

# Building a Safety Risk Management System: A Proof-of-Concept Prototype

*James T. Luxhøj, Ph.D.  
Rutgers University*



***FAA/NASA Risk Analysis Workshop***

***Arlington, VA  
August 19, 2004***



# Outline

- Background
- Elements of the Analytical Method
  - Human Factors Analysis and Classification System (HFACS)
  - Aviation System Risk Model (ASRM)
- Preview of the ASRM Decision Support Tool Prototype
- Ongoing Research



# *University/Industry Team Approach*

## **Faculty:**

- **Dr. James T. Luxhøj, Industrial & Systems Engineering (ISE)**
- **Dr. David Coit, Industrial & Systems Engineering (ISE)**



## **NASA:**

- **Ms. Sharon Monica Jones, Technical Monitor**



## **FAA:**

- **Ms. Rosanne Weiss, Technical Monitor**
- **Dr. Scott Shappell, Subject Matter Expert, FAA's CAMI**
- **Mr. Don Arendt, Subject Matter Expert, FAA's FSAIC**



## **Graduate Research Assistants:**

- **Mr. Ram Kuturu, ISE M.S. Student**
- **Mr. Ahmet Oztekin, ISE M.S. Student**
- **Ms. Denise Andres, ISE M.S. Student**
- **Mr. Nathan Greenhut, ISE M.S./Ph.D. Student (NASA GSRP Fellow)**
- **Mr. Chad Bareither, ISE M.S. Student**
- **Mr. Valentin Helou, ISE Ph.D. Student (to join September 1, 2004)**

## **Undergraduate Research Assistants:**

- **Ms. Huda Hadi, ISE senior (RU Undergraduate Research Fellow)**
- **Ms. Cara Lee, ISE senior**
- **Ms. Debora Cabezas, ISE senior**

## **Programmer:**

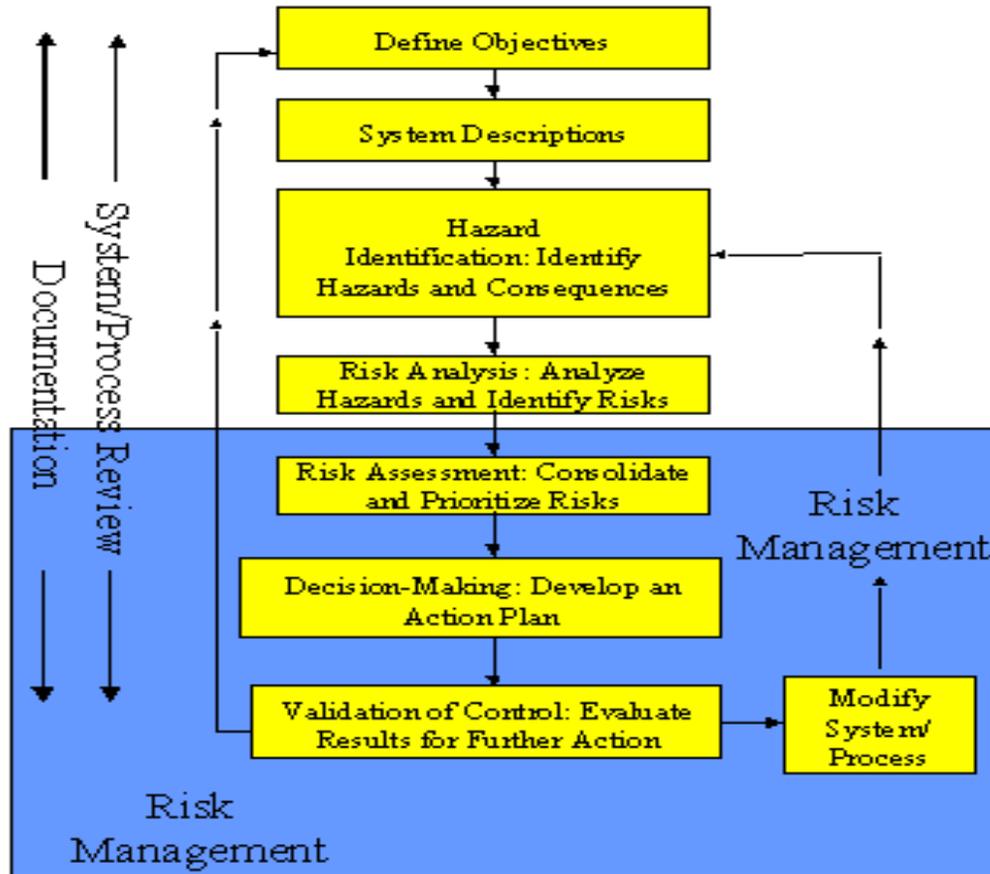
- **Mr. Joe Irgon, Rutgers University, B.S. Computer Science/B.S. Biochemistry**

# Safety Risk Management (SRM)

- *"Safety is the goal of transforming the levels of risk that inheres in all human activity."* (Dr. Geoff McIntyre, *Patterns in Safety Thinking*, p. 81).
- **Safety Risk - expression of the probability and impact of an undesired event in terms of hazard severity and hazard likelihood (FAA Order 8040.4).**

# Safety Risk Management (SRM)

## System Safety Process



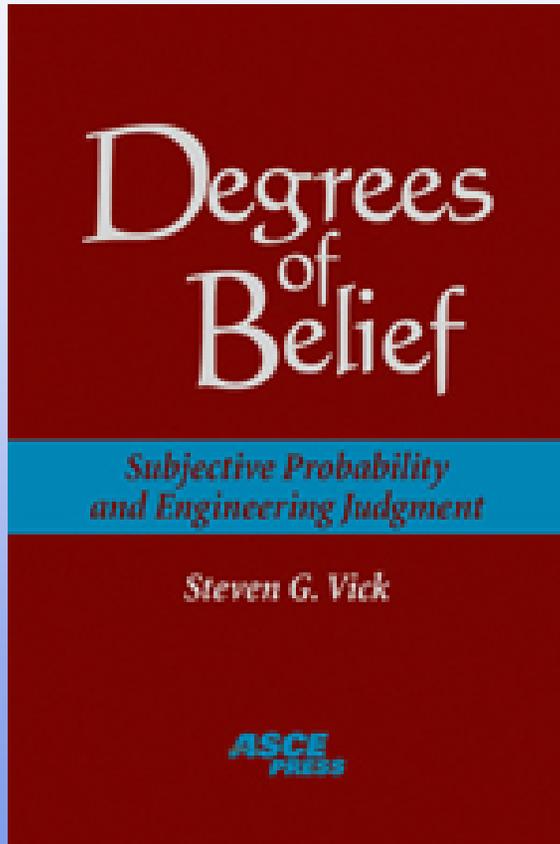
**FAA SRM  
Order  
8040.4**

Source: <http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm>

# A Safety "Belief"

## Degrees of Belief: Subjective Probability and Engineering Judgment

Steven Vick (ASCE Press, 2003)



"Safety itself is an internal construct, a concept and not a measurable quantity or any objective attribute of a structure...

Safety is inevitably a judgment that cannot be proven true by any method of deductive logic.

Safety resides in belief, and when we say that a structure is safe, this means we hold some sufficient degree of belief that it is" (p. 257).

# FAA Office of System Safety

RISK ASSESSMENT MATRIX

	Severity			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	High	Serious	Medium	Low
Probable				
Occasional				
Remote				
Improbable				

Source: <http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm>



# NASA Aviation Safety Program Projects

## *Vehicle Safety Technologies*



**Synthetic Vision Systems (SVS)**  
Make every flight the equivalent of clear-day operations

### **Single Aircraft Accident Prevention (SAAP)**

Self-healing designs and “refuse-to-crash” aircraft

### **Accident Mitigation (AM)**

Increases survivability when accidents and aviation fires occur

## *Weather Safety Technologies*



### **Weather Accident Prevention (WxAP)**

Brings intelligent weather decision-making to every cockpit

### **Aircraft Icing (AI)**

Eliminate icing as an aviation hazard

## *System Safety Technologies*



### **Aviation System Monitoring & Modeling (ASMM)**

Monitor and assess all data from every flight for known & unknown issues

### **System-Wide Accident Prevention (SWAP)**

Improves human/machine integration in design, operations, & maintenance



# AvSP Product Dictionary

## Accident Mitigation (AM)

- Next Generation Crash Analysis Codes
- Energy Absorbing Seat, Restraints and Structures
- Next-Generation Crashworthiness Design Guidelines
- Fuel Tank Fire Prevention and Fire Suppression System Technologies
- Cargo Hold Fire Detection and Detection Design Guidelines
- Elevated Flash Point Fuel Technologies

## System-Wide Accident Prevention (SWAP)

- Human Performance Models
- Crew Activity Tracking
- Pilot Skill Training for Cockpit Automation
- Training Modules and Simulators for General Aviation
- Instructor Training and Evaluation
- Maintenance Risk and Task Analysis Tools
- MRM Training Program for Maintenance
- Augmented/Virtual Reality Displays
- Human Factors Tools

## Synthetic Vision Systems (SVS)

- SV Technology for Commercial and Business Aircraft
- SV Technology for GA Aircraft
- World-Wide Geospatial Databases
- Runway Incursion Prevention Technologies

**Single Aircraft Accident Prevention (SAAP) => 9 products**

**Aircraft Icing (AI) => 7 products**

**Weather Accident Prevention (WxAP) => 7 products**

**Aviation System Modeling and Monitoring System (ASMM) => 6 products**

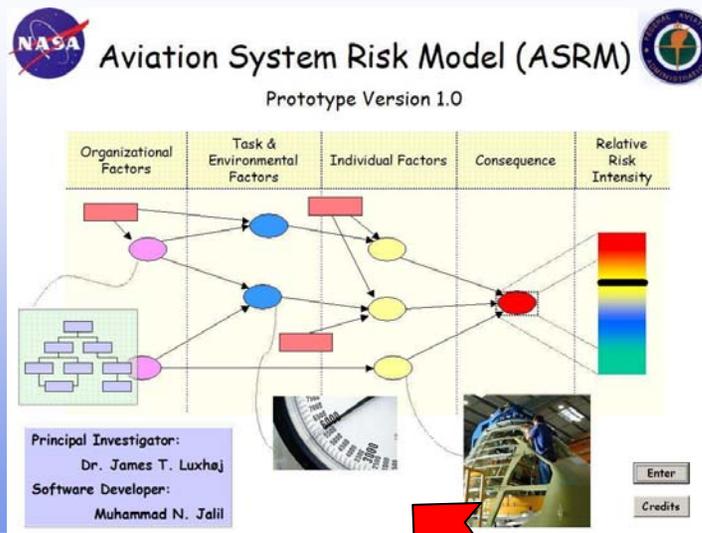
**48 Total Products**

Source: Jones and Reveley, June 2004



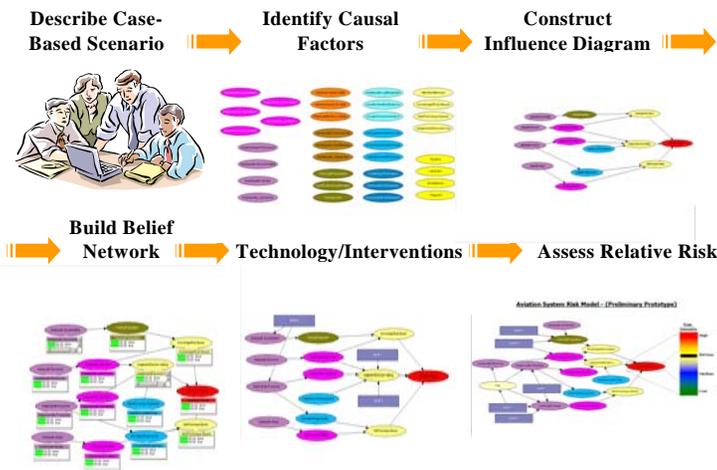
## Decision Support to Evaluate Technology Insertion - Research Objective -

- Provide a prototype capability that demonstrates the effectiveness of *risk mitigation strategies*, such as *technology insertions / interventions* in the National Airspace System (NAS).



