Probabilistic Causal Analysis for System Safety Risk Assessments in Commercial Air Transport

James T. Luxhøj, Ph.D.; Department of Industrial and Systems Engineering, Rutgers University;
96 Frelinghuysen Road, Piscataway, NJ 08854-8018 USA

Keywords: Aviation Safety, Risk Management

Abstract

Aviation is one of the critical modes of our national transportation system. As such, it is essential that new technologies be continually developed to ensure that a safe mode of transportation becomes even safer in the future. The NASA Aviation Safety Program (AvSP) is managing the development of new technologies and interventions aimed at reducing the fatal aviation accident rate by a factor of 5 by year 2007 and by a factor of 10 by year 2022. A portfolio assessment is currently being conducted to determine the projected impact that the new technologies and/or interventions may have on reducing aviation safety system risk. This paper reports on advanced risk analytics that combine the use of a human error taxonomy, probabilistic Bayesian Belief Networks, and case-based scenarios to assess a relative risk intensity metric. A sample case is used for illustrative purposes.

Introduction

Commercial air transportation in the United States is a complex array of many diverse, yet interrelated system components. There is a plethora of varied human, technical, environmental, and organizational factors that affect the performance of the National Airspace System (NAS). Through the years, numerous qualitative and quantitative approaches to aviation risk identification, modeling, and evaluation have been developed and have contributed in a seminal way to the understanding of aviation safety risk [1]. However, while methods exist for identifying aviation risk factors, there is a paucity of analytical methods for analyzing and interpreting the complex interactions of the various system risk factors. There has been a persistent need to develop advanced risk analytics that move beyond the essential identification of risk factors to enhanced system modeling and evaluation of complex causality as well as to assessing various combinations of risk mitigation strategies [2-8].

The NASA Aviation Safety Program (AvSP) Office located at the NASA Langley Research Center is managing the joint industry/government/university development of 48 new technologies/interventions intended to improve aviation system safety [9]. Figure 1 displays the principal categories of the new technologies. As an example, there are four NASA AvSP technologies focused at aircraft Loss of Control (LOC) issues: (1) Auto-configurable aircraft controls given upset or specific system failures (2) Database of upset/control and recovery phenomena that provides data for simulation training and/or decision-aids (3) Maintenance visualization support/training such that system failures are reduced (these failures could lead to LOC in the causal chain) and (4) Weather (Wx) decision-aids that evaluate and warn pilot of conditions (icing, turbulence, etc.) that may cause upset. There is a requirement to develop an analytical method that facilitates assessing the projected impact of the various technologies and/or interventions upon system risk reduction [10].

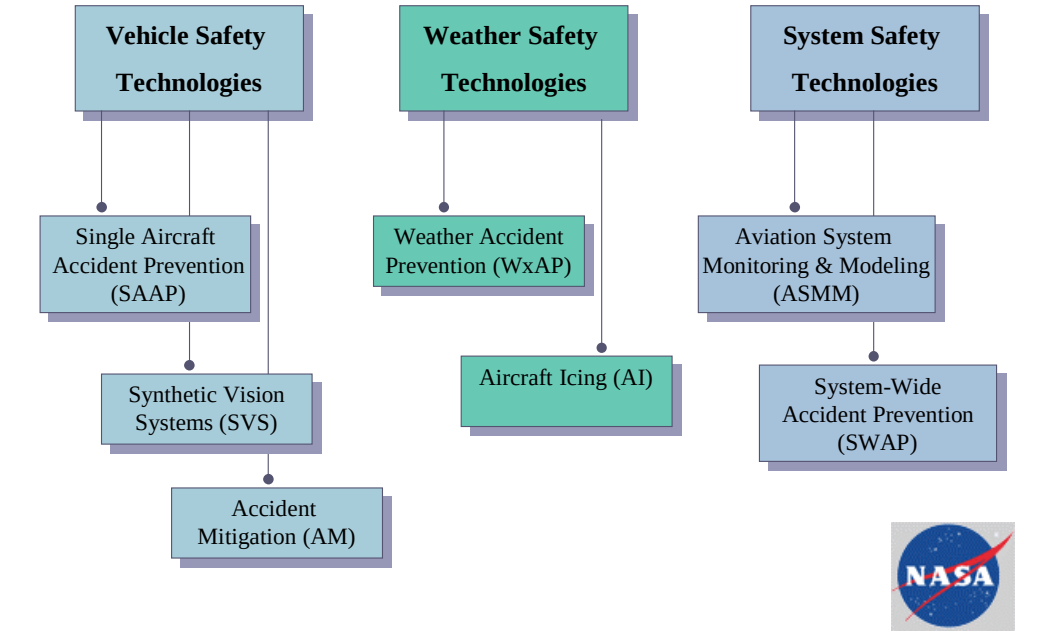

Figure 1 - Categorical Overview of NASA Technologies

Luxhøj, et al. [11-14] report on the development of an *Aviation System Risk Model (ASRM)* that uses the underlying probabilistic methodology of Bayesian Belief Networks (BBNs) and influence diagrams to graphically portray causal factor interactions. The ASRM uses the Information Technology (IT) embedded in the HUGIN BBN software as an enabling technology [14]. HUGIN is software to facilitate BBN modeling [15-17]. The ASRM is being modified to graphically portray a risk metric, termed the *relative risk intensity*, to illustrate perturbations from a baseline period. In Phase 1 of this research, aircraft accident scenarios, such as Loss of Control (LOC) and Maintenance (MAIN)-related, have been developed using the combined approach of *analytic generalization* from case studies [18] and from knowledge engineering sessions with subject matter experts (SMEs). van Vurren [19] uses a similar approach in his study of mishaps in the steel industry and medical domain.

Typically, 60%-80% of all accidents are attributed to human error. While mechanical, environmental, and operational factors are necessarily to be included in a full system precursor analysis, certainly, understanding human error is essential to aviation system risk modeling. In a recent research modification, the ASRM has been adapted to include the Human Factors Analysis and Classification System (HFACS) [20-22] taxonomy to expand the examination of human causal factors and to support the identification of safety risk intervention strategies. HFACS [21] focuses on human error modeling and includes organizational influences (resource management, organizational climate, and organizational processes), preconditions for unsafe acts (adverse mental states, adverse physiological states, physical/mental limitations, crew resources management, and personal readiness), and individual unsafe acts (decision errors, skill-based errors, perceptual errors, routine violations, and exceptional violations). While other general domain taxonomies exist for the classification of human error, such as the Eindhoven Classification Method (ECM) [19], HFACS is becoming widely disseminated in both military

and commercial organizations as a tool for understanding the role of human error in aviation accident analysis. Shappell and Wiegmann have led an effort to code all military, commercial and general aviation accidents in the United States using the HFACS framework. The database consists of over 16,000 aviation accidents involving human error and includes all the Parts 121 and 135, scheduled and non-scheduled, airline accidents since 1990. These data are being used in the ASRM to initially seed the model and to facilitate exercising the model.

The ASRM prototype methodology and tool have been through an initial testing and evaluation period and offer promise. However, additional analytical research and tool development are required in order to realize the full potential of this new type of system risk model. The joint research between the Federal Aviation Administration (FAA), NASA, and Rutgers University involves extending the ASRM to modeling the complex interactions of the many diverse human, technical, environmental, and organizational factors that affect commercial air transportation. The intent of the new research is to develop more comprehensive ASRM case studies reflective of multiple accident scenarios selected by the NASA Aviation Safety Program (AvSP). The case studies model the change in system safety risk within the accident scenarios due to risk mitigation strategies proposed by NASA AvSP by examining the impact that technology insertions and/or interventions may have on reducing the relative system safety risk. For example, it is envisioned that the size of the HFACS database will exercise the ASRM and yield a model capable of evaluating the NASA AvSP intervention/mitigation strategies focused on human factors before they are fielded. Eventually, other data sources dealing with mechanical, software, environmental, and operational risk factors will be integrated into the ASRM as these data sources become available.

Risk Analytics

Risk is a mathematical expression that has two components - *likelihood* and *severity*. Risk is an expression that attempts to answer two questions at the same time; how likely? and with what consequence? These components of risk can be defined as follows:

Hazard
A hazard implies any event that has the potential to produce an adverse outcome with respect to the system. The system can refer to a piece of equipment or a single engine or an entire airplane [23]. In most situations, the fact that a hazard is present does not necessarily mean that there will be an adverse outcome with respect to a system. A “successful” hazard is an event when a hazard attacks the system and results in damages.

Likelihood
Likelihood or probability represents the chance that a given hazard will lead to an adverse impact on a system. It can be described qualitatively as well as quantitatively.

