SANDIA REPORT
SAND2000-2955
Unlimited Release
Printed December 2000

Aviation Safety Human Reliability Analysis Method* (ASHRAM)

Dwight Miller and John Forester

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2000-2955
Unlimited Release
Printed December 2000

AVIATION SAFETY HUMAN RELIABILITY ANALYSIS METHOD* (ASHRAM)

Developed by:
Dwight Miller
Systems Reliability Department

Project Manager:
John Forester
Risk and Reliability Analysis Department

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185

Abstract

Since the late 1950s, Sandia National Laboratories has played a leadership role in the development of human reliability analysis (HRA) techniques for high-risk/consequence operations. The most recent of these is the Aviation Safety Human Reliability Analysis Method, (ASHRAM), which gets its basic theoretical underpinnings from an HRA method developed by Sandia National Laboratories for the U.S. Nuclear Regulatory Commission, called ATHEANA (A Technique for Human Event Analysis). The underlying premise is that significant human errors occur as a result of a combination of plant conditions and certain human factors that trigger cognitive error mechanisms in personnel. The error mechanisms can lead to the execution of unsafe acts, such as bypassing engineered safety features. Due to the usefulness of the approach, and the Clinton administration's initiative to improve commercial airline safety, Sandia funded the initial development of ASHRAM. The result is a method that allows aviation researchers to analyze aviation accidents and incidents that involve human errors in ways that account for the operational context, crew expectations, training, airframe-related human-system interfaces, and crew resource management. ASHRAM is packaged in a brief, readable format, with step-by-step instructions, and with real-world examples so that it can be utilized by a variety of users, including researchers, modelers, analysts, trainers, and pilots.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The author would like to acknowledge the participation of some key people, without whom this project would not have been possible. First and foremost is my colleague John Forester, who participated in the development of ATHEANA, acquired the funding for ASHRAM, managed the development of ASHRAM, reviewed many iterations of the manuscript, and wrote several sections of this report. Next, I would like to thank Hugh Whitehurst, a project team member, who worked on the early stages of applying ATHEANA to aviation, reviewed the text several times, and ultimately wrote the references section. Special thanks go to Allen Camp, whose vision fueled this project from start to finish, and to Bob Waters who provided much appreciated encouragement and review comments. Heartfelt appreciation is extended to Liza Tam for visiting us and working on the ASHRAM techniques, reviewing the manuscript, and supplying insightful ideas for improvement. And finally, much applause is due to Emily Preston, who took all the pieces, glued them together, and produced a coherent, final, SAND report. Thank you, everyone, for your technical expertise and cheerful support.

AVIATION SAFETY HUMAN RELIABILITY ANALYSIS METHOD

1. INTRODUCTION

1.1 Purpose and Scope

This report describes a human reliability analysis (HRA) technique called "Aviation Safety Human Reliability Analysis Method," or ASHRAM. The technique allows aviation researchers to analyze aviation accidents, incidents, and near misses that involve human errors in ways that account for the operational context, crew expectations, training, airframe-related human-system interfaces, crew resource management, and generic human-error mechanisms. Using ASHRAM, researchers can:

- more completely understand the human-system interactions that contribute to aviation accidents, incidents, and hypothetical scenarios
- identify potentially unsafe human actions and accident scenarios that have, as of yet, not been documented
- identify elements of error-forcing contexts that contribute to known unsafe actions
- analyze and model situations where pilots may perform actions not required for emergency response, or intentionally disable safety systems, in the course of attempting to solve or reduce problems
- model and document families of related undesirable aviation events

More specifically, the technique provides a step-by-step method for aviation administrators, safety researchers, human factors engineers, and training specialists (henceforth referred to as users, analysts, or the team) to:

- document accidents retrospectively in a format amenable to assessing cognitive errors
- consider crew errors of commission that make dangerous situations even worse
- take advantage of the synergy from involving subject-matter experts representing a variety of contributing fields of study and experience
- analyze accidents in terms of the contexts that lead pilots to take unsafe actions
- identify salient, potential accident scenarios, based upon event initiators
- enumerate numerous variations of the potential unsafe actions and accident scenarios

- develop novel scenarios for simulator training

1.2 Background

The development of ASHRAM is the result of Laboratory Directed Research and Development (LDRD) investment made by Sandia National Laboratories* (SNL) in Albuquerque, New Mexico. ASHRAM is a variation of "a technique for human event analysis," or ATHEANA, which was developed for the US Nuclear Regulatory Commission's (NRC) Office of Nuclear Regulatory Research, by SNL, and various other contractors, including Brookhaven National Laboratories which participated in the early stages of the development process (see Ref. 9.1, for a complete description of ATHEANA).

ATHEANA was developed as an HRA modeling process that can accommodate and represent the human performance found in real nuclear power plant (NPP) events, and can be used with probabilistic risk assessments (PRAs) or other safety perspectives to resolve safety questions. On the basis of observations of serious events in the operating history of the commercial nuclear power industry, the underlying premise of ATHEANA is that significant human errors occur as a result of a combination of plant conditions and certain factors that trigger error mechanisms in the plant personnel. The combination of plant and human factors is referred to as the error-forcing context (EFC). As the term suggests, plant operators can be tricked into executing unsafe acts, such as bypassing engineered safety features, in the right EFC. ATHEANA is one of the first HRA techniques that explicitly addressed human intervention as an important failure mode.

Due to the usefulness of ATHEANA, other applications of the technology were sought. At roughly the same time, the Clinton administration put forth an initiative to improve commercial airline safety tenfold and SNL had begun working with the National Aeronautic and Space Administration (NASA) on the application of risk-assessment methods. For that reason and because approximately 70 percent of aircraft accidents are still caused by human error, additional safety-analysis techniques were needed. Therefore, a proposal was made for SNL funds to modify ATHEANA concepts and techniques for the commercial-aviation domain. The proposal won a two-year internal research grant to develop ASHRAM in FY99 and FY00.

1.3 ASHRAM Development

The ASHRAM development began with a retrospective analysis on three documented airline crashes using original ATHEANA methods. The objectives of performing the retrospective analyses were to identify the characteristics of actual aviation accidents, determine any important differences between such events in the aviation and NPP domains, and test/illustrate the usefulness of the modeling approach for understanding aviation related accidents. The crash-selection criteria included available and detailed documentation, a wide range in the types of accident, and an obvious human-error component. The events chosen were:

---

* *Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.*

1. The controlled flight into terrain (CFIT) accident near Cali, Columbia, 1995
2. The landing crash of China Air at Nagoya Airport, Japan, 1994
3. The loss-of-engine crash near Kegworth, England, 1989

The three events were documented in a format prescribed by ATHEANA that breaks out event factors in a manner that facilitates examination of the timing and human-factors elements. The retrospective documentation includes sections covering:

- Event Identification
- Event Summary and Description
- Event Surprises
- Safety Recommendations (following the event)
- Most Negative Influences
- Most Positive Influences
- Significance of the Event
- Key Flight Parameter/Aircraft Status
- Event Timeline
- Human Dependencies
- Unsafe Action Analysis
- Accident Diagnosis Log

The complete retrospective documentation of the Kegworth event can be found in Appendix A. The Kegworth event was chosen for full analysis using ATHEANA methods, due to the relative simplicity of the timeline and the clear and unambiguous human-error contributions to shutting down the wrong engine. The abstracted, single-engine-out event was then used as a "test case" for applying the ATHEANA prospective analysis procedure for potential scenarios that include unsafe actions. Documentation of the results of applying the ATHEANA prospective methods to the test case can be found in Appendix B. Samples of the retrospective and prospective analyses are used throughout the report to demonstrate principles and methods via example. Experience in applying the existing methods to the aviation example helped to identify modifications needed for ASHRAM.

1.4 Similarities and Differences Between Nuclear Power and Aviation

A major underlying assumption to the process of adopting and adapting an HRA method to a different domain is that there is enough similarity between the two domains to reap the benefits of not starting over from scratch. The dominant similarities between the domains include:

- highly technological systems
- high consequences of failure
- very few significant failure events
- governmental regulation of hardware and operations

- small, highly qualified crew in control
- simulators used in crew training
- dependence upon displays for much of environmental perception

As the retrospective documentation proceeded and the ATHEANA prospective analysis steps were applied to the test case, the differences between nuclear power and commercial aviation became more and more apparent. A table was created early in the process and added to as the differences manifested themselves. Table 1 summarizes the major differences that were seen to most impact the methodology.

Table 1. Summary of the Major Differences Between Nuclear Power and Aviation

	Nuclear Power	Commercial Aviation
Licensing agency	NRC	Federal Aviation Administration
Potential accident consequences	Extremely High; thousands of lives	Very High; hundreds of lives
Incentives to operate w/inadequate safety	Power grid needs, profits of utility	Meet schedule, passenger frustration, airline profits
Reports of errors and near misses—human error probabilities (HEPs) available?	The industry has developed an HEP databank, called NUCLARS, but participation has been minimal	There are several databases of near misses and accidents, some are privately owned by airlines, others are public—no known banks include HEPs
Contact with help in emergencies	Shift Technical Advisor, Incident team at Emergency Operations Center, Technical Evaluation Center	Radio to radar centers, tower, airlines, manufacturer
Normal operations	Continuous, mostly supervisory control, with periods of direct, manual control	Each flight is a discrete event and is dependent on crew for initiating and orchestrating. During cruise supervisory control is used.
Minimum elements needed for mission: critical functions	Fuel, cooling, pressure control, power conversion systems, crew, safety systems	Flight controls, thrust, cabin pressure or supplemental oxygen, navigation information, pilot, communication w/destination, flyable weather
Physical inertia	High, with a few notable exceptions, such as large loss-of-coolant accidents (LOCAs), changes in physics take place slowly—minutes and hours	Low, changes happen rapidly—seconds and minutes
Speed of system response	Relatively slowly, except large LOCA – slow feedback from inputs	Relatively fast—rapid feedback from inputs
Feedback from system to control inputs	Remote reports and instrumentation; mostly discrete readouts, but some integrated displays, mixture of electromechanical and electronic	"Seat-of-pants", real-time visual, aural, kinesthetic, also instrumentation; mostly discrete readouts, but some integrated displays, mixture of electromechanical and electronic

	Nuclear Power	Commercial Aviation
Emergency operation written guidance	Written, symptom-based procedures	"Manual decision-making," and checklists for most critical flight operations
Accident sequences	A few major decisions and actions can cover several hours	Many decisions and actions can cover only a few minutes
Transient conditions	Difficult to integrate all info to construct valid mental model	Easier to construct mental model from discrete displays
Activation of emergency subsystems	Automatic, in most cases, with crew notification	Pilots are in the loop—get warning displayed and have to initiate safety system response

1.5 Major Changes in Analysis Techniques

The set of differences in Table 1, combined with the test-case experience, suggested modifications be made to the original ATHEANA procedures, leading to the ultimate ASHRAM techniques. The following list outlines the most significant differences:

1. Perhaps the largest difference is based on the fact that the application of ATHEANA in the nuclear power industry usually can rely on existing PRAs to facilitate the identification of potential human failure events (HFEs) associated with critical functions. Aviation safety, as we know it today, most often does not benefit from the availability of existing PRAs. Therefore, the prospective analysis, described in Section 6, is designed to *generate* potential unsafe actions (the equivalent of ATHEANA's HFEs) based upon the EFC.

2. The retrospective analysis, described in Section 4, is shorter in format, includes less redundancy, and is suggested as a means of generating issues for the prospective analysis.

3. A more explicit iterative process of changing the scope delineations, initiating events, and consequent base-case scenarios is introduced to facilitate the exploring the breadth of an aviation-safety issue.

4. Fill-in forms are provided for consistent analysis and output format.

5. Event-tree style flowcharts are suggested to diagram the multitude of ways that scenarios can unfold rather than using strictly text-based descriptions. This approach not only saves time, but also allows analysts to review many scenarios on one page.

6. An attempt was made to clarify the iterative process of identifying the EFC and its influence on deviant scenarios.

7. The concise format and simple language make the method friendly to users outside traditional cognitive psychology, such as aviation-safety researchers and airline simulator-training specialists.