## Analytical Modeling Approach

### Analytical Approach



Analytical Method

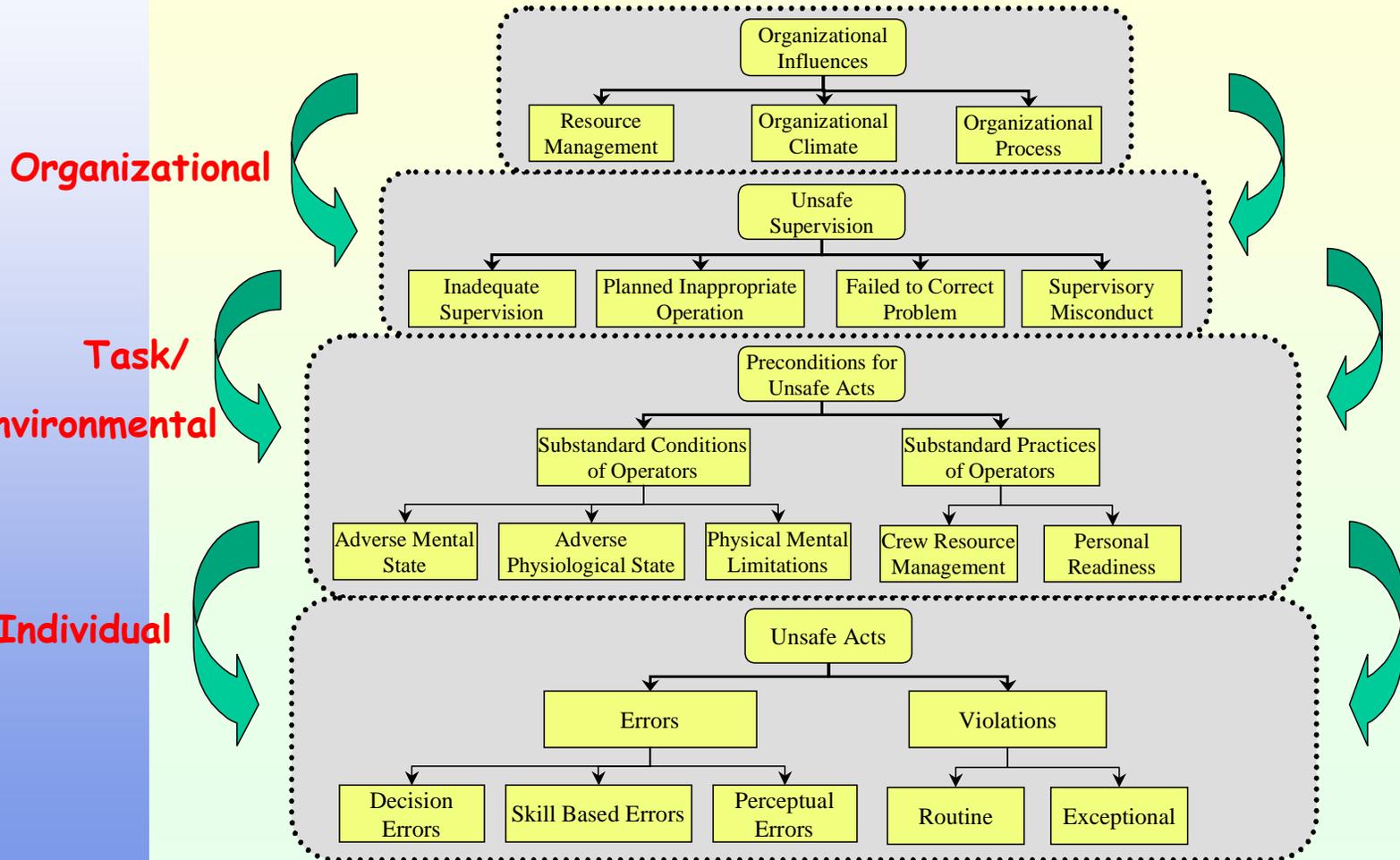
Decision Support Tool

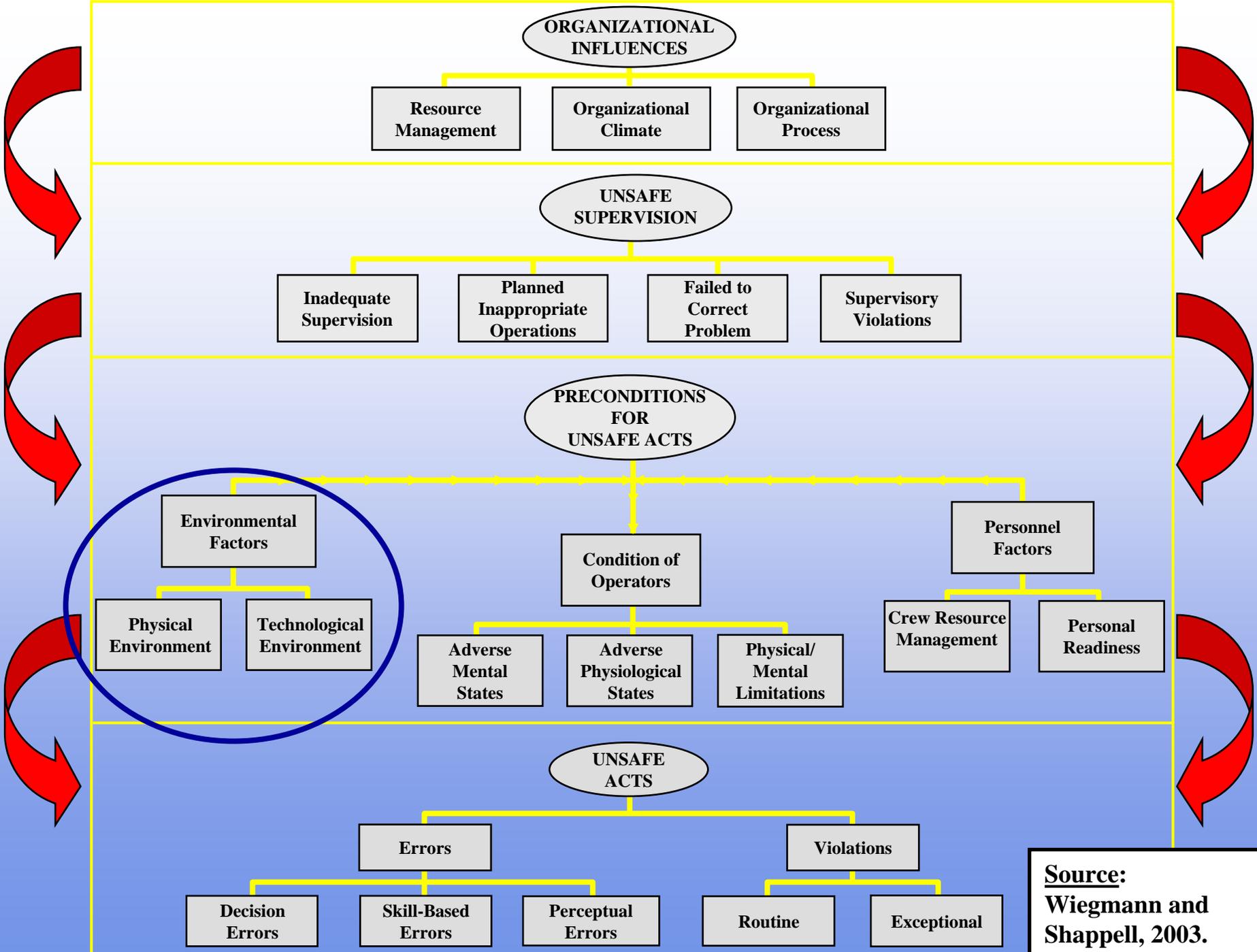
The primary cause of aviation accidents is aircraft striking the ground.