Severity
Severity represents the damages that result in the case of successful hazard event. The severity could be measured in terms of dollar value, human life or etc. Risk, in its quantitative form, risk can be expressed as follows:

$$R = P * S$$

where R is risk, P is probability or likelihood of an event and S is severity.

Since it is not always possible to calculate the risk quantitatively or since it is sometimes necessary to assign qualitative descriptions to likelihood and damages, risk is frequently expressed in relative or qualitative terms. Figure 2 illustrates qualitative descriptions of likelihood, severity and risk developed by the FAA's Office of System Safety (ASY-300).

FAA Order 8040.4 establishes the safety risk management policy and prescribes procedures for implementing safety risk management as a decisionmaking tool within the FAA (see http://www.asy.faa.gov). This document provides general guidelines and principles for safety risk assessment and risk characterization.

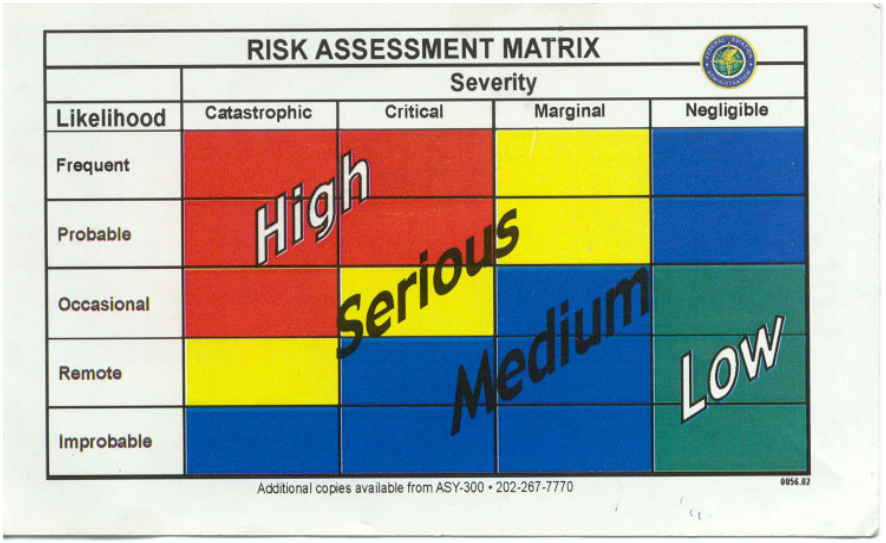

Figure 2 - Risk Matrix
(Source: ASY–300, Office of System Safety, FAA)

Relative Risk Intensity Metric: This research introduces the notion of a *relative risk intensity* metric. This metric uses the matrix cells of Figure 2 to create a visual profile of risk relative to some baseline. Note that the risk matrix in Figure 2 is a 5 x 4 matrix. Thus, from observing Figure 2, the following risk intensity levels are computed:

# of cells	Risk Intensity Level	
3/20	0%-15%	Low
8/20	15% - 55%	Medium
4/20	55% - 75%	Serious
5/20	75% - 100%	High

Figure 3 displays the use of the relative risk intensity combined with an influence diagram. The ASRM itself facilitates the computation of the likelihood portion of risk, or notionally, the "intensity". To fully understand risk, the ASRM software prototype is also being updated to enable the user to view a severity histogram per accident type (e.g., LOC, Controlled Flight Into Terrain (CFIT), etc.) as determined by data analysis.

Research Methodology

The underlying research methodology is comprised of three analytical approaches:

- the Human Factors Analysis and Classification System (HFACS)
- Bayesian Belief Networks (BBNs)
- case studies

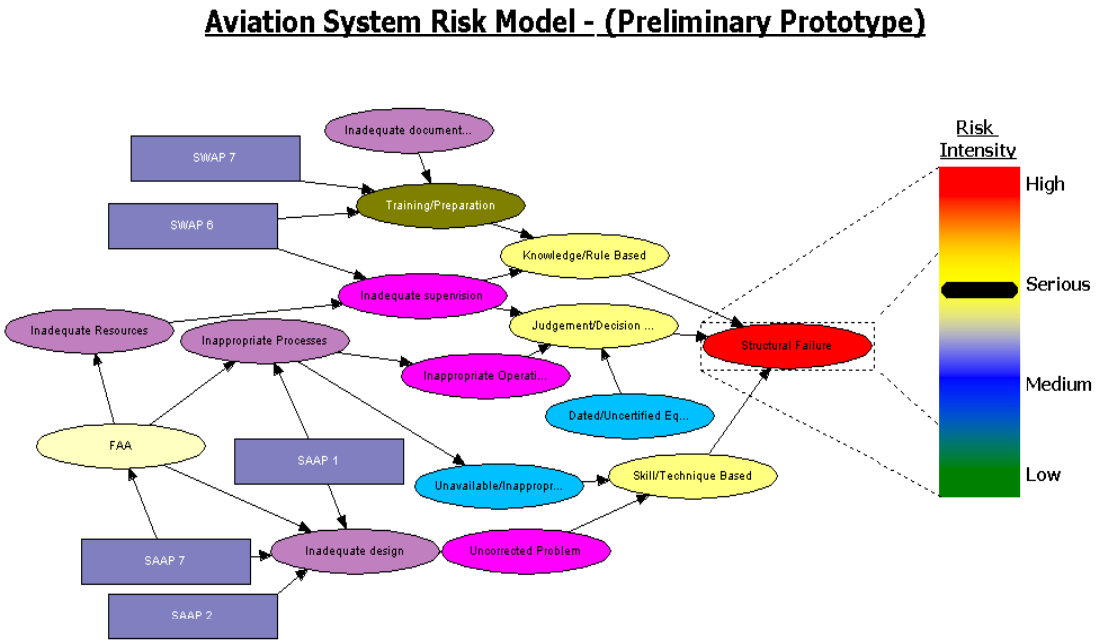

Figure 3 - Relative Risk Intensity Metric

The Human Factors Analysis and Classification System (HFACS): The HFACS is an analytical approach for classifying human error that is based on the Reason framework of system safety theory. While there are numerous contributing factors to aircraft accidents, such as operational, weather, etc., nevertheless, 60%-80% of all accidents are attributed to human error. The HFACS provides a fundamental analytical method for approaching causal modeling and the factors are illustrated in Figure 4. For a detailed description of the HFACS taxonomy, see [20].

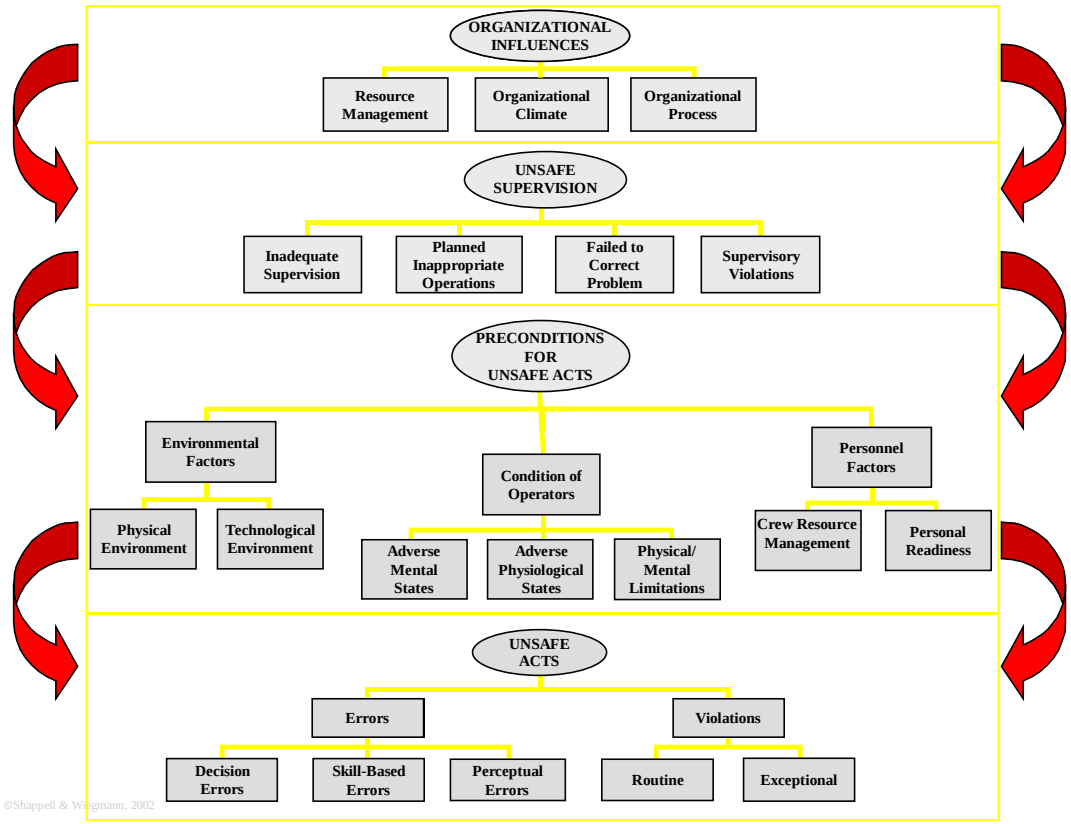

Figure 4 - The Human Factors Analysis and Classification System (HFACS) (Source: [20])

Bayesian Belief Networks (BBNs): One of the most important factors that should be taken into account when building models of accident causation is uncertainty. Probability theory derives solutions to the problem of reasoning under uncertainty in the face of limited information. In recent years, Belief Networks have been used as the main methodology for numerous tasks that involve reasoning under uncertainty. Belief networks provide efficient symbolic representations of probability models, together with the efficient inference algorithms for probabilistic reasoning [24-25].