8. Examples of the method are integrated into the text, rather than put in appendices.

1.6 Report Contents

The remainder of this report:

- explains the assumptions and cognitive models underlying ASHRAM
- defines terms used in the method
- identifies critical functions needed for safe aviation
- describes the ASHRAM processes briefly and holistically
- provides a step-by-step, detailed process description
- utilizes a workbook approach to guide users through the process
- uses a running example to help explain the methods used
- provides tables and resources needed to complete the steps
- draws conclusions about the results of the method
- suggests potential follow-on activities

1.7 ASHRAM Products

After having used ASHRAM on a particular aviation event or set of events, the analyst/team can expect to have the following products to show for their efforts:

- a detailed retrospective description of an existing accident (optional)
- a list of relevant classes and examples of initiating events
- a detailed description of a nominal, base-case scenario and ideal responses
- identification of potential unsafe actions
- an outline of the general timeframe of the scenarios
- descriptions of deviation (from the base-case) scenarios
- an analysis of relevant performance-shaping factors
- an evaluation of potential recovery modes
- a set of novel accident scenarios
- observations and conclusions about the scenarios
- recommendations to the aviation-safety community

2. CONTEXT FOR ASHRAM

2.1 Need and Rationale for ASHRAM

As a derivative of ATHEANA, ASHRAM has very similar roots. ATHEANA was developed partly to address cases where NPP operators performed apparently unnecessary or illogical actions in the course of responding to emergency or accident situations. For example, in the Three-Mile Island accident, operators inappropriately terminated high-pressure injection, resulting in reactor core undercooling, and eventual fuel damage. In a subsequent report, published in 1995, the NRC's Office of Analysis and Evaluation of Operation Data, reported 14 events over the previous 41 months in which an engineered safety system was inappropriately bypassed. The report (Ref. 9.2) concluded that "human intervention may be an important failure mode."

Similarly, pilots are often confronted with emergency situations in which terminating, turning off, or otherwise altering the state of a safety-related subsystem, or critical flight function, may appear to be the best course of action when following a solution strategy. For example, in the Kegworth accident, summarized in various formats in Appendix A, both the pilot in command (PIC) and first officer (FO) misidentified which engine was malfunctioning and jointly decided to shut it down for safety reasons. It was a good, safe, strategy, given that the correct engine was identified. However, combined with misidentification, it proved disastrous. ASHRAM examines the airframe and airspace situational factors, pilot performance-shaping factors, and error mechanisms identified by cognitive psychology to explain and model the overt and covert events leading up to an unsafe act. This approach is particularly suited to scenarios where:

- the symptoms and aircraft behaviors deviate from pilots' expectations, based on training and experience
- the scenario is readily perceived as a relatively common, recognizable event, when it is, in fact, a completely novel situation
- there are multiple equipment failures/unavailabilities, including those that are human-caused
- there are instrumentation problems, for which pilots are not fully prepared, and which can cause misrepresentations or misunderstandings about the event

Unfortunately, when aircraft accidents are attributed to human error, there is a temptation to feel resignation—that human error is something we just have to live with, because the aircraft and Air Traffic Control (ATC) system are already optimally designed. People who work in aviation safety and understand how humans perform in complex systems know otherwise. ASHRAM is a tool offered to these people so that we can ultimately reduce the number of accidents attributable to the human element.

2.2 Relationship to Other HRA Techniques

Because it was based on the ATHEANA technique, ASHRAM is similar in its purpose, structure, and theoretical underpinnings.[1] By emphasizing the importance of the EFC in evaluating the potential for human error, by attempting to explicitly model aspects of human cognition that can contribute to such errors, and by striving to include the modeling of mistake driven errors of commission (EOCs), ATHEANA and ASHRAM diverge significantly from earlier HRA methods such as Techniques for Human Error Rate Prediction (THERP) (Ref. 9.3), Success Likelihood Index Methodology-Multi-Attribute Utility Decomposition (SLIM-MAUD) (Ref. 9.4), HCR (Human Cognitive Reliability) (Ref. 9.5), OAT (Operator Action Tree) (Ref. 9.6), HEART (Human Error Assessment and Reduction Technique) (Ref. 9.7), and ORCA (Operator Reliability and Characterization) (Ref. 9.8). While the developers of these earlier methods were not unaware of the importance of such considerations, given the state-of-the-art at the time they did not provide adequate models and guidance by which they could be addressed. However, ASHRAM, like ATHEANA has not been developed in isolation from other projects that have also identified limitations in earlier methods. For example, EPRIs Cause-Based Decision Tree (CBDT) (Ref. 9.9) approach at least attempted to explicitly address causal factors that could lead to human error. In addition, more recently developed methods such as the Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté (MERMOS) developed by Electricité de France (Ref. 9.10); the Connectionism Assessment of Human Reliability (CAHR) method by Sträter and Bubb (Ref. 9.11); the Cognition Simulation Model (COSIMO) (Ref. 9.12) and its implementation in the Human Error Reliability Methods for Event Sequences (HERMES) (Ref. 9.13) by Cacciabue et al, INTENT by Gertman, Blackman et al, (Ref. 9.14); the two methods developed by Julius, Jorgenson, et al, often referred to as the "Borssele-Method"(Refs. 9.15 and 9.16); the HITLINE method developed by Macwan and Mosleh (Ref. 9.17); and the Cognitive Reliability and Error Analysis Method (CREAM) by Hollnagel (Ref. 9.18), have all attempted in one way or another to model some specific aspects of an operator's, or the operating crew's, cognitive processes and to provide guidance for considering the influence of context.

Furthermore, the European Commission supported an extended network of experts in human performance, called the European Association on Reliability Techniques for Humans (EARTH), to identify a range of factors and issues that can cause failures in operator cognitive processes (Ref. 9.19). This catalog of issues has provided developers of the new methods with a common source of ideas for modeling.

Finally, one of the first and most influential attempts to take better account of developments in the understanding of the mechanisms giving rise to erroneous actions and to recognize that human errors are not random occurrences, was the pioneering work by Woods, Roth, and others in the development of a simulation-based model of nuclear power plant operators' cognition in the NRC-sponsored cognitive environment simulation (CES) (Ref. 9.20).

ASHRAM and ATHEANA have taken advantage of ideas conceived and refined by the above developments, and there are several existing reviews of most of the above methods that articulate

[1]However some significant differences do exist. Comparisons with ATHEANA are outlined in the previous chapter.

and discuss their advantages and disadvantages, e.g., Swain (Ref. 9.21), Kirwan (Ref. 9.22), Hollnagel (Ref. 9.23) and Strater, Dang, and Hirschberg (Ref. 9.24). However, there are several aspects of ATHEANA, and in turn ASHRAM, that go beyond existing approaches, at least as they are currently represented. There are also important aspects of HRA addressed by other investigators that are not well covered by ATHEANA or ASHRAM, and they are also mentioned below.

2.2.1 Improvements in Identifying and Evaluating Unsafe Actions

First, and foremost, ATHEANA and ASHRAM provide an explicit process for identifying potential unsafe actions, including EOCs, and the EFCs that can lead to those unsafe actions. With the exception of the Borssele-Method and the HITLINE method and the possible exception of MERMOS, other methods provide explicit guidance only for how to evaluate and quantify potential human errors that have already been identified, perhaps through the traditional PRA approach. Thus, an advantage of ATHEANA and ASHRAM is the explicit search process for potential accident scenarios and associated unsafe actions. ASHRAM has improved the guidance for this process by striving to make the iterative nature of the search process more explicit.

An important related aspect is the guidance provided by ATHEANA and ASHRAM for how to evaluate the relationship between system (e.g., aircraft or plant) conditions, PSFs, and human error mechanisms in identifying and quantifying potential unsafe actions and EFCs. Using information displayed in tables, guidance for use of the tables, and an underlying human information processing model, the methods illustrate and model potential relationships between these elements and the types of human errors that could occur. Analysts can use this information in identifying potential errors, their causes, and their likelihood. The specific approach is unique to ATHEANA and ASHRAM, but other methods have attempted to provide similar guidance.

Although available documentation on MERMOS has been very limited to date, MERMOS identifies sets of "human factors missions" (HFMs) which represent what operators must accomplish in responding to an initiating event, i.e., what has to be accomplished for success in an accident scenario modeled in a PRA. The search process for potential errors in MERMOS involves looking for ways that the HFM can fail. The HFM usually requires success in three functions: strategy, action, diagnosis (hence the terminology 'SAD' functions). The MERMOS search strategy is to look for ways that the SAD functions can fail, using inductive thinking and simulator experience as a basis. The SAD functions fail as a result of combinations of 'CICAs' (emergency-response control strategies) and 'characteristics of the situation' (similar to 'plant conditions'). Thus, MERMOS attempts to identify how people and the situation can cause the failures of the functions. This is done on the basis of examining the SAD functions and then using brainstorming based on their experience with simulator training. ATHEANA and ASHRAM do this on the basis of the cognitive process model and an explicit set of search processes. It does appear that MERMOS provides guidance for linking human cognitive processes and related factors and uses a model of human-system performance. However, until formal documentation of their approach is available, further assessments must be held in abeyance.

The Borselle-Method focuses on procedure reviews to help with the identification of EOCs. The approach examines how operators may inappropriately follow and act upon incorrect paths in procedures, for example, because they misinterpret indications. While this work provided direction for aspects of the initial search process developed in ATHEANA, the overall guidance in the Borselle-Method for searching for EOCs is relatively limited. Furthermore, the method does not use an explicit underlying psychological model to address human error mechanisms.

Similarly, HITLINE seeks to identify opportunities for misdiagnosis or other cognitive errors in which operators take actions that are not needed. The likelihood of such errors is based on assessments of various scenario-independent and scenario-dependent factors. The scenario-independent factors include crew training and experience, crew confidence, etc.; and the scenario-dependent factors are related to the plant, the procedures, and the operator actions in the event. The method is based on a rudimentary framework of operator decision-making and focuses primarily on plant procedures in terms of identifying potential EOCs. Moreover, the guidance for searching for EOCs is relatively limited, particularly in the sense of identifying scenarios and actions that could present serious problems for the operators. Nevertheless, the HITLINE methodology is a structured approach that attempts to explicitly address the kinds of factors and information that were noted as weaknesses in earlier methods.

2.2.2 Use of Underlying Cognitive Model

As noted above, ATHEANA and ASHRAM use an underlying cognitive model in conjunction with guidance for how to consider the relationship between plant/aircraft conditions, PSFs and human error mechanisms. CREAM also attempts to model this relationship, but the approach is very different than that described in ATHEANA. Hollnagel has created a detailed, integrated model that relies on assumptions about the characteristics of tasks and other factors that will influence human performance. For example, his contextual control model of cognition assumes four basic human "control modes" that will lead to variations in performance. While a thorough discussion of the empirical basis for the assumptions and the associated model is not provided, they appear reasonable and useful (and they certainly have face validity). In any case, CREAM is a significant effort toward a "complete" HRA method and provides more detail and guidance than ATHEANA and ASHRAM in some areas. In particular, the method provides an integrated quantification approach that is closely tied to the underlying cognitive model and provides at least some guidance to address management and organizational (M&O) factors and the impact of crew interactions. While ATHEANA's guidance for considering M&O factors and crew interactions is currently limited, ASHRAM does provide guidance for addressing crew interactions from the perspective of crew resource management. The main advantage provided by ATHEANA and ASHRAM is the explicit and detailed search process for unsafe actions and dangerous accident scenarios (as discussed above). In addition, these methods focus more on providing a useable model and guidance for analysts to think about and evaluate the way a scenario might evolve to lead to a human error, rather than constraining the analysis to a limited set of factors and assumptions that may or may not be valid. Furthermore, ATHEANA provides a useable quantification approach that allows analysts to appropriately consider EFCs, human error mechanisms, and the potential for recovery in determining human error probabilities.

Another relatively new method, CAHR (Ref. 9.11), also strives to structure HRA through use of an underlying psychological model. However, decision making, planning, etc. appear to be absent from the model. The method does stress the relationship between external conditions and human information processing and the interrelationships between PSFs are seen to provide insights into the error mechanisms. The role of communications between personnel and the flow of information are also considered. However, one of the main unique contributions of the CAHR method is that it attempts to address the limitations of data for quantification that comes from expert judgement, simulator exercises, or generic sources. The method provides an analytic approach that allows for production of plant-specific data, which would appear to be more appropriate than the more "generic" data from methods like THERP. However, the approach for using the data involves psychological scaling, and the basis for the derivation of HEPs is not completely clear.

2.2.3 Dynamic Methods

One "weakness" of all of the "methodological" approaches such as ATHEANA, CREAM, MERMOs, CAHR, and all of the earlier methods, is that their ability to model the dynamic aspects of accident scenarios is somewhat limited compared to cognitive simulation efforts such as those of COSIMO, IDA (not an acronym), and Man-machine Integration Design and Analyses System (MIDAS) (Refs. 9.12, 9.25, 9.26). Cognitive simulation modeling attempts to model cognition, but through the use of computerized simulations of operator performance. Information-processing models, symbolic processing theory, etc., are used in appropriate architectures to predict human errors. One of the advantages of such approaches is that they attempt to simulate dynamic operator and scenario behavior. However, such cognitive simulations can be expensive to develop and use, and they have not been validated any more than other methods. Moreover, it is not immediately clear how such methods can be used realistically in the identification of possible dangerous human errors and their causes in real world environments. Although the ability of ATHEANA, ASHRAM, and other more "static" methods to model a multitude of dynamic changes in a scenario may be limited, the scenarios that are identified are those likely to give operators or pilots problems, and they do reflect the impact of changing conditions on performance. Eventually, it may be possible to use the simulation approaches in conjunction with HRA approaches such as ASHRAM, to test their predictions about operator performance in particular scenarios. Such interactions may lead to appropriate revisions of the cognitive modeling approaches being used by either of the approaches.

