

ARES CORPORATION



A SIX-STEP PROCESS FOR PERFORMING SCENARIO-BASED HAZARD ANALYSIS

Presented by
Andy Nelson

Paper by
Allan Benjamin and Philip Mongan

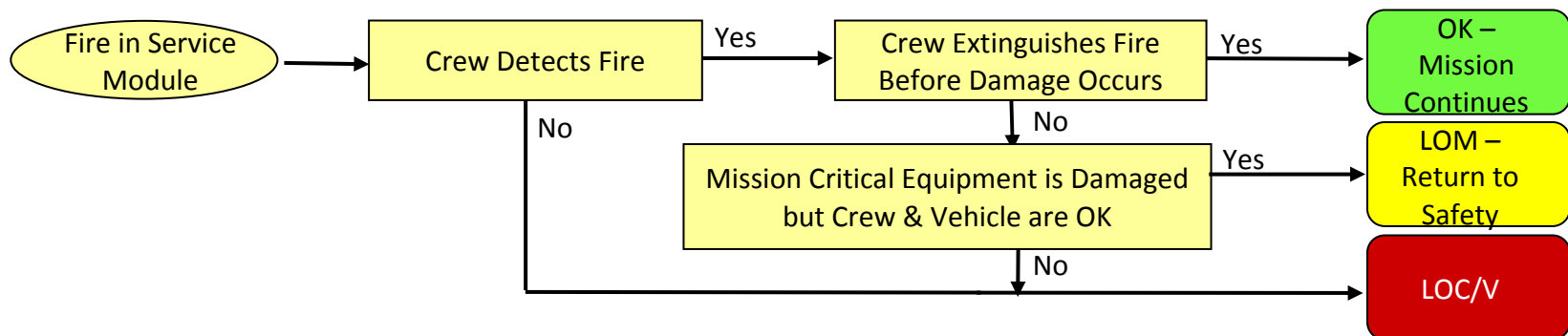
IAASS Conference, Rome, Italy
October 21 – 24, 2008



What is Meant by Safety, Hazards, Hazard Causes, Underlying Controllable Causes, and Scenarios?

- ◆ Safety is defined as freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment
- ◆ A hazard is a condition that can potentially contribute to one or more accident scenarios resulting in adverse consequences. Example: a fire exists in the service module.
- ◆ A hazard cause is an event (usually expressed as a hardware failure) that can lead to a hazard. Example: An electrical short produces a fire.
- ◆ An underlying controllable cause is a controllable subordinate cause that can lead to a hazard cause. Example: aging of wiring insulation causes an electrical short.
- ◆ A scenario is a sequence of events and conditions comprised of an initiating event and subsequent enabling conditions or events that lead to an adverse consequence.

Scenarios can be considered as alternate paths through a flow chart displaying sequences of events, which is called an event sequence diagram



Enabling conditions often involve failure to recognize a hazard or failure to implement appropriate controls such as protective barriers or safety subsystems

