis*, Vol. 21, No. 5.

Keller, F. (2006), "Is There Hope for Quantitative Risk Analysis in Commercial Aviation?" *Proceedings of the 24th International System Safety Conference*, Albuquerque, New Mexico.

Lechner, K. (2007), *Security Risk Assessment Using Bayesian Belief Networks and Logic-Evolved Decision Models*, M.S. Thesis, Department of Industrial and Systems Engineering, Rutgers University, Piscataway, New Jersey.

Luxhøj, J.T. (2003), "Probabilistic Causal Analysis for System Safety Risk Assessments in Commercial Air Transport," *Proceedings of the Workshop on Investigating and Reporting of Incidents and Accidents (IRIA)*, Williamsburg, Virginia, pp. 17-38.

Luxhøj, J.T. (2005a), "Model-Based Reasoning for Aviation Safety Risk Assessments," *SAE World Aerospace Congress*, Dallas/Fort Worth, Texas.

Luxhøj, J.T. (2005b), "Aviation Safety in Practice: Applying Principles and Tools to Measure Risk Reduction," *Safety Across High-Consequence Industries*, Saint Louis University, St. Louis, Missouri.

Luxhøj, J.T., A. Choopavang, and D.N. Arendt (2001), "Risk Assessment of Organizational Factors in Aviation Systems," *Air Traffic Control Quarterly*, Vol. 9, No. 3, pp. 135-174 *(Special Issue on Flight Safety)*.

Luxhøj, J.T., M. Jalil, and S.M. Jones (2003), "A Risk-Based Decision Support Tool for Evaluating Aviation Technology Integration in the National Airspace System," *Proceedings of the AIAA's 3rd Annual Aviation Technology, Integration, and Operations (ATIO) Technical Forum*, Denver, Colorado.

Modarres, M. (2006), *Risk Analysis in Engineering: Techniques, Tools, and Trends*, New York: Taylor & Francis/CRC.

Moriaty, B. and H.E. Roland (1990), *System Safety Engineering and Management*, 2nd ed., New York: John Wiley & Sons, Inc.

Pate-Cornell, M.E. (1984), "Fault-Tree vs. Event Trees in Reliability Analysis," *Risk Analysis*, Vol. 4, No. 3, pp. 177-186.

Pearl, J. (1988), *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, San Francisco, California: Morgan Kaufmann.

Rausand, M. and A. Høyland (2003), *System Reliability Theory*, New York: John Wiley & Sons, Inc..

Roelen, A.L.C., R. Weaver, R.M. Cooke, R. Lopuhaa, A.R. Hale, and L.H.J. Goosens (2003a), "Aviation Causal Modeling Using Bayesian Belief Nets to Quantify Management Influence," *Safety and Reliability*, Bedford and van Gelder, eds., Swets & Zeitlinger, Lisse, The Netherlands, pp. 1315-1320.

Roelen, A.L.C., R. Weaver, A.R. Hale, L.H.J. Goosens, R.M. Cooke, R. Lopuhaa, M. Simons, and P.J.L. Valk (2003b), "Causal Modeling for Integrated Safety at Airports," in *Safety and Reliability*, Bedford and van Gelder, eds., Swets & Zeitlinger, Lisse, The Netherlands, pp. 1321-1327.

Safety Management Services (2006), HAZOP Basis, retrieved June 12, 2006, from http://www.sms-ink.com/services_pha_hazop.html

Vick, S.G. (2002), *Degrees of Belief*, Reston, Virginia: American Society of Civil Engineers.

APPENDIX B—THE UAS e-WORKBOOK

As a major added value, the Unmanned Aircraft System (UAS) e-Workbook is simply a repository of tools, documents, and references used throughout the current Phase 1 research and its results. In this appendix, the e-Workbook is introduced, and some of its main features are briefly discussed.

B.1 MAIN FEATURES OF THE e-WORKBOOK.