In summary, the development of ASHRAM has relied upon and tried to build on previous work in addressing the shortcomings of earlier HRA methods. While additional work will certainly be able be improve ASHRAM, the method is an attempt to adapt and improve ATHEANA, which has in its own right improved on several important aspects and shortcomings of existing methods.

2.3 How ASHRAM Fits into an Overall Risk-Management Approach

In the commercial aviation world, there are many aspects relevant to risk, including getting people to their destinations on time, protecting ground and airborne equipment, and keeping airlines profitable. Regardless, when aviation safety is the issue, the only risk of interest is the safety and well-being of the crew, passengers, and citizens on the ground. Typically, there are two general avenues to reducing risk; reducing the probability of the accident, and/or reducing the consequences of the accident. The physics of flight dictate light, strong, structural designs. However the impact that gravity exerts on physical bodies over long distances makes terminal velocities virtually always terminal for airframe and human occupants. In other words, there is little that can be done to mitigate the consequences of an airline accident, so emphasis must be placed on reducing the probability of its occurrence. Following this premise, there are five categories of potential risk reduction in commercial aviation:

1. *Improve the aircraft hardware* (includes software). This approach has benefited aviation safety in the last hundred years by making the airframe systems and subsystems more reliable. Modern jets also utilize computers and software to control and automate lower-level functions, but for this treatment, the software is seen as integral to the hardware.

2. *Improve the hardware maintenance.* The capability to predict hardware problems before they become safety problems is a major area of study. In a few short decades, planes will likely tell us when their parts will fail and when they need to be replaced to avoid compromises in safety.

3. *Improve the aircraft environment.* Reference here is to the airspace, traffic patterns, and ground operations environment. Unfortunately, the heavy concentrations of people living in major metropolitan areas force airplanes to concentrate similarly in the airspace above. Fortunately, advances are being made in technologies that help control separation, ATC identification, airspace communication, and takeoff and landing precision.

4. *Improve procedures.* The thoroughness of operational procedures has to be balanced with timeliness and efficiency. Better crew resource management (CRM) and increasing the use of automation for many lower-level procedures have contributed towards improved procedures.

5. *Improve the pilot.* There are several means of improving the pilot and his/her ability to cope with unexpected emergency events. Improved training can prepare the pilot for a wider variety of events, refresh or reinforce knowledge previously learned, and shift attitudes toward safe operation. Improved recency requirements can help to ensure that flying skills remain sharp between assignments.

Information gleaned from ASHRAM analyses can be used to reduce risk by application to all five aspects of aviation above. More specifically, knowledge about how the pilots interact with hardware and software, and what kinds of potential errors exist can be fed into the hardware and software design processes. With the advent of flight management systems, two-person cockpits,

and GPS navigation, there is increased pressure on the pilots to manage increasing amounts of information. When hardware maintenance is supported by active state-of-health monitoring, additional information will be available to maintenance and flight crews about the availability timeline of the aircraft and its major subsystems. The ability to communicate this knowledge and utilize it effectively in planning flights and service activities will depend heavily upon understanding human-system interactions and designing the interfaces appropriately.

3. UNDERLYING COGNITIVE MODEL

3.1 Introduction

The primary objectives of this section are to describe the assumptions and underlying cognitive model supporting ASHRAM. Aspects of the model will be identified and defined, and their interactions will be discussed. It should be pointed out that users of the ASHRAM method will benefit from reading this seemingly academic material. Subsequent discussions of model elements and use of the specific ASHRAM procedures will be more comprehensible after having read and understood the theoretical underpinnings addressed in this chapter. Users are encouraged to save time in future activities by investing time to read the rest of this chapter.

There have been many attempts over the past century to understand the causes of human error (see Appendix C for a discussion of the term "human error"). The main conclusion is that few human errors represent random events; instead, most can be explained on the basis of the ways in which people process information and make responses in complex and demanding situations. Thus, it is important to understand the basic cognitive processes associated with monitoring, decision-making, and control, and how these can lead to human error. A number of good discussions of the cognitive factors associated with human performance and error in complex dynamic tasks are available in the literature.

The cognitive model used in ATHEANA is largely based on the work of Woods, Roth, Mumaw, and Reason (Refs. 9.27, 9.28, 9.29, 9.30, and 9.31). The basic model put forth by these authors is an information-processing model that describes the range of human activities required to respond to abnormal or emergency conditions. The model considers actions in response to abnormalities as involving basically four cognitive steps:

1. situation assessment
2. monitoring/detection
3. response planning
3. response implementation

3.2 ASHRAM Cognitive Model

In a holistic world, dividing cognitive processes and placing them in boxes is somewhat arbitrary and reductionistic. However, as various environmental and internal factors tend to influence decision-making and action differently, it can be helpful to identify essential stages of cognitive processing. In the interest of simplification, brevity, and clarity for the non-psychologists, it was decided, for this application, to condense the four-stage model cited above, by combining related and undifferentiated aspects. As depicted in Figure 1, the three identifiable classes of cognitive functioning are identified as:

1. environmental perception
2. reasoning and decision-making
3. action

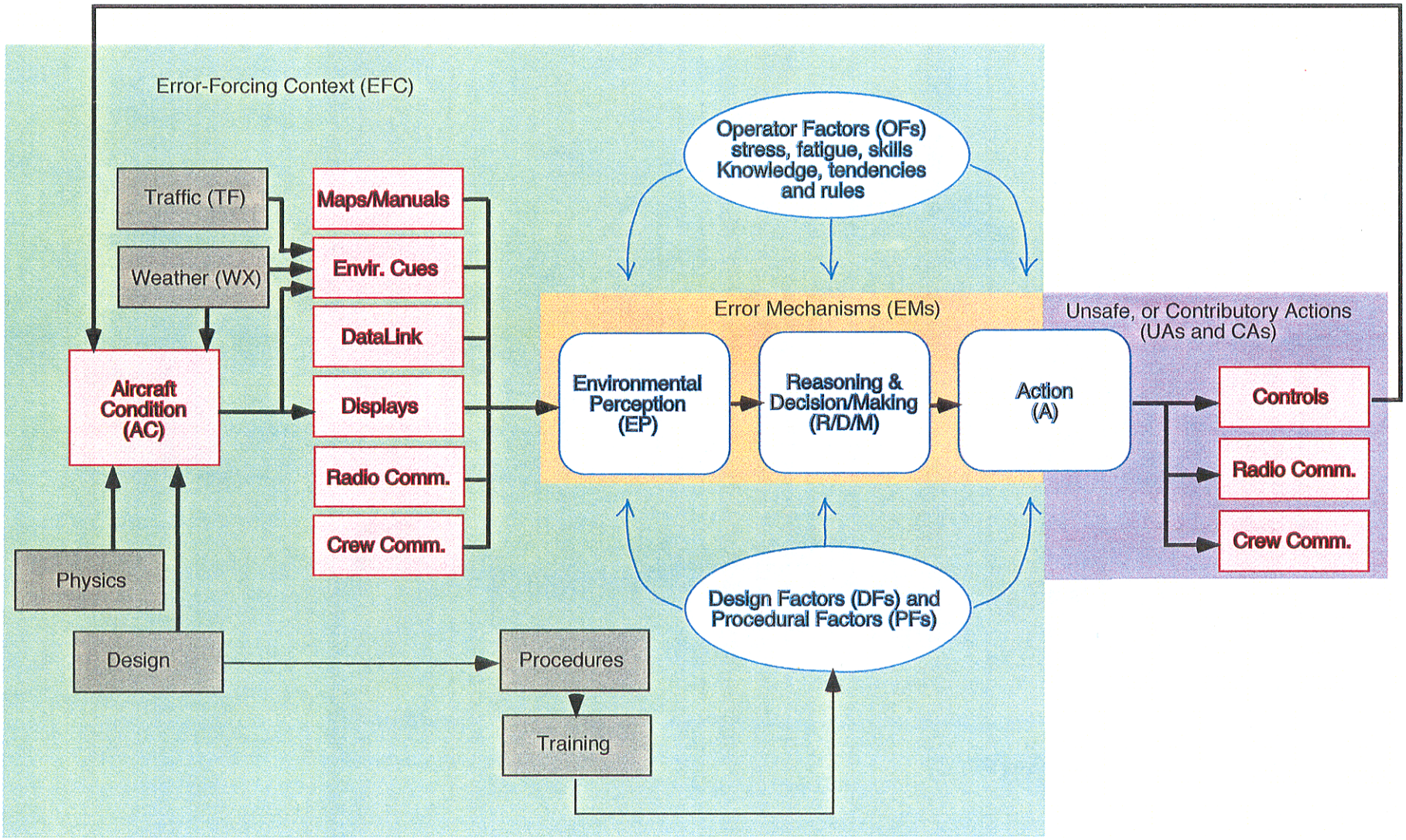

Figure 1. ASHRAM Cognitive Model Diagram

The three segments of the cognitive model are necessarily interactive and non-sequential. That is, all environmental perception (EP) does not occur prior to reasoning and decision-making, and all reasoning and decision-making (R/D/M) does not occur prior to initiation of action. There is overlap and non-linearity. There are implied feedback and feed-forward loops among the stages. Automatic motoric processes could be seen as a bypass around the R/D/M stage. The model is not intended to describe how people think and behave, but is more a structure from which intelligent discussions of human information processing and human reliability can evolve. A detailed description of the individual stages may further illuminate these concepts.

1. *Environmental Perception (EP).* Much deliberation has taken place regarding the term to be used for this stage of processing. Although it may have been easier to just use the term "situation awareness," the authors feel that some of the controversy surrounding this term may be avoided by using a connotatively neutral term (see Appendix D for a discussion on this). EP includes perceptual processes, attention, detection, recognition, monitoring, interpretation of environmental cues, and overall understanding of the state of the aircraft/environment system.

2. *Reasoning and Decision-Making (R/D/M).* This stage includes cognitive or thinking processes, such as awareness and deduction of unsafe or dangerous conditions, remembering situation-specific training, deciding to follow recommended procedures, planning flight navigation, diagnosis of trouble symptoms, deciding how to respond to situations, problem solving, and novel or creative use of existing tools or systems).

3. *Action* (A): This stage includes control inputs to airframe, operating control hardware in the cockpit, communications to crew and passengers, and any other overt physical behaviors.

Referring to Figure 1, environmental information is divided into six channels for the pilots, including: environmental cues (things happening outside the aircraft, such as weather), radio communications (includes ATC, ground control, other planes, and intercom to other crew members), displays and controls (flight and systems instrumentation, control yoke, trim wheels, switches and cockpit computer input devices), a datalink (screen listing pilot reports [PIREPs] etc.), verbal communication with other crew members, and available literature in the cockpit (maps, charts, procedures, and checklists). Three of these six channels are driven by external (to the cockpit) events, including weather; the airspace and its monitoring by ATC and other aircraft; and current airframe status, which is determined by the design, the laws of physics, and inputs made on the control surfaces made by the pilot(s).

At the right side of Figure 1, are the outputs of the pilot, namely pressures put on controls which operate control surfaces (such as elevators) and other airframe systems (such as engines or hydraulic pumps); radio/intercom communications (to crew, passengers, and entities external to the aircraft); and interpersonal communications with crew.

In the middle of Figure 1, is the three-stage operator model (rounded boxes) between the environmental inputs and the control outputs. The two ellipses above and below the three stages depict two sets of influences on performance-shaping factors (PSFs) that affect all three stages of processing. Swain (Ref.9.3) introduced the term PSFs back in1967, and it has become common usage. By PSFs, he meant "any factor that influences human performance." Swain further differentiates PSFs into internal and external varieties. By internal, he meant operator characteristics that would affect the performance of a job, such as stress, fatigue, knowledge, personality, bodily structure, skills, experiences, and attitudes. External PSFs include factors external to the individual, such as human-system interface (HSI) design, organizational structure and rewards, training programs, and written procedures. External and internal PSFs can be closely associated—to the point where they can become difficult to distinguish. Consider something in the environment that causes stress within the individual. The stressor might be a poorly designed flight instrument, while the stress induced within the individual might manifest itself as poor tracking performance.

Because PSFs have served in the past as a catch-all for explaining less-than-adequate human performance in complex systems, and because mitigations have very different implications, we think a larger distinction needs to be made between internal and external PSFs. Since internal PSFs are those elements internal to the human operator, such as experience, intelligence, fatigue, etc., we'll refer to these as *operator factors* (OFs). Improving OFs, or making them less susceptible to error might include additional simulator training, longer rest periods between flights, more frequent eye exams, etc. External PSFs, on the other hand, are features of the man-made environment that may affect performance, such as navigational display design, safety procedures, approach chart nomenclature, etc. These factors will be referred to as *design factors* (DFs). Improving DFs, or attempting to make pilot errors less likely, might include relabeling instruments with more legible lettering, designing flight management systems to be more easily manually overridden, or establishing wider mandatory separations among aircraft on final approach. Table 2 illustrates the distinction between OFs and DFs.