Figure 5 displays an influence diagram with chance modes or variables represented as circles and decision nodes (see D1, D2, and D3) shown as rectangles. A decision variable can be related to one or multiple chance variables or multiple decision variables can be related to one particular chance variable. In this research, the decision nodes represent the AvSP technology and/or intervention insertions.

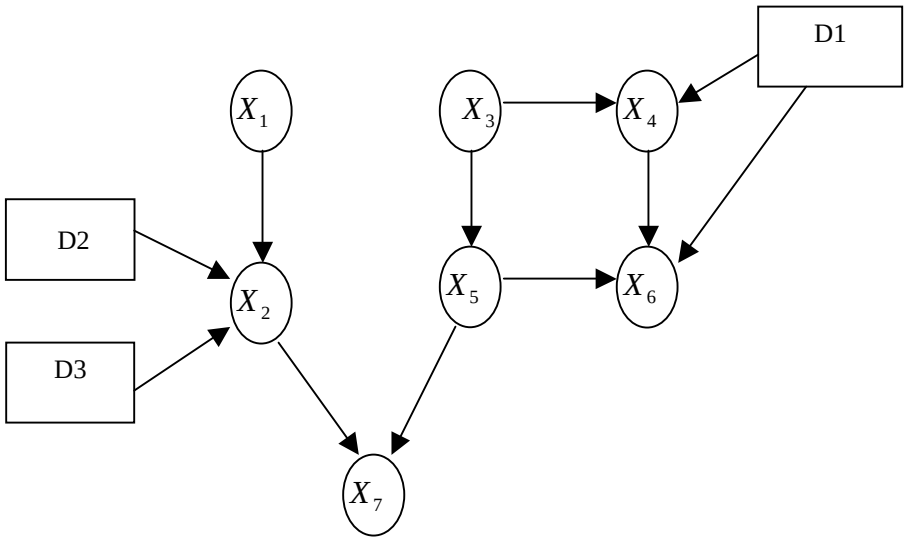

Figure 5 - An Influence Diagram

The HFACS framework, based on Reason's model of latent and active failures [26-27], provides a comprehensive framework to investigate the organization at multiple socio-hierarchical levels. As it originates from Reason's framework, therefore it also inherits the limitations of Reason's model. The HFACS framework qualitatively and quantitatively does not address the interdependencies among different socio-hierarchical elements. A Bayesian Belief Network (BBN), however, provides a probabilistic framework to address and quantify the causal relationships under uncertainty. Fenton, et al. [28] report on the use of BBNs to model the safety assessment of nuclear computer-based systems, for example. By using graph theory, the interrelationships among causal factors can be defined and Bayesian probability theory is used to quantify these relationships. Model quantification occurs by developing Conditional Probability Tables (CPTs) using data when it is available. In the absence of data, an experts' "beliefs" are used. Typically, model quantification involves the fusion of both hard data and "beliefs" and BBNs are ideally suited to such a hybrid or mixed modeling approach. Various elicitation methods of expert beliefs are provided in [29-30]. There are a number of issues concerning human capabilities to consider when eliciting beliefs from the experts as reported in [31-33].

Knowledge elicitation in BBNs involves both qualitative and quantitative forms. Qualitative knowledge comprises identifying causal factors and their interactions by specifying the graphical structure with directed arcs and nodes. Quantitative or semi-quantitative knowledge involves providing numerous conditional probabilities for the BBN. The elicitation of numerous probabilities is typically considered the bottleneck in BBN construction. Renooij [32], Renooij and Witteman [34], van der Gaag, et al. [35], Druzdzel and van der Gaag [36] present an approach to facilitate probability elicitation in BBNs. This approach involves the use fragments of text to provide a conditioning context that are derived from the graphical BBN structure. Then the fragments of text are placed adjacent to a probability scale that contains both verbal probability expressions and numerical values. The verbal expressions are of the form "(almost) certain, probable, expected, fifty-fifty, uncertain, improbable, and (almost) impossible"[32]. The authors contend that the combined approach of both verbal and numerical anchors accelerate conditional probability assessments in BBN when used in conjunction with the fragments of text [32]. This combined approach of using verbal and numerical anchors is being adapted in this

research to assist with probability elicitations for the BBNs dealing with risk assessments of the AvSP technologies/interventions.

The ASRM research uses a case study approach. With a case study approach, statistical generalization is not used. In statistical generalization the samples are chosen randomly and then generalization is observed as a replication of a specific behavior. However, cases are not random samples and each case study represents a unique portrayal. Rather, with case study research, *analytic generalization* and a replication logic is used to generalize to a theory, in this case, system safety theory [18]. Therefore, multiple case studies can be considered as multiple experiments. If two or more case studies show the same behavior, replication can be claimed; however if contrasting results are produced, there should be predictable reasons for this divergent behavior. While specific case studies are used to initiate a dialogue-based process, the resulting influence diagram represents a realistic portrayal of a more generalized model.

Data Analysis: Some key data sources are briefly described below:

HFACS Database: Dr. Scott Shappell (FAA) provided the HFACS data to the Rutgers team. The HFACS data is organized by casual factors such as decision errors, adverse mental states, supervisory violations and organizational processes. It includes all the factors in the generic HUGIN model and also factors such as location and date of the owner, airline owner, etc. Pilots coded the HFACS database that serves as a starting point for the Rutgers research as it helped ground the models in real world data and provided support for establishing connections (i.e. statistical correlations) between causal factors. Figure 6 illustrates the percentage frequency of causal factors for Part 121 scheduled operations. NASA has identified 1990-96 as the baseline period for the AvSP technologies/interventions. The HFACS database may also be used to identify correlations between the different causal factors. Correlation analysis assists with gaining an understanding of the degree to which certain causal factors may be related but it does not necessarily have to be the case for every accident.