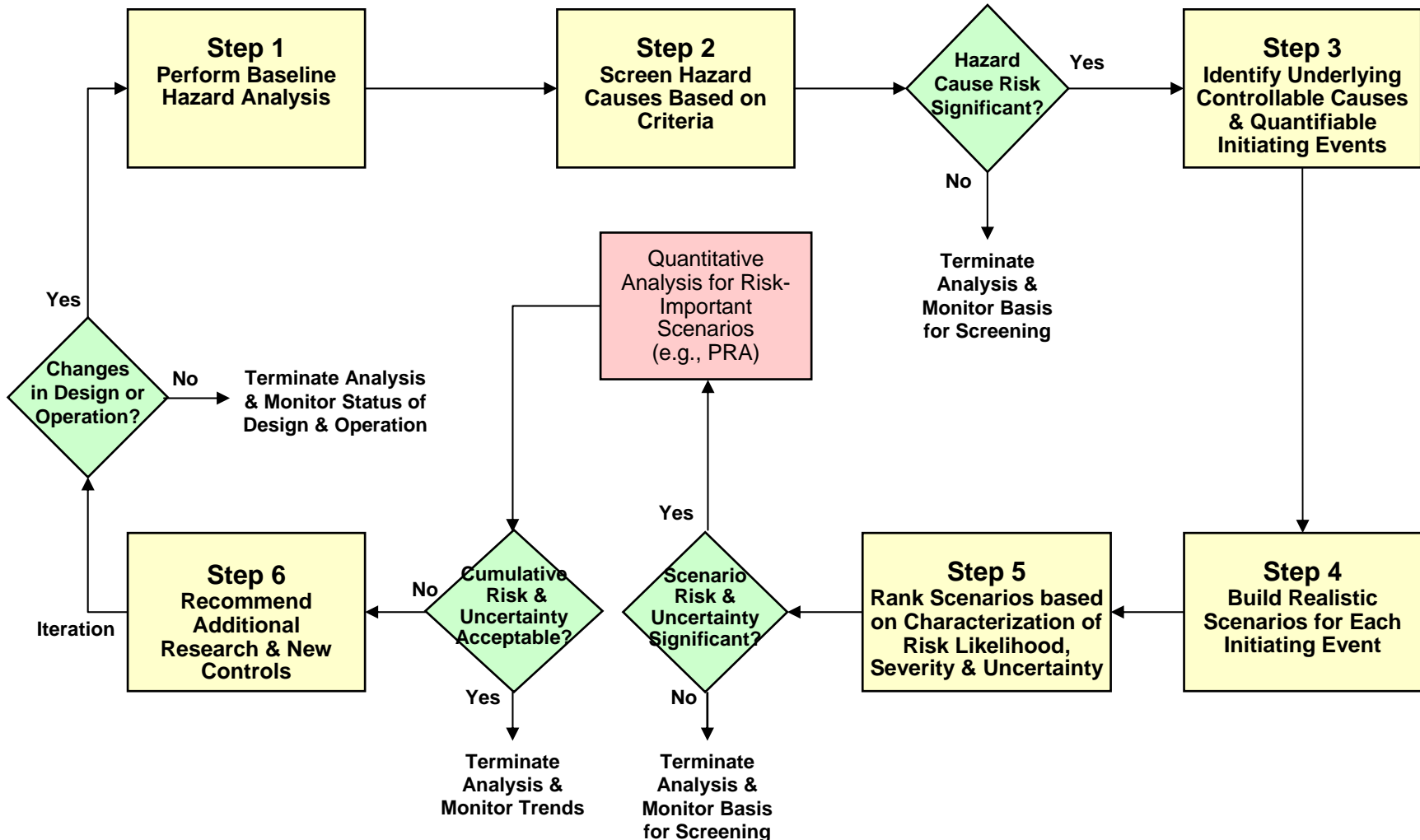
New Requirements for Conducting Hazard Analysis

- Enhancements to the Hazard Analysis process are supported by updates to NPR 8715.3, “NASA General Safety Program Requirements”
- NASA OSMA issued NPR 8715.3A in September 2006 as a first step in addressing these improvements to hazard and safety analyses.
 - Latest revision is NPR 8715.3C, issued in March 2008
- Sections 2.3 and 2.4 urge a number of changes to hazard analyses to include:
 - Modeling the linkage between a given hazard and the occurrence of other conditions and failure events (e.g., hardware failures, software errors, human errors, or phenomenological events)
 - Evaluation of a hazard’s contribution to initiating events and the loss of the system’s ability to compensate for those initiating events
 - Identification of who or what the consequence affects
 - Evaluation of uncertainties

“It is important to emphasize that qualitative safety analysis, to be most effective, needs to be scenario-based, even if the risks of scenarios are not explicitly quantified”

Six Step Process Overview

The approach can be simplified to a six-step process with an iteration loop



Six Step Process – An Example

- We will apply the Six-Step Process for an example hazard relevant to an experimental aircraft
- The hazard to be considered is loss of information to the Flight Control System (FCS)
- Objectives:
 - Demonstrate the six-step technique
 - Demonstrate how this process encourages the identification and examination of specific high-risk scenarios that may otherwise be overlooked
 - Illustrate how scenario-based HA can naturally interface with PRA and other analyses to produce a stronger foundation for risk-informed decision making.