The layout of the e-Workbook mimics the layout of a web page. The user navigates through it by clicking various links along with familiar Back, Forward, and Home buttons. Due to its ease of use and its extensive user base, Microsoft® Excel® was chosen to be the platform used to build a prototype. However, a Microsoft Access®- or Microsoft Visual Basic®-based tool for the e-Workbook would offer more functionality for future applications. Figure B-1 shows the e-Workbook title page. It provides basic information on the research such as title, research personnel, and affiliations.

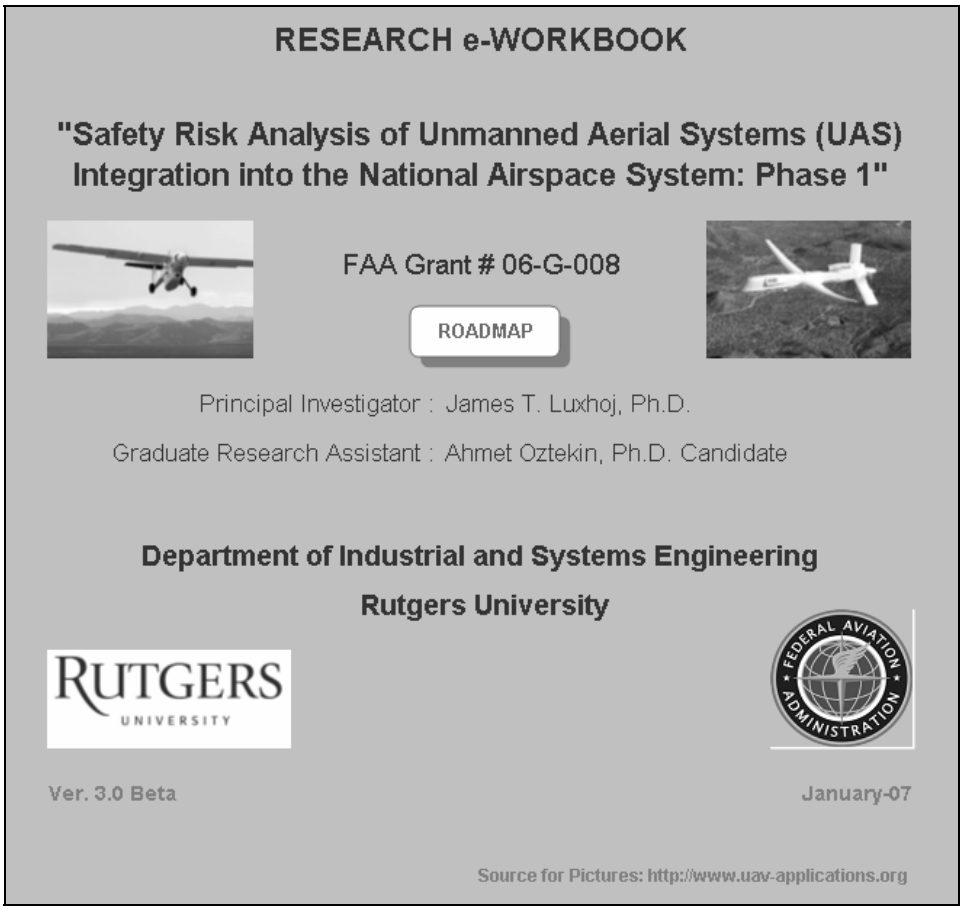


Figure B-1. Screen Capture of the e-Workbook Title Page

By clicking the Roadmap button at the middle of the title screen the user is led to the main page, which serves as a hub for links to various components of the research. A screen capture of the roadmap is provided in figure B-2.