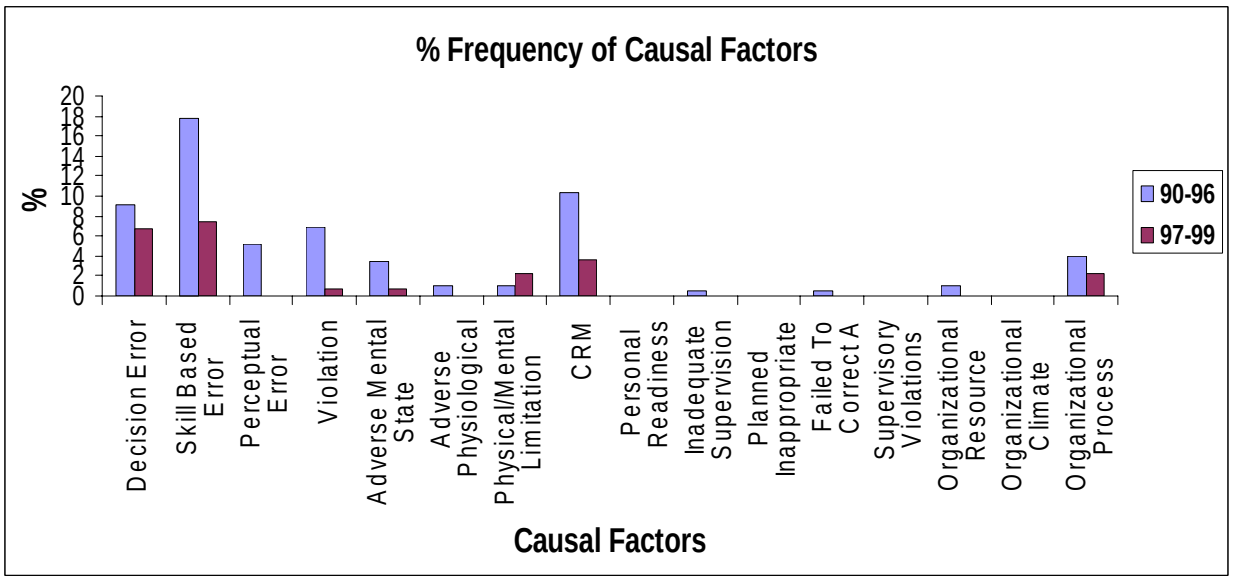

Figure 6 - HFACS Causal Factors

National Aviation Safety Data Analysis Center (NASDAC): The National Aviation Safety Data Analysis Center (NASDAC) [37] is managed by the FAA. The database identifies several causal factors and provides the possibility of identifying different types of accidents. The NASDAC database has a uniform data format and draws on several data sources including the NTSB. Internet accessible, it is possible to specify numerous criteria to limit the results from our data search. The results of the search are displayed in a Microsoft Excel sheet format. It is possible to click on a particular accident report to access a summary description of the final NTSB report for that accident. In this research, the NASDAC database is used to identify LOC cases and to develop an understanding of the overall accident rates for different types of accidents.

Figure 7 graphically portrays the applied approach used in this research. It is a systematic, analytical, dialogue-based approach that initiates with discussions of accident cases with subject matter experts. The causal factors are identified using an expanded HFACS taxonomy, and then the interactions among the causal factors are modeled using influence diagrams. After the influence diagrams are constructed and reviewed by subject matter experts, conditional probability tables are elicited from the "beliefs" or value judgments of the subject matter experts, in conjunction with empirical data where available, to create the BBN. Typically, during this step, 2-3 subject matter experts are used. Generally, a "behavioral aggregation" or consensus-based approach is used during the probability elicitation process, since such an approach encourages the experts to view the final product as a group effort [38]. However, any wide disagreement between the experts is noted for future sensitivity analysis. Then action nodes are added to the BBN to represent the technology/intervention insertions. Additional technologist experts will be included in these discussions. Finally, the projected risk is displayed relative to a baseline period on the relative risk intensity graph.

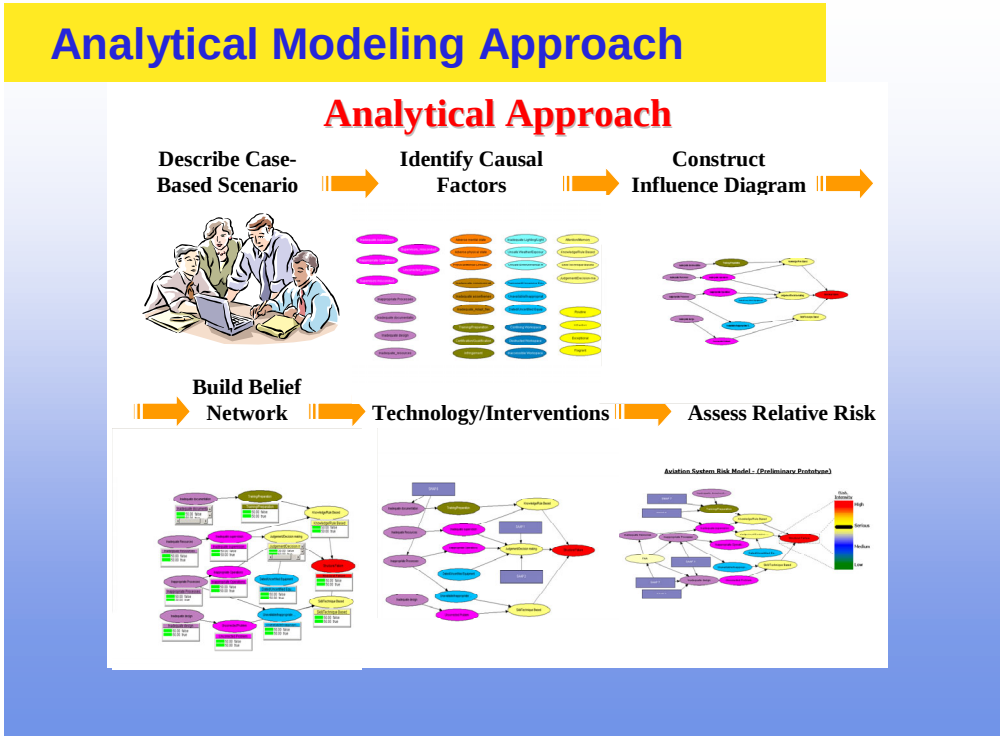

Figure 7 - Applied Research Modeling Approach

Figure 8 graphically illustrates the knowledge acquisition plan for the inclusion of a variety of Safety Inspectors with their general domain knowledge of airworthiness, operations, and avionics are used during the causal modeling and probability elicitation steps. Opportunities will exist for joint discussions between the NASA technologists and the FAA Aviation Safety Inspectors during the technology insertions step. Where possible, the model is supported with data from the NTSB, HFACS, NASDAC, and NASA's ASAFE program. Researchers at the Volpe National Transportation Systems Center are constructing event tree conditional probabilities based on existing aviation safety data sources. These conditional probabilities may be used as "seed" values by the experts that may be modified through the expert elicitation process. It is planned that an Expert Advisory Panel comprised of aviation experts not involved with model construction will be created to review all models and to suggest possible refinements.

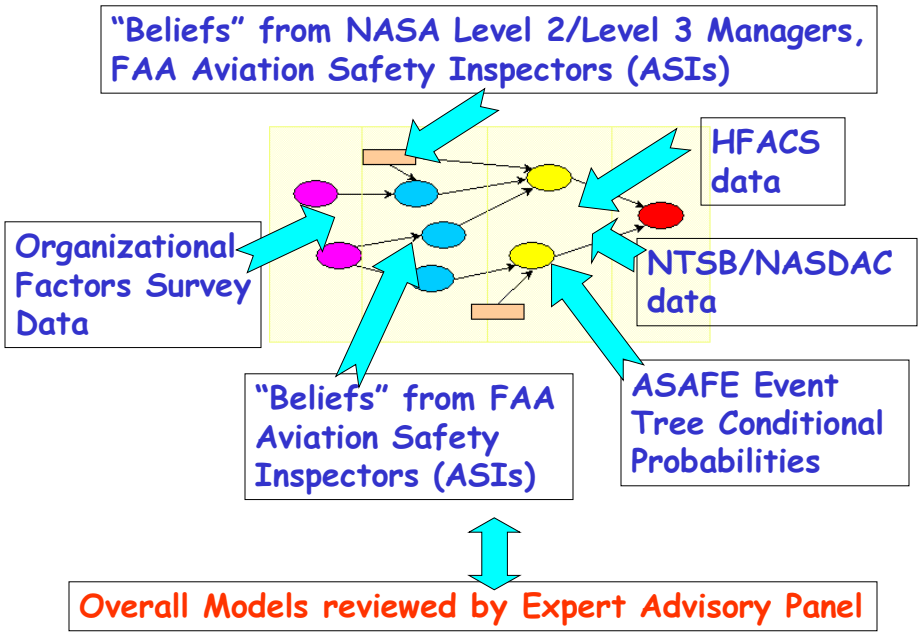

Figure 8 - Multiple Sources Used for "Model Quantification"

"Representative" Loss of Control (LOC) Case: Air Ontario Flight 1363

Accident Summary: The following accident summary presents a "Loss of Control (LOC)" accident where lack of de-icing was a major causal factor. Even though a specific accident is used to provide the "analytical structure" for the case, it should be remembered that through the construct of "analytic generalization" this case is used to generalize to a theory of system safety. The proposed approach is logically consistent while indicating the "causality flows", yet broad enough to consider more general socio-technical factors. The accident summary is adapted from the description and analyses presented in [5].

At 12:09 pm CST on Friday, March 10, 1989, Capt. George C. Morwood, a 24,000-hour flight time veteran, advanced the throttles of Air Ontario Flight 1363, a Fokker F28 1000, initiating the take-off roll at Dryden Airport, Ontario, Canada. Flight 1363 was the second part of the day's

flying schedule that consisted of a Winnipeg to Thunder Bay round trip, with intermediate stops at Dryden (Flights 1362/1363).