Table 2. Differences Between Operator and Design Factors

Operator Factors	Design Factors
Fatigue level	Instrument set, layout
Stress level	Logic of FMS
Knowledge	Airframe response
Skills and talents	Radio protocols
Personality, leadership	Chart legibility
Experience	CRM practices

Error mechanisms (EMs) are psychological mechanisms that can contribute to human errors if employed inappropriately, or out of context. That is, they are internal cognitive processes that have been cultivated over time to deal with environmental demands that may tax limited processing resources, such as attention or short-term memory. Inappropriately applied, they lead to confusion and can precipitate unsafe acts. An example may best illustrate the concept. A pilot develops an expectation bias for events to unfold in a way similar to previously experienced

events. When cleared to taxi to a given runway for takeoff, a pilot may assume that the ground controller has given permission to cross active runways, if that has been the preponderance of his experiences, when in fact the current situation may require him to hold and ask for clearance to cross at each opportunity. Here, the expectation bias may influence the pilot not to ask for clarification. Although this assumption would be valid and time-saving at the appropriate airports, it can lead to unsafe conditions at other airports. Figure1 shows EMs as primarily affecting the first two cognitive stages, i.e. EP and R/D/M. This is because by the time action is being taken, cognitive processes have largely played themselves out and motor-control issues pertain. The concept of identifying EMs explicitly lies at the heart of ASHRAM and may be a key differentiating aspect of the technique.

Unsafe actions (UAs) refer to those overt actions inappropriately taken by crew members, or those not taken when needed, that result in a degradation in safety. In our example from above, the act of crossing the active runway without permission would be the UA. The term does not mean to imply that the human was the cause of the problem. This distinction avoids any inference of blame and accommodates the assessment that people are often "set up" by circumstances to make actions that are unsafe. In these circumstances, the crew does not knowingly commit an error. They were performing the "correct" action as it seemed to them at the time. UAs, by definition, violate critical flight functions (see Table 3 below).

Contributory actions (CAs) are actions taken (or omitted) that precipitate, or ultimately lead up to the UA. In and of themselves, CAs are not necessarily inappropriate or unsafe. However, in the context of the scenario, they set up, or set the stage for an unsafe act. In the runway-incursion scenario used as an example above, the assumption by the pilot that the active runway could be crossed was a CA.

Aircraft condition (AC) is the collective status of all the plane's systems and subsystems, including the plane's attitude and trajectory in the airspace. This includes the states of repair or repair history, instrument readings, performance parameters (such as altitude, rate of descent, etc.), amounts and locations of fluids onboard, cargo, engine speed, and internal air pressure. It does not include design features of the aircraft that apply to all examples of the particular model; these would be considered DFs.

The ***error-forcing context (EFC),*** a term borrowed from ATHEANA, is the combined effect of aircraft conditions, operator and design-based PSFs, procedural factors, weather, and traffic conditions that create a situation where an unsafe act is likely. This concept is central to the ASHRAM technique in that pilots are assumed to be performing to their best ability (we cannot address malevolent behavior per se) to complete the mission at hand. Usually, the mission is to deliver passengers and crew safely and on-time to a destination, and happily, this is usually the outcome. However, occasionally pilots are confronted with trying or confusing situations that elicit inappropriate responses, and these situations are called EFCs.

3.3 Critical Flight Functions

Critical flight functions (CFFs) are those that are necessary for safe flight. Examples include thrust, navigation, and airframe integrity. By definition, UAs are unsafe because they jeopardize a CFF, or eliminate a required resource for a CFF. For instance, a pilot dumps fuel to decrease the risk of fire on an emergency landing, but dumps too much, so that reaching the runway is impossible due to fuel-starvation of the engines. In this case, the decision to dump fuel is a good one, and is not necessarily unsafe. In fact, it is in the name of safety that fuel dumping is employed. The decision may be a CA, however, as the UA of dumping too much would not have been possible without it. Calculating how much to dump may have been the source of the error, however the act of dumping a certain number of gallons is considered the UA. Failures in CFFs are termed critical flight function failures, or CFFFs.

Due to differences in the criticality of functions during the various phases of flight (takeoff, cruise, landing, taxiing), Table 3 has been developed to identify them explicitly.

Table 3. Critical Flight Functions for Various Phases of Flight

	Taxi	Takeoff	Cruise	Appr./Depart.	Landing
Thrust	√		√	√	
Max. Thrust		√			
Navigation				√	
Attitude Control		√	√	√	√
Radio Comm.	√	√		√	√
Pressurization/O2			√		
Nosewheel Steering	√				
Flight Instruments		√	√	√	√
Airframe integrity		√	√	√	√
Separation	√	√	√	√	√

Again, the purpose of the cognitive model is not to provide a detailed map of how people think and behave, but to establish a common language upon which the ASHRAM procedure can rely. Users are encouraged to keep a copy of Figure 1 handy when completing steps in either the retrospective analyses of accidents that have already taken place, or in the prospective analyses of accidents and incidents yet to happen.

4. RETROSPECTIVE ANALYSIS

4.1 Introduction

A retrospective analysis technique has been developed for examining and analyzing aviation accidents and incidents that have already taken place and been documented (or personally experienced by the user). The purpose of the retrospective analysis is to unravel the event anew, using ASHRAM model constructs and terminology to ultimately uncover and describe the error-forcing context (EFC) that contributed to the event. This EFC can then be considered in terms of how it may occur in similar aviation scenarios, so that mitigating measures can be employed to reduce the risk of future errors and ensuing incidents or accidents.

There is another purpose in analyzing an event retrospectively. In later chapters of this report, users will learn how to develop a base-case scenario, from which variations are spawned, representing the many ways things can go wrong. In an effort to link the seemingly disparate retrospective and prospective analyses, an optional final step of the retrospective analysis will ask the analyst to consider what issues and base-cases could be abstracted from the specific accident scenario. Having identified the EFC and the base-case, the potential for other actions and errors that are not necessarily part of the accident, might be identified. The identification of potential errors and their likely causes is a primary objective of the prospective analysis.

The analyst should consider at this point whether a retrospective analysis is the appropriate next step, or if proceeding to the next chapter on the prospective analysis method is warranted.

4.2 Retrospective Process Overview

The user will collect all of the resources describing the event and proceed to:

1. identify the event of interest via aircraft type, location, date, etc.
2. identify the author of the current analysis
3. write a brief summary of the event
4. suggest the significance of the event
5. identify the critical flight function that was lost
6. identify all pertinent conditions, OFs, and DFs as positive and negative influences
7. identify initial conditions of aircraft and/or crew prior to the event
8. identify the initiator of the event
9. construct a graphic timeline of the event
10. develop a time-based event log
11. perform an unsafe action analysis
12. perform a recovery analysis
13. make specific recommendations for improving flight safety
14. abstract from the current scenario, a potential issue or base-case scenario for a prospective analysis

4.3 Detailed Process Description

For the remainder of this section, a split page will be used to provide examples for the sections of the retrospective analysis as they are described. [Note that the half-page format does not allow the true portrayal of the format. See Appendix E for the full-page width example of the same event.]:

1. Event Identifier. This section identifies the incident/accident by a shorthand name, aircraft type, event date and time, problem, unsafe actions, outcome, and data sources.	**1. EVENT IDENTIFIER – Kegworth Crash** **Event Name:** Kegworth Crash **Aircraft Type:** B737 Series 400 **Date & Time:** 01/08/89, 20:24 **Problem:** Engine vibration and fire **Unsafe Acts:** Crew shut down good engine **Outcome:** Crash with 47 fatalities **Sources:** SkyNet special report, Air Accidents Investigation Branch Aircraft Accident Report No: 4/90 EW/C1095
2. Author(s). This section merely identifies the author(s) of the analysis, his/her/their organization, the date on which it was performed, and any contact information the author wishes to include.	**2. Analysis Performed by:** Dwight Miller Sandia National Laboratories dpmille@sandia.gov (505) 845-9803 March 12-25, 1999
3. Event Summary. This describes the event in sufficient detail to extract the key elements for the analysis, including, ACs, CAs, UAs, and significant PSFs. This summary could be taken in total from source material, excerpted, or rewritten in a concise summary form. [The example shown is a combination of excerpts and rewritten summation.] If some documentation is biased, in error, or leads to incorrect conclusions, the author may wish to include it and add his/her interpretation of the events.	**3. Event Summary: (abbreviated)** A British Midland Airways Boeing 737 Series 400 aircraft, while climbing through FL283 on its flight from London to Belfast, experienced moderate to severe vibration, shuddering, or rattling, accompanied by the smell of fire in the cockpit. Although the airborne vibration monitoring (AVM) system indicated elevated vibration levels there was no warning of fire on the flight deck. The commander took control of the aircraft and disengaged the autopilot. The commander asked the first officer which engine was causing the trouble and the latter responded "it's the le...it's the right one." At 19 seconds after the onset of the vibrations the commander requested the first officer to "throttle it [#2] back." [According to the FDR, the #2 engine (on the right side) had steady indications, but engine #1 (on the left side) showed strong vibrations, elevated exhaust gas temperatures, increased fuel flow...

	3. Event Summary: (abbreviated) (Cont.) ...About 13 nautical miles (nm) from touchdown, ATC advised a right turn. Power was increased to the operating engine (#1) and the FDR recorded a maximum vibration again. One minute later at 900 ft. and 2.4 nm from touchdown, there was an abrupt decrease in power from the #1 engine. Despite attempts to restart the #2 engine, the airplane crashed short of the runway, killing 47 of its 118 passengers.
4. Significance of Event. This is an optional statement about the event that addresses the uniqueness, representativeness, or impact the event had (or should have) on aviation safety.	**4. Significance of Event** This event never had to happen. With proper cockpit instrumentation, or a fire management system that worked, or better communication with the cabin crew, this aircraft could have easily flown home on the one 100% good engine and the second at reduced power (or shut down). It also demonstrates how a normally appropriate safety practice (shutting down a malfunctioning engine) can lead to a disaster.
ASHRAM Summary. This is solely a header that indicates the beginning of the analysis of the event using ASHRAM-defined terminology.	**ASHRAM SUMMARY**
5. Identify Critical Flight Function. Use Table 3 to identify the phase of flight and the critical flight function that was compromised.	**5. Critical Flight Function** Departure, climb to cruise - Thrust
6. Most Negative/Positive Influences. List those factors or conditions that contributed to the problem, incident, or accident. However, the user must differentiate between the good and bad influences. That is, did the factor help to create the EFC, or provide means to avoid or recover from a UA. Also, the user is asked to identify each factor as one of the following: AC – aircraft condition DF – design factor OF – operator factor WX - weather condition TF - traffic condition	**6. Most Negative Influences (abbreviated)** - The #1 engine, which lost a fan blade tip, could continue to run at over 90% power. If the engine blew up completely, or had lost more thrust, instead of being partially disabled, the crew could have determined the source of the vibration with much higher reliability **(AC)**... - The design of the AVM display was such that neither pilot could infer from the instrumentation which engine was causing the initial vibration **(DF)** - At no time did the cabin crew, who were busy cleaning up the cabin, hear or challenge the commander's hypothesis that the vibration was coming from engine #2 **(CRM)**...

