

---

# Literature Search for Methods for Hazard Analyses of Air-Carrier Operations

---

Prepared for the

Aircraft Safety Research & Development Branch, AAR-420  
Federal Aviation Administration  
FAA William J. Hughes Technical Center  
Atlantic City International Airport, NJ 08405  
Research Grant Number 99-G-012

by

G. Martinez-Guridi and P. Samanta

Brookhaven National Laboratory  
Energy Sciences and Technology Department  
Upton, NY 11973

June 2002

This research was supported by the U.S. Department of Energy  
Contract No. DE-AC02-98CH10886

OPTICAL COPY

#### **DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency, contractor, or subcontractor thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency, contractor, or subcontractor thereof.

**BNL-69279**

**Literature Search for Methods for Hazard Analyses  
of Air-Carrier Operations**

**G. Martinez-Guridi and P. Samanta**

**Brookhaven National Laboratory  
Energy Sciences and Technology Department  
Upton, NY 11973**

June 2002

Work was carried out as part of FAA Research Grant No. 99-G-012

# TABLE OF CONTENTS

**Page**

<b>List of Figures</b> .....	v
<b>List of Tables</b> .....	vi
<b>Acknowledgments</b> .....	vii
<b>List of Acronyms</b> .....	viii
<b>Executive Summary</b> .....	ix
<b>1. Introduction</b> .....	1
<b>2. Brief Description of ACOSM</b> .....	3
<b>3. Process for Identifying Applicable Approaches</b> .....	7
3.1 Approach Used for the Literature Search .....	7
3.2 Sources of the Literature Search .....	7
3.3 Review of Publications to Identify Potentially Applicable Methods or Approaches .....	9
3.4 Grouping of the Selected Publications or Methods .....	9
3.4.1 Aviation-safety Programs .....	9
3.4.2 Methods Addressing Hazards in Management of Operations .....	12
3.4.3 Techniques for Evaluating Human Error .....	13
3.4.4 Techniques for Identifying and Assessing Hazards in Hardware-oriented Operations .....	15
3.4.5 Techniques for Identifying and Assessing Hazards During Maintenance and Inspection .....	15
3.4.6 Software-safety Analysis .....	15
3.4.7 Other Relevant Studies or Approaches .....	16
<b>4. Discussion of Approaches and Applicability to ACOSM</b> .....	18
4.1 Applicability of Approaches to ACOSM .....	18
4.2 Applicable Methods for ACOSM from Literature Search .....	19
<b>5. Bibliography</b> .....	23



# LIST OF FIGURES

	<u>Page</u>
Figure 2.1 . A Typical IDEF0 Diagram Hierarchy .....	5

## LIST OF TABLES

	<u>Page</u>
Table 4.1    Applicable Methods for ACOSM Relating Different Areas of Methods Development .....	21

## **ACKNOWLEDGMENTS**

We thank Kathy Fazen of the FAA's Aircraft Safety Research & Development Branch at the Technical Center for her support, interactions, and useful discussions in conducting this work. We also thank John LaPointe and Mike Vu for their interest and support.

## ACRONYMS AND ABBREVIATIONS

ACOSM	Air Carrier Operations System Model
AHP	Analytical hierarchy process
ASP	Aviation Safety Program
BASI	Bureau of Air Safety Investigation
CFR	Code of Federal Regulations
FAA	Federal Aviation Administration
GAIN	Global Aviation Information Network
Hazan	Hazard analysis
Hazop	Hazard and operability studies
HEMP	Hazards and effects management process
ICAO	International Civil Aviation Organization
IDEF0	Integrated Definition Function Model
O&SHA	Operations and Support Hazard Analysis
PSA	Probabilistic Safety Assessment

## EXECUTIVE SUMMARY

Representatives of the Federal Aviation Administration (FAA) and several air carriers under Title 14 of the Code of Federal Regulations (CFR) Part 121 developed a system engineering model of the functions of air-carrier operations. Their analyses form the foundation or basic architecture upon which other task areas are based: hazard analysis, performance measure, and risk indicator design. To carry out these other tasks, models may need to be developed using the basic architecture of Air Carrier Operations System Model (ACOSM).

A literature search was conducted to identify and analyze the existing models that may be applicable for pursuing the task areas in ACOSM. The intent of the literature search was not necessarily to identify a specific model that can be directly used, but rather to identify the relevant models that have similarities with the processes and activities defined within ACOSM. Such models may provide useful inputs and insights in structuring the models for relevant task areas using ACOSM. ACOSM models processes and activities in air-carrier operations, but, in a general framework, has similarities with other industries where attention also has been paid to hazard analyses, emphasizing risk management, and designing risk indicators. To assure that efforts in other industries are adequately considered, the literature search includes publications from other industries, e.g., chemical, nuclear, and process industries.

The methods identified from the literature search are grouped for applicability in pursuing ACOSM modeling for hazard analysis, risk management, and risk-indicator design. A significant literature exists addressing these task areas in different industries. The methods identified are delineated and discussed by the subject areas. They can provide a useful basis and insights in developing models for many aspects of the ACOSM task areas.

ACOSM encompasses and integrates many activities in air-carrier operations that have unique features requiring specific modeling. Considering the broad issues that comprise ACOSM and need to be addressed, we defined the areas for model development. In this initial determination, we identified the following six areas that can be refined based on input from interested subject-matter experts:

1. Hazard identification
2. Hazard assessment techniques
3. Modeling dependencies and interrelations
4. Risk management tools
5. Data assessment techniques
6. Risk indicator identification

We present a preliminary assessment from the literature survey on how the existing methods can support each of these areas. We conclude that the existing models and insights from them will significantly aid in meeting the needs of the ACOSM modeling. The specific choice of the model will depend on the level of detail desired and the data available. The latter is relevant both in

developing the models and in validating them. The establishment of models for ACOSM task areas will greatly benefit from the modeling pursued, and the insights gained, in some areas in other industries. The unique ACOSM modeling needs can be effectively and efficiently assured using the knowledge gained from the literature survey.

# 1. INTRODUCTION

Representatives of the Federal Aviation Administration (FAA) and several air carriers under Title 14 of the Code of Federal Regulations (CFR) Part 121 developed a system-engineering model of the functions of air-carrier operations. Their analyses form the foundation or basic architecture upon which other task areas are based: hazard analyses, performance measures, and risk indicator design. To carry out these other tasks, models may need to be developed using the basic architecture of the Air Carrier Operations System Model (ACOSM). Since ACOSM encompasses various areas of air-carrier operations and can be used to address different task areas with differing but interrelated objectives, the modeling needs are broad.

A literature search was conducted to identify and analyze the existing models that may be applicable for pursuing the task areas in ACOSM. The intent of the literature search was not necessarily to identify a specific model that can be directly used, but rather to identify relevant ones that have similarities with the processes and activities defined within ACOSM. Such models may provide useful inputs and insights in structuring ACOSM models. ACOSM simulates processes and activities in air-carrier operation, but, in a general framework, it has similarities with other industries where attention also has been paid to hazard analyses, emphasizing risk management, and in designing risk indicators. To assure that efforts in other industries are adequately considered, the literature search includes publications from other industries, e.g., chemical, nuclear, and process industries.

This report discusses the literature search, the relevant methods identified and provides a preliminary assessment of their use in developing the models needed for the ACOSM task areas. A detailed assessment of the models has not been made. Defining those applicable for ACOSM will need further analyses of both the models and tools identified.