Capt. Morwood reviewed the operational status of the aircraft before departing Winnipeg (Flight 1362) and verified, among other maintenance deferred detects, that the Auxiliary Power Unit (APU) was unserviceable. The operational implications of this defect were that the engines had to be started from an external power unit, or one engine had to be kept running to cross-start the other engine. If both engines were shut down at a station where no external power unit was available, the aircraft would be stranded until the APU was fixed or an external power unit became available. There was no external power source at Dryden and therefore one engine would have to be kept running. The manufacturer, Fokker, and Air Ontario strictly prohibited de-icing with either engine running.

Since the original flight release from Thunder Bay to Dryden prepared by the Air Ontario Systems Operations Control (SOC) had not been updated, ten passengers were added to Flight 1363 after it had been refueled. Now overweight for take-off, Capt. Morwood elected to off-load the ten passengers and their baggage. However, the Air Ontario SOC duty manager overrode the captain's decision and chose to achieve weight reduction by off-loading fuel. The de-fueling caused an additional 35-minute delay in the departure of Flight 1363 from Thunder Bay and increased the "hot refueling" time at Dryden. Flight 1363 departed Thunder Bay with a full load of passengers and arrived in Dryden one hour behind the schedule.

The hot refueling process started with passengers on board, which is considered to be an unsafe practice, and is difficult to reconcile with Capt. Morwood's style of decision-making, characterized by conservatism and strict adherence to rules and procedures. The Commission of Inquiry indicated that Capt. Morwood had a heated conversation with the SOC over the telephone regarding the passenger load and weather conditions in Winnipeg prior to the departure from Dryden. The Commission established that the demeanor of Capt. Morwood deteriorated visibly while in the terminal after his telephone contact with the SOC, and that, clearly frustrated, he briskly walked back to the aircraft.

Upon his return to the aircraft Capt. Morwood asked the ground handler whether de-icing was available; however he did not request de-icing after being told that it was. When the aircraft was about to leave the terminal platform, snow was falling heavily, and its wings were covered in snow to depths varying from one-eighth to one-quarter of an inch. While taxiing out, FSS advised Flight 1363 of a Cessna 150 in a VFR recreational flight, which was due to land at Dryden. The pilot of this aircraft had requested that Flight 1363 hold its departure until he had landed, because of the deteriorating weather. The request was eventually granted and the ground hold further compounded the delay of Flight 1363.

The combination of the one-half inch deep slush on the ground and the wet snow, which had frozen into opaque ice on the forward half of the wings, significantly degraded the performance capabilities of the F-28. After a longer than normal take-off roll, the aircraft rotated, lifted off slightly, began to shudder and settled back onto the runway. It rotated a second time, lifting off at the 5,700 ft point of the 6,000 ft runway. It flew briefly, clearing the end of the runway at approximately 15 ft above the ground. It failed to gain altitude and crashed, coming to rest approximately one km. away from the end of the runway.

A Commission of Inquiry was formed on March 29, 1989 to investigate the accident. The Dryden Report, as it has become widely known as, represents one of the first large-scale applications of a systemic, organizational approach to the investigation of an aviation accident.

Aviation System Risk Model (ASRM): The following model depicts the causal factors and the interactions among them.

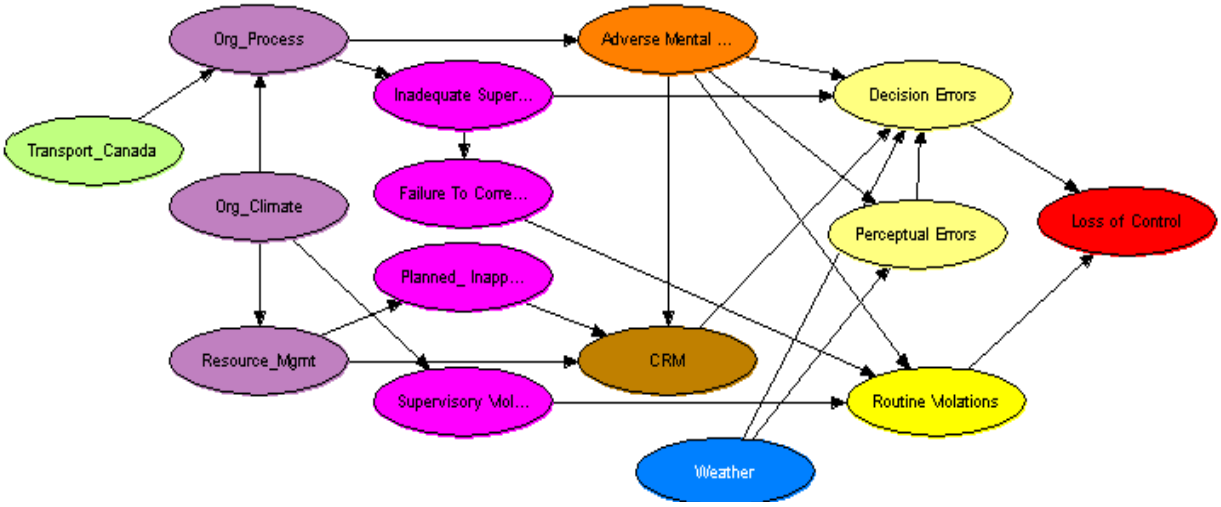

Figure 9 - ASRM for Air Ontario 1363

The interactions among the causal factors of this accident are depicted through the links among the nodes in Figure 9. These interactions were reviewed by the subject matter experts and are based upon a qualitative reasoning process in interpreting the causal factor descriptions provided in the accident report. A snapshot of the reasoning behind a few selected links is provided below:

Organizational Climate ➔ Resource Management
After the merger with Air Canada, Air Ontario was not provided with sufficient levels of training and resources. Due to the inappropriate management style, some of the appointments, such as those of president's close relatives to key managerial positions were the subject of considerable discussions at the Air Ontario committee meetings. Consequently, some Air Ontario managers were confronted by demands for which their experience may not have been adequate.

Inadequate Supervision ➔ Decision Errors
Some F-28 pilots used the Piedmont F-28 Operations Manual while others used the US Air F28 Pilot's Handbook, since Air Ontario did not have its own F-28 operations manual. There was the obvious lack of standardized operations manuals. These deficiencies created problems on the flight deck.

Failed to Correct a Known Problem ➔ Routine Violation
Failures to de-ice and maintenance problems were known by supervisors and yet allowed to continue. Hence, these practices had the form of routine violations.

ASRM with AvSP Technology / Interventions: The definitions and descriptions in this section are based on the NASA Product Dictionary (2002). Based on discussions with subject matter experts and on my research team's knowledge of the 48 technologies, the following represents a

"sample" of the reasoning why certain technologies are added to the model of Air Ontario Flight 1363. Figure 10 depicts the modified ASRM with technology elements.

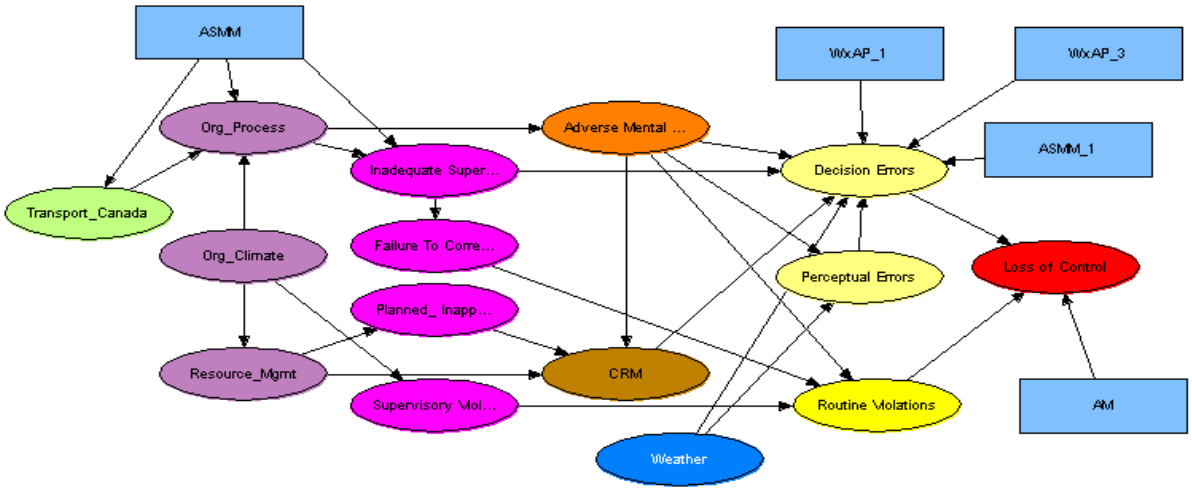

Figure 10 - ASRM for Air Ontario 1363 with Technology Insertions

ASMM4 – Performance Data Analysis & Reporting System (PDARS) Tools: This technology element provides the capability to collect and process Air Traffic Control (ATC) operational data; compute quantitative operational performance measures on a regular basis relating to system safety, delay, flexibility, predictability and user accessibility; conduct causal analyses and operational problem identification and analyses; archive performance statistics and basic operational data for use in research, development and planning studies. The objective here is to monitor performance metrics continuously to enable the implementation of a policy of proactive NAS management. Extending Aviation Performance Measurement System (APMS) concepts to the ATC environment is proposed. Iterative evaluation by ATC users is expected to improve the measurement and tool requirements. Thus, insertion of ASMM4 in 'Transport Canada' node has a potential impact.