- *U.S. Army*  
~ 1920



# Human Factors Analysis and Classification System (HFACS) (Shappell and Wiegmann)

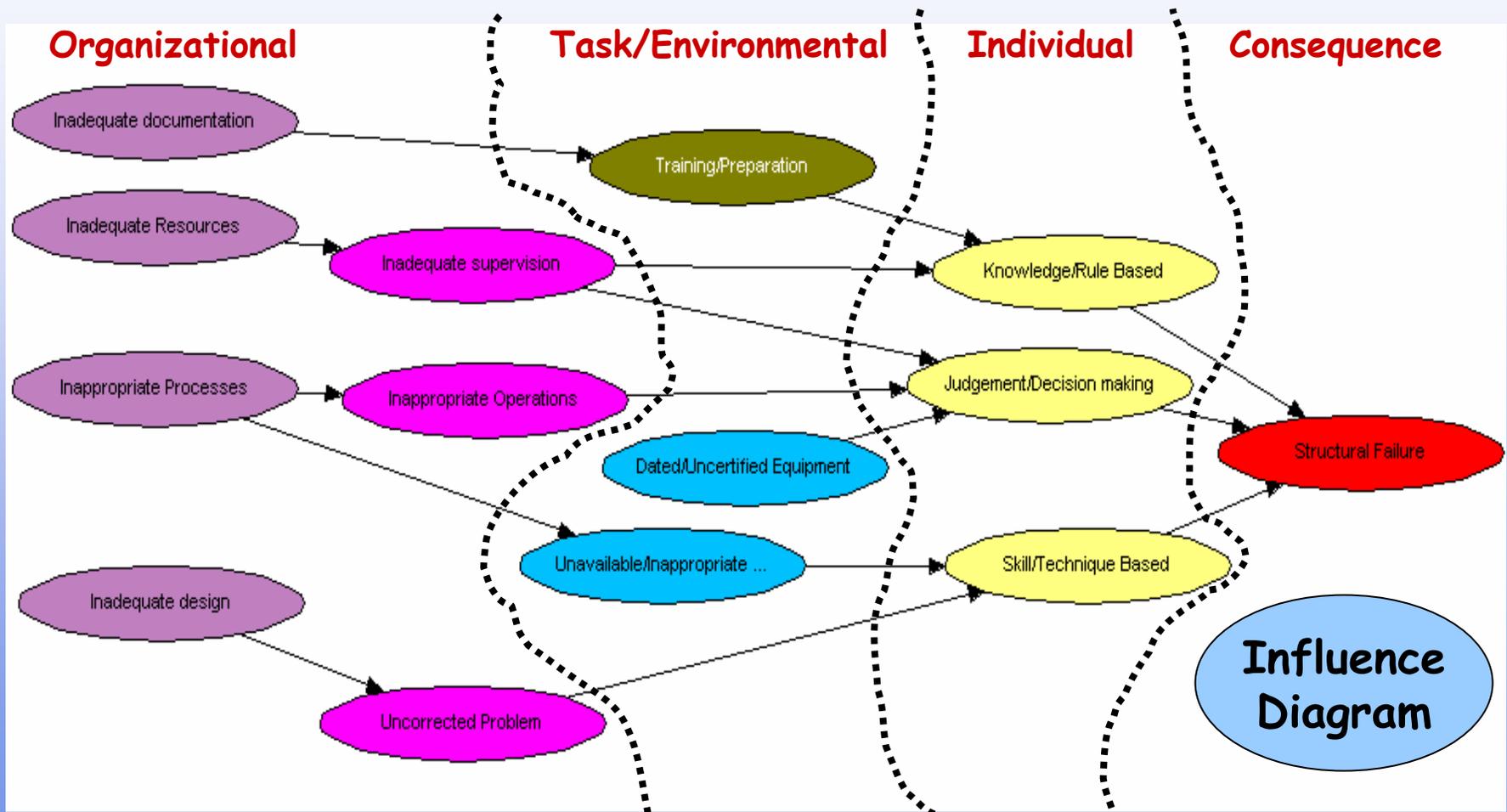




**Source:**  
**Wiegmann and**  
**Shappell, 2003.**

# Aviation System Risk Model (ASRM)

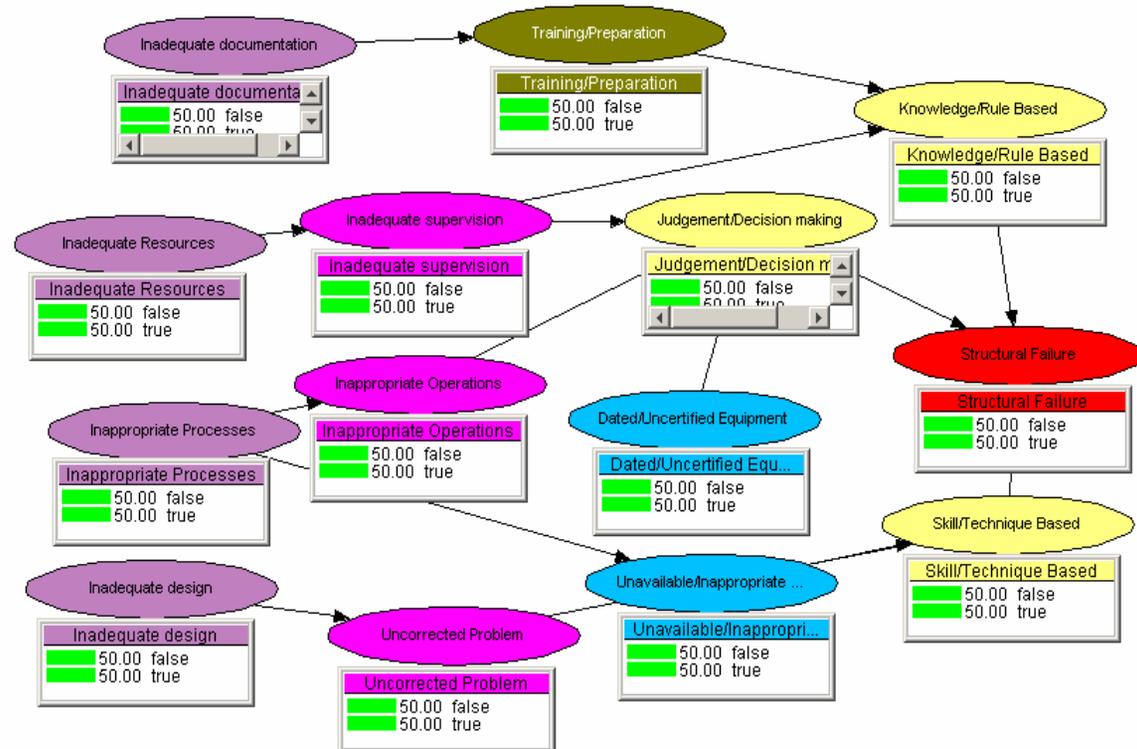
## Reason Socio-Technical Framework



# Baseline Probabilities

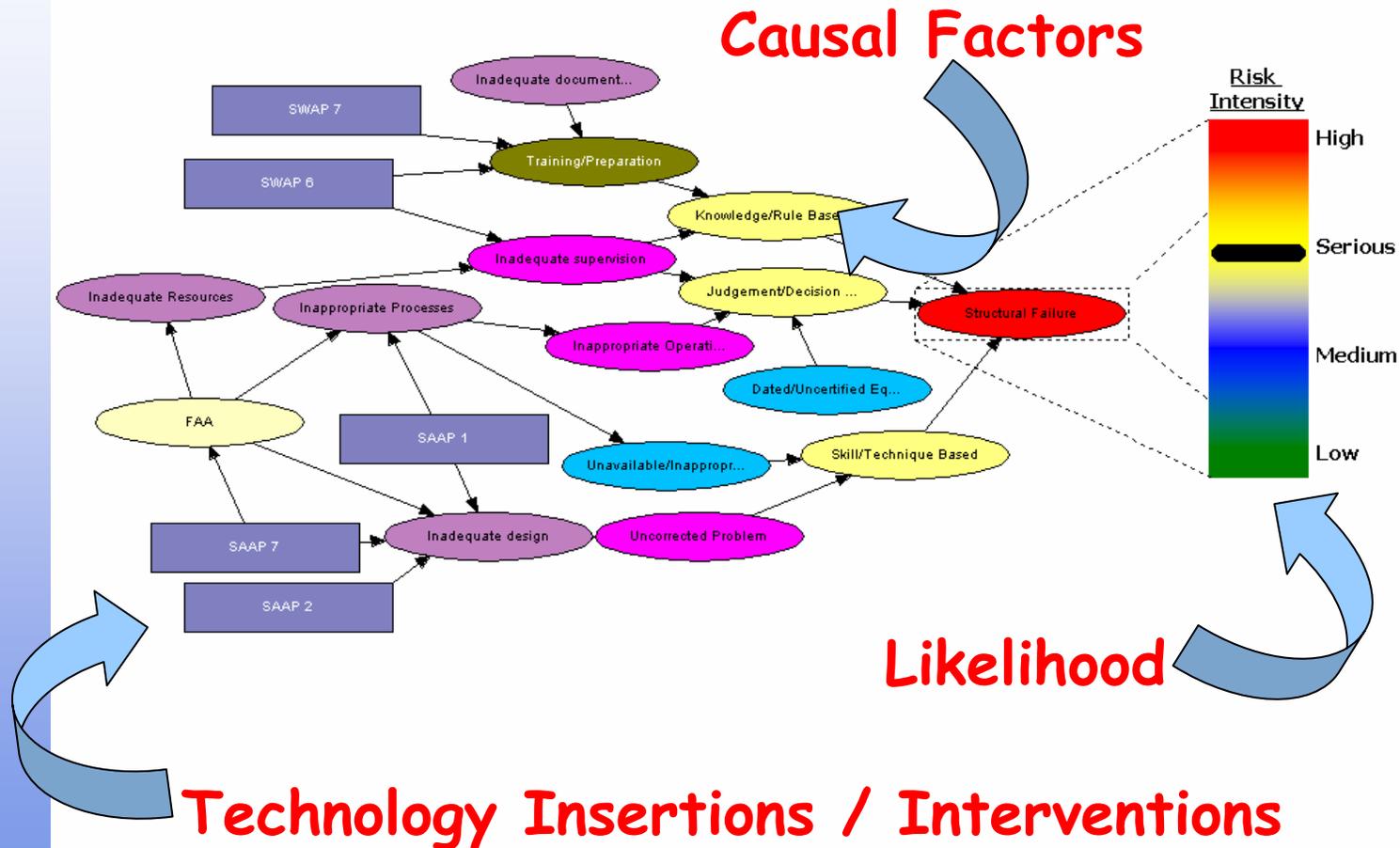
Organizational      Task/Environmental      Individual      Consequence

Bayesian Belief Network (BBN)



# Relative Risk "Intensity"

## Aviation System Risk Model - (Preliminary Prototype)



# Analytical Modeling Approach

## Analytical Approach

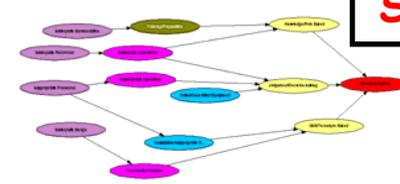
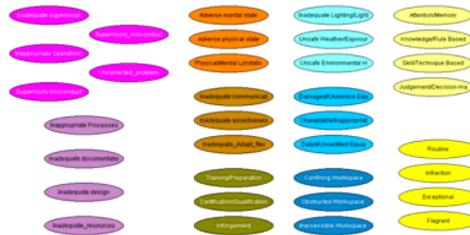
Describe Case-Based Scenario



Identify Causal Factors



Construct Influence Diagram



**Causal Structure**

Build Belief



Network

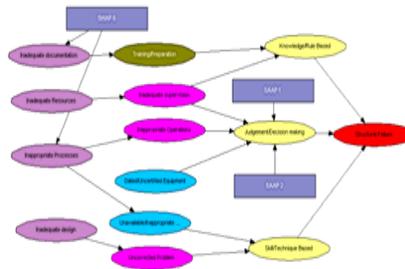
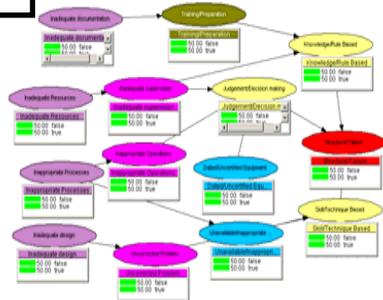


Technology/Interventions

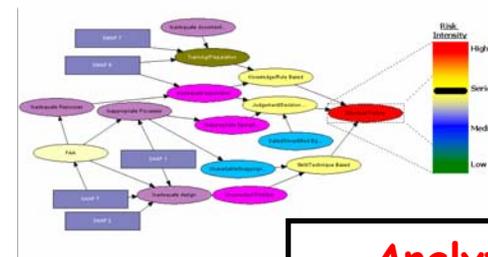


Assess Relative Risk

**Conditioning Context**



Aviation System Risk Model - (Preliminary Prototype)



**Analytic Generalization**

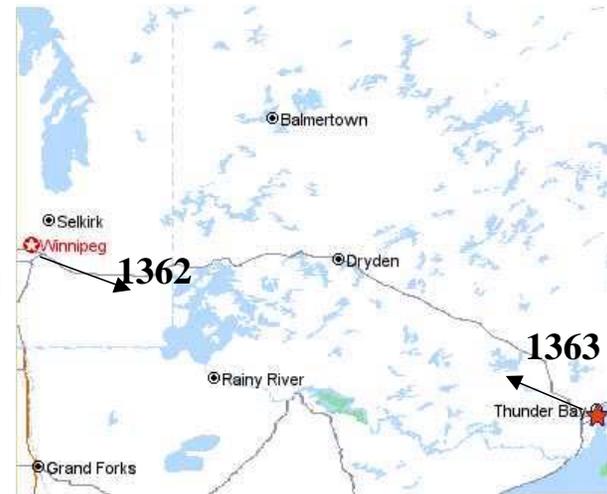


# Case-Based Scenario



## Air Ontario Flight 1363

- On March 10, 1989
- Winnipeg to Thunder Bay round trip with intermediate stops at Dryden (1362/1363)
- Poor weather conditions
- Casualties included 21 passengers and the crew including Capt. Morwood
- One of the largest systemic, organizational approaches to the investigation of an aviation accident