The report is organized in four chapters. Chapter 2 briefly describes ACOSM, and its structure, using the format of the Integrated Definition Function Model (IDEF0). A reader who is familiar with ACOSM may want to skip this chapter and continue with Chapter 3 that discusses the process we used for identifying applicable approaches for hazard analysis of air-carrier operations as modeled in ACOSM. It consisted of the following three main steps:

1. Search the literature containing articles related to hazard- or risk-analysis with potential applicability to air-carrier operations,
2. Review the selected publications and identify those with possible relevance to ACOSM,
3. Group the selected publications or methods according to certain characteristics, such as their pertinence to specific areas of ACOSM.

Chapter 4 discusses the applicability of the identified approaches to ACOSM, the areas of methods development, and comments related to methods development for ACOSM. The following areas were defined to identify the methods that may be applicable for ACOSM:

1. Identification of hazards associated with operations and activities
2. Hazard-assessment techniques
3. Modeling dependencies and interrelations leading to vulnerabilities
4. Risk-management tools
5. Data-assessment techniques
6. Risk-indicator identification

In addition, issues of human reliability and operational culture are relevant for all the above areas. They are expected to be addressed within each of them.

We do not include in this report all the lists of publications that we obtained because they are voluminous. We keep them in our records which are available to the interested reader.

## **2. BRIEF DESCRIPTION OF ACOSM**

The purpose of the Air Carrier Operations System Model (ACOSM) is to develop a system-engineering model of the generic functions of the activities of Title 14 CFR Part 121 air-carrier operations and the interactions among functions used to accomplish them.

ACOSM concentrates on the following key air-carrier operational processes:

- Manage air-carrier operations
- Perform air transportation
- Undertake aircraft maintenance, inspection, and engineering
- Train personnel
- Provide resources for air-carrier operations

The ACOSM version 2.0 is described in detail in [FAA, 2001]. The following description of these processes is based on this reference.

**Manage Air-carrier Operations.** This function directs, schedules, and coordinates the following work components of air-carrier operations:

- Perform air transportation
- Undertake aircraft maintenance
- Train personnel
- Provide air-carrier resources for operation

This function provides directives, defines requirements and controls, establishes performance standards for executing those activities, and also checks that they are carried out in accordance with company policies and procedures, and any required regulations. It also affords controls (on-line/off-line directives) to other process modules.

**Perform Air Transportation.** Air transportation means interstate, overseas, or foreign air transportation, or the transportation of mail by aircraft (CFR Part 1). This function carries out the task of transporting payload (passengers/cargo) from one place to another. It includes customer services/passenger services, ground operations, and aircraft operations.

**Undertake Aircraft Maintenance, Inspection and Engineering.** This function maintains and surveys aircraft to prevent deterioration of the inherent safety and reliability of the equipment to ensure the aircraft is in a safe, efficient condition for flight services. This process is usually called MIE, meaning Maintenance, Inspection, and Engineering. Here, maintenance encompasses inspecting, overhauling, repairing, preserving, and replacing parts (FAR Part 1). Inspection refers to quality assurance and quality control that continually surveys and analyzes the performance and effectiveness of the Comprehensive Maintenance Program. Engineering means providing engineering support for aircraft maintenance. After this MIE process, the aircraft will be used for flight services.

**Train Personnel.** This function plans, designs, implements, and evaluates an array of procedures, methods, and practices to improve the workforce's capabilities to meet mission/workload requirements, and to increase/maintain individual employee's knowledge, skills, and abilities.

**Provide Resources for Air-carrier Operation.** This function allocates and supplies aircraft, personnel, parts, materials, facilities, equipment, automation, information infrastructure, tools, budget, publications, and any other required resources to support the execution of air-carrier operations.

ACOSM's model structure uses the format of the Integrated Definition Function Model (IDEF0), as set out in Federal Information Processing Standards (FIPS) Publication 183. IDEF0 (pronounced eye-deaf-zero) is a modeling technique that creates a description of a business or organizational process and is used where process- or functional-models are beneficial in analyzing how the organization or system conducts its business. IDEF0 is a graphical approach using boxes and arrows to depict a process. The boxes represent activities conducted within the organization or system, and arrows represent objects or information involved in those activities.

An IDEF0 model starts by representing the whole system as a simple activity in a single diagram called the context activity. A diagram is the detailed description of a certain activity (or function) whose name (TITLE) and activity number (NODE) in the activity's hierarchy are shown at the bottom of each diagram. A diagram consists of boxes representing the activities (functions) and arrows representing the information or objects interacting with the related activities.

The context diagram, the A-0 diagram, called the "A minus 0 diagram," defines the context and boundary of the system addressed by the model. Only one box, called the context activity, on this diagram represents the function of the system; arrows entering and exiting this box indicate interactions between the system and the external environment. When the context activity is decomposed into detailed levels, those arrows will automatically link to corresponding subactivities and appear on the subdiagrams. Each of these subactivities will be further broken down into its own subactivities, using subdiagrams, to describe the process in more detail. This decomposition process continues until each activity is shown in enough detail to evaluate all its processes. These hierarchical diagrams comprise the core of the IDEF0 model. Figure 2.1 shows a typical hierarchy in a decomposition diagram.