WxAP1 – Cockpit Weather System Technologies for Enhanced Situational Awareness & Decision Making: WxAP1 is about the development of substantiated aviation weather information system guidelines for flight deck user interface and for operational use. The objective is to develop enhanced weather presentations that minimize interpretation and enhance situational awareness. Therefore, this technology is considered to have a potential impact on the 'Decision Errors' node.

WxAP3 – Weather Information Datalink Systems Technologies for Ground-to-Air Dissemination: WxAP3 involves the development of datalink system and architecture guidelines supporting the transfer of weather information from ground-to-air. The targeted problem in developing this technology is the poor dissemination of weather information to the flight deck. This technology element is considered to have an impact on the "Decision Errors" node.

Other technology elements included the modified model are:

AM1 – Next Generation Crash Analysis Codes
AM2 – Energy Absorbing Seats, Restraints and Structures

AM4 – Next Generation Crashworthiness Design Guidelines
ASMM1 – Incident Reporting Enhancement Tools
ASMM2 – National Aviation System Operational Monitoring System (NAOMS)

Preliminary Results

Figures 11-12 display screens from the working ASRM prototype that were developed during the Phase 1 research. Figure 12 displays, in general, how the interactions of various causal factors may be depicted, but does not correspond to the aforementioned LOC model. Possible technology insertions are easily portrayed. The working prototype enables sensitivity analyses for both single- and multiple technology insertions. Note that one technology may impact a single and/or multiple causal factors and that multiple technologies may also impact a single and/or multiple causal factors. Changes in relative risk intensity may be displayed on the color-coded bar chart. Both absolute and relative perturbations from a baseline are reported.

Preliminary Risk Assessments: Table 1 illustrates some "representative" preliminary risk assessments using the analytical approach as described previously. The current LOC model has only been through one complete iteration including model quantification with the subject matter experts and thus, any risk assessments should be considered as preliminary. Also, it is intended that an advisory panel will be formed to review all models as well as the beliefs of the experts.

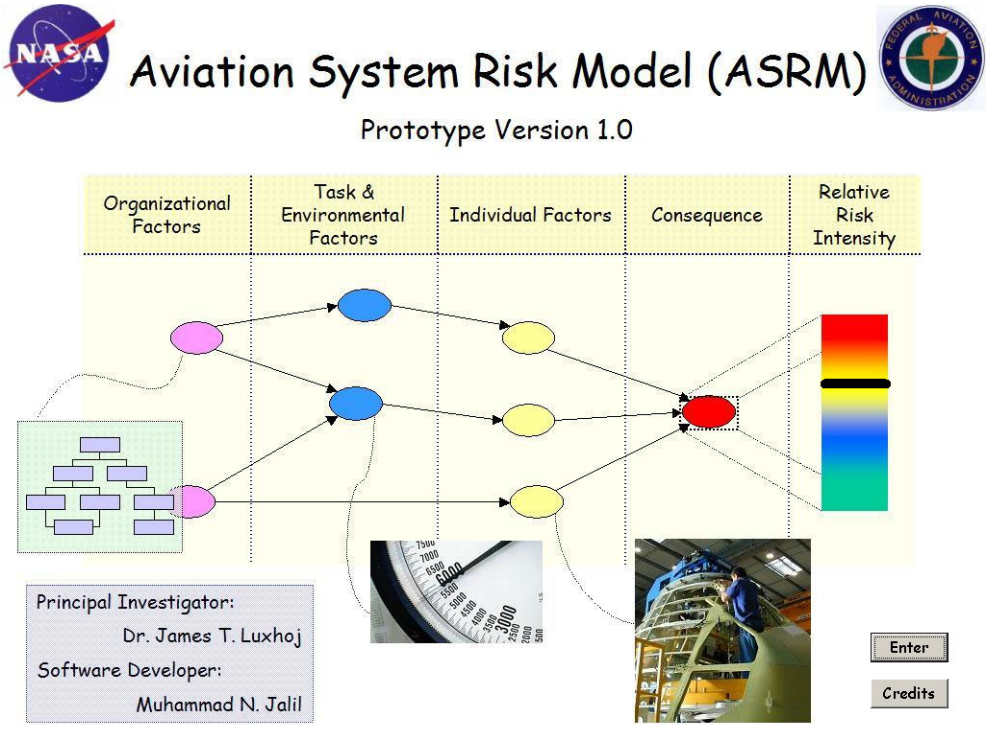

Figure 11 - Initial Screen for the ASRM Prototype

An important point to note from Table 1 is that the overall relative risk reduction on a consequence, such a LOC, may not be as high as the relative risk reduction on a particular causal factor or set of causal factors. The real value of a proposed AvSP technology insertion and/or intervention may lie on the impact on causal factors.

At this point it is important to clarify some terminology used in order to better communicate the analytical approach. A certain modeling "hierarchy" exists, if you will, in the proposed analytical approach. The "Approach" refers to the systematic, step-by-step, ASRM analytical approach as outlined in Figure 7. "Model" is used to refer to the various consequence models, such as Loss of Control (LOC), Controlled Flight Into Terrain (CFIT), Runway Incursion (RI), etc. It should be noted that in Phase 1, four representative "models" are developed for each consequence (LOC1, LOC2,) since there are alternative ways that causal factors could combine for a consequence to occur. Fore example, there could be an LOC accident due to icing or an LOC accident due to improper loading. These models are not exhaustive, but through the construct of *analytic generalization*, we are able to generalize the models to a theory of system safety. For each of the models, various "Scenarios" are created based on alternative combinations of technology insertions/interventions. As noted by Kahn and Wiener [39], a scenario is a "hypothetical sequence of events constructed for the purpose of focusing attention on causal processes and decision-points."