E. Kardes, K. Kauffeld



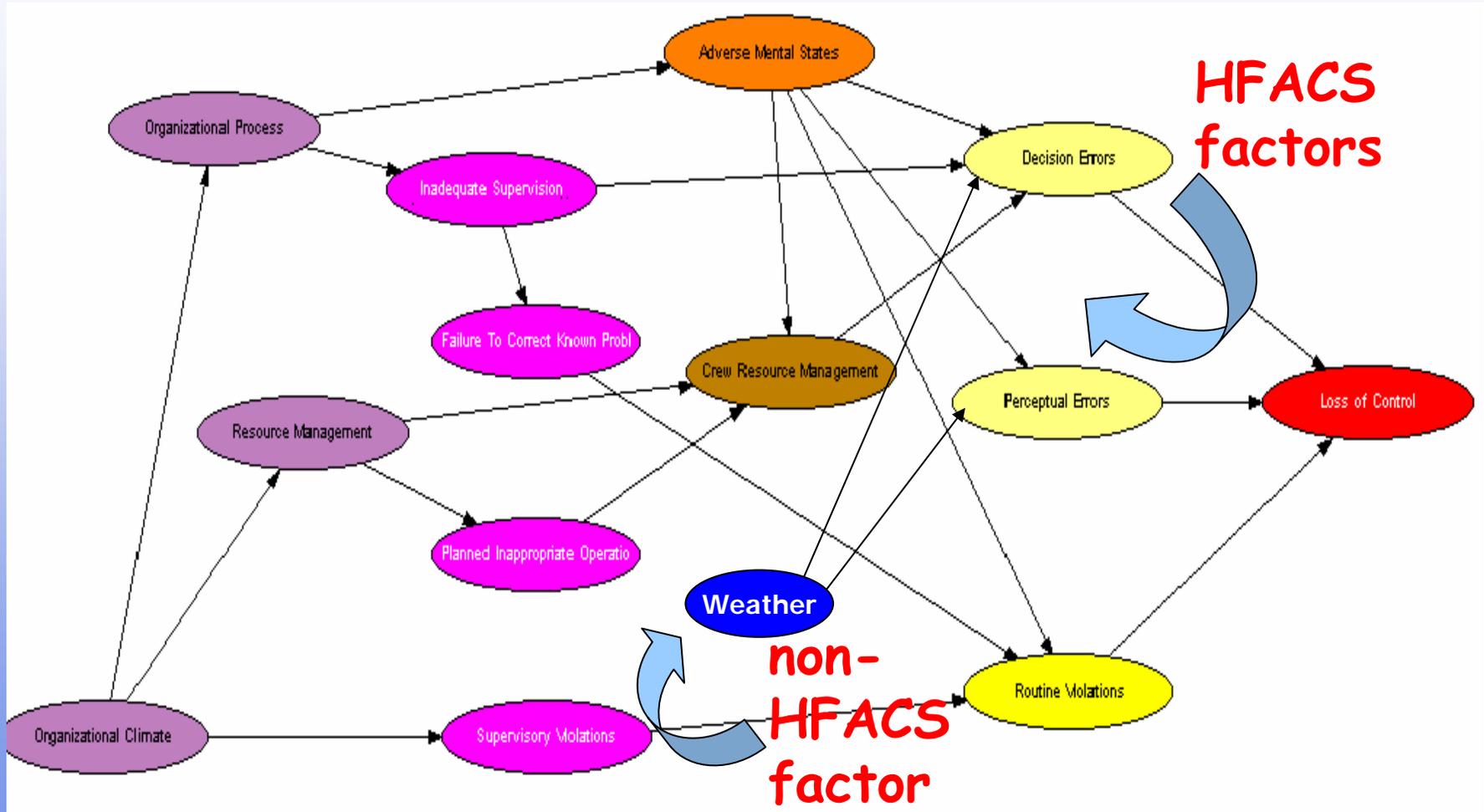
# Causal Factors Interactions

Organizational

Task/Environmental

Individual

Consequence





# Technology Insertion



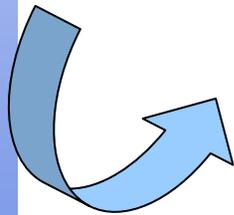
## Air Ontario Influence Diagram

CRM → Decision Errors

» **SWAP-1**

- » Software to predict human error due to inadequate crew coordination issues

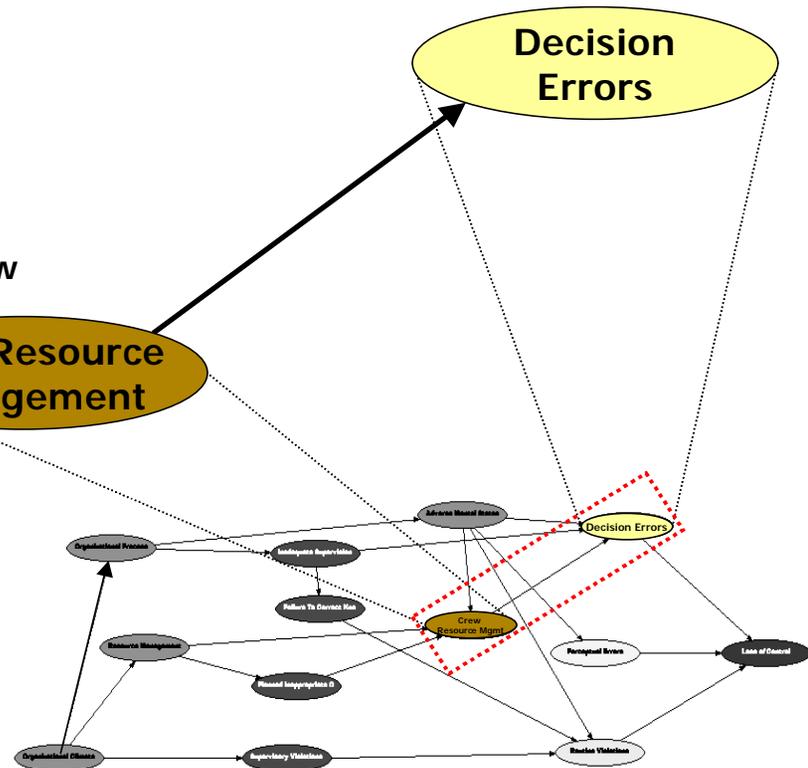
Technology Insertion



**SWAP-1**

Crew Resource Management

Decision Errors



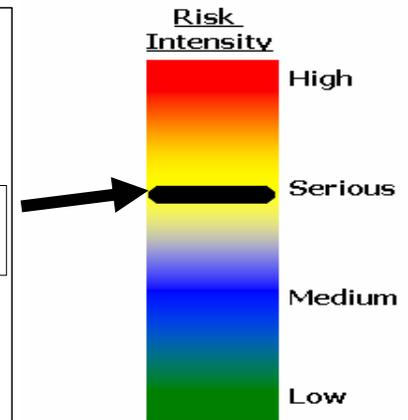
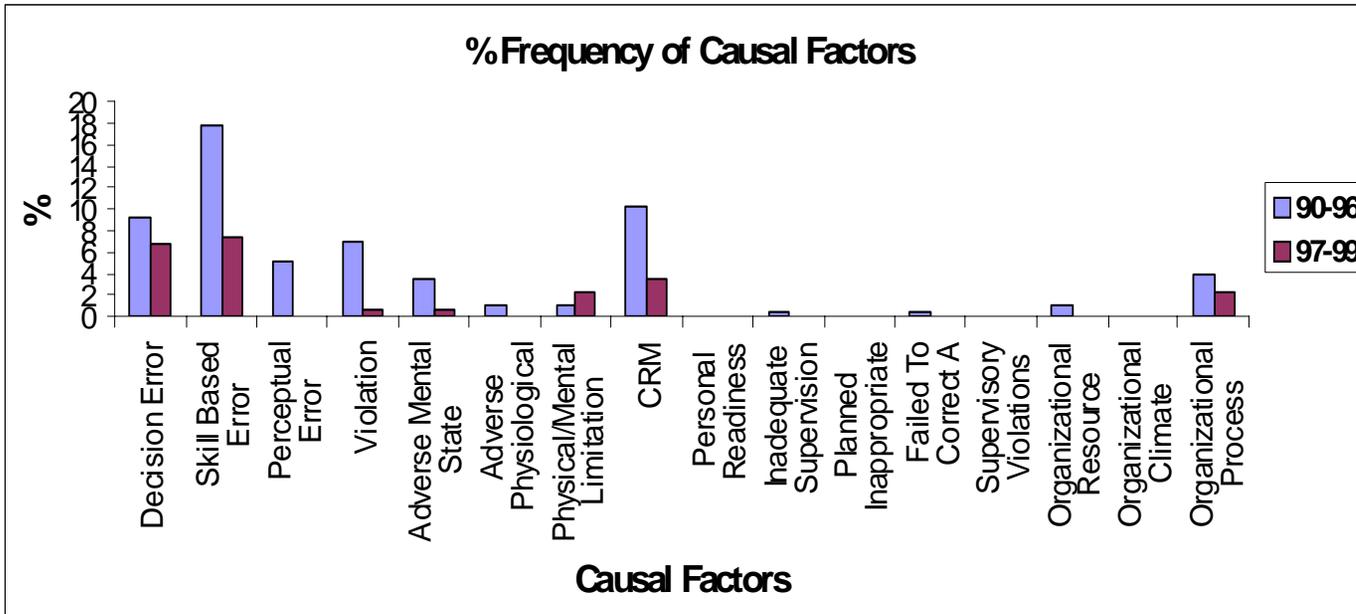
E. Kardes, K. Kauffeld



# Quantifying the Model - HFACS



## Baseline & Model Quantification



R. Kuru

**Baseline period is 1990-1996**



# SME Sessions (2003)



## SME Profiles

Location	Model	Contact	Dates
FAA's FSAIC, Dulles, VA	MAIN 1-4, LOC 1-4	Don Arendt, Rick Krens	July 8-9;28- 30; Aug. 4; 11-12; Sept. 15
FAA AEG, Seattle, WA	CFIT 1	Keeton Zachary	Aug. 11-14; Oct. 7-10
FAA FSDO, Pittsburgh, PA	CFIT 2,3	Al Zito	Sept. 9-11; Oct. 21-22



# SME Sessions (2004)



## SME Profiles

Location	Model	Contact	Dates
AOPA, Frederick, MD	GA 1-3	Bruce Landsberg	Jan. 22-23; July 7-8
FAA Office of Runway Safety	RI 1-2	Mike Lenz	Feb. 5-6; Feb. 20; June 8-9
FAA FSDO, Pittsburgh, PA	Engine 3, RI 3	Al Zito	June 17-18; July 28-29
FAA Transport Airplane Directorate, Seattle, WA	Engine 1	Bill Emmerling	Mar. 17-18
FAA Engine and Propeller Directorate, Burlington, MA	Engine 2	Ann Azevedo	May 25-26

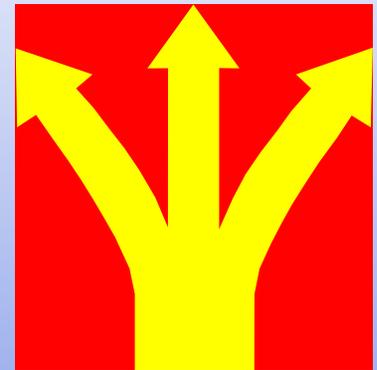
**Total of 20 Models**



# Case Study Research

- **Analytic Generalization** - not statistical sampling, but generalizing findings to theory (i.e. *replication logic*, see Yin, 1994, 2003; Rasmussen, 1993)
- **Case Study research quality:**
  - construct validity
  - internal validity
  - external validity
  - reliability

Induction



# Probability Interpretations (Vick, 2002, p. 10)

<i>Attribute</i>	<i>Relative frequency</i>	<i>Subjective, degree-of-belief</i>
<i>Applies to</i>	Repeatable occurrences	Single-event or repeatable occurrences
<i>Based on</i>	Data statistics	State of knowledge
<i>Measure of</i>	Stable long-run frequency	Belief or confidence
<i>Property of</i>	The event	The observer
<i>Reasoning used</i>	Deductive	Inductive
<i>Information incorporated</i>	Measured data	Data and/or other knowledge
<i>Subjective factors</i>	Implicit or external	Explicitly incorporated
<i>Criteria for validity</i>	Statistical rules	Actual beliefs and coherence with probability axioms
<i>Uniqueness</i>	Singular value exists in principle	No singular value exists



# LOC Case Studies

Case	Descriptor	Main Feature	Possible Technology Insertion
<b>Air Ontario Flight 1363</b> <ul style="list-style-type: none"> <li>Fokker-28</li> <li>Dryden, Ontario, Canada, March 10, 1989</li> </ul>	<b>Loss of control due to improper de-icing.</b>	<ul style="list-style-type: none"> <li>Surface contamination of the wings</li> <li>Combination of several related factors</li> <li>Lack of guidance on the need for de-icing</li> <li>Regulatory failure of Transport Canada arose from deep-rooted systemic failures</li> </ul>	ASMM - 1,2,3,4,5,6 SWAP - 1,2 SAAP - 4 WxAP - 1,2,3,4 AI 4,5,7
<b>Fine Air Flight 101-A</b> <ul style="list-style-type: none"> <li>Douglas DC-8-61</li> <li>Miami, Florida, Aug 7, 1997</li> </ul>	<b>Loss of control due to improper loading.</b>	<ul style="list-style-type: none"> <li>Improper aircraft weight and balance</li> <li>Failure of Fine Air to exercise operational control over the cargo loading process</li> <li>Failure of Aeromar to load the airplane as specified by Fine Air</li> <li>Failure of FAA to adequately monitor Fine Air's cargo loading process</li> </ul>	ASMM - 1,2,5,6 SWAP - 1,2 SAAP - 7
<b>US Air Flight 405</b> <ul style="list-style-type: none"> <li>Fokker-28-4000</li> <li>Flushing, NY, Mar 22, 1992</li> </ul>	<b>Loss of control due to improper de-icing.</b>	<ul style="list-style-type: none"> <li>Lack of criteria regarding the effective holdover time for Type I de-icing fluid</li> <li>Delays after de-icing</li> <li>Inadequate crew coordination and adverse mental state of the crew due to tight scheduling</li> </ul>	SWAP – 1,2,3,5 ASMM – 1,2,4,5,6 WxAP – 1 AI 1,2,3,4,5,6,7
<b>Atlantic Southeast Flight 2311</b> <ul style="list-style-type: none"> <li>Embraer Brasilia, EMB-120RT</li> <li>Brunswick-Glynco Jetport, GA, April 5, 1991</li> </ul>	<b>Loss of control due to deficient design.</b>	<ul style="list-style-type: none"> <li>Malfunction of the left engine PCU</li> <li>Deficient design of the PCU by Hamilton Standard and approval by the FAA</li> </ul>	ASMM – 5 SAAP – 3,7