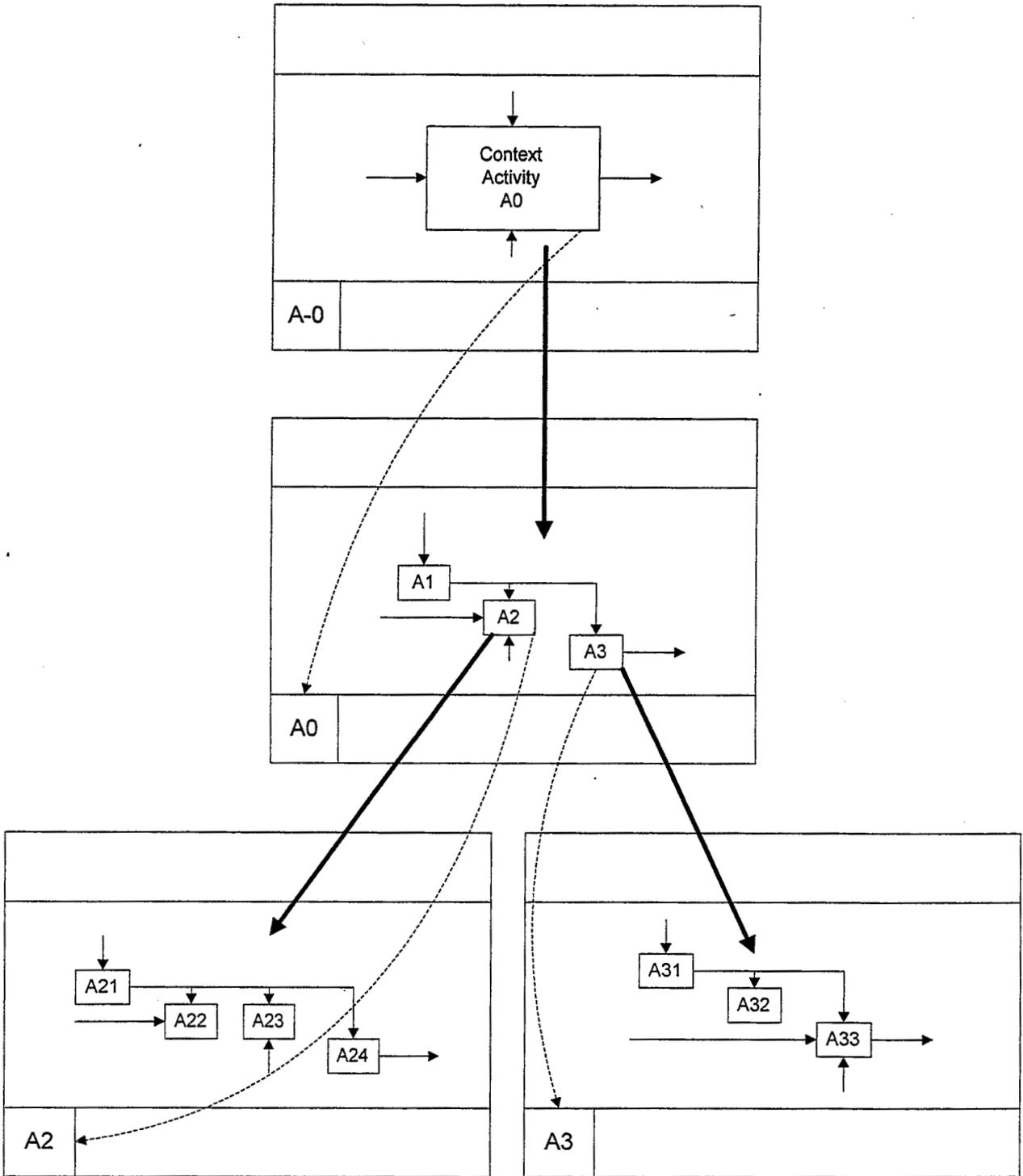


Figure 2.1 A Typical IDEF0 Diagram Hierarchy

Each ACOSM's diagram is modeled by dividing the activities into three main areas:

1. The Manage Activity on the diagram denotes the activity's management functions, including scheduling, directing, and coordinating the execution of other activities on the same diagram. It also identifies the resources required for those activities.
2. The Execute Activity on the diagram converts the input into output under the directives from the Manage Activity, and with the resources from the Provide Resources activity.
3. The Provide Resources Activity on the diagram selects, allocates, and supplies any necessary resources to support the above two. Here "resources" means the components necessary to successfully accomplish certain functions. The components are defined as properly trained and certified personnel, adequate facilities, required information, and material support.

### **3. PROCESS FOR IDENTIFYING APPLICABLE APPROACHES**

The process for identifying potentially applicable approaches for hazard analysis of air-carrier operations, as modeled in ACOSM, consisted of the following steps:

1. Search of the literature containing articles related to hazard or risk analysis with potential applicability to air-carrier operations,
2. Review of the selected publications to identify those with possible relevance to ACOSM.
3. Group the selected publications or methods according to certain characteristics, such as their pertinence to specific areas of ACOSM.

These steps are described in the following sections.

#### **3.1 Approach Used for the Literature Search**

A search of the literature was conducted for articles related to hazard or risk analysis with applicability to air-carrier operations. It encompassed hazard analyses made in industries than the aviation industry, including the chemical, petrochemical, nuclear, medical, automotive, and rail/train industries.

The intent was to make a literature search looking not only for a model that directly matches all of the ACOSM's needs, but also for approaches to specific aspects and activities that define ACOSM. Since ACOSM's needs are unique, there is unlikely to be a single satisfactory model. Accordingly, a search identifying approaches for aspects of ACOSM can be fruitful, and potentially, they can be combined to develop the hazard approaches that are unique to ACOSM's requirements.

The search covered the last ten years, from 1991 to date. Since publications on safety analysis in the aviation industry appeared mainly within the last few years, searches of earlier publications were not deemed necessary.

#### **3.2 Sources of the Literature Search**

We used three sources to find publications on methods or approaches to hazard analyses:

1. The Dialog® service, a commercial database,
2. The Science Server, a public database,
3. The analytical methods and tools compiled by Working Group B of the Global Aviation Information Network (GAIN).

These sources contain references to journal articles, conference proceedings, and technical reports. The first two were searched using their query capabilities that retrieve potentially relevant publications. Queries were prepared using logical expressions with keywords, such as

((AIRCRAFT\* OR AIRPLANE\* OR AIRLINE\* OR AVIATION\* OR AIRCARRIER\* OR AERONAUTICS\*) AND (HAZARD\* OR RISK\*))

The symbol \* means that any characters may be in this place. We describe our use of these three sources next.

The main source for the literature search was the Dialog® service of The Dialog Corporation. This company offers organizations the ability to retrieve data from more than six billion pages of key information on business, science, engineering, finance, and law. This vendor provides a common user-interface, unique features for search, retrieval and analysis, consistency of basic indexes, and a framework for quality control of file contents by individual database (file) producers. Individual databases (files) are privately developed, published, and updated by the individual producers.

We considered the following databases (files) for our multidisciplinary search:

1. Aerospace database
2. Chemical Safety Newsbase
3. EI Compendex
4. Energy Science and Technology
5. Janes Defense & Aerospace News / Analysis
6. NTIS – National Technical Information Service
7. PASCAL – French Scientific and Technical Information
8. Transportation Research Information Services (TRIS)

The Science Server is provided by the Research Library of Los Alamos National Laboratory.

We also explored the applicability of the analytical methods and tools compiled by the GAIN's Working Group B to hazard analysis of air-carrier operations. GAIN promotes and facilitates the voluntary collection by, and sharing of, safety information among users in the international aviation community to improve aviation safety.

The search in the eight databases selected from the Dialog® service yielded the titles of 769 publications. The search in the Science Server obtained 2,215 documents and we retrieved the top rated 750. We scanned all analytical methods and tools compiled by the GAIN's Working Group B and identified five books on safety and risk analysis. Overall, our search yielded 1,519 documents and five books. The publications retrieved by the Dialog® service and the Science Server contained duplicates because of some overlap in the original sources.

We did not include in this report all the lists of publications that we obtained because they are voluminous. We keep them in our records where they are available to the interested reader.

### **3.3 Review of Publications to Identify Potentially Applicable Methods or Approaches**

The literature search just described yielded lists with titles of 1,519 documents plus five books. Since most of these documents were identified using computerized queries of databases, there were many that contained the keywords used but were not relevant to our purpose; that is, hazard analysis of ACOSM. Therefore, we carefully looked at each title to assess its potential applicability to our goal.

By these means, we identified about forty apposite publications. We then obtained full copies of the selected ones.

These publications were reviewed in detail to identify approaches with unique capabilities that match the needs of ACOSM or specific aspects or activities within it. In making this review, we obtained references from them to other publications which appeared relevant, and, whenever possible, we obtained copies of these publications. All publications reviewed are listed in the Bibliography.

### **3.4 Grouping of the Selected Publications or Methods**

We classified the promising techniques and approaches into seven general groups:

1. Aviation safety programs
2. Methods addressing hazards in managerial operations
3. Techniques for evaluating human error
4. Techniques for identifying and assessing hazards in hardware-oriented operations
5. Techniques for identifying and assessing hazards during maintenance and inspection
6. Software safety analysis
7. Other relevant studies or approaches.

These are rough classifications, and some methods or publications address several of the groups. Each group is described in the following subsections.