Example System Familiarization

➤ Flight Control System (FCS):

- Translates instrumentation inputs and pilot commands into control of the aircraft
- Manual Operating Mode (normal)
- Reversionary Operating Mode (emergency)
 - Used when there is loss of input
 - Pilot must immediately return to base (LOM)
- Total loss of control is catastrophic (LOC/V)

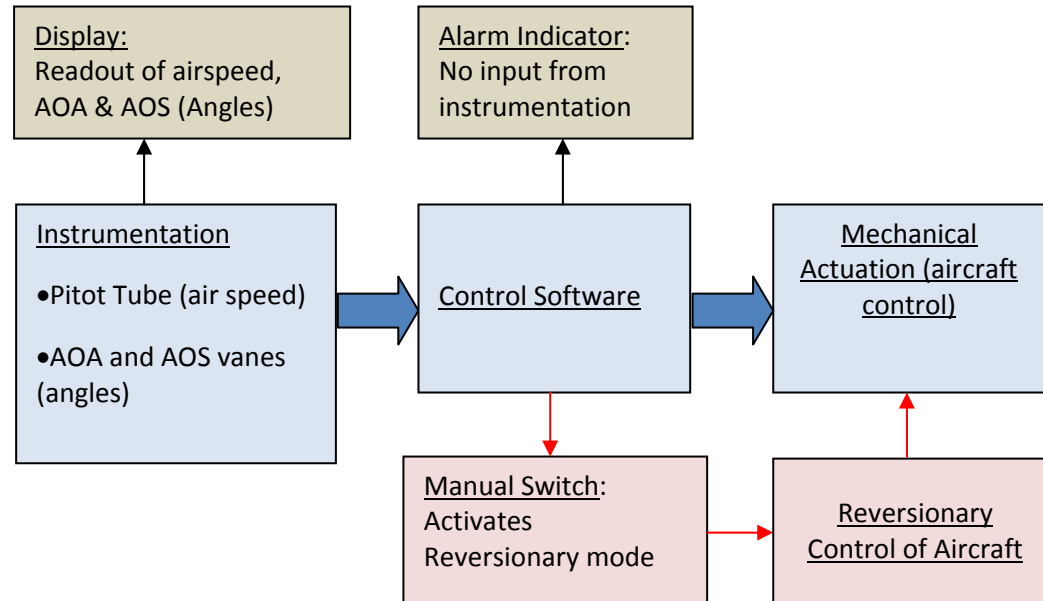
➤ FCS Instrumentation:

- Pitot Tube (Airspeed)
 - Equipped with heater (manual)
- AOA/AOS Vanes (Angle)

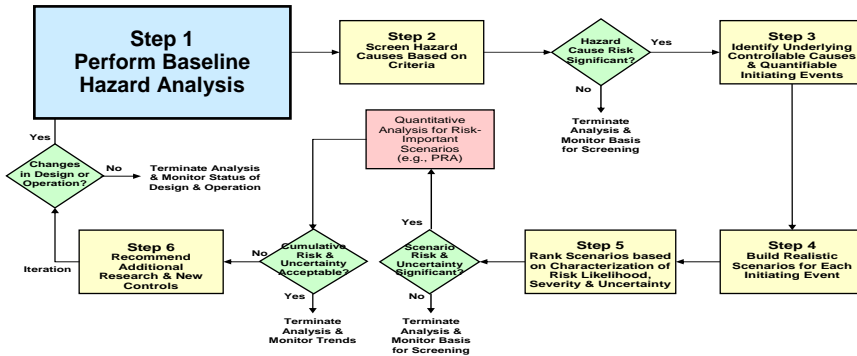
➤ Indicators:

- Airspeed and angles on HUD
- FCS failure alarm and indicator for total loss of input

FCS Simplified Functional Diagram



Step 1: Perform Baseline Hazard Analysis



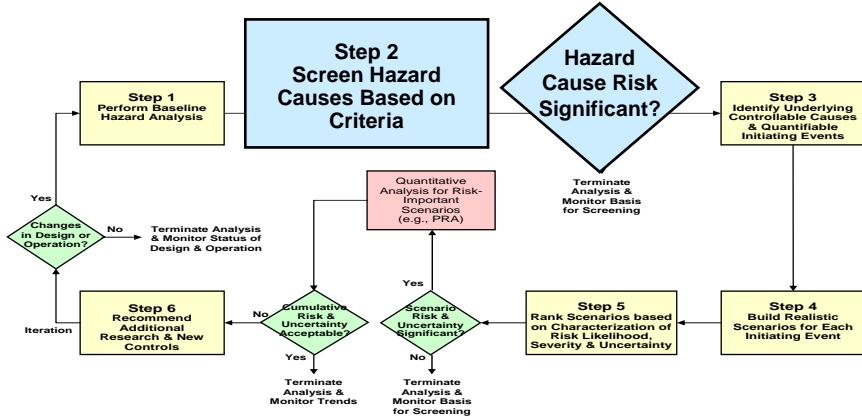
- Hazard Identification
- H/W Hazard Cause & Worst-Case End State Identification
 - LOV/C is a possibility because there is no indication to switch to reversionary mode if there is incorrect input to the FCS
- Existing Control Identification