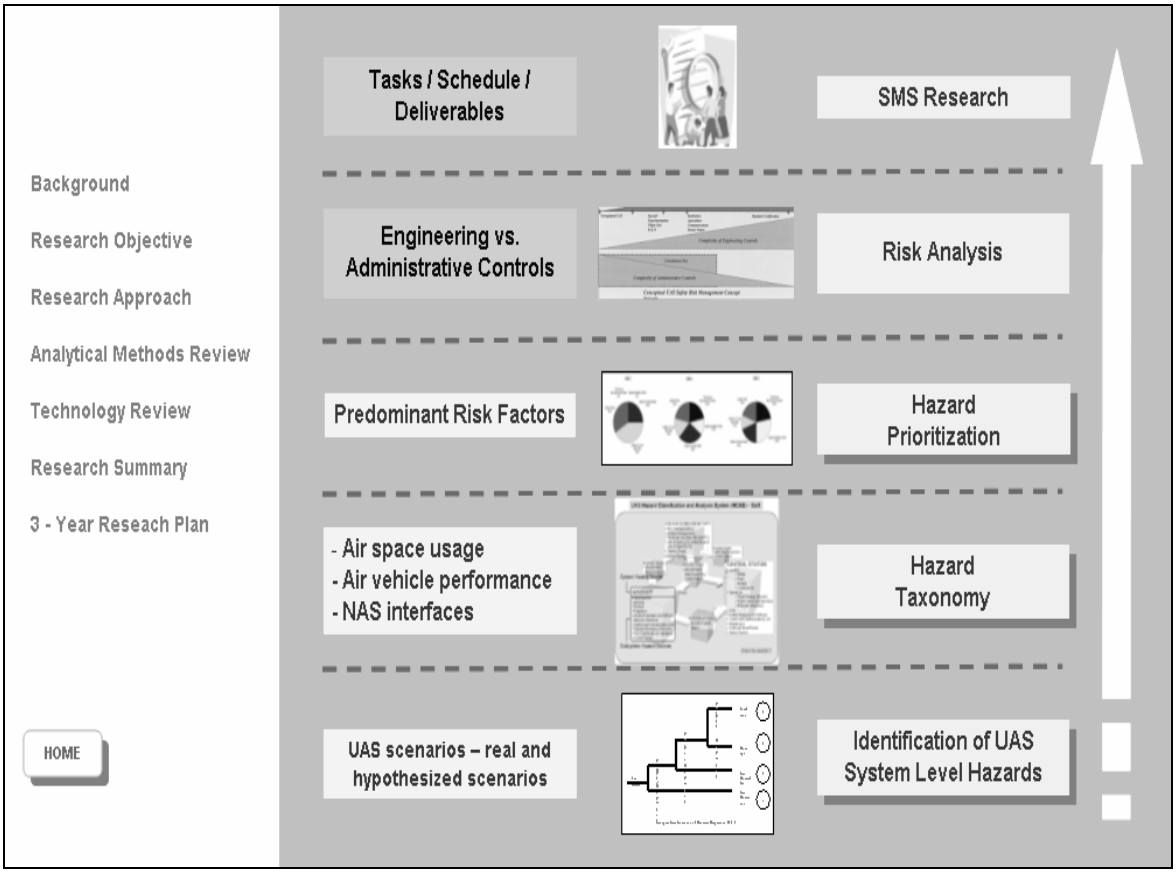


Figure B-2. The Roadmap Screen Functions as a Hub for all Links to the Components of the UAS Research

Background, Research Objective, Research Approach, Analytical Methods Review, Technology Review, Research Summary, and 3-Year Research Plan constitute the links listed on the left part of the screen. The links listed on the left side of the screen provide access to the related parts and sections of the final research report for the Rutgers UAS Phase 1 research. The illustrated part of the roadmap has three live links: Identification of UAS Hazards, UAS Hazards Taxonomy, and Hazard Prioritization, which cover the results of the year-one research.

The identification of UAS System Level Hazards link leads to the source file, which includes the raw data for the results of the HCAS mapping process. A sample screen shot is provided in figure B-3.