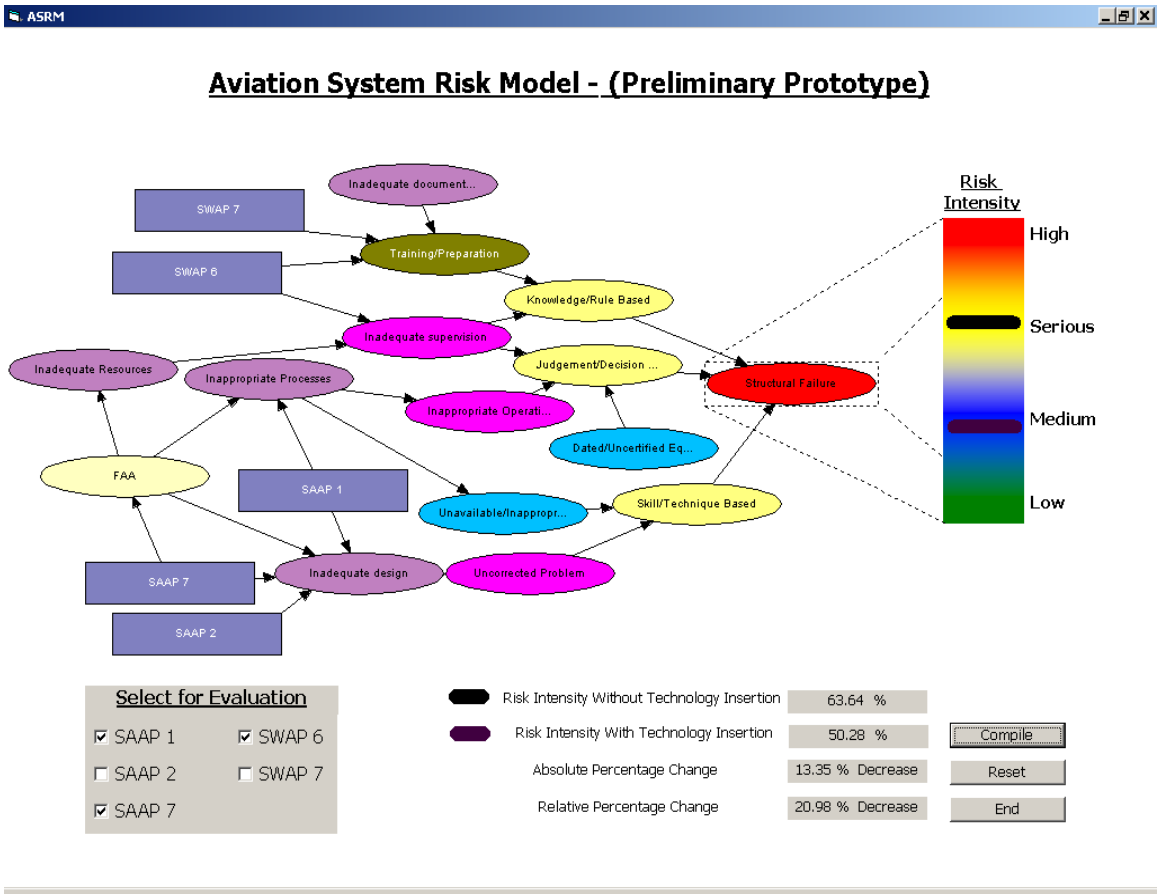

Figure 12 - "Relative Risk Intensity" of the Working ASRM Prototype

In the Phase 1 research, both the LOC and Maintenance accident categories have four models each. Some of the models are not fully quantified at this point in time and some models are partially quantified, so research with these models will continue under Phase 2. In addition, the models need to complete an internal validation step. As previously noted, each of the LOC and Maintenance-related models enables the analysis of *scenario variants*, or different combinations of possible technology insertions. So with the Phase 1 analytical approach, it is possible, for

example, that with 3 models, approximately 30 different scenario variants may be analyzed. This enables both a *literal replication* of cases and a *theoretical replication* of cases [18] and leads to an enrichment of and support for the proposed system safety theoretical approach.

Remaining Research

Over the next three years, the proposed analytical approach and the ASRM software will be used to perform risk assessments for all 48 new technologies/interventions in NASA's AvSP portfolio. The development of these risk assessments will be based on numerous meetings with subject matter experts in the aviation community. In addition, an expert advisory panel will be created to assist with model validation by examining construct validity, internal validity, and external validity as well as repeatability [18]. Belief assessment remains an emerging and developing research field [40].

As an update to the ASRM, it is planned to provide severity distributions for each accident type. As the risk intensity is notionally the likelihood portion of risk, the prototype software will enable the user to drill down to view a "representative" severity distribution and the corresponding risk matrix as illustrated in Figure 13.

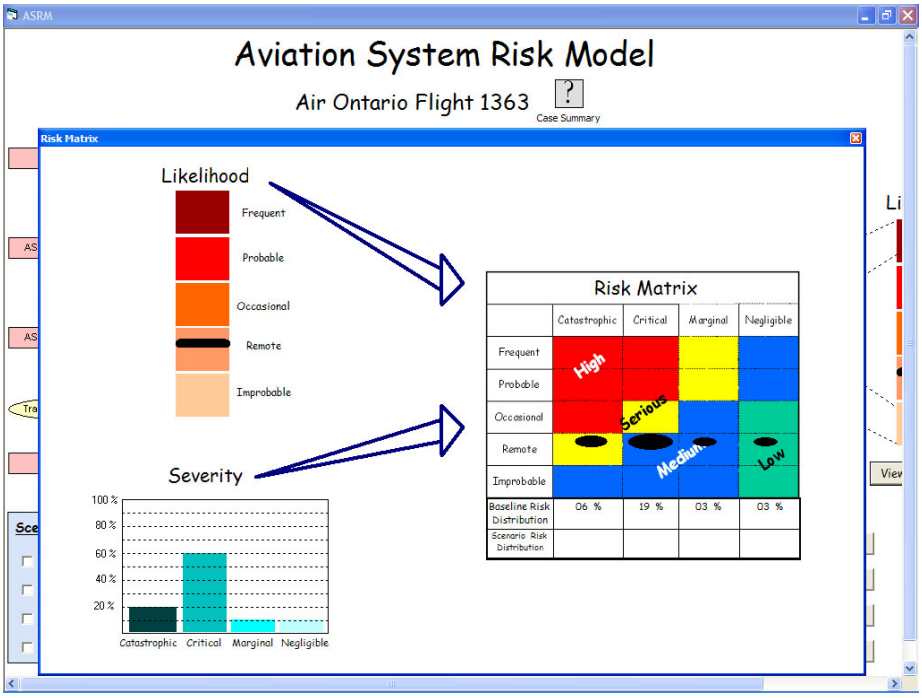

Figure 13 - Inclusion of "Representative" Severity Distribution

Eventually, a suite of models will be developed by accident type, such as Controlled Flight Into Terrain (CFIT), Runway Incursions (RI), etc. Collectively, these models will paint a mosaic of the various contributions that the new technologies/interventions make towards system safety risk reduction in the National Airspace System (NAS).

Acknowledgements

Dr. Luxhøj acknowledges the support of the Federal Aviation Administration (FAA) and NASA through FAA grant number 00-G-006. This research has been extended under NASA contract number NAS1-03057. He also acknowledges the contributions of his research assistants: Mr. Songwut Apirakkhit, Mr. Apichart Choopavang, Mr. Muhammad Jalil, Mr. Erim Kardes, Ms. Kimberlee Kauffeld, Mr. Ram Kuturu, Mr. Ahmet Oztekin, Mr. Ryan Dickey, Mr. Nathan Greenhut, Ms. Denise Andres, as well as Dr. David Coit. Dr. Luxhøj and his research team are also grateful to the FAA's Aviation Safety Inspectors who served as initial subject matter experts for this research. This paper is based on the research performed at Rutgers University. The contents of this paper reflect the views of the author who is solely responsible for the accuracy of the facts, analyses, conclusions, and recommendations represented herein, and do not necessary reflect the official view or policy of either the Federal Aviation Administration or NASA.

Table 1 - LOC 1 (ICING) – Air Ontario 1363

Description	Scenario	Targeted causal factor(s)	Technology element(s) inserted	Risk intensity (Factors)	Absolute % Decrease or (Increase) On factors	Relative % Decrease or (Increase) On factors	Risk Intensity (Consequence)	Absolute % Decrease or (Increase) on consequence	Relative % Decrease or (Increase) on consequence
Baseline scenario	No technology insertion	----	----	----	-	-	31.14% (Medium)	-	-
LOC 1 Scenario 1	ASMM suite	Regulator Org. Process Res. Mgmt. CRM	ASMM 1,2,3,4,5,6	N/A	N/A	N/A	28.34% (Medium)	2.8%	8.99%
LOC 1 Scenario 4	WxAP suite	Org. Process Decision Errors	WxAP 1,2,3,4	N/A	N/A	N/A	26.76% (Medium)	4.38%	14.06%
LOC 1 Scenario 5	Effect of interventions on regulator	Regulator	SAAP-4 ASMM 1,2,3,4,5,6	18.00%	4.00%	22.22%	28.14% (Medium)	3.00%	9.63%
LOC 1 Scenario 7	Effect of interventions on Decision Errors	Decision Errors	WxAP 1,2,3,4	34.27%	8.72%	25.44%	26.76% (Medium)	4.38%	14.06%
LOC 1 Scenario 8	Effect of interventions on Org. Process	Org. Process	WxAP 2, SAAP 4, ASMM 1,2,3,6	69.09%	15.89%	22.99%	28.00% (Medium)	3.14%	10.08%
LOC 1 Scenario 10	Effect of all possible interventions	Model	ASMM 1,2,3,4,5,6 SWAP 1,2 SAAP 4 WxAP 1,2,3,4	N/A	N/A	N/A	23.75% (Medium)	7.39%	23.73%

References

1. Leveson, N., "A New Foundation for System Safety" (http://sunnyday.mit.edu), 2002.

2. Leplat, J., "Occupational Accident Research and Systems Approach," in *New Technology and Human Error* (J. Rasmussen, K. Duncan, and J. Leplat, eds.) New York: John Wiley and Sons, Inc., 1987, pp. 181-191.

3. Pate-Cornell, M.E., "Organizational Aspects of Engineering System Safety: The Case of Offshore Platforms," *Science* 250, 1990, pp. 1210-1217.

4. Pidgeon, N. and M. O'Leary, "Organizational Safety Culture: Implications for Aviation Practice," in *Aviation Psychology in Practice* (N. Johnston, N. McDonald, and R. Fuller, eds.), Hove, The Netherlands: Lawrence Erlbaum, 1994.