Excerpt from Example Baseline Hazard Analysis Results

Hazard	H/W Cause (Including Environmental Influence on H/W)	Direct Effects	End States	Existing Controls
Loss of Critical Input into Flight Control System (FCS)	Icing of Pitot Tube	Loss of Manual Control	LOM or LOV/C	Heater (manually switched) Reversionary mode (manually switched)
	Failure to Remove Probe Cover	Loss of Manual Control	LOM or LOV/C	Multiple checks preflight FCS alarm and reversionary mode (manually switched)

The baseline hazard analysis is a high-level assessment that should catch major hardware and operational deficiencies

Step 2: Select Hazard Causes Needing Further Analysis



- To be passed forward, hazard cause must have potential for a critical end state and satisfy one other criterion
- Criteria can be generic (as in this example) or project-specific
- Generic criteria include those below plus others such as:
 - Low technology readiness level
 - Complexity of design
 - Dependent on software
 - Inadequate time for recovery actions

Qualitative Criteria for Deciding Whether Pitot Tube Icing Needs Further Evaluation

Pitot Tube Icing	1	Potential that the hazard cause could lead to a critical end state	<u>Evaluate Further</u>
	2	A critical component that has a single point of failure	
	3	There have been occurrences of this event in previous flights	
	4	The system design inhibits the ability to detect the hazard	

Qualitative Criteria for Deciding Whether Cover Not Removed Needs Further Evaluation

Cover Not Off	1	Potential that the hazard cause could lead to a critical end state is the only criterion that is satisfied	<u>No Further Evaluation</u>
---------------	---	--	------------------------------

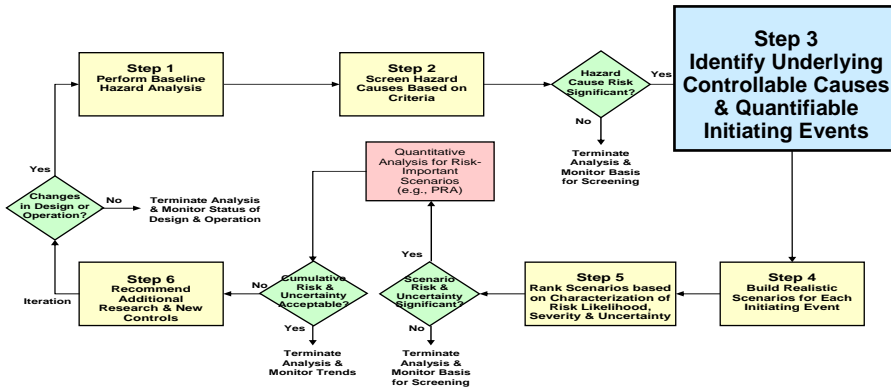
This step enables the analysts to save time and cost by screening out hazard causes that do not need to be analyzed further

Step 3: Identify Underlying Controllable Causes and Define Initiating Events

➤ Underlying controllable causes include those below plus others such as:

- Latent manufacturing defect
- Installation or maintenance error
- Inadequate analytical modeling
- Failure to test as-flown
- Contamination, corrosion, aging

➤ Initiating events may be defined at underlying controllable cause level or at higher cause levels, depending on which level has the best frequency data

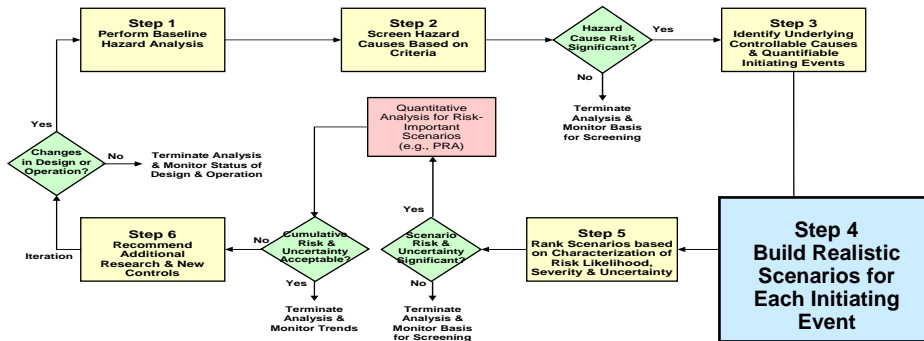


Example Underlying Controllable Causes and Initiating Event for Pitot Tube Icing

Identified Hardware Cause	Potential Underlying Controllable Causes	Initiating Event Selection	Rationale
Pitot tube icing	<ol style="list-style-type: none"> 1. Unanticipated icing weather conditions 2. Decision to fly during anticipated icing weather conditions 	Pitot tube icing	Frequency can be estimated from prior occurrences