HOME ROADMAP ANALYSIS

Scenario #	Hazard Definition	AIRCRAFT													
		Aerodynamics	Airframe	Payload	Propulsion	Aviaonics Hardware & Software	Sensors / Antennas	Onboard Power	Control & Communications Link	Onboard Conflict Avoidance Subsystem (DSA)	Onboard Emergency Recovery	Verification & Validation	Design Reliability & Availability	Generic Design	Generic Redundency
	TOTAL														
1	The transitional planning for UAS NAS integration is LTA											1	1		
2	Assumptions concerning reliability and availability maturity are LTA											1	1		
3	Current DoD and contractor system safety and system reliability analyses a														
4	vehicles may not meet NAS-level availability and reliability requirements ass		1										1		1
5	UAS designs do not meet quantitative levels for Catastrophic and Hazardou	1	1		1	1	1	1							
6	The allocation of risk control is LTA													1	
7	The autonomous UAS system is not adequately evaluated														
8	Initial airspace exposure Special Use Airspace or Access Areas may not be														
9	Advanced designs take time to mature														
10	Transitional risks associated with the "build a little, test a little" approach oc												1		
11	LTA planning or procedures development														
12	unique risks associated with UAS high altitude (TBD) operations														
13	coordination, communication (between UAS operator/pilot, observer, or ve														
14	LTA Contingency Procedures and Planning														
15	Vehicle sensors provide limited field of view						1								
16	Vehicle video/IR sensors provide limited field of view						1								
17	Vehicle video/IR sensors provide limited field of view						1								
18	Vehicle video/IR sensors provide limited field of view						1								
19	Vehicle video/IR sensors provide limited field of view						1								
20	Vehicle video/IR sensors provide limited field of view						1								
21	Airport/airstrip selection is LTA														
22	Communication (VHF, UHF, data link, radio) is lost					1			1						
23	UAS onboard autonomous conflict avoidance subsystem fails					1				1					
24	Semi- autonomous conflict avoidance subsystem fails					1				1					
25	LTA design UAS autonomous or semi-autonomous weather detection/sen					1	1								
26	Conflict avoidance subsystem fails at a critical time					1				1					
27	LTA input data/information					1									
28	Unsuccessful go-around occurs					1			1	1					
29	Unsuccessful go-around occurs					1									
30	Autonomous UAS identifies hazard and must deviate from flight plan and deviation is r					1									
31	Loss of surveillance occurs					1									
32	LOC due to icing	1	1												

Figure B-3. Screen Capture From the UAS e-Workbook

In figure B-3, the user can view the individual hazards identified by the Hazard Classification and Analysis System (HCAS) mapping process associated with any particular UAS scenario included by the current scenario set. Additionally, by clicking on a scenario number, the user can view the original narrative for that particular scenario. Access to the documentation for a particular scenario will provide the user with the ability to verify the results of the HCAS mapping process and to gain a better understanding of the meaning of individual hazards within the context of that particular scenario.

The "UAS Hazards Taxonomy" link refers to a page where a three-dimensional illustrated version of the taxonomy is presented to the user. Figure B-4 depicts a screen capture from that page. By clicking on each cube, the user is referred to the definition of that system-level HCAS hazard source group and to the results of the mapping process accompanied by their analysis.

Finally, the Hazard Prioritization link on the Roadmap screen (see figure B-2) refers the user to the results of the HCAS hazard prioritization process.

The results of the prioritization analysis are presented as a succession of consecutive pages, which are linked together and to the Roadmap and title page of the e-Workbook by using the navigation buttons provided on each page visited. A sample screen is provided in figure B-5.