#### **3.4.1 Aviation-Safety Programs**

To identify and assess the hazards in aviation operations, some companies have implemented a company- or industry-wide safety program. Quoting C.J. Edwards [2000]:

...The commitment and organization that assures continuing safe operations is achieved through the introduction of a safety management system. A safety management system must be led by top management and must address all aspects of the business that have the potential to cause harm...

Different authors and organizations give different names to this safety program. Here, we use the term proposed by Wood [1997], Aviation Safety Program (ASP). Wood's book gives background information on aviation safety, discusses how to build an ASP, and presents a sample ASP. We

identified two instances of an ASP: one implemented by Shell Aircraft and other operators in the United Kingdom and another developed by the Australian Transport Safety Bureau; each is briefly discussed.

Shell Aircraft and other operators in the United Kingdom propose a safety management system. Edwards [2000] describes this program as follows:

...A company's safety management system is defined as a systematic and explicit approach to managing risk...The structured approach taken to identify, assess and control the hazards is known as hazard management, a process that results in the development of a hazard register. Throughout 1999, Shell Aircraft worked with a number of airlines and other operators to build a generic hazard register (Figure 1)<sup>1</sup> that can be tailored to any operator, enabling resources to be focused on the areas of greatest risk. An efficient way to manage this process is the safety case...A safety case is the “systematic and structured demonstration by a company to provide assurance, through comprehensive evidence and argument, that the aircraft operator has an adequately safe operation.” The company identifies and assesses major hazards and safety risks and then manages them to levels or risk which are as low as reasonably practicable. A safety case may cover all or part of an operation and, where more than one case is developed, each is described and controlled locally but managed through a corporate safety management system. Delineating cases is a management choice, but the resulting package of safety cases should cover all safety-critical activities. Safety cases may be set up for operations, for engineering, or both, or even used for specific projects such as the introduction of a new aircraft type.

...Central to a safety case is the identification and management of hazards. Clearly, without a robust list of hazards, a company cannot assure itself that it has established effective controls. Hazards, once identified, are assessed by utilizing a safety assessment matrix to determine their level of risk...

...Identification of hazards started with the definition of each hazard and what analysis tools would be used to define them. In the safety case described here, standard tools and definitions that had been used successfully elsewhere were employed. The primary tools were the “bow-tie” analysis model and a risk matrix. The bow-tie has proactive and reactive elements (Figure 3 (in Edwards’ paper, not included here)) that systematically work through a hazard and its management, using a methodology that Shell Aircraft calls the hazards and effects management process (HEMP). This requires that the hazards be identified, assessed and controlled - and also sets out recovery measures.

Edkins [1998] presents a “proactive airline safety program called INDICATE (Identifying Needed Defences In the Civil Aviation Transport Environment) that has been applied within the Australian regional airline industry.” This program, developed by the Australian Transport Safety Bureau and Bureau of Air Safety Investigation (BASI), includes

---

<sup>1</sup>The text refers to Figure 1 in Edwards’ paper, not included here.

... implementing and maintaining six core safety activities:

1. appointing an operational safety manager or officer who is available to staff as a confidante for safety related issues,
2. conducting a regular series of staff focus groups to identify safety hazards within the organisation,
3. establishing a confidential safety hazard reporting system,
4. conducting regular safety meetings with management,
5. maintaining a safety information database, and
6. ensuring that safety information is regularly distributed to all staff.

...To evaluate the INDICATE program, a major Australian regional airline agreed to implement the program in one of its operational bases while another base was used as a control group...Results from the trial suggest that the program can have a positive influence on airline safety performance...The success of the trial has resulted in a number of Australian and international airlines adopting the program.

Edkins [1998] also indicates that “...There is a great deal of published material on the subject of safety management. Most of this material identifies the essential elements that make up a typical safety program. However, few authors provide a simple methodology to implement these essential elements and evaluate whether they are working...,” and identifies two “useful sources: the British Airways Managing Engineering Safety Health (MESH) program (Reason, 1994) and the Boeing Safety Program Model.” Edkins also reports that the International Civil Aviation Organization has an Accident/Incident Reporting System that was used to compile a list of the commonest aviation safety hazards in commuter/regional aircraft operations, based on accident data between 1990 and 1996.

Another relevant publication for an ASP is Mil-Std-882. As Bahr [1997] points out,

...(it) is the most famous system safety document in existence. Because accidental release of a nuclear warhead could have devastating consequences, it became imperative for the aerospace and military industries to develop and implement a comprehensive safety program. Identification of hazards early on in the program life cycle was paramount, because of the high costs of retrofitting mature systems...

This Department of Defense’s standard was revised over the years, and its current version is Mil-Std-882D, dated February 2000. It states, in part,

...This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities.

Mil-Std-882D has a section on identifying hazards that reads

Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended use or application. Consider and use historical hazard and mishap data, including lessons learned from other systems. Identification of hazards is a responsibility of all program members. During hazard identification, consider hazards that could occur over the system life cycle.

Both Edwards [2000] and Edkins [1998] report that the ASPs were successfully applied to actual situations identifying or assessing hazards. We recommend a more detailed study of the technical methods used by these ASPs to assess their applicability to ACOSM.

### **3.4.2 Methods Addressing Hazards in Management of Operations**

The top or A-0 diagram in ACOSM is a managerial operation: Manage air-carrier operations. In addition, each ACOSM's diagram contains the area called "Manage Activity." For this reason, we grouped methods that address these operations.

Wojcik [1989] discusses the importance of managerial and organizational factors in his article entitled "Probabilistic Risk Assessment and Aviation System Safety":

...Probabilistic risk assessment is a promising avenue to aviation system safety indicators, if not used too rigidly, because good risk assessment constantly prompts questions about what factors or events could come together in one place to cause an accident...Risk assessment must acknowledge both human performance limitations and human resourcefulness; perhaps the best way is through management and organizational factors that influence behavior. A comprehensive aviation risk assessment capability, incorporating operational, management and organizational factors, is clearly a long-term goal, but efforts to achieve it could help increase awareness of incipient safety problems...

Three approaches addressing organizational or managerial errors were identified:

1. Reason [1995] developed a model of "organizational accident causation." Edkins [1998] reports as follows:

...Reason [1995] contends that modern aircraft accidents are generally the result of *latent failures*, arising from the broad management functions of an organization. Latent failures are decisions or actions originating within management, that have damaging consequences but may lie dormant for a period of time...Accidents originate from latent failures, arising from managerial decisions and organizational processes. These latent failures combine with local workplace factors, and errors or violations usually committed by operational personnel. If system defenses are breached, the result may be an accident...

2. Saaty [1980] proposed the Analytic Hierarchy Process (AHP) for “modeling unstructured problems in the economic, social, and management sciences.” He indicates

(If our) models do not work well because we have left out significant factors by making simplifying assumptions, at least in the social sciences, we blame the result on politics and on capricious human behavior and other factors regarded as annoying aberrations of human nature which will disappear in time. But these are precisely the controlling factors that we must deal with and measure in order to get realistic answers. We must stop making simplifying assumptions to suit our quantitative models and deal with complex situations as they are. To be realistic our models must *include* and *measure* all important tangible and intangible, quantitatively measurable, and qualitative factors. This is precisely what we do with the analytic hierarchy process (AHP). We also allow for differences in opinion and for conflicts as the case is in the real world...

AHP’s approach appears to be well suited for ACOSM because both of them use hierarchies to analyze a system.