6. Most Negative/Positive Influences. (Cont.) CRM – crew resource management Significant actions taken by the crew will be analyzed in the next section.	**6. Most Negative Influences (abbreviated) (Cont.)** - Airframe dynamics, in the form of vibration and roll, were not perceived as being diagnostic of a problem in the left engine **(OF)** - The commander had only 23 hours on the series 400 B737, while the first officer had only 53 hours **(OF)** - Despite a fire in the outboard section of #1 engine for 24 minutes prior to final approach, its fire alarm did not sound until 36 seconds prior to impact **(DF)** **Most Positive Influences** - Some of the passengers noticed the inconsistency of the fire in the left engine and the commander reporting that the problem with the right engine was essentially solved, but unfortunately, none alerted the crew **(CRM)** - The commander reported that he tried to review the cockpit crew's actions when time permitted on initial approach to make sure they got it right, but the only running engine lost power and interrupted his train of thought **(AC)** - The aircraft was equipped with an airborne vibration management system (AVM), which is designed to inform the cockpit of engine vibration problems. **(DF)**...
7. Initial conditions. This section reviews all of the pertinent states of the aircraft, weather, traffic, and crew at the point of departure from routine flight conditions. If the event was initiated with a mechanical failure, emphasis should be placed on aircraft data and flight parameters at the time of failure (ACs). If the event was driven by crew errors, emphasis should be placed on crew experience, recency, etc. (OFs).	**7. Key Flight Parameter/Crew Status** **Phase:** Climbing to cruise altitude, 295 kts. CAS **Altitude**: Climbing through 28,300 ft. **Location:** 13 minutes into flight from London to Belfast **On Board:** 8 crew, 118 passengers **Mechanical**: All systems normal **Air Frame hrs.** 521 **Fuel on board:** 9281 lbs. **Cockpit crew**: Commander – male, 43, 763 hrs. in 737, 23 in Series 400, 12 hrs. last 28 days First Officer – male, 39, 192 hrs. on 737, 53 in Series 400, 37 hrs. last 28 days **Cabin crew**: Six attendants with cumulative B737 experience of 2 years 5 months

8. Initiating Event. If possible, an initiating event should be identified at a particular point in time, as this will help delimit the timeline of the analysis. If, on the other hand, a plane slowly veers off course or safety begins to degrade, the point at which the deviation is larger than normally acceptable would serve as the point of initiation.	**8. Initiating Event** 20.05.05 Loss of turbine blade tip in engine #1, leading to compressor stalls, vibration, and eventually fire.
9. Event Timeline. This analysis summarizes the events' sequence and timing by putting the initiator, CAs (contributory actions), UAs (unsafe actions), recovery actions, and equipment failures on a semi-proportional horizontal timeline along with elapsed time.	Initiator Progression Termination 0:00 +0:19 +2:07 ... 18:44 +19:38 ^ ^ ^ ^ ^ E1 CA1 UA1 E3/R4 T
10. Event Log. This table explains the elements of the timeline in order of their occurrence. It includes the event, time, and text description. Event that intervene labeled events can be added, even though the times may not be known. Also, if more than one plane, or ATC is involved, multiple, labeled columns may be used for the descriptions.	**Timeline Events (abbreviated)**

Event	*Time*	*Description*
E1	0:00	Loss of turbo fan blade tip in engine #1, onset of vibration and slight loss of thrust
CA1	+0:19	FO throttles back engine #2...
UA1	+2:07	FO shuts down engine #2...
...T	+19:38	Crash short of runway

11. Unsafe Action Analysis. This is the most important part of the retrospective analysis. The preceding ten steps were performed in preparation for this analysis. Given that the user knows and understands the UA that led to the loss of a critical flight function, he/she can work backward through the sequence of events to infer the information-processing failures in either pilot action. The flowchart shown in Figure 2 may help to elucidate this process.

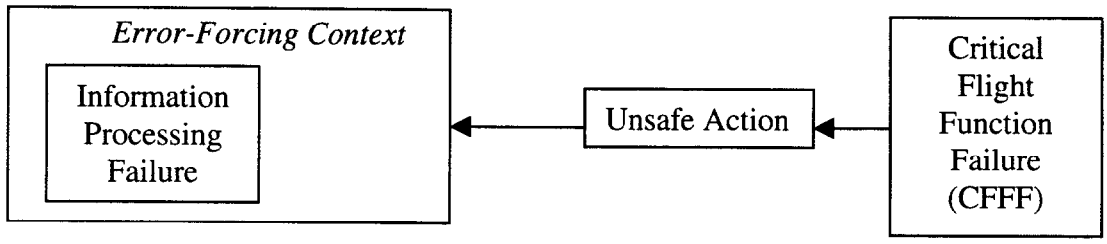

Figure 2. Flowchart of Unsafe Action Analysis

In the Kegworth example that we've been using, the following would apply. The loss of thrust (CFFF) was caused by the crew shutting down engine #2 (UA). The crew shut down engine #2 for two reasons: 1) it was incorrectly diagnosed as being problematic, and 2) safe flying practices dictate that disabled engines be shut down to prevent possible fire and/or airframe damage.

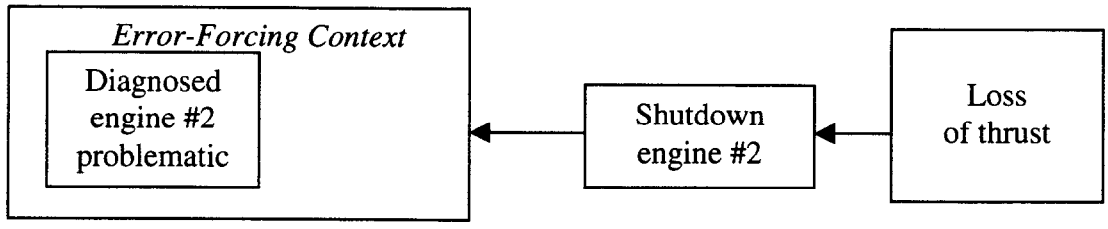

Figure 3. Kegworth Example Data

If there are more than one UA, this process should be followed for each one.

The next step is to analyze the factors and events within the left-hand box—the EFC and the information-processing errors that led to the UA. As you may recall from the cognitive model (Figure1), the EFC is comprised of the current environmental conditions, the aircraft's current state, and PSFs based on operator factors (OFs), procedural factors (PFs), design factors (DFs), and crew resource management (CRM).

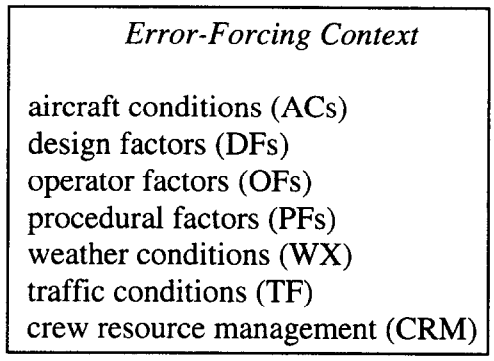

Figure 4. Elements Contributing to the EFC

One way to separate general information from factors that may have affected performance in the accident scenario is to answer the following questions:

1. *Which aircraft-related events or conditions helped to create confusion about the actual status of the plane?*

   - Minor decrease in thrust from affected engine made diagnosis ambiguous
     - Minor roll induced by asymmetric thrust
     - Instrument values did not unambiguously indicate which engine was in trouble
   - Vibration decreased when engine #2 was throttled back, confirming erroneous hypothesis
   - Smell of smoke seemed to be coming from cabin A/C vents, suggesting engine #2

2. *What aircraft design issues contributed to either poor environmental perception or interfered with appropriate control of the aircraft or its systems?*

   - Airborne vibration monitoring (AVM) displays were not adequately designed and historically are not trusted by pilots to give useful information
   - Functioning engine fire alarm system did not sound for 24 minutes

3. *Which operator or crew factors contributed to insufficient environmental perception, faulty reasoning and decision-making, or inadequate response actions?*

   - Both Pilot In Command (PIC) and First Officer (FO) had minimal hours in Series 400 B737
   - Both PIC and FO had low hours (12 and 37) in previous 28 days
   - PIC had systems knowledge of A/C system, which he used to diagnose smell of smoke coming from the wrong engine
   - Both PIC and FO did not have familiarity with AVM displays, or may have mistrusted them
   - Inability of PIC or FO to infer engine trouble from other instruments
   - Assumption that reducing thrust on bad engine alone would reduce vibrations

4. *What rules or procedural factors contributed to the accident?*

   - Procedure of reducing thrust to diagnose which engine is faulty
   - Safe-operating rule of shutting down faulty engine

5. *What weather factors contributed to the accident?*

   - None that we know of

6. *What traffic states or events contributed to the accident?*

   - None that we know of

7. *What CRM issues factored in the accident?*

   - PIC had pretty strong hypothesis that engine #2 was affected and may have biased FO in his diagnosis

   - Cabin crew did not feel responsible to take an active role in assisting cockpit crew

   - Cockpit crew did not utilize cabin crew in diagnosis process.

All of these factors had a negative influence on the situation, leading the crew to the UA of shutting down a good engine. These factors, when combined in this manner, make up the EFC for the UA. [As the EFC for the UA are enumerated, they can be entered into the unsafe action and recovery analysis summary form, shown in Section 7.1]. Additional UAs could be influenced by these same factors or completely different ones. Consequently, an individual analysis must be performed for each EFC that sets the stage for a given UA.

Once the EFC for the UA has been established, the next step is to infer the associated failure(s) in information processing that led to the UA. The cognitive model (Figure 1) shows three stages where information processing can fail; environmental perception, reasoning and decision-making, and action. Taken individually, the following example descriptions can help the analyst identify the appropriate processing stage for a given failure:

- Environmental Perception
  - pilots unaware of actual aircraft state
  - pilots unaware of the severity of aircraft conditions
  - pilots unaware of continued degradation in aircraft conditions
  - information is erroneous or misleading
  - aircraft indicators are misinterpreted
  - pilots recognize similarity of the event to other better-known events

- Reasoning and Decision-making
  - aircraft or equipment behavior is misunderstood
  - pilots select inappropriate plans/procedures
  - pilots follow prepared plans that are wrong or incomplete
  - pilots do not follow prepared plans of action or written procedures
  - pilots rely upon knowledge-based behavior, but forget key issues
  - pilots inappropriately give priority to one critical flight function over another

- Action
  - important procedural steps are missed
  - controls are inappropriately selected or operated
  - miscommunication with crew or ATC
  - equipment failures hinder pilots' ability to respond

The following analysis pertains to the Kegworth example:

For the UA of shutting down engine #2, we know that it was an intentional act, and that no errors were made in its execution. Therefore, no errors were committed in the Action stage. We know however, that the pilots could not ascertain from their instruments which engine was exhibiting vibration and diminished thrust. These are problems in environmental perception. We also know that there was some faulty reasoning in diagnosing which engine was problematic. Therefore, there were errors committed in the R/D/M stage.

Identify Error Mechanisms that Pertain

At this point the analyst would proceed to Table 4, which contains several error mechanisms associated with each information-processing stage. The error mechanisms are generic descriptions of common types of cognitive operations pilots can use in performing their job tasks. When these cognitive operations are used in situations that do not warrant their use, and actually impede progression toward a desired goal state, they are labeled error mechanisms. The analyst would go through the list for each information-processing stage and attempt to find a match between the listed error mechanisms and the inferred information processing problems associated with CAs and UAs from the timeline, or from the inferred information-processing errors from the previous section.

Table 4. Error Mechanisms Associated with Three Stages of the Cognitive Model

Stage of Cognitive Model	Error Mechanism
Environmental Perception	Wrong visual search strategy used leading to missed information
	Attention diverted to more salient stimulus
	Pattern of information directs attention away from source
	See/hear/feel stimulus, but do not perceive as relevant or important
	Cannot detect small change in stimulus
	Exhibit tunnel vision, reducing field to small subset of available stimuli
	Perceive similar stimulus as same as one in recent past, or attributable to same source, when it is different or comes from different source—recency or recognition bias

Stage of Cognitive Model	Error Mechanism
Environmental Perception (Continued)	The stimulus is out of the expected range and therefore not believed
	Stimulus is not believed to be diagnostic or trustworthy, and therefore not sought out or used when perceived
	Faulty display is followed despite incongruence with other information
	Stimulus is not actively attended to out of boredom, apathy, complacency, or fatigue
	Stimulus is not actively attended to due to belief that another is responsible for
	Sampling rate is too slow/fast to appreciate changes in value over time—if too slow, missed derivative information, if to fast changes not perceived
	Simplification—only look at or listen to part of stimulus information as shortcut
	High stress or mental workload prevent correct interpretation of perceived information
	Fixation – preoccupation with one or a few stimuli at the cost of others
	Stimuli not actively sought out because of recent experience (recency bias)
	Failure to interpret a pattern in several displays, due to the piecemeal nature of the information presentation
	Masking – one stimulus is louder or more visually salient than another simultaneous stimulus
	Failure to read correct display due to negative transfer of training (previous experience that has built up habits and expectations to look in an inappropriate place for the display of interest)
	Stimulus strength is below operator's threshold (e.g. too small to see, to faint to hear)
	Lack of familiarity with display stimuli prevents comprehension
	Expected correlations of parameters is violated, causing confusion or rejection
Reasoning/Decision-Making	While attempting to deal with multiple problems simultaneously, operator's cognitive resources are exceeded
	Fixation – operators need to move attention from one aspect of a problem to another, yet remain focused on the initial problem area, which may be minor

Stage of Cognitive Model	Error Mechanism
Reasoning/Decision-Making (Continued)	Substitution – operator relies on technical knowledge/strategy to solve problem, but uses the inappropriate knowledge/strategy
	Lack of technical knowledge
	Anxiety about taking wrong action delays or prevents action
	Expectation or Confirmation bias – operator gives more significance to information that confirms beliefs than to information which contradicts beliefs
	Frequency bias – interpretation of event based on frequently occurring events with similar characteristics
	Primacy bias – tendency to give more significance to early information, hypotheses and conclusions than later
	Recency bias – Events that happened recently are recalled more easily than events that occurred a long time ago. People tend to interpret events in terms of what has happened recently rather than relevant events that occurred in the more distant past.
	Satisfying – tendency to stop looking for a solution when an acceptable, but not necessarily optimal one is found.
	Simplification – tendency to disregard complex aspects of data, such as interactions, and give more significance to aspects they more completely understand
	Ego involvement – operator believes his diagnosis/solution is best, despite competing and possibly more appropriate ones
	Single fault assumption – tendency to disregard the possibility of two or more independent failures occurring closely together
	Cause/effect relationship assumption – tendency to assume a cause-effect relationship between or among events that occur simultaneously
	Eagerness to solve or respond quickly leads to sub-optimal performance
	Trust in instrumentation despite inconsistencies that would suggest faulty instruments
Action	Inappropriate motor response (motor program) initiated
	Environmental factors force an action error (e.g. G forces)
	Operate incorrect control due to proximity/similarity confusion
	Inability to perform fine motor controls required
	Inability to apply required force to control
	Control reversal (e.g. turn clockwise instead of counterclockwise)
	Take action with inappropriate timing (late or early)
	Repeat action when not necessary or appropriate
	Misspeak to associate or crew member
	Inability to control dynamics while tracking a high-order system
	Muscular tremor prevents smooth fine motor control

This step goes beyond the traditional level of analysis for aircraft accidents or incidents. Why is this done? What is the purpose? Recall that one of the goals of ASHRAM is to identify problems or predict accidents that have not yet occurred. The abstraction of applicable error mechanisms that can occur in a particular EFC can lead to the suggestion of whole families of events that can lead to disaster. It is one of the benefits of scientific inquiry to abstract from the specific to the general, state the theory or hypotheses about the operating mechanisms, and then attempt to predict future, unexperienced cases from the general. That is what is expected here. The error mechanisms in Table 4 are recognizable, frequent information-processing operations that are used by people all the time. Most of the time they facilitate performance by reducing demands on limited cognitive resources. However, when they are inappropriately applied, unsafe acts can occur. If an appropriate error mechanism can be found which matches the event, it or they can be entered into the unsafe action and recovery analysis summary form, shown in Section 7.1.