This step links hazards to specific scenarios and provides a basis for selecting the most effective controls

Step 4: Build Realistic Scenarios



- Ask “What-If” questions about the effects and possible end states associated with each underlying controllable cause
- Consider common causes, dependencies, multiple events, and degraded states

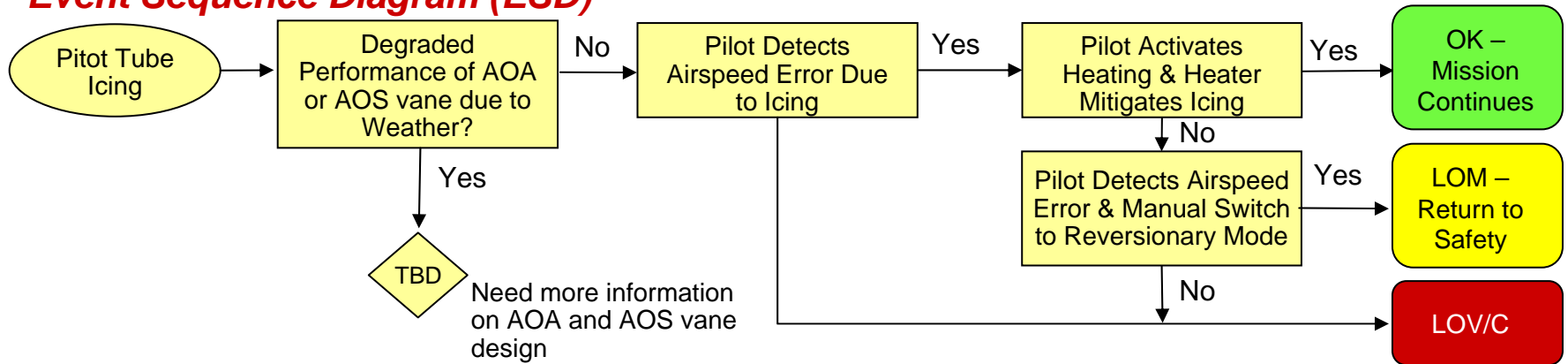
Example Development of Potential Enabling Events Following Pitot Tube Icing

What-If Questions	Type of Cause	Possible Effects (Enabling Events)	End States
What can happen as a result of Pitot tube icing?	Hardware failure	Loss of input, leading to indication for reversionary mode	LOM, LOV/C
		Inaccurate reading, leading to loss of control <i>without indication for heater or reversionary mode</i>	LOM, LOV/C
What can happen as a result of unexpected icing weather conditions?	Underlying controllable cause	Poor visibility or secondary failures/difficulties distract the pilot, making him less likely to check his heads up display	LOM, LOV/C
		Mechanical failure or degraded performance of other exposed components	LOM, LOV/C

Consideration of underlying controllable causes introduces important new scenario possibilities

Step 4 (Cont): Build Realistic Scenarios

Event Sequence Diagram (ESD)



Potential Underlying Controllable Causes of Enabling Events Following Pitot Tube Icing

Enabling Event		
Icing Not Detected	Heater Not Activated or Not Working	Reversionary Mode Not Activated
Pilot fails to check airspeed	Pilot flips wrong switch or is distracted by other factors	Pilot flips wrong switch or incorrectly believes heater is working properly
Indicator defect, installation error, or maintenance, error	Heater defect, installation error, or maintenance error	Switch connection installation error
Inadequate design for detectability	Heater not tested at operating conditions	Inadequate operating procedure for partial icing

Event sequence diagrams are a good way of visualizing and keeping track of scenarios, while consideration of potential underlying causes for enabling events suggests additional controls

Step 5: Rank Scenarios

- A red risk (18 - 25) means the scenario must be elevated to quantitative analysis
- A yellow risk (11 - 17) means the scenario may or may not be elevated to quantitative analysis depending on special factors such as its uniqueness or importance
- A green risk (1 – 10) means the scenario does not require further analysis