# ASRM - LOC

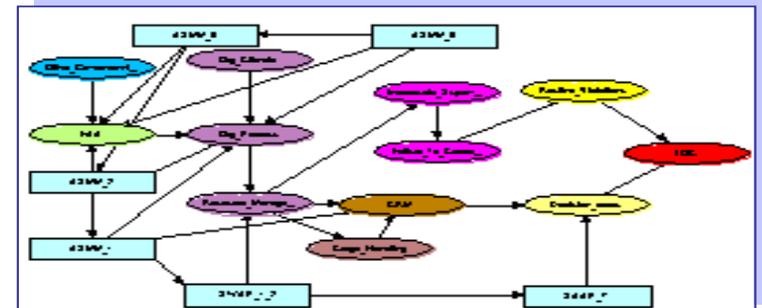
Complete documentation on each case

## LOC Models

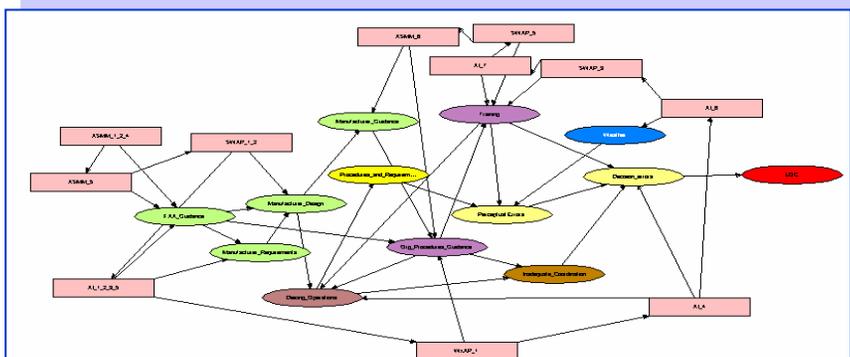
AO 1363



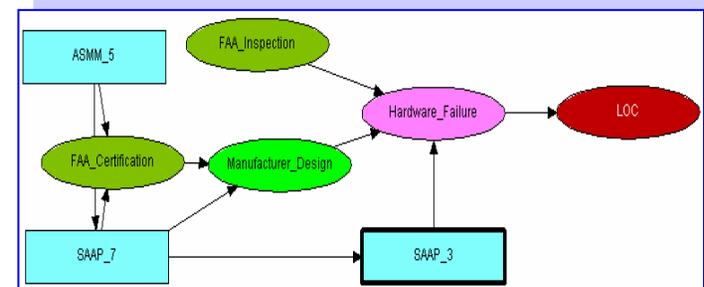
FA 101



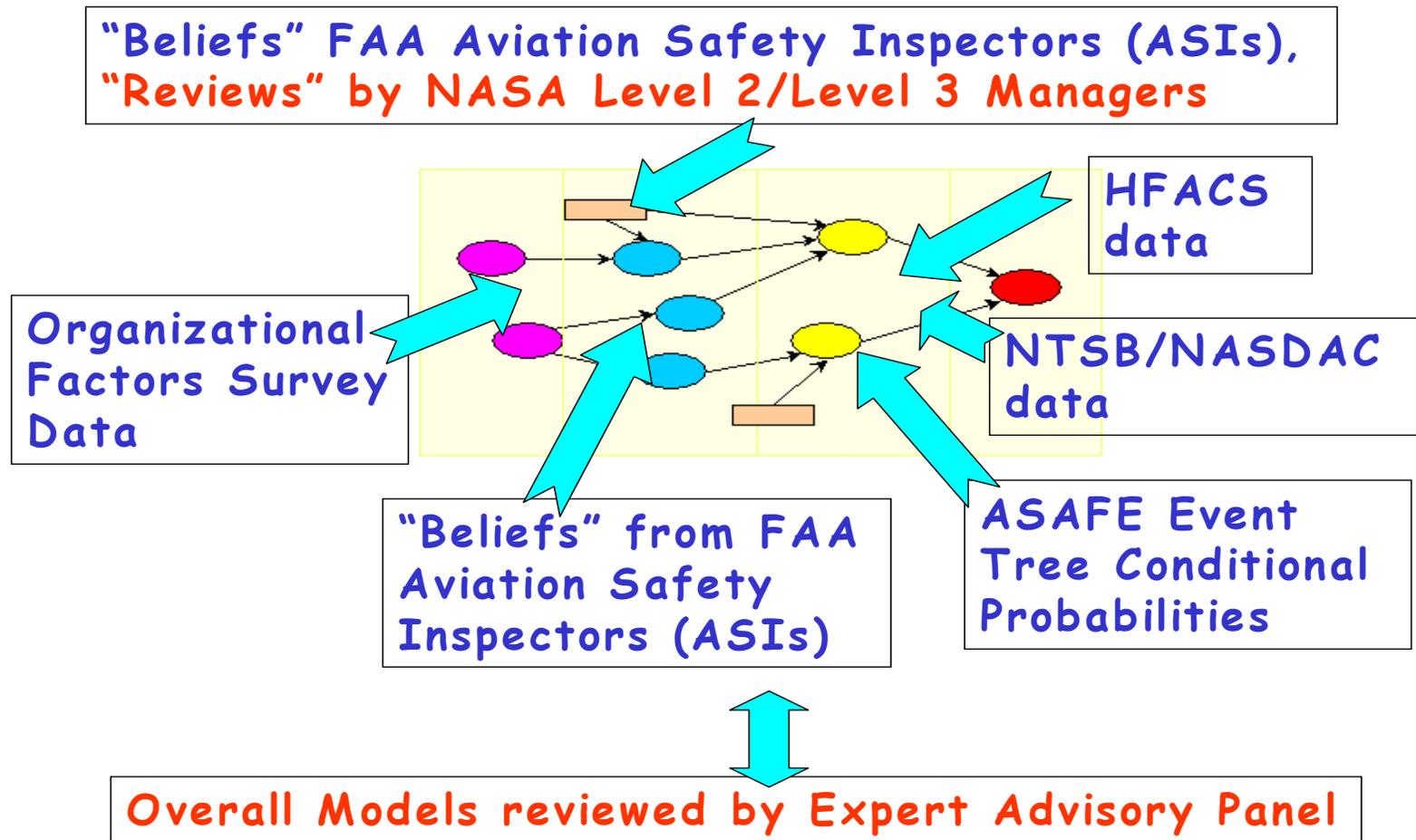
UA 405



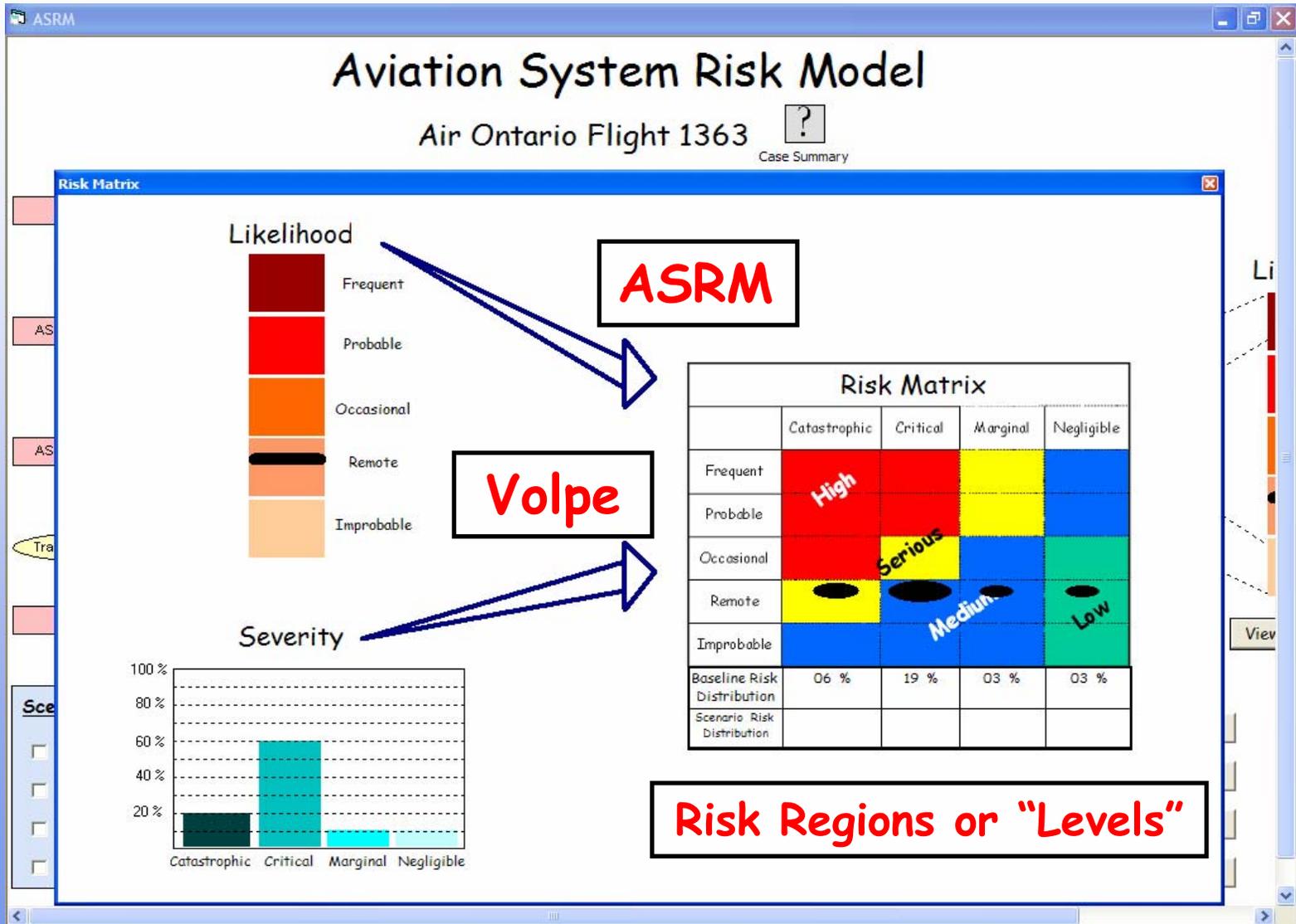
ASE 2311



# Multiple Sources for Belief Assessments



# "Representative" Severity



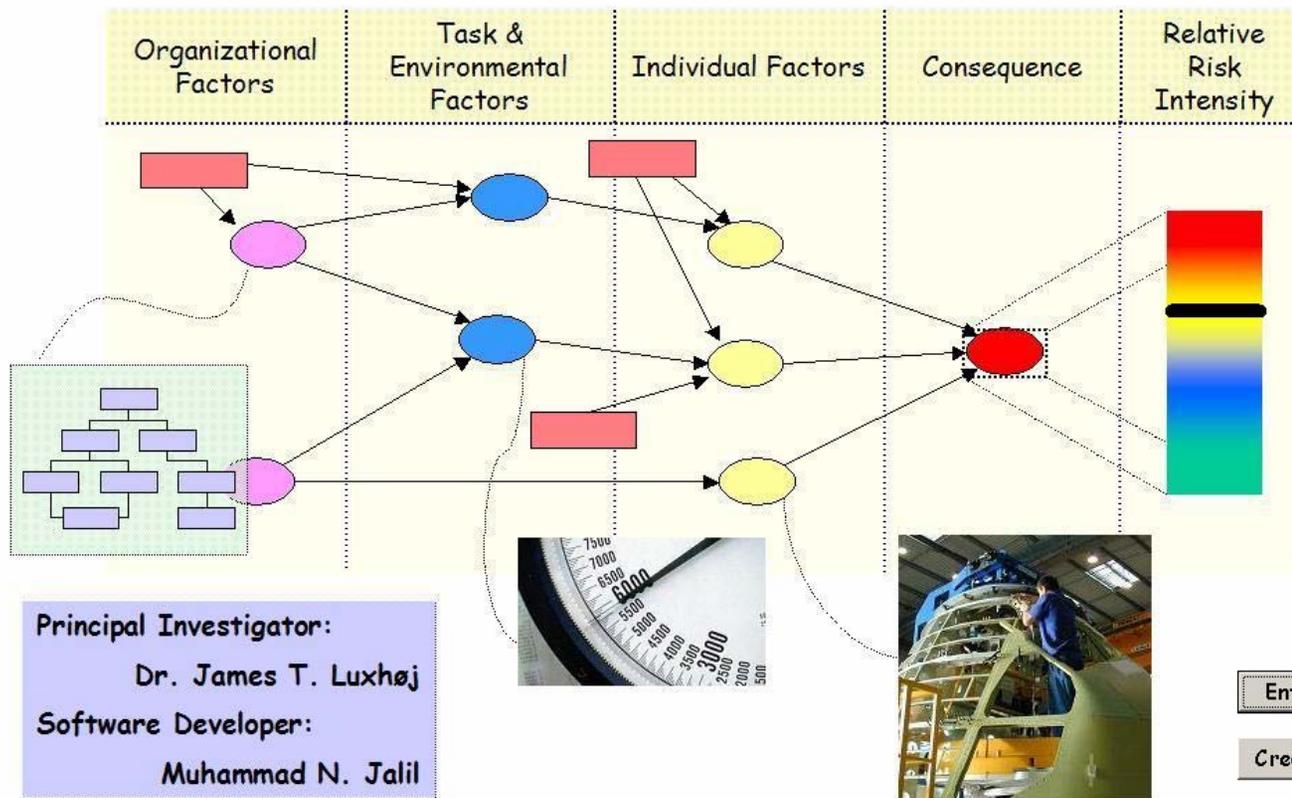
# ASRM Prototype

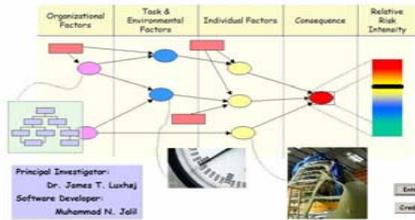


## Aviation System Risk Model (ASRM)

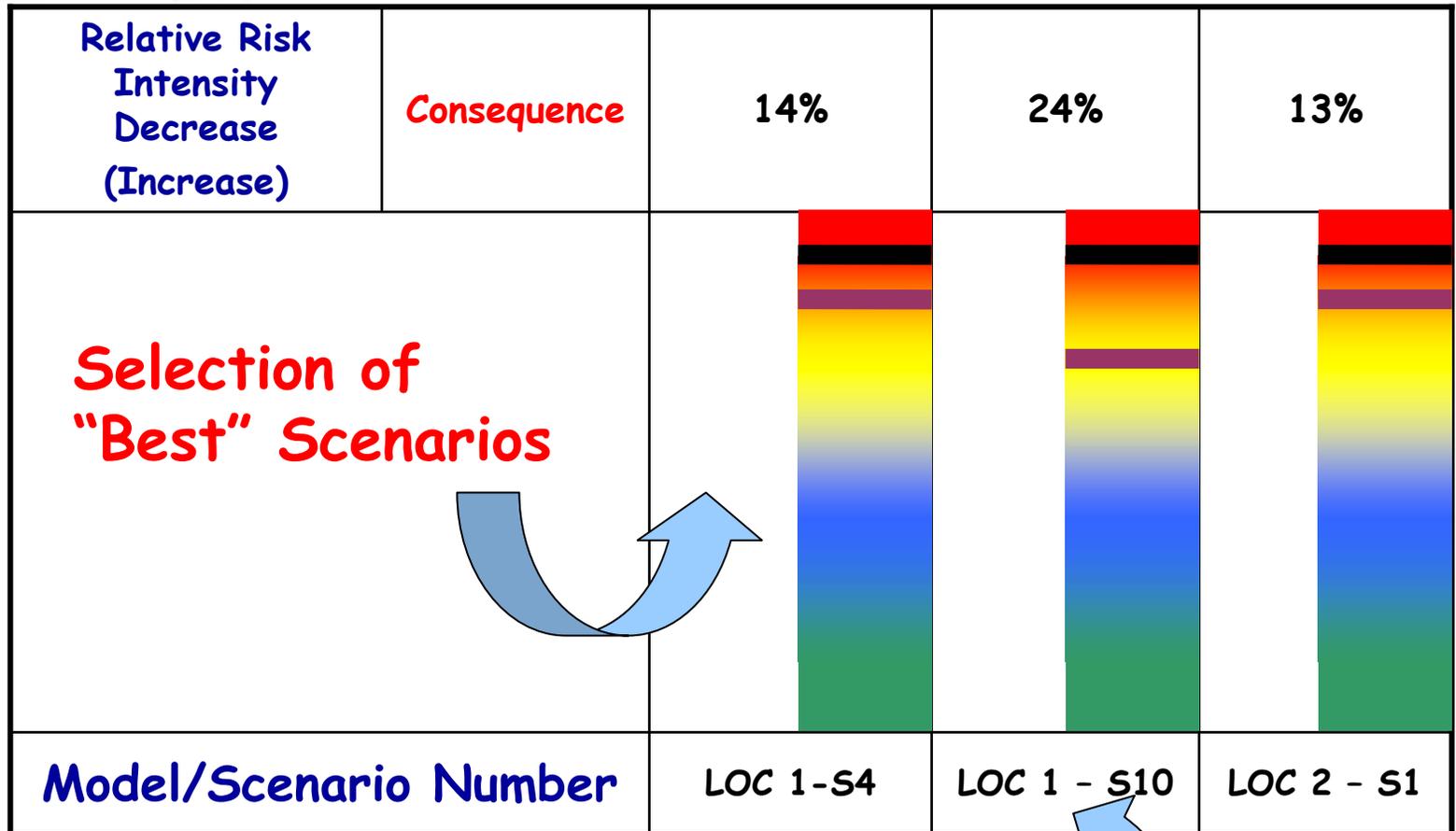


Prototype Version 1.0





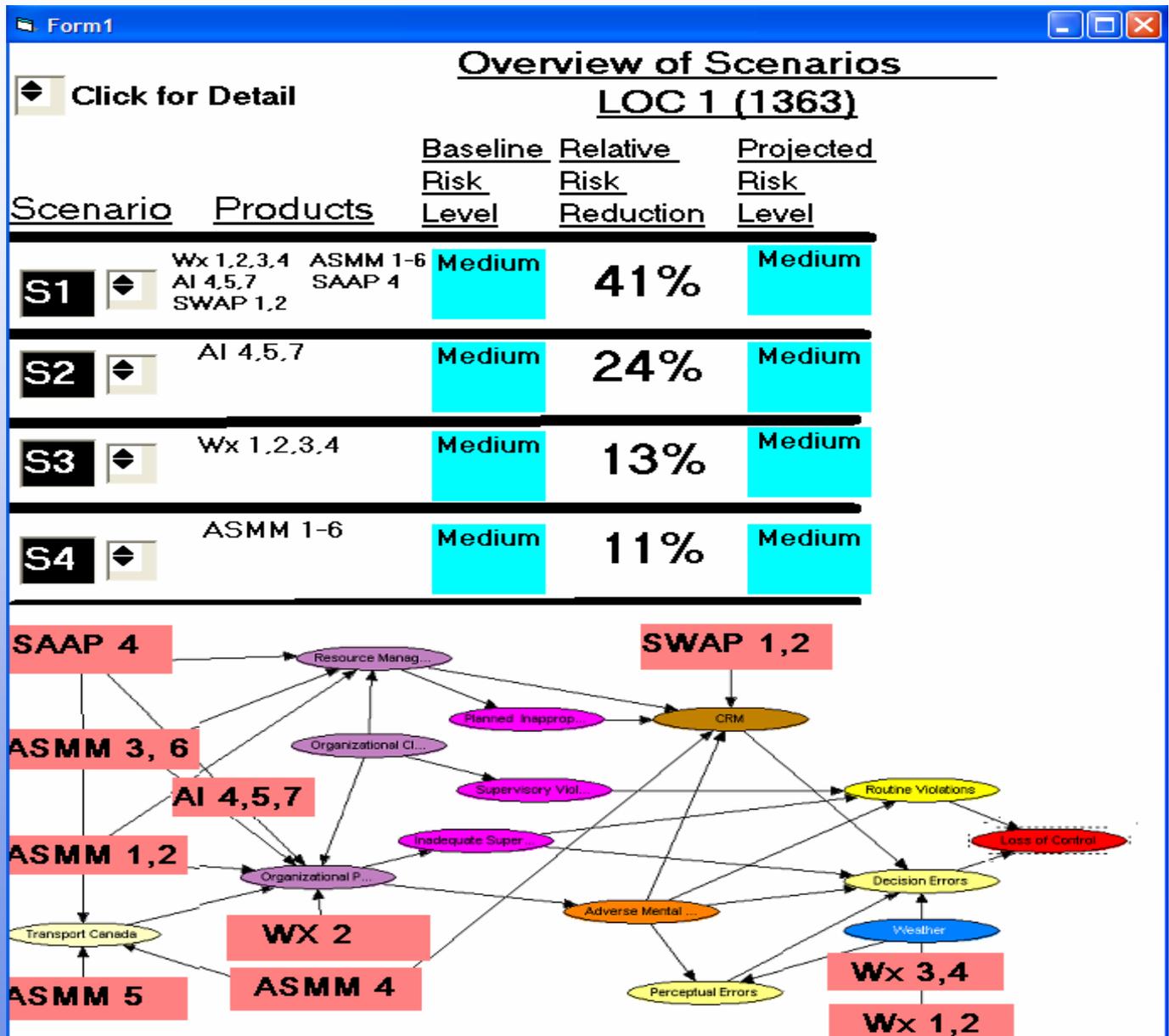
# ASRM - Executive Summary



"drill down" to scenario details

# Executive Summary

*Scenario* =  
different  
combinations  
of risk  
mitigations



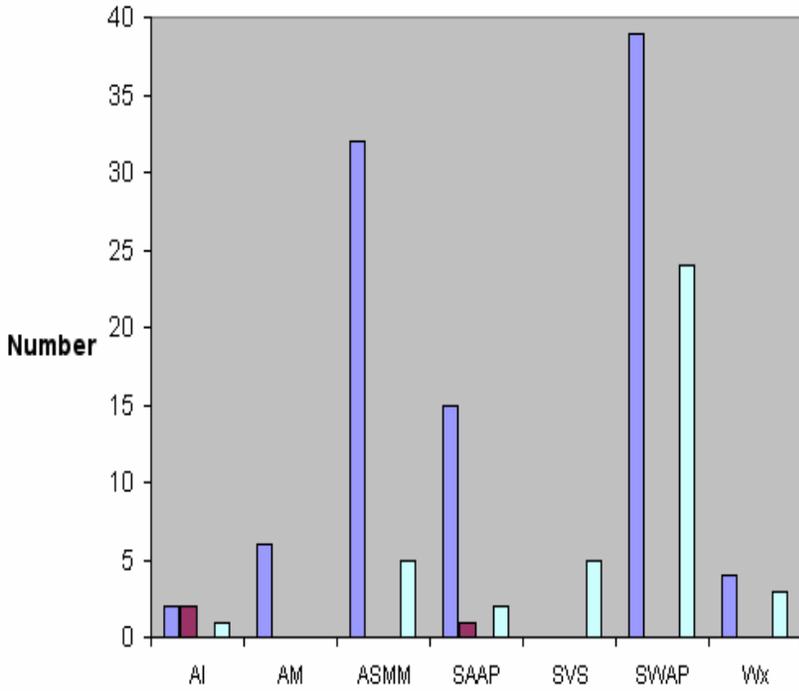
# "Within Case" Scenario Analyses

## Partial Results for LOC 1363 Case

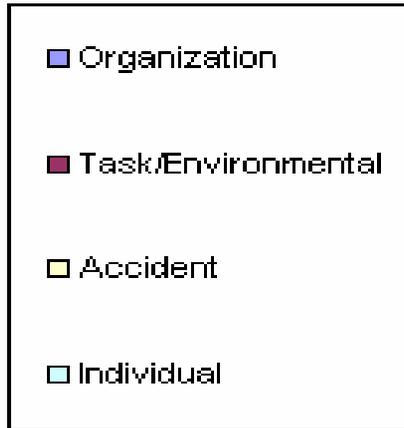
Description	Scenario	Targeted causal factor(s)	Technology element(s) inserted	Relative % Decrease or (Increase) on Factors	Risk Intensity (Consequence)	Relative % Decrease or (Increase) on Consequence
<b>Baseline scenario</b>	No technology intervention	----	----	-	<b>31%</b>	-
LOC 1 Scenario 1	ASMM suite	<ul style="list-style-type: none"> <li>• Regulator</li> <li>• Org. Process</li> <li>• Res. Mgmt.</li> <li>• CRM</li> </ul>	ASMM 1,2,3,4,5,6	<b>17%</b> <b>20%</b> <b>30%</b> <b>14%</b>	<b>28%</b>	<b>9%</b>