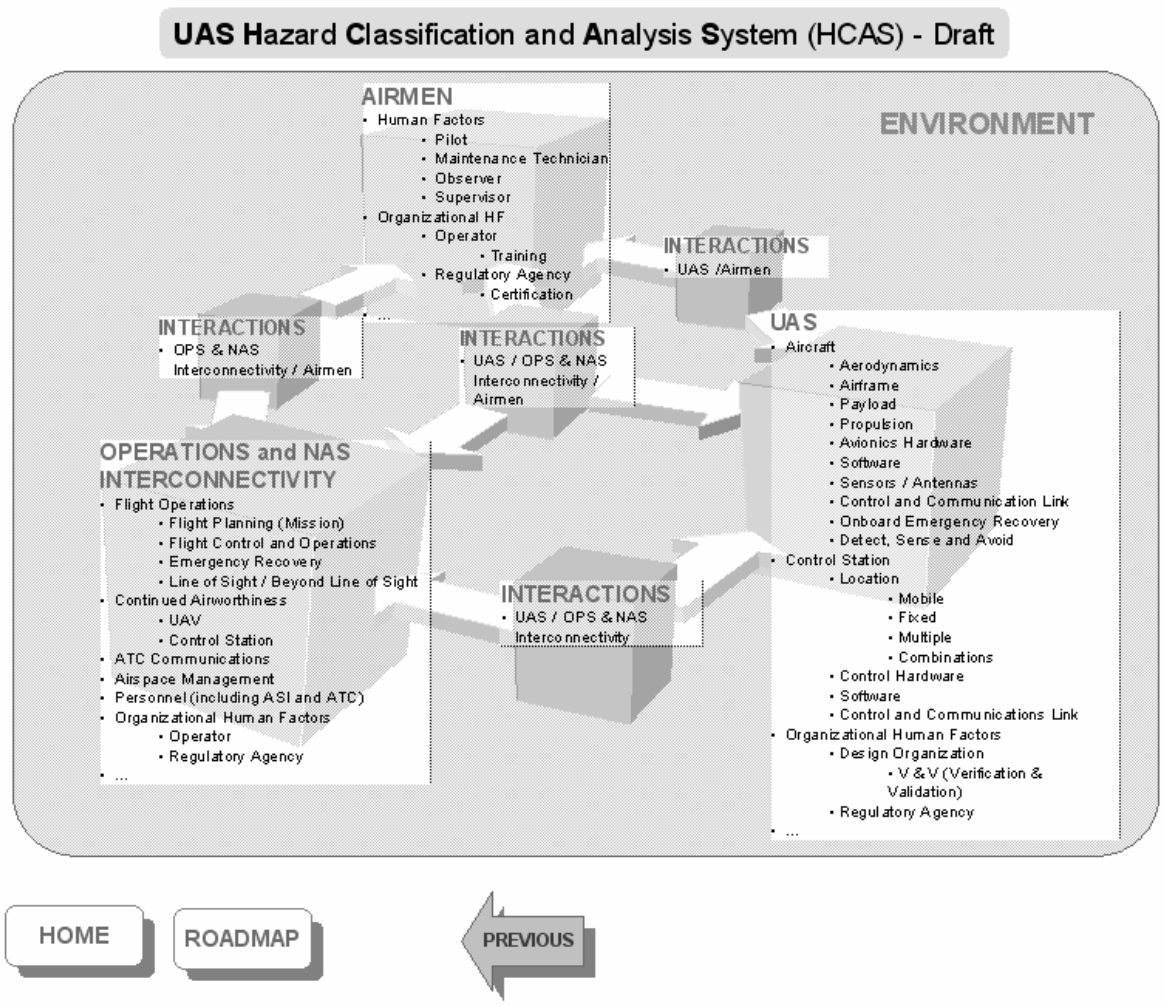
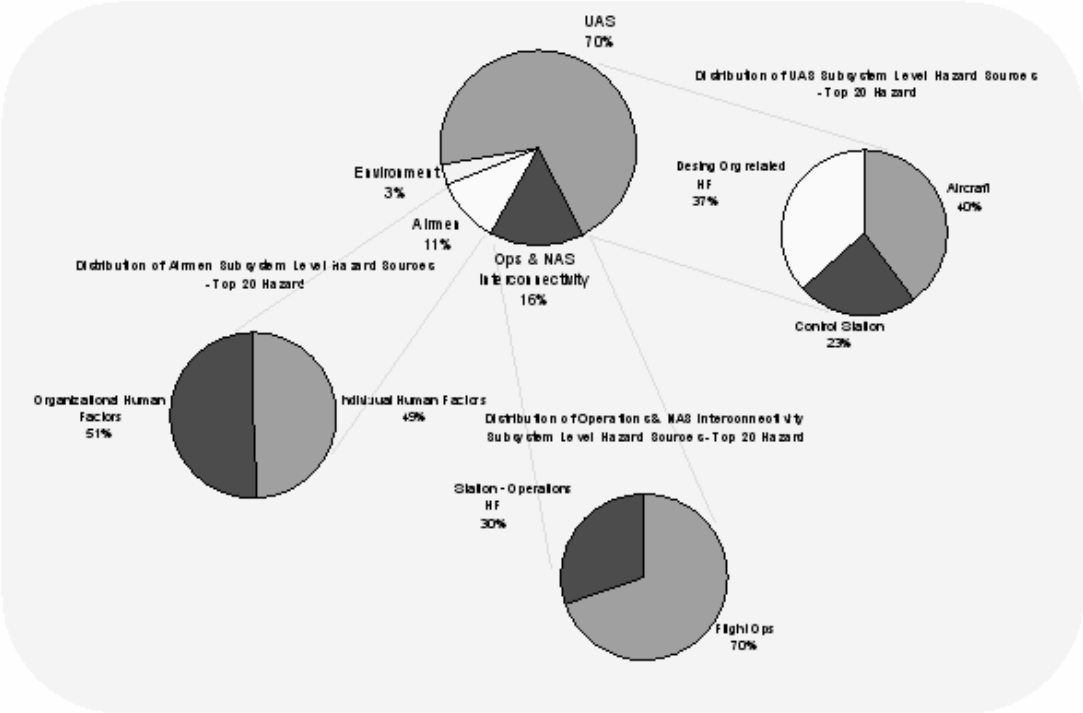