Example Event Ranking

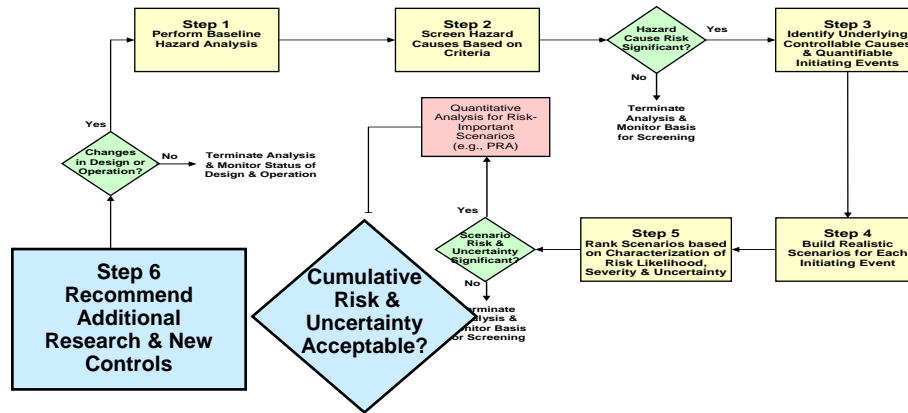
Event No.	Event Description	Likelihood Rank	Rationale	Uncertainty Rank	Rationale	Adjusted Likelihood Rank
1	Icing IE	4	Average over 10 years = 30 cases of icing in 1000 flights	4	Factor of 10 variability in yearly number of icings due to unpredictable weather stability	4 + 1 = 5
2	Pilot Detects Air Speed Error	5	Pilot can usually estimate air speed from visual observation of ground	2	Likelihood is already very high	5 + 0 = 5
3	Pilot Fails to Actuate Heater or Heater Fails	3	Generic human error probability (HEP) for high workload conditions	5	Applicability of generic HEP data is highly uncertain; also possible installation / maintenance error	3 + 1 = 4
4	Pilot Again Detects Air Speed Error and Switches to Reversionary Mode	5	Same as for Event 2	2	Likelihood is already very high	5 + 0 = 5
5	Pilot Fails to Switch to Reversionary Mode	5	Partial icing cannot be verified during flight and display does not warn pilot to switch	2	Likelihood is already very high	5 + 0 = 5

Example Scenario Ranking

This step enables the analysts to save time & cost by reducing the number of scenarios to be modeled in a quantitative analysis

Scenario No.	Scenario Events	Scenario Likelihood Rank (1-5)	End State Consequence	Consequence Rank (1-5)	Scenario Risk Rank (1-25)
1	1, 2, 3, 4	$5 - 0 - 0 - 1 - 0 = 4$	LOM	4	4 x 4 = 16
2	1, 2, 3, 5	$5 - 0 - 0 - 1 - 0 = 4$	LOC/V	5	4 x 5 = 20

Step 6: Recommend New Research & New Controls



- If the residual risk is unacceptable based on quantitative evaluation, new controls should be proposed
- Some controls should be directed to specific underlying controllable causes that are high contributors to the risk
- Other controls should be broad enough to apply to underlying causes in a more generic manner
- Some controls should address protections against erosion of due diligence
- All proposed controls should be subject to a gap / verification analysis
- If the unacceptability of the risk is because of high uncertainty, additional research may be proposed