LOC 1 Scenario 4	WxAP suite	<ul style="list-style-type: none"> <li>• Org. Process</li> <li>• Decision Errors</li> </ul>	WxAP 1,2,3,4	<b>2%</b> <b>26%</b>	<b>27%</b>	<b>14%</b>
LOC 1 Scenario 8	Effect of intervention on Org. Process	<ul style="list-style-type: none"> <li>• Org. Process</li> </ul>	WxAP 2, SAAP 4, ASMM 1,2,3,6	<b>23%</b>	<b>28%</b>	<b>10%</b>

# "Across Case" Analyses

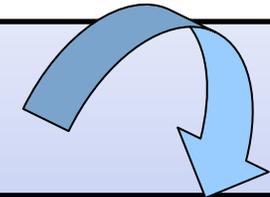
Parents vs. Factor



## Causal Factor "Clusters"



Across All Accident Models



Gap Analysis

## Technology Products

Node Name	Technology Name	AI_1_2_3_5	AI_4	AI_6	AI_7	AM_1	ASMM_1	ASMM_1_2	ASMM_1_2_4	ASMM_2	ASMM_3_6
Air_Carrier_WS							1				
AMS							1	1			1
APS									1		
CRM			1								1
DE					1		2			1	
Deicing_Ops					1						
Design_Tech_Environ											
Environ_Cond											
Exceptional_Violations			1								
FAA											

Source: Greenhut and Luxhøj, 2004



# ASRM "Tool Kit"

- Product Support Tool (PST) - Table of Contents slide provides links to Multimedia and Product Dictionary for each Technology

Technology Multi-Media Tool

### Descriptions in Excel

Accident Mitigation

System Wide Accident Prevention

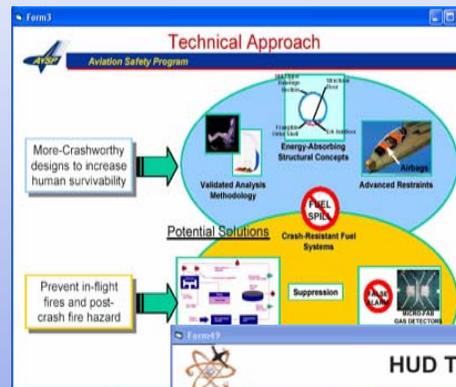
Single Aircraft Accident Prevention

Aviation System Monitoring and Modelling

Weather Accident Prevention

Aircraft Icing

Synthetic Vision



### Candidate Implementation #2

Scanning Weather Radar (WxR)

Summary of [Annex 8.09]

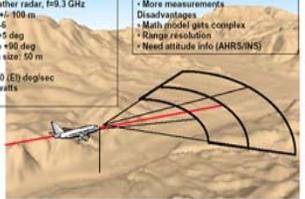
- Interleave measurements of weather and surface
- Proof-of-concept using Allied Signal RDR-4B
- Coherent pulsed weather radar, F9.3 GHz