12. ***Recovery Analysis.*** In most situations, if a pilot or ATC controller makes a mistake, he/she has opportunities to recover from the error. There are exceptions however, as when the timeline no longer allows the recovery action to negate the error. An example is when a go-around is desired after the landing plane has passed through decision height. The physical inertia of the system disallows cost-free recovery. Similarly, extinguishing an engine fire on takeoff roll or initial climb handcuffs the crew into needing to perform their responses quickly and accurately, with little room for error, because the timing and the physics do not allow for recovery from error. However, in most cases, pilots can take some time to make decisions and take actions. Additionally, they often have time after the actions to evaluate what they have done and determine if it was correct.

In a sense, missed recovery paths are errors in and of themselves. They are often errors in environmental perception and often lead to errors of omission in the sense that action is *not* taken to recover. Analysis of why recovery actions are not made can be as important to the field of aviation safety as the study of the initial UA. For the sake of clarity, recovery actions and missed opportunities for recovery will only apply to events following the UA, and not share the terminology of the actions leading to the unsafe condition. For instance, in the Kegworth scenario, the FO was asked by the PIC which engine he thought was problematic, and he identified #2—the wrong one. Although this may have been a recovery loop for the faulty diagnosis of the PIC, the UA of shutting down the wrong engine had not yet occurred, so there was no overt act from which to recover yet. Therefore the FO's response to the PIC, confirming his hypothesis as to which engine was failing, would not be considered a missed opportunity for recovery, but more a missed opportunity for avoiding the UA.

The Kegworth crash is a good example for missed opportunities for recovery. When the plane was headed for its diversion air field, the PIC attempted to review all of the decisions and actions one more time, just to make sure the cockpit crew had acted appropriately. Unfortunately, he was interrupted by a radio message from ATC and never resumed the review. Additional recovery paths in the Kegworth accident that were missed, including:

- No fire alarm for affected engine until final approach
- Passengers and cabin crew looking out window at engine fire
- No observance of worse-than-typical engine performance from instruments

Perhaps the most obvious error mechanism that was operating during the Kegworth event was confirmation bias. In this case, someone gets an idea of the nature of the problem and becomes much more receptive to information that confirms the hypothesis than to information that refutes it. Confirmation bias can become so effective as to virtually extinguish searching for alternatives or for new information after a decision is made, as in the Kegworth scenario. It can operate in the early diagnosis phases of an emergency, as well as during the remainder of the flight, when recovery paths present themselves and are not taken advantage of.

13. ***Safety Improvements.*** At this point in the process, the analyst is asked to provide suggestions for improving different aspects of the system, based on the findings. Often source documents describing the event can be used for suggestions. However, because the ASHRAM technique examines information-processing errors in such detail, the analyst is uniquely equipped to provide insightful suggestions for changes to hardware, software, training, procedures, and CRM protocols. Improvement suggestions should not be limited to cockpit operations, but should address some aspect of human performance. The entire ATC system is fair game. Suggested improvements can also be supplied by source documentation.

14. ***Issue Source.*** The next two chapters explain how a safety issue of concern that involves the effect human performance on risk can be addressed prospectively. Typically the source of an issue is one of the following:

- Federal Aviation Administration
- National Transportation Safety Board
- National Aeronautics and Space Administration
- Airline management
- Pilots associations
- ATC unions
- Insurance companies
- The general public
- The courts

The retrospective analysis can also serve as an additional source of issues for study. An abstraction from the specific accident scenario to a more general case may be warranted. For instance, the Kegworth crash might be used to suggest a base case involving an engine failure during cruise. [In fact, this is what was chosen as an example of a base case in the following chapters.] The Kegworth crash may also suggest other issues for study, including interaction with cabin crew for systems status diagnosis or the investigation of ATC radio communication and its impact on critical cockpit operations.

5. PROSPECTIVE ANALYSIS OVERVIEW

5.1 Introduction

The prospective analysis is a means of generating a number of plausible scenarios for a given seed issue. This chapter is optional for the reader, but recommended, as it establishes the goals and rationale, and summarizes the general process and expected results of the prospective analysis. The flowchart of the search process (Figure 5) is especially useful for getting an overall feel for the technique. Section 6 gives the step-by-step details for performing a prospective analysis.

5.2 Rationale and Goals

The rationale for performing a prospective ASHRAM analysis is always, generally speaking, based on the intention of improving aviation safety. Having stated the obvious, there are other reasons, which should be weighed against the anticipated level of effort required. If the need is to develop a quantitative estimate (either single point or distribution) for a given scenario or UA, other HRA techniques may need to be used in conjunction with ASHRAM (see Section 6.12). However, if the analyst is interested in exploring cognitive functions that may explain why errors were made, or how UAs can occur given different sets of environmental conditions, then ASHRAM is a sufficient and good choice.

The overall goals of the ASHRAM are stated in Section 1. The four that apply specifically to the prospective analysis are repeated here:

- identify potential unsafe human actions and accident scenarios that have, as of yet, not been documented
- identify elements of error-forcing contexts that contribute to known unsafe actions
- analyze and model situations where pilots may perform actions not required for emergency response, or intentionally disable safety systems, in the course of attempting to solve or reduce problems
- model and document families of related undesirable aviation events

The ASHRAM prospective analysis achieves these goals by creating large numbers of plausible scenarios from a given set of initial conditions and other basic assumptions and criteria. Although the emphasis is on generating plausible scenarios and UAs, ASHRAM also provides for the search for contributing factors in an EFC, given a UA has already been identified.

5.3 Assembling the Team of Subject-Matter Experts

ASHRAM calls for the assemblage of a group of subject-matter experts (SMEs), which can systematically proceed through the 'search' process for sequences of events and plausible

scenarios that can lead to aviation accidents. The more areas of relevant expertise that can be applied to the prospective process, the higher the probability of a more complete and valid outcome. One analyst can probably perform a prospective analyses, if he/she has adequate systems knowledge and experience in the areas listed below, however, the use of several subject-matter experts increases the breadth of knowledge and experience, stimulates contrasting views, and provides a self-correcting system of checks and balances. The suggested areas of expertise include:

- current state of aviation safety and political climate (issue selection)
- familiarity/experience with ASHRAM
- information sources and availability (data, statistics, procedures, etc.)
- flying an aircraft of same type or model
- ATC or ground control operations (optional)
- aircraft mechanical/electrical/hydraulic systems (optional)
- weather (optional)
- aviation safety analysis, HRA, human factors engineering, or cognitive psychology
- team process facilitator (optional)

The optional areas of expertise apply only to specific needs based on the issues. If response to wind shear is being studied, a weather expert may be appropriate. If response to a hydraulic leak and pressure loss is involved, a hydraulic or mechanical engineer might be appropriate. Because the cost of assembling a team of professionals for just a few days can be surprisingly high, the principals will have to exercise sound judgment and forethought in planning the exercise.

5.4 Time to Complete Prospective Analysis

It is estimated that, depending on the issue, the availability of critical source information, and the capability of the experts to exercise constructive teamwork, a typical prospective analysis could take as little time as a few days to complete a simple analysis. At the other end of the spectrum, with exceptions to those assumptions, a team could take several weeks or even months to hash out all the details of a large set of deviation scenarios. The ASHRAM procedures and materials have been designed to promote efficient analysis and documentation. Under normal circumstances, a nominal prospective analysis should take approximately one week.

5.5 Process Overview

Figure 5 is a flowchart representing the major steps of the prospective analysis. Details on the steps outlined here are provided in the next chapter. The first step is to establish the issue to be researched. Issues can be generated from a number of sources, including recent hardware failures, event reviews, research programs and, as suggested in Chapter 4, retrospective analyses. Step 2 defines the scope by putting limitations on the domain of analysis. This is accomplished by establishing initial conditions, assumptions, and initiating events. A base-case scenario is defined next--usually a hypothetical scenario, where the crew successfully deals with a given initiating event in a textbook manner, called the Consensus Operator Model (COM). The base-

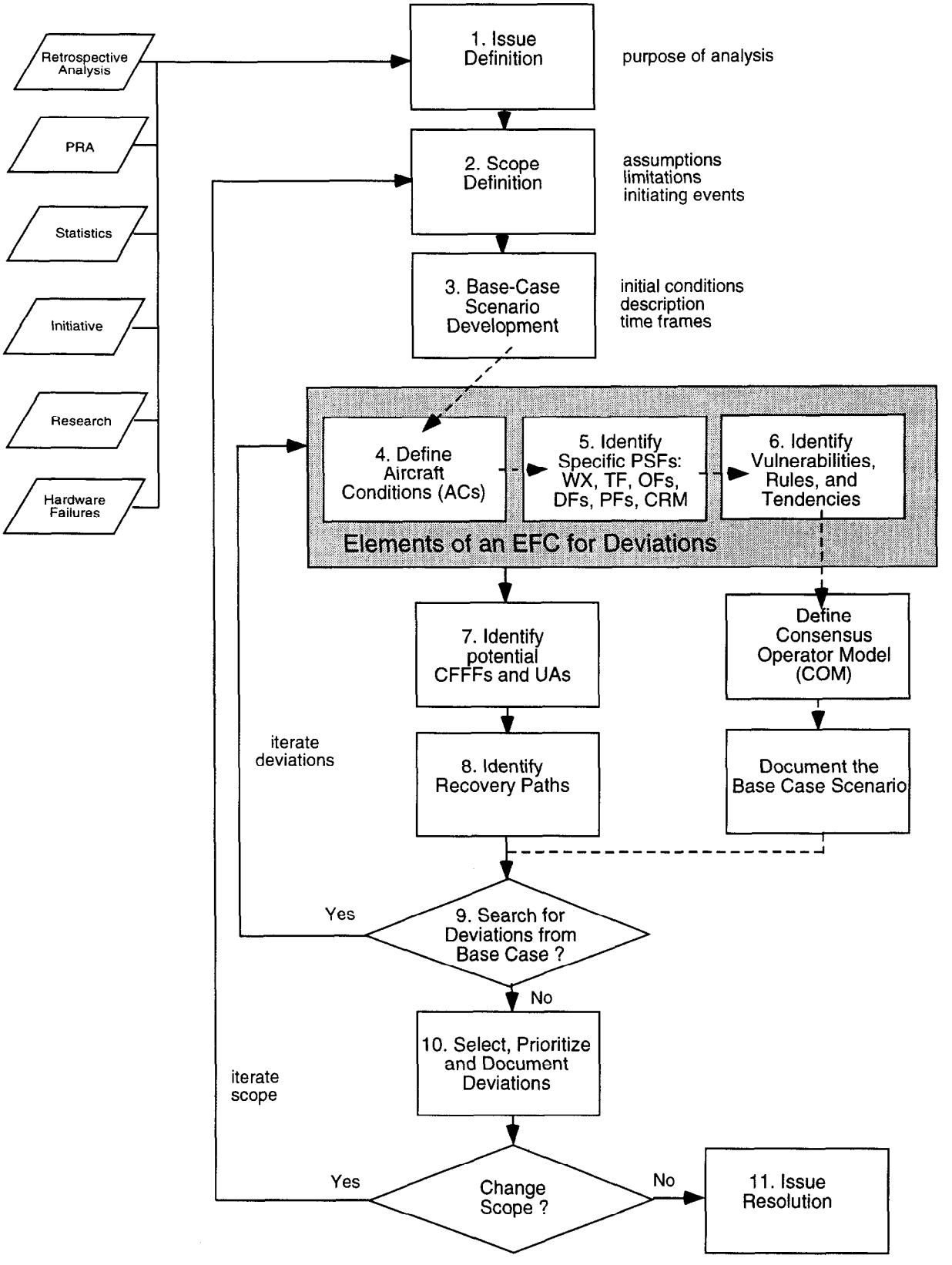

Figure 5. Flowchart Outlining the Prospective Analysis Process

case scenario also includes initial conditions, time frames of interest, nominal aircraft states (ACs), and assumptions about PSFs.