Specific Controls for Underlying Causes and Effects

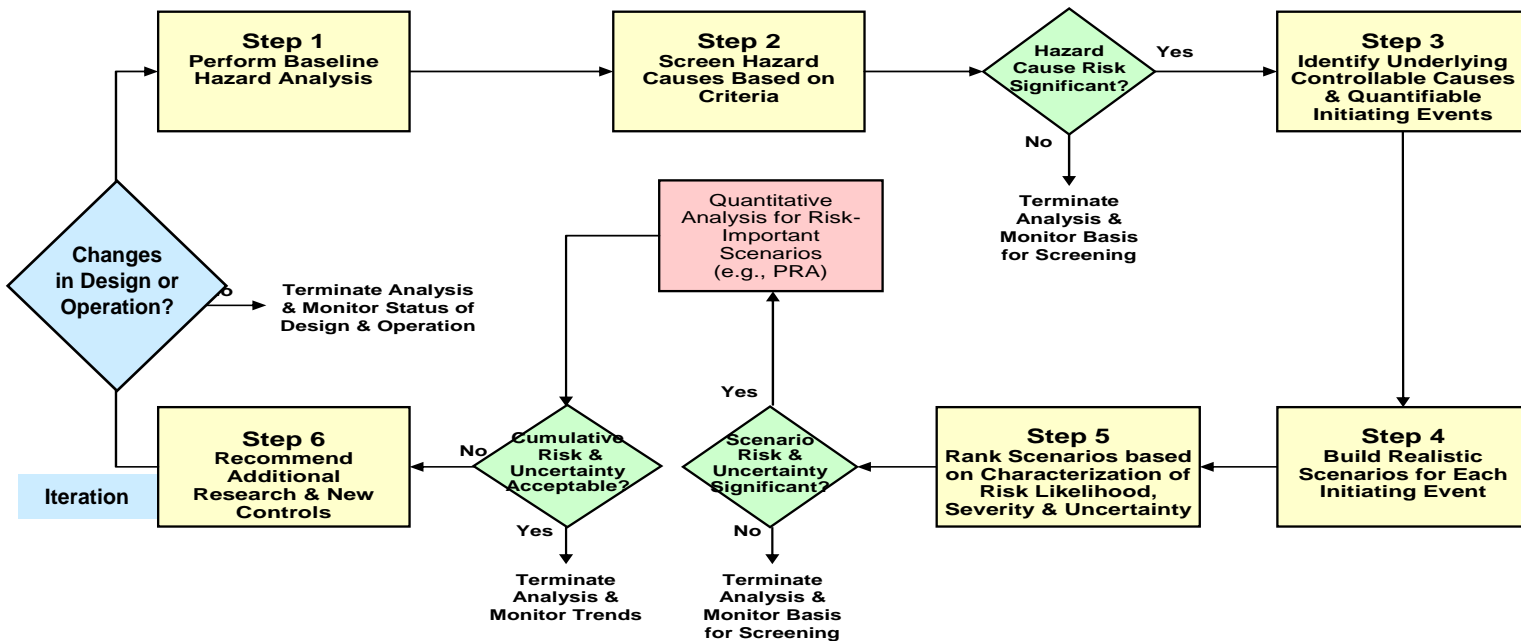
- Two measures of air speed with Indication if different
- Pre-flight operational test of heater
- Feedback to pilot if heater is failed

Generic Controls

- Hazard analysis is updated whenever there is a design change
- Critical components are tested as-flown
- Ground operations properly verifies pilot actions

The scenario based hazard analysis process combined with the graded quantitative approach leads to a better way of identifying controls to reduce risk

Feedback Loop for Changes in Design, Operation, or New Data Generated During the Project Life Cycle

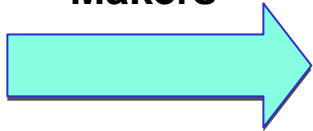


A feedback loop is incorporated to ensure that new controls, design or operational changes that evolve over time, or new data and information:

- Reduce hazard risk to acceptable level
- Do not introduce new failure mechanisms

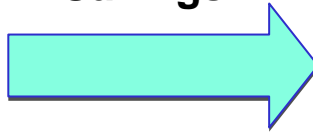
Advantages of the Scenario-Based Hazard Analysis Approach

Improved Input to Decision Makers



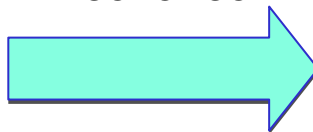
- Improved modeling and understanding of:
 - Underlying controllable causes from all contributing factors
 - Software and human influences on the system
 - Scenarios that cross subsystem and organizational lines
 - Combinatorial and multiple events and how they can lead to undesired end states
 - Enhanced due diligence throughout the project life cycle
 - Inclusion of more end states than just worst-case (LOV/C)
 - Evaluation of uncertainties and treatment of uncertainties as an element of risk
 - Findings from scenarios feed directly into quantitative analyses

Cost Savings



- Graded approach leads to reduction of unneeded quantitative analyses
- Feedback between hazard analysis and other quantitative analyses reduces overall workload and improves results
- Reduction in costly accidents and near misses

Technical Excellence



- Sharing analytical insights across subsystems and organizations through a systematic, scenario-based approach provides:
 - Development of subject matter experts
 - Improved and more integrated system safety oversight
 - Improved documentation of system safety risks and controls