5. Maurino, D.E., J. Reason, N. Johnston, and R.B. Lee, *Beyond Aviation Human Factors*, Vermont: Ashgate Publishing Company, 1997.

6. Reason, J., Managing *the Risks of Organizational Accidents.* England: Ashgate Publishing Limited, 1997.

7. Sarsfield, L.P., "Aviation in the Next Millennium: A National R&D Plan for Improving Air Transportation Safety and Security in the 21st Century", Draft, RAND Science and Technology Policy Institute, October 1, 1998.

8. Strauch, B., *Investigating Human Error: Incidents, Accidents, and Complex Systems*, England: Ashgate Publishing Limited, 2002.

9. NASA Aviation Safety Program (AvSP) Product Dictionary, February 2002.

10. NASA Aviation Safety (AvSP) Program Commitment Agreement, July, 2000.

11. Luxhøj, J.T., D.N. Arendt, T.P. Williams, and T.G. Horton, "An Application of Advanced Information Technology for Assessing Aircraft Accident Causation," Proceedings *of International Society of Air Safety Investigators*, Anchorage, Alaska, September 29 - October 3, 1997.

12. Luxhøj, J.T., D.N. Arendt, and T.G. Horton, "An Intelligent Computer-Based Tool for Evaluating Aircraft Accident Causation," *Proceedings of European Safety and Reliability International Conference ESREL '98*, Trondheim, Norway, June 17-19, 1998, pp. 839-846.

13. Luxhøj, J.T., K. Bansal, A. Choopavang, A., T.G. Horton, and D. N. Arendt, "An Aviation System Safety Model for Improved Risk and Management," *Proceedings of the European Safety and Reliability Conference ESREL'99*, Munich, Germany, September 13-17, 1999, pp. 1285-1290.

14. Luxhøj, J.T., A. Choopavang, and D.N. Arendt, "Risk Assessment of Organizational Factors in Aviation Systems," *Air Traffic Control Quarterly*, 9 (3), *(Special Issue on Flight Safety)*, 2001, pp. 135-174.

15. Andersen, S.K., F.V. Jensen, and K.G. Olesen, "The HUGIN Core – Preliminary Considerations on Systems for Fast Manipulation of Probabilities," in *Proceedings of Workshop on Inductive Reasoning: Managing Empirical Information in AI-Systems,* Risø National Laboratory, Roskilde, Denmark, April, 1987.

16. Andersen, S.K., K.G. Olesen, F.V. Jensen, and F. Jensen , "HUGIN - A Shell for Building Bayesian Belief Universes for Expert Systems," in *Proceedings of the Eleventh International Joint Conference on Artificial Intelligence*, Detroit, Michigan, August 20-25, 1989, pp. 1080-1085.

17. Jensen, F.V., S.L. Lauritzen, and K.G. Olesen, "Bayesian Updating in Causal Probabilistic Networks by Local Computations," *Computational Statistics Quarterly,* 4, 1990, pp. 327-352.

18. Yin, R., *Case Study Research: Design and Methods, 3rd ed.*, London: Sage Publications, 2003.

19. van Vuuren, W., Organizational *Failure: An Exploratory Study in the Steel Industry and Medical Domain*, Institute of Business Engineering and Technology Application, Eindhoven University of Technology, Eindhoven, Netherlands, 1998.

20. Shappell, S.A., and D.A. Wiegmann, "The Human Factors Analysis and Classification System-HFACS," Office of Aviation Medicine Technical Report No, DOT/FAA/AM-00/7, Civil Aeromedical Institute, Oklahoma City, OK, February, 2000.

21. Shappell, S.A. and D.A. Wiegmann, "Applying Reason: The Human Factors Analysis and Classification System (HFACS)," *Human Factors and Aerospace Safety*, 1 (1), 2001, pp. 59-86.

22. Wiegmann, D.A., and S.A. Shappell, "A Human Error Analysis of Commercial Aviation Accidents Using the Human Factors Analysis and Classification System (HFACS)," Report Number DOT/FAA/AM-01/3, Washington DC: Federal Aviation Administration, 2001.

23. Gardiner, P., and R. Wood, "Operational Risk Management," *Handbook of Airline Operations,* New York: McGraw-Hill, 2000.

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

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

26. Reason, J., *Human Error*, Cambridge, UK: Cambridge University Press, 1990.

27. Reason, J., "A System Approach to Organizational Error," *Ergonomics* 38(8), 7, 1995, pp. 1708-1721.

28. Fenton, N.E., B. Littlewood, M. Neil, L. Strigini, D.R. Wright, and P.J. Courtois, "Bayesian Belief Network Model for the Safety Assessment of Nuclear Computer-based Systems, ESPRIT DeVa Project 20072, Center for Software Reliability, City University, London, January, 1998.

29. Ayyub, B.M., *Elicitation of Expert Opinions for Uncertainty and Risks,* New York: CRC Press, 2001.

30. Vick, S., *Degrees of Belief: Subjective Probability and Engineering Judgment,* Reston, VA: ASCE Press, 2002.

31. Wilson, A.G., "Cognitive Factors Affecting Subjective Probability Assessment," *ISDS Discussion Paper # 94-02*, Institute of Statistics and Decision Sciences, Duke University, February, 1994.

32. Renooij, S., "Probability Elicitation for Belief Networks: Issues to Consider," *The Knowledge Engineering Review,* 16(3), 2001, pp. 255-269.

33. Gilovich, T., D. Griffin, and D. Kahneman, *Heuristics and Biases: The Psychology of Intuitive Judgment,* New York: Cambridge University Press, 2002.

34. Renooij, S. and C.L.M. Witteman, "Talking Probabilities: Communicating Probabilistic Information With Words and Numbers," *International Journal of Approximate Reasoning,* 22, 1999, pp. 169-194.

35. van der Gaag, L.C., S. Rennoij, C.L.M. Witteman, B.M.P. Aleman, and B.G. Taal, "How to Elicit Many Probabilities," *Proceedings of the Fifteenth Conference on Uncertainty in Artificial Intelligence,*1999, pp. 647-654.

36. Druzdzel, M.J. and L.C. van der Gaag, "Elicitation of Probabilities for Belief Networks: Combining Qualitative and Quantitative Information," *IEEE Transactions on Knowledge and Data Engineering,* 12(4), 2000. pp. 481-486.

37. *NASDAC Database Report No. AAR 96*-06, National Aviation Safety Data Analysis Center, Federal Aviation Administration, Washington DC, 1996.

38. Meyer, M.A., and J.M. Booker, *Eliciting and Analyzing Expert Judgment: A Practical Guide,* New York: Academic Press, 1991.

39. Kahn, W. and A.J. Wiener, *The Year 2000: A Framework for Speculation on the Next Thirty-Three Years*, New York: Macmillan, 1968.

40. Benson, P.G., S.P. Curley, and G.F. Smith, "Belief Assessment: An Underdeveloped Phase of Probability Elicitation," *Management Science,* Vol. 41, No. 10, October 1995, pp. 1639-1653.

Biography

J.T. Luxhøj, Rutgers University, Department of Industrial and Systems Engineering, Piscataway, NJ 08854-8018 U.S.A.; telephone 732.445.3625; fax 732.445.5467; e-mail – jluxhoj@rci.rutgers.edu

Dr. James T. Luxhøj is Associate Professor of Industrial and Systems Engineering at Rutgers University. In 1994-95 and Fall 2001 he was a Visiting Professor at Aalborg University in Denmark. He received his Ph.D. in industrial engineering and operations research from Virginia Polytechnic Institute and State University in 1986. He has been involved in aviation systems analysis over the past 12 years. He served as the Principal Investigator on Federal Aviation Administration (FAA) research grants to develop an intelligent decision support system for aviation safety analysis and to develop analytical methods for aviation safety risk modeling, assessment, and management. Jim is currently collaborating with NASA's Aviation Safety

Program to apply risk modeling techniques to evaluate the impact of technology insertion upon system risk in the National Airspace System. He is the former Co-Chair for the international GAIN Working Group B: Analytical Methods and Tools and has served as the Co-Chair of the FAA's recent National Workshops on Risk Analysis and Safety Performance Measurement in Aviation. He has published extensively on topics such as risk analysis, reliability and maintenance modeling, econometric modeling, and decision support systems. Dr. Luxhøj serves as a Department Editor for *IIE Transactions on Operations Engineering*, and as Associate Editors for the *Journal of Design and Manufacturing Automation* and the *Journal of Engineering Valuation and Cost Analysis*. Jim resides in Somerset, New Jersey with his wife and two children.