3. The technique Management Oversight and Risk Tree (MORT) addresses the relationship between management and hazard analysis. This technique is discussed in several publications; Bahr [1997] reports

Its purpose is to analyze a system methodically and identify the interrelationships among the plant operations and management organizations. A predefined graphical tree, much like a fault tree (with similar symbols) analyzes management policy in relation to risk assessment and the hazard analysis process.

An engineer works through the predefined tree comparing his management and operations structure to the ideal system safety tree structure. Like the fault tree, the engineer works from the top event down to determine what oversights and omissions were in place that caused the accident or created an unsafe situation. The tree also forces the analyst to look at the risk assumed by the management organization and whether it makes sense or not.

Bahr [1997] also points out some of the disadvantages of MORT:

...MORT is a strictly qualitative safety tool that has fallen into disuse...(it) is highly labor-intensive, though very easy to learn. It takes about a day to learn how to “read” the tree. Its major drawback is that the tree is so large and unwieldy (it has 98 generic problems and over 1,500 basic events) that it is very easy to get lost in the process. Another significant problem is that it assumes that there is an *ideal* safety system. Also, it does not lend itself very well to *tailoring* the tree to a smaller problem.

### 3.4.3 Techniques for Evaluating Human Error

If the operations analyzed include manual actions by operators, such as a pilot or a maintenance technician, then methods for evaluating human reliability are appropriate. Bahr [1997] points out that

...Billings and Reynard [1981] say that 70 to 90 percent of system failures are due to human error. To try to mitigate this, engineers have used a potpourri of human factors controls. There really is no such thing as one human factor analysis technique -there are many. A handful of the more interesting (though not necessarily the most important) names are confusion matrix, expert estimation, THERP, HEART, SLIM-MAUD, human cognitive reliability model, operator action tree, and sociotechnical assessment of human reliability. This section<sup>2</sup>, however, will focus on more mundane definitions and techniques for figuring out how to deal with those pesky humans...

Bahr [1997] presents two techniques for evaluating human reliability:

1. Human Reliability Analysis.

...Much research has been conducted in the fields of human factors and human reliability. As a result of the Three Mile Island nuclear near-miss accident in the United States in the late 1970s, the U.S. Nuclear Regulatory Commission developed a standard for conducting human reliability analysis for commercial nuclear power plant operators. These quantitative human reliability analyses are plugged into the nuclear plant probabilistic risk analysis. The *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*<sup>3</sup>, NUREG/CR-1278 (Swain and Guttman, 1983), is an excellent source of information that the engineer is strongly urged to read. The document presents a methodology for identifying human errors and even predicting quantitative human error rates. The International Electrotechnical Commission (a sister organization of the International Standards Organization) has convened a working group that is currently writing an international standard on human reliability...

2. Operations and Support Hazard Analysis (O&SHA).

Most hazard analysis (and safety analyses, in general) are directed toward uncovering hardware design problems; however, this is not the intent of an O&SHA. Simply put, an O&SHA *identifies and evaluates the hazards associated with the operations of a system*. As with all hazard analyses, it looks at hardware systems, software, facilities, support equipment, procedures, personnel, operating environment, human-machine interfaces, and other interfaces, but with the telling difference of how all of these factors relate to the operation of the system by people...It is very good at evaluating safety of procedures and checking maintenance activities; it identifies training requirements.

Note that the O&SHA addresses only human errors or operator errors -not hardware failures. This is its strength and its weakness. Because this hazard analysis technique focuses on the operations of a system, it is very good at identifying the kinds of operational hazards that are often obscure to the engineer... (Since O&SHA does not address hardware failures,) the O&SHA should never be used alone, but only in tandem with a hardware hazard analysis...

---

<sup>2</sup>The text refers to a section in Bahr's book.

<sup>3</sup>This handbook presents the methodology known as THERP (Technique for Human Error Rate Prediction).

### **3.4.4 Techniques for Identifying and Assessing Hazards in Hardware-Oriented Operations**

The process industries, such as chemical and oil, and others have developed many technical methods to identify and assess hazards. Most methods are applicable to “hardware” operations--that is, they are related to random failures of equipment comprising a system(s). The System Safety Society [1997] compiled 101 technical methods, including methods to assess human errors. Lees [1996] also gives a list, but the methods in it are more directed to the process industries. Kletz [1999] describes in detail Hazop (hazard and operability) studies that identify hazards, and Hazan (hazard analysis) that assesses and quantifies hazards. However, his book is directed to the chemical industries.

### **3.4.5 Techniques for Identifying and Assessing Hazards During Maintenance and Inspection**

One of the five key air-carrier operation processes of ACOSM is “Perform aircraft maintenance, inspection and engineering.” We identified three approaches that address part of this process.

#### **1. Ostrom and Wilhelmsen [1999] point out that**

One of the causes of aviation accidents is lack of proper maintenance and, subsequent, lack of proper inspection for any anomalies. It has been known for a long time that proper inspection is an important part of the maintenance process... (Their paper presents) the important issues in the inspection process itself, as well as discuss problems with how inspection is modeled using current human reliability analysis (HRA) models.

#### **2. Roland and Moriarty [1990] propose an analysis technique called Maintenance Hazard Analysis (MHA):**

Examination is made of all the product/system operations and the use of personnel interfacing to do maintenance activities. The purpose of the MHA is to identify hazards to personnel and equipment that may be encountered or could result in improper maintenance so that appropriate action can be taken for their elimination and control. MHA is originated prior to the first design review and is maintained current with system modification or redesign. The final analysis normally is completed prior to the start of system qualification testing. Subsequent changes to the design should have further MHA work performed to ensure that hazards in the maintenance activity are known and controlled.

#### **3. As mentioned above, the Operations and Support Hazard Analysis (O&SHA) “...is very good at evaluating safety of procedures and checking maintenance activities; it identifies training requirements...”**

### **3.4.6 Software-Safety Analysis**

Bahr [1997] discusses the impact of software failures by stating, in part,

...The safety management program<sup>4</sup> presented in Chapter 4<sup>5</sup> discusses the need to include all aspects of system operations in the safety process. Software use and control is no exception. A software safety program should be an integral part of the system safety program. In fact, it would be dangerous to segregate software safety from the rest of the safety process...

Pressman [2001] indicates that

*Software safety ... focuses on the identification and assessment of potential hazards that may affect software negatively and cause an entire system to fail...*

The severe impact that a software failure can have is illustrated by the crash of the rocket Ariane 5, as Gleick [1996] comments:

It took the European Space Agency 10 years and \$7 billion to produce Ariane 5, a giant rocket capable of hurling a pair of three-ton satellites into orbit with each launch...All it took to explode that rocket less than a minute into its maiden voyage last June, scattering fiery rubble across the mangrove swamps of French Guiana, was a small computer program trying to stuff a 64-bit number into a 16-bit space...One bug, one crash...

Leveson's [1995] book on software safety is a good reference on the subject.