Figure B-4. The UAS Hazards Taxonomy Screen

As the repository of results and related documentation of the current research, the UAS e-Workbook includes all the work performed by the Rutgers team under the first year of the current cooperative agreement with the Federal Aviation Administration William J. Hughes Technical Center. However, the Roadmap page of the e-Workbook introduces a vision for future work with regard to UAS risk analysis. Therefore, only the links that are covered by the current phase of the research are active. The inactive links, such as Risk Analysis, are provided to indicate future work that has not yet been conducted. They serve as guidelines for future work as well as milestones on the roadmap, which provide context for the current research within the larger domain of UAS risk and safety analysis.

HOME ROADMAP

Distribution of Top 20 Hazards - HCAS System Level Categorization



Ranking	System Level Hazard Sources	Subsystem Level Hazard Sources	Hazard Source	Count
1	UAS	Aircraft	Flight Management and Aviaonics Hardware / Software	65
2	UAS	Control Station	Control Hardware and Software	54
3	Ops & NAS Interconnectivitynectivity	Flight Ops	Flight Control and Operations	37
4	Airmen	Organizational Human Factors	Human Factors - General	31
5	UAS	Aircraft Desing Org related HF	Oversight	30
6	Airmen	Individual Human Factors	Loss of Situational Awareness	30
7	UAS	Aircraft Desing Org related HF	LTA Requirements / specifications	29
8	UAS	Aircraft	Generic Design	28
9	Ops & NAS Interconnectivity	Control Station - Operations HF	LTA Procedures / Processes	26
10	UAS	Aircraft	Airframe	24
11	UAS	Aircraft Desing Org related HF	Inadequate Knowledge / information / Data	23
12	Ops & NAS Interconnectivity	Flight Ops	Flight Planning (Mission)	23
13	UAS	Aircraft Desing Org related HF	LTA Planning	22
14	UAS	Aircraft	Sensors / Antennas	21
15	UAS	Aircraft Desing Org related HF	LTA Procedures / Processes	21
16	UAS	Control Station	Control & Communications Link	19
17	UAS	Aircraft	Propulsion (incl. Fuel Source)	18
18	UAS	Aircraft Desing Org related HF	Omission	18
19	Environment		Weather	18
20	UAS	Control Station	Generic Design	17

Figure B-5. A Sample Page of Prioritization Results Using the Hazard Prioritization Link