After defining the base-case scenario, variations or "deviations" are generated via two iterative cycles, beginning with Step 9. The first iterative loop has the analyst systematically vary ACs, PSFs, and relevant knowledge vulnerabilities, applicable rules and pilot tendencies. The second loop iteratively alters the scope of the analysis, thereby creating new base-case scenarios. CFFFs and UAs of interest are identified in Step 7. These can come from predetermined interests in the issue and scope, or can be generated by the analyst, based on the EFCs. Potential recovery paths are considered in Step 8, and if no additional iterations are appropriate, the issue is documented in Step 10 and resolved in Step 11. This approach provides a systematic, exhaustive, prospective analysis for the issue at hand. When the issue changes, another prospective analysis can be performed.

5.6 Evolution of the EFC

Perhaps the most important box in Figure 5 is the EFC (shaded). Recall that one of the underlying premises of ASHRAM is that pilots and others in the aviation system make mistakes and perform UAs not because they are incompetent or forgetful, but because the situation they are emersed in triggers behaviors that are inappropriate, thus the term "error-forcing context". Because the base-case scenario is defined as a successful, textbook scenario (no errors), the EFC does not really apply, or at least the pilots do not fall prey to the EFC. However, because there are ACs, PSFs, and rules and tendencies that do apply to the base-case scenario, the same box is used in Figure 5 to indicate the similarity or parallelism. A generic term for the box might be "performance context," rather than EFC.

The analyst or team can revisit the Steps 4 through 6 and change the conditions to explore what effects they might have on performance. For example, adverse weather may be added to Step 5, causing more ambiguity to airframe handling cues in the base-case of single engine failure. Turbulent conditions may make engine identification more difficult, increasing the likelihood of a misdiagnosis. There is no limit to the number of changes that can be made in Steps 4 through 6, except by limitations imposed by the scope, or by logic, physics, and aerodynamics.

5.7 Process Output

A concerted effort was made to develop a process that is not only easy to follow, but one where the look and feel of the final products could be set up as concrete expectations. Consequently, the support documentation for the prospective analysis process has been designed to lead the analyst through the process and provide standardized format for the output. A running example will be used in the next chapter (just as in the retrospective case) to demonstrate the concepts, processes, and outputs. The example will be differentiated from text and tables by its characteristic box, indented margins, and slightly smaller, slightly different font.

5.8 Priorities

Although best results will be obtained from a team-based effort, it may be financially necessary for the team of SMEs to assemble and work collectively on only part of the prospective analysis. We think the critical steps benefiting from this approach are issue selection, base-case scenario development, and the search for deviations.

The following chapter, which gives the detailed steps for the prospective analysis is written to support the following procedure:

1. make a copy of the prospective analysis blank form in Section 7.2
2. read and follow the detailed step description
3. fill out the appropriate part of the blank form as each step is completed

As an alternative, the headings of the fill-in forms can be electronically reproduced in a word-processing application, and analysts can fill in electronically as the process unfolds. Eventually, if an electronic or on-line version of ASHRAM is developed, this process will be made even more convenient.

5.9 End Products

At the end of the prospective analysis, if no steps are omitted, the team will have the following:

- a list of relevant classes and examples of initiating events
- a detailed description of a base-case scenario and consensus operator model
- identifications of UAs, CFFs and error mechanisms
- an outline of the anticipated timeframe of the scenarios
- descriptions of deviation (from the base-case) scenarios
- an analysis of relevant performance-shaping factors
- an evaluation of potential recovery modes
- an appraisal of which deviant scenarios are most relevant to the future of aviation safety.

6. PROSPECTIVE ANALYSIS – DETAILED PROCESS

6.1 Step 1. Define the Issue

In defining the core issue to be explored and analyzed, the user is, in effect, stating the purpose or the reason for performing the prospective analysis. In writing this step, and referring to it regularly during the prospective analysis, the user can more consistently remain on target as questions arise during the ensuing branching and decision-making required in the search process. This step also communicates the direction and content of the prospective analysis to the readers of the report.

The sources for issues primarily include the following:

- ASHRAM retrospective analysis of an accident or incident
- probabilistic risk assessments (PRAs)
- statistics from government agencies, such as FAA, NTSB, etc.
- airline safety management programs
- aviation-safety initiatives
- research results from government institutes, private companies, or universities
- recent observed upward trend in hardware or system failures
- a recent accident that raises operator performance concerns
- members of the public

The analyst clearly and concisely states the issue to be analyzed. Background information is optional, but if included, should be brief. What is required is a succinct statement describing the issue, indicating to the extent practicable the general boundaries for the analysis, the goal, and the relationship of the issue to risk and aviation safety. In cases where the issue is selected and provided by others, but defined and written up by the ASHRAM team, review and approval of the issue definition by the provider is highly recommended.

6.1.1 Abstraction from a Specific Case

The Kegworth crash provides us with a recognizable example of a class of problems where an engine fails during the final stages of climb to cruise and the crew must respond appropriately. However, whereas the Kegworth story is very specific, an issue is more generic. The Kegworth scenario may very well be one scenario that is a product of the prospective analysis, but it is by no means the only product. The analyst who looks to specific accidents for inspiration, needs to step back from them to abstract a more generic class of events, based on similar initiating events, flight circumstances, and EFCs. *[This is a very important, necessary part of the issue-development process!]* A more general case of the Kegworth accident is abstracted below for use as an example for the prospective analysis. The product of step one may look something like what follows:

1. Define the Issue

Within the past 20 years, there have been several cases where cockpit crews have inadvertently shut down operable engines. Examine the issue of a crew experiencing a partial-engine failure and reacting appropriately to conclude the flight safely. Investigate deviations and reasonable variations that could lead to UAs.

a. *Boundaries* – limit analysis to jet airframes that are significantly affected by the loss of one engine – limit to partial loss of one engine, or where cues as to which engine is affected are ambiguous
b. *Goals* – identify potential UAs, and associated EFCs and error mechanisms that could lead to loss of thrust or some other CFFF
c. *Relationships to risk and aviation safety* – analysis may lead to improved designs or safety procedures.

6.2 Step 2. Define the Scope and Initiating Events

This step limits the scope of the analysis by setting additional boundaries of concern around the issue, including initiators, assumptions, system-related initial conditions, critical flight functional failures, and possible sets of human responses. The scope is best determined at the beginning of the prospective analysis, and should remain constant for the base-case scenario and the development of its plausible deviations (inner loop of Figure 5). Revisitation of the scope is recommended to limit the proliferation of deviations. As deviation scenarios are teased out and exhausted, the scope can be changed, and then iteratively revised (outer loop of Figure 5). Suggested parameters of scope include, but should not be limited to:

- type or series of aircraft
- number, and/or experience level of cockpit crewmembers
- phase of flight, or specific operation, such as "land and hold short"
- ground operations or communication with ground control
- CFFs compromised
- nature or class of the initiating event
- magnitude of the equipment failure (if applicable)
- cockpit workload level
- simultaneity of events
- specific emergency procedure
- specific PRA, or UA from a PRA
- parties responsible (ATC, cockpit crew, etc.)
- equipment being operated

For example, a recent surge in runway-incursion accidents and incidents at dusk has prompted a prospective analysis of communication problems among tower, ground control and pilots. The analysts wish to examine the process of getting taxi instructions for ground control to the

appropriate active runway. Since runway incursions occur among all types of aircraft, regardless of size, no limits are put on the aircraft type or number of crew. CFFs are limited to operations at an airfield, namely taxi, takeoff, and landing. In this case, we're primarily interested in two planes (or more) attempting to occupy the same space at the same time, or the CFF of separation. Equipment being operated could span the range of any communication, navigation, or other systems controls used during the preparation of a flight (during taxi), or in takeoff and landing. Cockpit workload could be assumed to be rather high, due to the necessary transitions being made and vigilant observation of other craft. The following product reflects the scope definition for the runway incursion example:

2. Define the Scope and Initiating Events (runway incursion)

a. Scope limitations:
   runway incursions (this is the UA being studied)
   dusk illumination conditions
   ground operations
   communication with ground control or transition to/from tower
   all mechanical and electrical systems operational as designed

b. Relevant Initiating Events:
   ambiguous communication from tower or ground control
   tower loses track of one plane

6.2.1 Initiating Events

An important element in defining the scope of the prospective analysis is establishing initiating events. Although initiating events is listed as a scope parameter in the previous discussion, if it is not used to limit scope, it can be used with other scope parameters to define the analysis space. In addition to providing domain boundaries, initiating events can also spark the generation of base-case or deviation scenarios. Typically, in aircraft accidents, an initiating event is a mechanical, electrical, or chemical failure or change of state that requires responses on the part of the crew. However, as we know, human actions can also be initiating events. A misinterpreted communication, a misperceived instrument, or a false assumption about an approach plate can lead to humans taking actions that lead to problems. All prospective accident scenarios have initiating events, even though they may not be overt or observable. It is important to identify the initiating event so that the timeline can be established as starting there. Although pre-existing conditions, such as maintenance errors, degraded parts, design flaws, and crew training, may be extremely important contributions to an accident, they are not considered as initiating events, but as contributing factors that can lead to initiating events, namely ACs, OFs and DFs. The initiating event is selected or identified for the convenience of the analysis. There is no exact set of rules that make an initiating event correct or incorrect. For the purposes of discussion, an initiating event is defined as:

- *any discrete event that happens during a flight that perturbs the steady-state, nominal, or expected operation of the flight, that challenges airplane control and creates a unique context for potential UAs.*

- *if no discrete event can be identified, as in a slow drifting off-course, the analyst may choose an arbitrary point during the continuous event, or the next identifiable, discrete event following the continuous event.*

If it is helpful, the analyst may consider the distinction between direct and indirect initiating events. Up to this point, the discussion has assumed direct initiating events. Indirect initiating events are those that contribute to or set the stage for an initiating event. They may, in and of themselves, never lead to an initiating event or an unsafe condition. For instance, a fuel tank drains itself through a leak and leads to a low-fuel-pressure warning light and eventual engine misfire or flameout. The initiating event is the fuel-starved engine and decrease in thrust, to which the crew must respond. The indirect initiator was the leak that was caused by a maintenance mistake, which could have taken place days or weeks before.

Another potentially helpful way of considering initiating events, is by looking at classes of initiating events and examples within each class. This organization technique can help the analyst tease out an exhaustive list of potential ways that a particular CFF may be compromised. In our example, the list of classes and examples of initiating events applies for loss of a single engine. Combined with the previously discussed scope limitations, the final product appears as follows:

2. Define the Scope and Initiating Events

a. Scope Limitations:

Engine failure occurs during normal cruise configuration
Engine failure leads to significant loss of thrust and destination diversion
Cockpit crew is functioning normally w/currency requirements fulfilled
Cabin crew is functioning normally w/currency requirements fulfilled

b. Relevant Initiating Events:

Class of Initiating Event	Example Initiating Event
Internal engine failure	Broken fan blade Bearing failure Turbine shaft failure Pump malfunction Fire
Supply failure (indirect)	Electrical Fuel problem Lubrication leak/inadequate reserve

Class of Initiating Event	Example Initiating Event
External event	Bird/debris ingestion Collision with another aircraft Weather-hail/snow/rain—flame-out Lightning
Cockpit-initiated	Power-back Fire extinguisher activated inadvertently Fuel pump cut-off switches, Etc.
Automated sources	Fuel management system Autopilot-related problem

6.3 Step 3. Describe the Base-Case Scenario

A base-case scenario is a normative, representative sequence of events that emerges naturally from the issue, scope, and initiating events. The base-case scenario represents the most realistic description of expected aircraft and crew behavior, and typically has a successful outcome. It provides a basis from which numerous deviation scenarios can be identified and described, hereafter referred to as simply deviations. It is the deviations that usually include UAs and can result in unsuccessful outcomes. Additional characteristics of base-case scenarios are:

- is well-defined operationally
- has well-defined physics and aerodynamics
- it makes reasonable assumptions based on most likely conditions
- may be well documented in public or proprietary references (e.g. training or qualification exam scenarios)

Because the base-case scenario is based on a textbook case and has a successful outcome, the progression through the flow chart in Figure 5 differs from the progression that deviations follow. Steps 7 and 8 are bypassed, as they do not apply. A bypass loop, where the COM is defined, substitutes for steps 7 and 8. Usually, one base-case scenario will be used in a prospective analysis at a time. Occasionally, there may be advantages to processing several related base-case scenarios in one analysis. An example of this is when several equally realistic initiating events might cause very similar symptoms and require similar responses by the crew. If this is the case, a change in scope is warranted.