### **3.4.7 Other Relevant Studies or Approaches**

We identified the following studies that may be useful to the hazard analysis of air-carrier operations but are less directly related to it:

1. The INDICATE safety program described by Edkins [1998] uses the Delphi technique (described by Delbecq et al. [1975]) to identify airline safety hazards. According to Edkins, this technique "...is designed to maximize the use of idiosyncratic information in the interests of consensual decision making."
2. Hazards in flight operations. Hadjimichael and Osborne [1999] report that

The Flight Operations Risk Assessment System (FORAS) is envisioned as a risk management tool that will enable operators at the safety, flight operations, and dispatch level to monitor and reduce the risks associated with individual flights, as well as the entire flight operation. FORAS will focus on flight operation processes and the initial work will provide a quantitative assessment of risk of controlled flight into terrain and risk of turbulence-related injury. The risk model is based on a large set of possible risk factors roughly classified under the categories of environment (including weather), operator, service provider, flight path, aircraft, cabin, and air handling." While the main thrust FORAS is to

---

<sup>4</sup>In our terms, the safety-management program is an Aviation Safety Program (ASP).

<sup>5</sup>The text refers to a chapter in Bahr's book.

develop a tool that carries our quantitative estimations of risk, this project may provide useful insights into the hazards associated with flight operations.

These hazards are related to the ACOSM's key air-carrier operation process named "Perform air transportation."

3. Captains Mimpriss and Savage [2000] of British Airways describe a technique called "Dependency Modeling" that was implemented into a tool called Risk Assessment Tool British Airways Group (RATBAG). From their paper, we understand that this technique is very similar to fault-tree analysis because both model logical relationships between events. The former technique models successes, and the latter models failures.
4. Probabilistic Safety Assessment (PSA), sometimes called Probabilistic Risk Assessment, is a comprehensive approach to assess and manage the impact of hazards. PSA encompasses many methods for hazard and safety assessment, such as Fault-Tree Analysis, Event-Tree Analysis, Common-Cause Analysis, Human Reliability Analysis, and Failure Modes and Effects Analysis. PSA uses a logic diagram, known as a Master Logic Diagram, to identify hazards. It basically is a logic tree built from the top-down. Martinez-Guridi et al. [2001, 1998] describe the application of PSA to aircraft safety.

## **4. DISCUSSION OF APPROACHES AND APPLICABILITY TO ACOSM**

### **4.1 Applicability of Approaches to ACOSM**

ACOSM is modeled using IDEF0, as described in Chapter 2 and depicted in Figure 2.1. Using the IDEF0 technique, the five key air-carrier operation processes are decomposed into successively refined levels of detail. In general, organizations define operations that are carried out by people supported by hardware and software equipment. We can use this breakdown of ACOSM into several levels of detail to propose approaches to hazard analysis.

Edwards [2000] and Edkins [1998] report that the aviation safety programs (ASPs) implemented by several airline operators were successfully applied to actual situations identifying or assessing hazards. A more detailed study of the technical methods used by these ASPs to assess their applicability to ACOSM is useful.

Significant literature exists on what is termed “hazard-analysis techniques.” By this term, we mean the techniques that several industries have developed for identifying and assessing hazards. Since the ACOSM is broken down into suboperations, the diagrams at the bottom of ACOSM model the most elementary ones. These usually will be well-defined activities, to which hazard-analysis techniques can be applied. In this way, hazards for the diagrams at the bottom of ACOSM can be identified and assessed. Since these diagrams are a breakdown of those immediately above them, then the hazards identified for the diagrams at the bottom (for example, diagrams A31, A32, and A33, not shown in Figure 2.1) will be applicable to the diagram immediately above them (diagram A3). The same process then is repeated for the diagrams that are above the bottom ones (diagrams A2 and A3 in the figure). In turn, hazard-analysis techniques are applied to the diagrams at this level to identify and assess hazards, and these new ones are added to the ones already identified for the bottom diagrams. This process continues until the top diagram is reached--that is, the A-0 diagram.

We can consider a combination of Operations and Support Hazard Analysis (O&SHA), which addresses only human errors but not hardware failures, and other hazard techniques that usually are applicable to hardware-oriented processes. Many hazard techniques were developed to address hardware failures; see Section 3.4.4, “Techniques for Identifying and Assessing Hazards in Hardware-Oriented Operations.” Examples are Hazard and Operability (Hazop) studies and Hazard Analysis (Hazan).

If the operations analyzed include manual actions by operators, such as a pilot or a maintenance technician, then methods for the evaluating human reliability are applicable, such as THERP; see Section 3.4.3, “Techniques for Evaluating Human Error.” Similarly, if the equipment or hardware analyzed includes software, then using a software safety-analysis is advisable; see Section 3.4.6, “Software-Safety Analysis.”

One of the five key air-carrier operation processes of ACOSM is “Perform aircraft maintenance, inspection and engineering.” The methods proposed by Ostrom and Wilhelmsen [1999], Roland and Moriarty [1990], and O&SHA are applicable to analyzing hazards in maintenance and inspection.

The top or A-0 diagram in ACOSM is “Manage air carrier operations.” Some of the methods identified can start by focusing at this level and then expanding to lower levels. A hazard analysis is conducted for the top or A-0 diagram in ACOSM and then for the diagram(s) immediately below and so on.

Using a top-down process can address management operations and dependencies between diagrams. The methods defined in (1) the Reason model, (2) the Analytic Hierarchy Process (AHP) and (3) the technique Management Oversight and Risk Tree (MORT) can be useful for such an approach.

The Analytic Hierarchy Process (AHP) proposed by Saaty [1980] uses a hierarchical structure to model a system and has been used in many applications. Saaty defines a hierarchy as

...an abstraction of the structure of a system to study the functional interactions of its components and their impacts on the entire system. This abstraction can take several related forms, all of which essentially descend from an apex (an overall objective), down to sub-objectives, down further to forces which affect these sub-objectives, down to the people who influence these forces, down to the objectives of the people and then to their policies, still further down to the strategies, and, finally, the outcomes which result from these strategies...

Both ACOSM, modeled using IDEF0, and Saaty’s hierarchy use a decomposition process. The top or A-0 diagram in ACOSM is similar to the apex described by Saaty. Thus, it may be convenient to use AHP to model relationships of hazards in ACOSM. Other considerations relating to development of inputs for using AHP will apply.

## **4.2 Applicable Methods for ACOSM from the Literature Search**

In conducting the literature search, we focused on identifying methods that can help conduct hazard analysis, define tools for risk management, and provide input for developing risk indicators. To identify methods applicable for ACOSM, we delineated the areas of method development appropriate for addressing these needs stated above. Following our identification of the areas or types of methods required, we searched for methods in the literature that may be applicable. At this stage, we reviewed them in detail and explored their specific applicability in defining the ACOSM needs. We provide our preliminary assessment by defining the suitability of the methods and by commenting on the ways that they can support the establishment of methods for ACOSM.

Table 4.1 presents the areas of methods development, the identified methods, their applicability, and our comments related to the establishment of methods for ACOSM. The table is intended to set out how the methods for ACOSM will be defined, but it also provides ideas for methods development relating to different areas of methods that can be pursued within ACOSM. Methods development may not necessarily need to address all the areas delineated here. For example, Risk Indicator identification may not necessarily entail modeling all the other areas. At the same time, developing

models in other areas may facilitate identifying specific risk indicators of interest. Also, data assessment techniques may be a supporting method for many of the defined areas.

The areas defined to identify the methods that may be applicable for ACOSM are as follows:

1. Identification of hazards associated with operations and activities
2. Hazard-assessment techniques
3. Modeling dependencies and interrelations leading to vulnerabilities
4. Risk-management tools
5. Data-assessment techniques
6. Risk-indicator identification

In addition, issues of human reliability and operational culture are relevant for all these areas and are expected to be addressed within each of them. Methods for these aspects were discussed in the previous chapter. Specific methods unique to the needs of a specific activity or issue also may apply. For example, modeling maintenance errors and software failures has been the focus of some models addressing the unique characteristics of the activities and the relevant hardware.