- Measurement error: +/-100 m
- Pd: 0.9999, Pfa: 10^-5
- Elevation coverage: -25 to +5 deg
- Az coverage: -90 to +90 deg
- Range bins: 384, Bin size: 50 m
- Pulse width: 330 ns
- Scan rate: 30 (Az), 30 (E) deg/sec
- Output power: 100 watts
- Range: ~10 nmi

Advantages

- Patented and tested using COTS WxR
- No additional equipment
- More measurements

Disadvantages

- Math model gets complex
- Range resolution
- Need altitude info (AHR/INS)

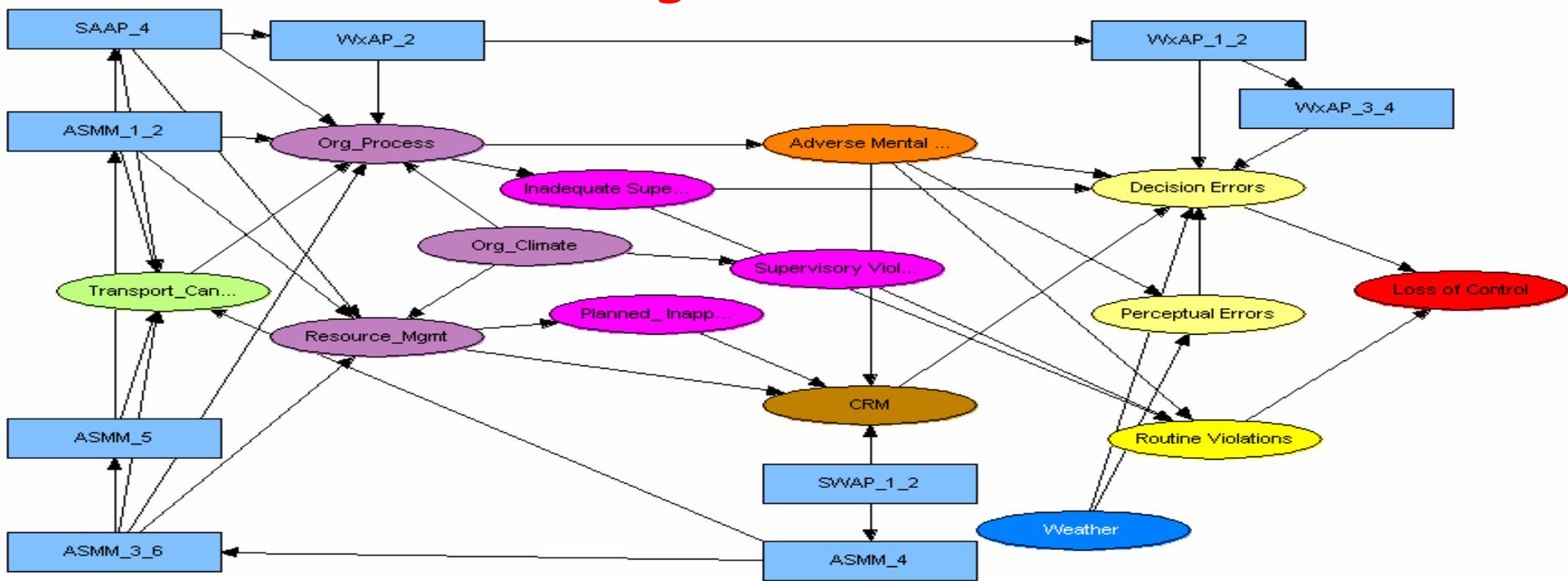


\*For terrain, elevation angle set to flight path angle  
\*\*For terrain, azimuth scan is -15 to +15 degrees



# Probability Elicitations

## Influence Diagram for LOC Case



Total number of

Nodes

14

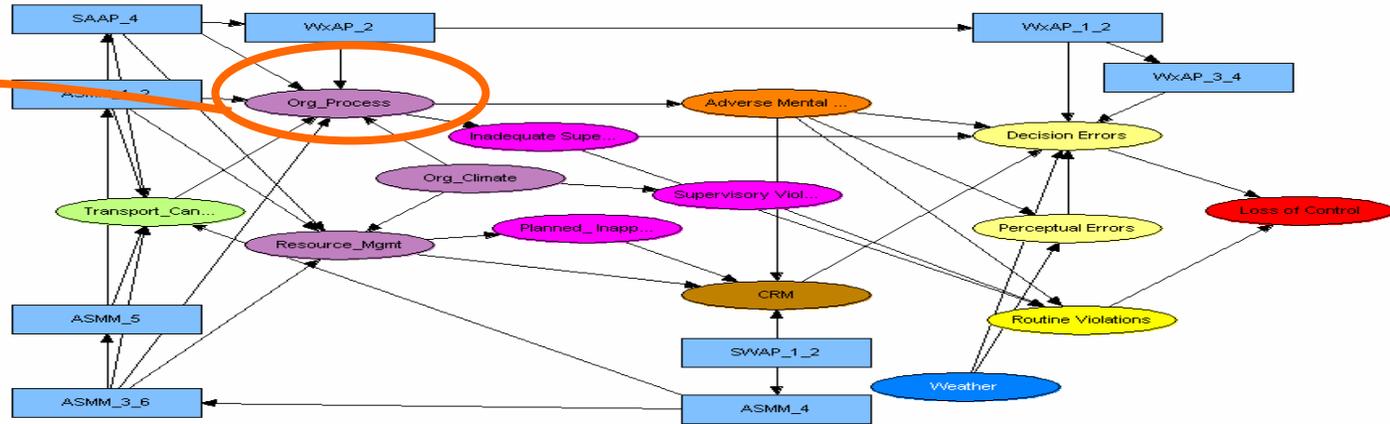
Products

9

Probabilities to be elicited

512

# Conditional Probability Table (CPT)



*Organizational Processes*

Organ\_Process    Labelled    Org\_Process

WxAP_2	Present															
SAAP_4	Present															
ASMM_3_6	Present								Absent							
ASMM_1_2	Present				Absent				Present				Absent			
Transport_Can...	Factor		Not a factor		Factor		Not a factor		Factor		Not a factor		Factor		Not a factor	
Org_Climate	Factor	Not a f...	Factor	Not a f...	Factor	Not a f...	Factor	Not a f...	Factor	Not a f...	Factor	Not a f...	Factor	Not a f...	Factor	Not a f...
Factor	0.616	0.154	0.616	0.154	0.736	0.184	0.736	0.184	0.656	0.164	0.656	0.164	0.776	0.194	0.776	0.194
Not a factor	0.384	0.846	0.384	0.846	0.264	0.816	0.264	0.816	0.344	0.836	0.344	0.836	0.224	0.806	0.224	0.806