Table 4.1 Applicable Methods for ACOSM Relating Different Areas of Methods Development

Areas for Methods Development	Identified Methods	Applicability of Methods Identified	Comments
Identification of hazards associated with operations and activities	<ul style="list-style-type: none"> <li>• Operations and Support Hazard Analysis</li> <li>• Hazop</li> <li>• Hazard Identification in Hazards and Effects Management Process (HEMP)</li> <li>• Logic diagrams to identify hazard initiators</li> </ul>	The methods identified include those used in the aviation and chemical industries. They depend on incident data, focus group discussions, study of processes using guide-words, what-if type analysis.	HEMP used in improving an aviation safety program can be the basis for hazard identification complemented by HAZOP and what-if type analyses.
Hazard-assessment techniques	<ul style="list-style-type: none"> <li>• Analytical hierarchy process (AHP)</li> <li>• Safety-assessment matrix; Bow-tie analysis in HEMP</li> <li>• Frequency-severity table</li> <li>• Quantitative probabilistic assessment using fault/event tree type analyses</li> <li>• Hazan</li> </ul>	Different hazard assessment techniques require different types of data. Hazard assessment of ACOSM is expected to depend on qualitative data requiring focus on methods able to extract the needed input from any available qualitative data.	Different assessment techniques may be used. Available methods are expected to provide the basis for ACOSM hazard assessment.
Modeling dependencies and interrelations leading to vulnerabilities	<ul style="list-style-type: none"> <li>• Dependency-modeling</li> <li>• Failure-modes and Effects Analysis</li> <li>• Common-cause Analysis</li> </ul>	Methods available have some similarities. Common-cause failure analysis, typically used for hardware and human actions relating to hardware, may not be directly applicable but provides the basis for extension to applications in ACOSM.	Existing methods can be adapted for ACOSM.

Areas for Methods Development	Identified Methods	Applicability of Methods Identified	Comments
Risk-management tools	<ul style="list-style-type: none"> <li>• Management Oversight and Risk Tree (MORT)</li> <li>• Probabilistic Safety Assessment (PSA) Tools</li> <li>• Identifying Needed Defenses In the Civil Aviation Transport Environment (INDICATE) program</li> <li>• Flight Operations Risk Assessment System (FORAS)</li> </ul>	The available tools are based on different approaches used for risk assessment and management.	ACOSM has unique features and broad application in studying options for risk management. A tool for risk management of ACOSM may need to be developed using many features and insights from the existing ones.
Data-assessment techniques	<ul style="list-style-type: none"> <li>• Statistical methods</li> <li>• Reliability models</li> <li>• Delphi techniques</li> </ul>	Statistical and reliability models are available for estimating parameters and determining risk-factor weights and factor dependencies. These parameters and weights will apply for the methods chosen.	Search and analysis of air-carrier operational data will be needed to develop the raw data in determining the input data.
Risk-indicator identification	<ul style="list-style-type: none"> <li>• Risk assessment - derived indicators</li> <li>• Indicators derived from key elements of safe airline operations</li> </ul>	Available literature on defining risk indicators is limited. There is relatively little experience on validating the indicators used.	ACOSM-specific risk indicators may need to be developed. Prior experience and the literature may provide some guidance.

## 5. BIBLIOGRAPHY

1. Khan, F.I., and Abbasi, S.A., "Risk Analysis of a Typical Chemical Industry Using ORA Procedures," *J. of Loss Prevention in the Process Industries*, Volume 14, pp. 43-59, 2001.
2. American Nuclear Society and the Institute for Electrical and Electronics Engineers, "Probabilistic Risk Assessment (PRA) Procedures Guide," NUREG/CR-2300, January 1983.
3. Arendt, J.S., "Management of Quantitative Risk Assessment in the Chemical Process Industry," *Plant/Operations Progress*, Volume 9, No. 4, pp. 262-268, October 1990.
4. Bahr, N.J., "System Safety Engineering and Risk Assessment: A Practical Approach," Taylor & Francis, Bristol, PA, 1997.
5. Billings, C.E., and Reynard, W.D., "Dimensions of the Information Transfer Problem," in C.E. Billings and E.S. Cheney (eds.), *Information Transfer Problems in the Aviation System*. NASA-TP-1875. Moffett Field, CA: NASA Ames Research Center, 1981.
6. Busch, A.C., Colamosca, B., Hunter, J.S., and Polhemus, N.W., "Assessing the Safety and Risk of Air Traffic Control Systems: Risk Estimation from Rare Events," *Transportation Research Record* 768, 1980.
7. Camatti, D., Chiesa, S., and Maggiore, P., "Risk Analysis: Sample Application to a Totally New Aircraft Design," *Aircraft Design*, Volume 1, pp. 1-11, 1998.
8. Delbecq, A.L., Van de Ven, A.H., and Gustafson, D.H., "Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes," Scott-Foresman, Glenview, IL, 1975.
9. Department of Defense, "Standard Practice for System Safety," Mil-Std-882D, February 2000.
10. Donoghue, A.M., "The Design of Hazard Risk Assessment Matrices for Ranking Occupational Health Risks and Their Application in Mining and Minerals Processing," *Occup. Med.*, Volume 51, No. 2, pp. 118-123, 2001.
11. Edkins, G.D., "The INDICATE Safety Program: Evaluation of a Method to Proactively Improve Airline Safety Performance," *Safety Science*, Volume 30, Issue 3, pp. 275-295, December 1998.
12. Edwards, C. J., "Aircraft Operators Have Built a Generic Hazard Model for Use in Developing Safety Cases," *ICAO Journal*, pp. 12-14 and 27, January/February 2000.

13. Einarsson, S., "Comparison of QRA and Vulnerability Analysis: Does Analysis Lead to More Robust and Resilient Systems?" ACTA Polytechnica Scandinavica, Civil Engineering and Building Construction, Series No. 114, ESPOO, 1999.
14. Federal Aviation Administration, "Air Carrier Operations System Model," Version 2.0, April 3, 2001.
15. Fleming, K.N., Mosleh, A., and Kelley, J.C., A.P., "On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation," Nuclear Safety, Volume 24, No. 5, pp. 637-657, 1983.
16. Ganger, J.J. and Bearrow, M.E., "How to Prioritize Process Hazard Analyses," Hydrocarbon Processing, Volume 72(10), pp. 95-98, October 1993.
17. Garrick G. and Kaplan, S., "On the Quantitative Definition of Risk," Risk Analysis, Volume 1, pp. 11-27, 1981.
18. Gleick, J., "A Bug and a Crash - Sometimes a Bug Is More Than a Nuisance," New York Times, December 1, 1996.
19. Hadjimichael, M. and Osborne, D.M., "The Flight Operations Risk Assessment System," Proceedings of the Advances in Aviation Safety Conference, pp. 37-43, 1999.
20. International Atomic Energy Agency, "Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 1)," Safety Series No. 50-P-4, Vienna, 1992.
21. International Atomic Energy Agency, "The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety," Safety Series No. 106, Vienna, 1992.
22. International Atomic Energy Agency, "Modeling and Data Prerequisites for Specific Applications of PSA in the Management of Nuclear Plant Safety," 1994.
23. International Civil Aviation Organization, "Accident/Incident Reporting Manual (ADREP)," ICAO, Montreal, Canada, 1987.
24. Kaplan, S., "Matrix Theory Formalism for Event Tree Analysis," Risk Analysis, Volume 2, pp. 9-18, 1982.
25. Khan, F.I. and Abbasi, S.A., "Techniques and Methodologies for Risk Analysis in Chemical Process Industries," Journal of Loss Prevention in the Process Industries, Volume 11, pp. 261-277, 1998.

26. Kimura, C.Y., Sandquist, G.M., Slaughter, D.M. and Sanzo, D.L., "Risk Assessment of High Altitude Free Flight Commercial Aircraft Operations," Lawrence Livermore National Laboratory, UCRL-JC-130435, April 23, 1998.
27. Kletz, T., "Hazop and Hazan - Identifying and Assessing Process Industry Hazards," Fourth edition, Institution of Chemical Engineers, printed in the United Kingdom by Galliards, Great Yarmouth, 1999.
28. Lees, F.P., "Loss Prevention in the Process Industries - Hazard Identification, Assessment and Control," Butterworth-Heinemann, Second edition, Woburn, MA, 1996.
29. Leveson, N.G., "Safeware: System Safety and Computers," Addison-Wesley, Reading, MA, 1995.
30. Madjar, M. and Rohr, R.V., "A Graphical Risk Analysis Method for Multi-Purpose and Multi-Product Plants," Institute of Chemical Engineering, Volume 74, Part B, August 1996.
31. Mansdorf, Z., "Analyzing Process Hazards," Occupational Hazards, Volume 56(9), pp. 11-13, September 1994.
32. Martinez-Guridi, G., Hall, R.E., Fullwood, R.R., "An Application of Probabilistic Safety Assessment Methods to Model Aircraft Systems and Accidents," Proceedings of the 16<sup>th</sup> International System Safety Conference, Seattle, Washington, pp. 352-361, 1998.
33. Martinez-Guridi, G., Samanta, P., Azarm, M.A., "Probabilistic Safety Assessment in Analyzing Aircraft Safety: A Framework for Understanding System Interactions, Operations Events, and Accident Vulnerabilities," Brookhaven National Laboratory, Draft Technical Report, August 2001.
34. McKay, G., "Designing a Process Hazards Analysis Methodology for a 'Non-Traditional' Chemical Facility," Loss Prevention Bulletin, Volume 147, pp. 22-26, 1999.
35. Melville, G.S., "When QRA is Not Quite the Right Approach," Journal of Loss Prevention in the Process Industries, Volume 7, No. 5, 1994.
36. Mimpriss, J., and Savage, J., "Risk Assessment-Hazard Management Using Dependency Modeling," FSF & ERA, 12th EASS, "Safety: Beginning at the Top," Amsterdam, Netherlands, pp. 29-46, March 2000.
37. Morgenstern, R.D., Shih, J.-S., and Sessions, S.L., "Comparative Risk Assessment: An International Comparison of Methodologies and Results," Journal of Hazardous Materials, Volume 78, pp. 19-39, 2000.

38. Odisharia, G.E., Safonov, V.S., and Yedigarov, A.S., "Risk Methodology in Safety Analysis of Typical Gas Industry Facilities," Proceedings of the International Gas Research Conference, D.A. Dolenc (editor), Gas Research Institute, Chicago, IL, pp. 564-572, November 1995.
39. Ostrom, L.T. and Wilhelmsen, C.A., "Task and Risk Analysis of Aviation Maintenance and Inspection Processes," Idaho National Engineering Laboratory, P.O. Box 1625, Idaho Falls, ID 83415-3855, 1999.
40. Potter, J.L. and Losee L.A., "Choosing Appropriate Hazards Analysis Techniques for Your Process," CPIA Publ., CPPUDT 674, Volume 1, January 1998.
41. Pressman, R.S., "Software Engineering, A Practitioner's Approach," Fifth edition, McGraw-Hill, New York, NY, 2001.
42. Reason, J., "A Systems Approach to Organizational Error," Ergonomics, Volume 38, No. 8, pp. 1708-1721, 1995.
43. Rohacs, J., "Parameter Anomalies in Aircraft Systems, Flight Safety Investigation," 5<sup>th</sup> Mini Conference on Vehicle System Dynamics, Identification and Anomalies, Budapest, pp. 61-69, November 1996.
44. Roland, H.E. and Moriarty, B., "System Safety Engineering and Management," Second edition, John Wiley, New York, NY, 1990.
45. Saaty, T.L., "The Analytic Hierarchy Process," McGraw-Hill, New York, NY, 1980.
46. Sandquist, G.M. and Slaughter, D.M., "Risk Assessment for Aircraft Flight Operations at Salt Lake International Airport," PVP-Volume 320/SERA-Volume 5, Risk and Safety Assessments: Building Viable Solutions, ASME, pp. 313-319, 1995.
47. Smalko, Z., Jazwinski, J., and Zurek, J., "Application of Expert Methods to Risk Assessment of Air Transport Systems," 21<sup>st</sup> ICAS Congress, Australia, September 1998.
48. Smith, A., Cassell, R., Yang, Y.E., Sleep, B., and Cohen, B., "Feasibility Demonstration of an Aircraft Performance Risk Assessment Model," 19<sup>th</sup> Digital Avionics Systems Conference, pp. 4.D.4-1 to 4.D.4-8, 2000.
49. Society of Automotive Engineers' (SAE) Aerospace Recommended Practice (ARP) 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," December 1996.

50. Srinivasan, R. and Venkatasubramanian, V., "Multi-Perspective Models for Process Hazards Analysis of Large Scale Chemical Processes," *Computers Chem. Engineering*, Volume 22, pp. 5961-5964, 1998.
51. Swain, A.D., Guttmann, H.E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278-F, 1983.
52. System Safety Society, "System Safety Analysis Handbook," Second edition, July 1997.
53. United States Department of Energy, "Chemical Process Hazards Analysis - DOE Handbook," DOE-HDBK-1100-96, February 1996.
54. United States Nuclear Regulatory Commission, "A Review of NRC Staff Uses of Probabilistic Risk Assessment," NUREG-1489, March 1994.
55. United States Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis," Regulatory Guide 1.174, 1998.
56. Vesely, W.E., Goldberg, F.F., Roberts, N.H., and Haasl, D.F., "Fault Tree Handbook," NUREG-0492, U.S. Nuclear Regulatory Commission, 1981.
57. Werner, P., "A Three-Level Systems Approach to Hazards in High Consequence Organizations," Sandia National Laboratories, draft, August 11, 2001.
58. Wojcik, L.A., "Probabilistic Risk Assessment and Aviation System Safety," Flight Safety Foundation, Arlington, VA, 1989.
59. Wood, R.H., "Aviation Safety Programs - A Management Handbook," Jeppesen Sanderson Inc., 1997.
60. Yang, S.H. and Chung, P.W.H., "Life Cycle Hazard Analysis for Computer Controlled Processes," *Computers Chem. Engineering*, Volume 22, pp. 5483-5490, 1998.
61. Zoller, L. and Esping, J.P., "Use 'What-If' Method for Process Hazard Analysis," *Hydrocarbon Processing*, Volume 72(1), pp. 132-B to 132-D, January 1993.