Total number of

Parents

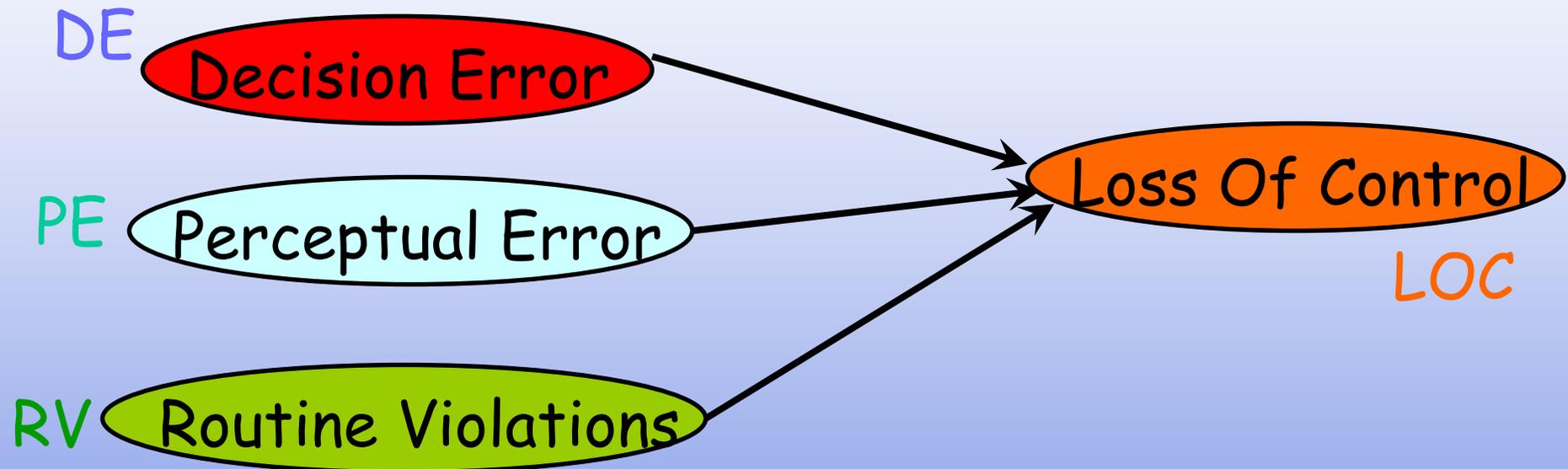
6

Probabilities to be elicited

128

# Relative Risk Ranking

Obtain a *relative risk ranking* for each parent node

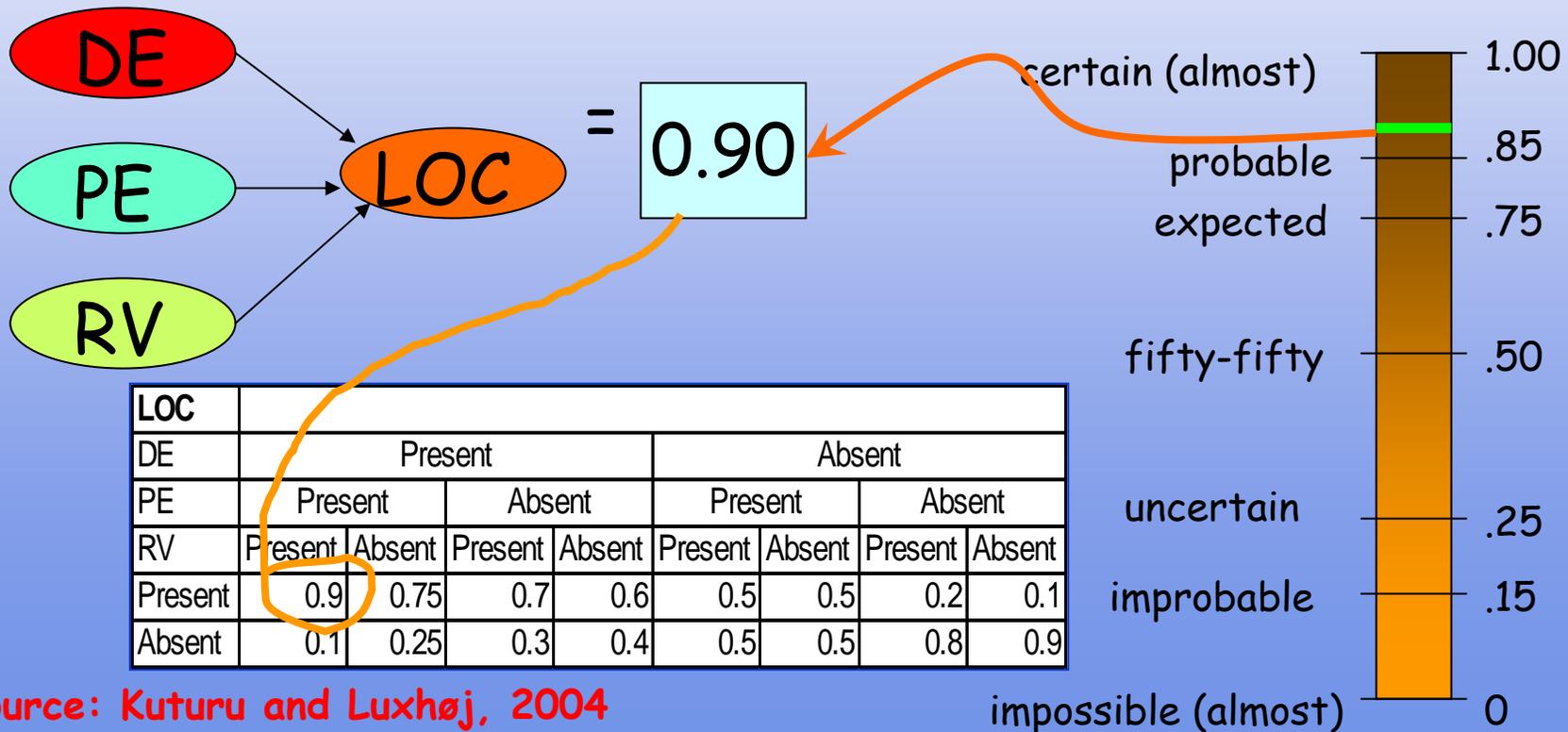


Rank	Conditional Probability
1	$P(\text{LOC}=\text{Y} / \text{RV}=\text{Y}, \text{PE}=\text{N}, \text{DE}=\text{N})$
2	$P(\text{LOC}=\text{Y} / \text{RV}=\text{N}, \text{PE}=\text{Y}, \text{DE}=\text{N})$
3	$P(\text{LOC}=\text{Y} / \text{RV}=\text{N}, \text{PE}=\text{N}, \text{DE}=\text{Y})$
4	$P(\text{LOC}=\text{Y} / \text{RV}=\text{N}, \text{PE}=\text{N}, \text{DE}=\text{N})$

# Belief Assessment in a Conditioning Context

In this **Contextual Domain**:

“There is evidence to suggest that an airline crew is experiencing **Decision Errors (DE), Routine Violations (RV) and Perceptual Errors (PE)**. *How likely* is it that such a crew experiences a **Loss of Control (LOC) accident?**” [UB=1, LB=0.75]



# ASRM Applications

## Analytical Approach

Describe Case-Based Scenario



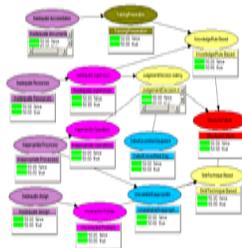
Identify Causal Factors



Construct Influence Diagram



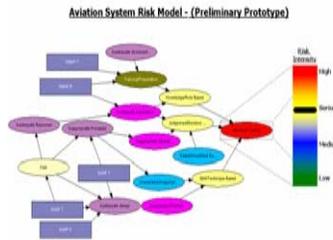
Build Belief Network



Insert Technology/Interventions



Assess Relative Risk



## Decision Support

Evaluate the Current Program

Influence Implementation Decisions

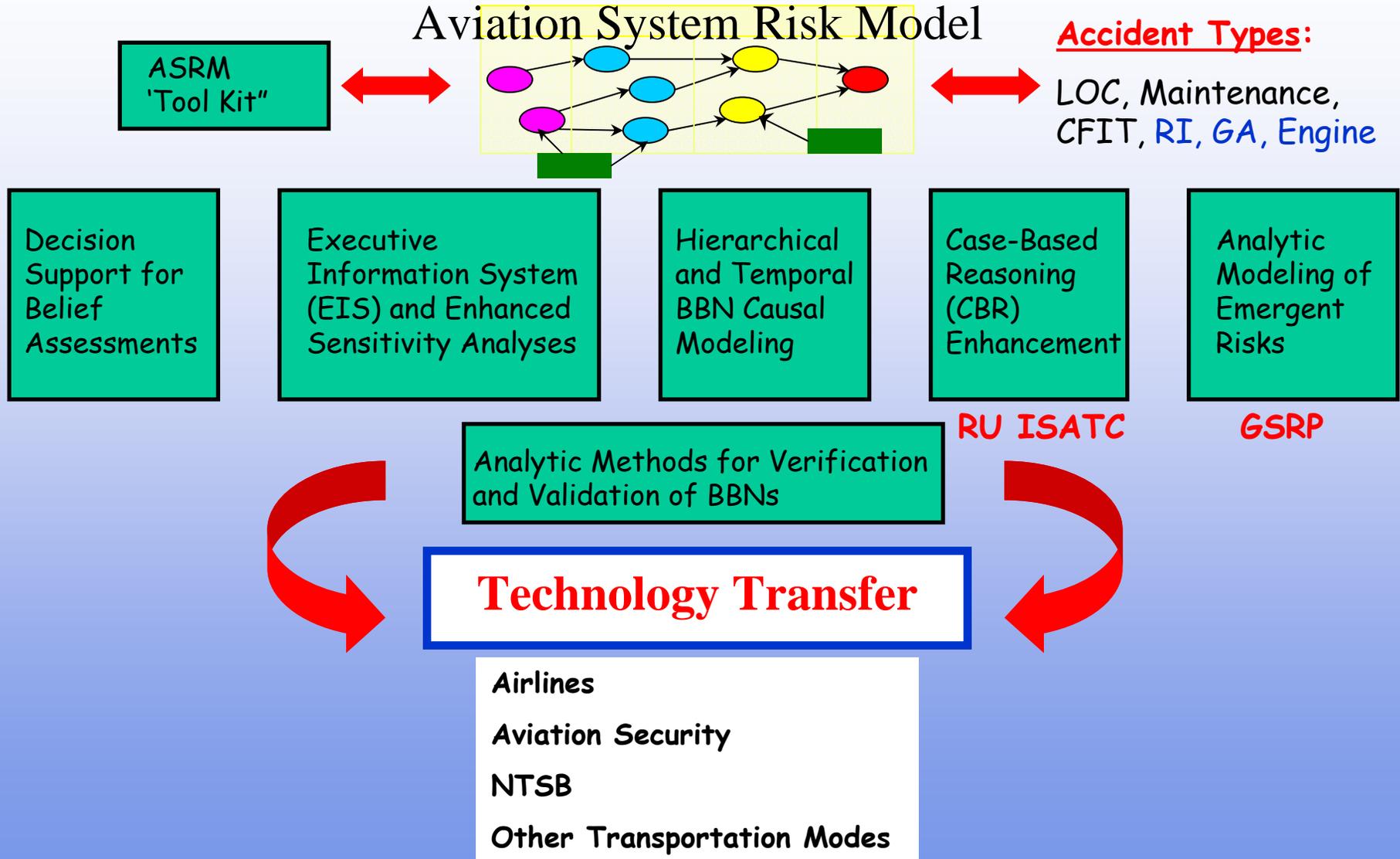
Develop the Business Case

# SME Session Outline/"Lessons Learned"

- **Warm-up** (introductions, review objectives/scope, SME backgrounds)
- **Initiation** (method summary, expected input by SMEs)
- **Review of Causal Diagram** (accident case summary, review/discuss causal connections, etc.)
- **Technology Insertions** ("filtering" process)
- **Probability Elicitations** (expert judgments)
- **Wrap-up** (remaining tasks, next meetings)

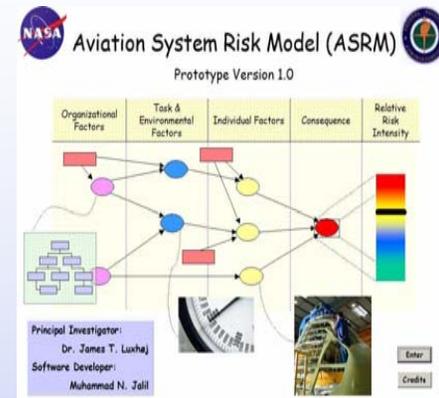


# Research Directions



# Further Remarks

- The ASRM provides an *analytical framework* for incorporating *both data and expert judgments* for projecting system risk and evaluating the impact of technology insertions/interventions.



*"I am confident that by working together with the aviation community, and using a more structured approach to the safety of aerospace systems, we will be successful in meeting the safety challenges of the next century of flight."*

Marion C. Blakey, FAA Administrator, "Safety Risk Management for the Next 100 Years," *Safety Risk Assessment News*, Mar/Apr, 2003.