6.3.1 Aircraft Conditions

In addition to a written description of nominal base-case events, the analyst must also consider what the most relevant nominal aircraft conditions (ACs) will be over the time frames of interest (see next step). These might include:

- flight attitudes affected (yaw and roll)
- vibration and noise
- status of certain instruments (N1, N2, EGT, oil press., vibration, fire alarms, etc.)

Although there may be no definitive source of information for the ACs of interest, the appropriate SMEs on the team will have to make their best estimates of the behavior of relevant parameters over the time frames of interest. Later, as deviations are generated, the team can create estimates of concomitant parameters. It may be valuable to generate parameter plots over time to sufficiently describe their behaviors. Figure 6 below provides examples of plots for the single-engine failure base-case scenario. They demonstrate that noise and vibration increase very quickly from the initiating event (at T_0) and remain high until the source is altered in some way. Asymmetric yaw is introduced at the same time, but that normal pilot (or autopilot) reaction is to counter the effect with opposite rudder, negating the yaw (if not excessive).

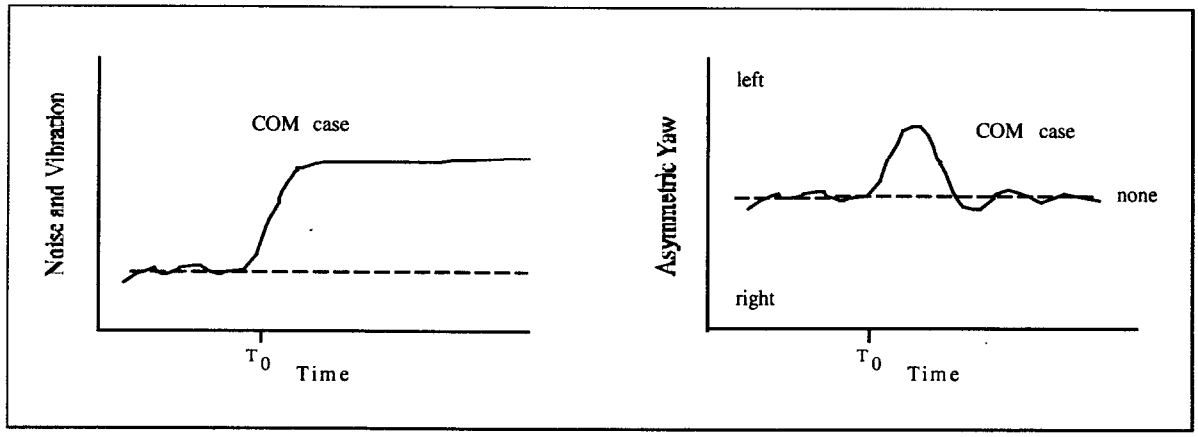

Figure 6. Example Parameter Plots for Noise and Vibration and Asymetric Yaw

6.3.2 Estimate Time Frames of Interest

Because events can happen quickly in flying operations, it is advantageous to have a set of anticipated time frames. Each time frame can serve as an estimated window of opportunity for a certain event to take place. Knowing which segments of a base-case scenario can happen quickly and which can happen more slowly, can help the analyst anticipate the information-processing constraints put on the crew. For example, if a response is needed in 5 seconds, a checklist will most likely not be consulted prior to the response. Recall that a timeline was developed for the retrospective analysis. This treatment is analogous to the timeline, however, estimated bands of time are used instead of point estimates, as the analyst will not know actual, precise timing for a prospective event. The following is an example, based on the single-engine failure base-case scenario, and would normally be expected to pertain to many of the deviations, except those based on timing changes:

Time Frame	Major Occurrences	Influences on/by Pilots
Initial conditions	Normal cruise conditions	Routine, pilots in supervisory mode
Source event 0-5 sec.	Onset of vibrations, loss of thrust, possibly change in pitch and yaw	Pilots alert and begin to react by correcting any change in attitude via flight controls, disengage autopilot
Environ-ment perception 5-20 sec.	Vibrations continue and probably continue to worsen, possibly additional cues such as smell of smoke, etc.	Pilots search for cues in environment that would suggest nature of problem, airframe, engines, subsystems, etc.
R/D/M - Preliminary dia-gnosis 15-35 sec.	Problem may stabilize or continue to degrade	Pilots have narrowed possibilities and have agreed on probable source of problem—engine
R/D/M - Response plan 35-50 secs.	Problem may stabilize or continue to degrade	Pilots agree on action strategy to confirm preliminary diagnosis or to mitigate problem—power back one engine
Execute Action 50-90 secs.	Vibration may diminish if engine speed is reduced	Pilots power back suspected engine and appraise any change in symptoms
Situation communic ation 40-100 secs.	Problem may stabilize, or continue to degrade	Pilots report situation to radar control or ATC
Response confirmati on 60-120 secs.	Either a change in vibrations occurs or does not	Change in symptoms or instru-ment readings would confirm preliminary diagnosis and lead to safe shutdown of bad engine, no change would suggest it may be something else
Diversion plan 100-200 secs.	If craft has a disabled engine, a diversion should be sought after	Pilots look at maps and confer ATC to coordinate best diversion plan
Execute diversion plan 200 secs. - end	Regardless of problem stabilization, crew needs to divert as soon as possible	Pilots attempt to get plane on ground as quickly as possible

6.3.3 Consensus Operator Model

The most important component of the base-case scenario is the COM. If a scenario is well defined and consistently understood among many pilots, the COM is the consensus, most-appropriate set of crew responses. The COM may be reflected in airline-published checklists. If actual, best practices deviate from published checklists, the best practices would prevail as the COM, if pilots can agree. Not all events will have COMs that are agreed to by most pilots. In those cases, a COM will have to be decided upon by the analyst that represents the most appropriate set of pilot responses to the problems at hand.

The initiating event and the COM together form the basis for a base-case scenario. Ideally, the description for the base-case scenario should include the following:

- a description of initial conditions of the plane, flight, and crew
- a list of assumed causes of the initiating event
- a list of any other assumptions that are pertinent to the scenario
- a brief, general description of the expected sequence of events, starting slightly before the initiating event
- a description of the expected sequence and timing of aircraft behavior and responses
- the expected trajectories of key flight parameters, plotted over time
- key pilot actions expected during the scenario progression

Our example of Step 3, based on a partial engine failure, follows:

3. Describe the Base Case Scenario (single, partial engine failure)

a. *Assumed initial conditions, including aircraft conditions:*
level cruise altitude, wings level, trimmed pitch
all systems operational
current, legal, rested crew
passengers are onboard
enough time to deal with problem
pilot and copilot, minimum
good flight weather, IFR conditions
instrumentation is fully operational
adequate fuel onboard

b. *Assumed causes:*
turbine fan blade failure that leads to partial loss of power in the affected engine

c. *Expected sequence of events (COM)*
onset/increase of noise/vibration from somewhere
pilots notice (if perceptible) and make control changes necessary to maintain flight level

3. Describe the Base Case Scenario (single, partial engine failure)

c. *Expected sequence of events (COM) (Cont.)*

Pilots begin diagnosis of situation
- engine or some other source of vibration?
- check with other pilot for any changes made
- check engine gauges
- check systems panel

Pilots decide it is an engine problem
- which engine?

Pilots determine from gauges and yaw that engine #1 is failing
- how bad is it?

Pilots throttle back engine #1 to determine severity of problem
- shut affected engine down?
- route diversion options—fuel/time availability?

Pilots decide to shut down affected engine
- power back affected engine
- make control adjustments—power increase to good engines
- perform engine shut-down checklist procedures

Pilots report situation to radar control/company
- decide on best route diversion option
- make changes in flight controls to change course

Pilots report situation to cabin crew and passengers

Pilots conduct remainder of flight to diversion airport

d. *Full description of base-case/COM scenario*

The plane is cruising at altitude in IFR conditions, with legal, unexpired, unfatigued crew, in an otherwise fully operational airframe, when a turbine fan blade fails. The blade exits the rear of the engine but the imbalance imposed on the turbine shaft continues to cause progressive damage over time. This event causes an immediate decrease in engine RPM, a 10 percent decrease in thrust, noise (audible in cockpit), and noticeable airframe vibrations. The flight attitude is immediately affected in the following way: observable asymmetric yaw and slight roll towards the affected engine, slight nose-down, decrease in airspeed.

The first response of the pilot in command (in this case we'll assume it's the first officer) is to turn off the autopilot, apply opposite rudder, level the wings using the ailerons, and to grab the throttle controls to confirm power settings. Both pilots begin to diagnose the apparent failure by scanning the instruments and looking for external visual cues as to the cause of the symptoms. As time progresses, the vibrations get stronger and eventually smoke may be smelled on the flight deck. Due to

3. Describe the Base Case Scenario (single, partial engine failure)
d. *Full description of base-case/COM scenario (Cont.)*

experience with simulator training, the pilots' initial thought is that an engine has failed, and that a decrease in power to that engine might reduce the vibration and noise (and most certainly reduce the likelihood of uncontrolled fire or airframe damage). As the first officer flies the plane level, the captain examines the EPR gauges (or N1 and N2 if so equipped), EGR, fuel flow, and vibration indications fed by the airborne vibration monitor (AVM) system to see if one engine demonstrates any anomalies. He notices a slight decrease in EPR and fuel flow, and a non-zero indication of vibration for engine 1. He looks to the other instruments to find another possible source of the noise and vibration. Satisfying himself that it must be engine 1, he asks the first officer to confirm his hypothesis. When the flying first officer confirms that yaw and roll correction is consistent with engine #1 losing thrust, the captain throttles back engine 1, and power is increased to the other engines. Noise and vibration begin to abate, but flight attitude anomalies get stronger. Convinced that correct source of problem has been identified, the captain announces to the first officer that he will proceed with shutting down engine 1. If no fire alarms have sounded, the captain may choose not to pull the fire extinguisher T-handle, and proceeds with a checklist-based shutdown procedure. As the affected engine winds down, noise and vibration continue to decrease, as airspeed drops, and asymmetric attitudes require increasing opposite control inputs. Trim settings are readjusted by the first officer, as the captain remains vigilant for any signs of fire in engine 1.

Once the situation is stabilized, the pilots confer on diversion options and communicate with radar control for vectors to the nearest suitable diversion airfield. The pilots then make a change in heading to expedite safe arrival and reprogram the FMS with new data. At their first opportunity, the flight deck reports the situation to the cabin passengers and crew. The crew continues to fly safely to the diversion airfield.

6.3.4 Entering Step 4

At this point in the process, there is a divergence in procedure between base-case scenarios and deviations. For the base case, the EFC may be present, but the pilots respond correctly despite the factors that might otherwise entice them to perform UAs. As a result, it is not helpful to consider the definitions of ACs, PSFs, and knowledge vulnerabilities, rules and tendencies, defined in steps 4, 5, and 6, as the EFC per se. All of these factors are described in the base-case scenario narrative, or can be expressed in lists and tables, however they are not systematically

treated as in the process of developing deviant scenarios. Figure 5 is drawn to reflect this difference in base-case scenario development. The arrows indicating flow for the base case are dashed and "skip over" the shaded box labeled "Elements of an EFC for Deviations." They proceed to two boxes on the right-hand side to define the COM and document the base case. This loop is followed only once for each base-case and set of related deviations. In contrast, searching for deviant scenarios begins after base-case documentation with Step 9 and cycles up through Steps 4, 5, 6, 7, and 8 in an iterative manner until all deviant scenarios are exhausted for the given set of initial conditions, assumptions and limitations outlined in Steps 2 and 3.

6.4 Step 4. Define Aircraft Conditions

For the base-case scenario, aircraft conditions have already been described. After the decision to search for deviations has been made (in Step 9), new and different ACs need to be defined that change the situation and can potentially contribute to an EFC. Perhaps the most important source of variation to the EFC, the ACs need to be redefined as iterations of deviations proceed. As the way the plane responds to changes from the base-case scenario script, the EFC changes, generating additional potential deviations and associated UAs. For example, an engine that had significant vibrations smoothes out and runs normally for the remainder of the flight. This change of AC may lead to the assumption that the engine is in perfect condition, when it in fact has problems. The analyst should use Table 5 as an instigator to explore any reasonable (meaning that the physics are valid) changes in ACs that would account for candidate deviation scenarios.

Table 5. Classes and Examples of Ways in Which ACs Can Change

Class of AC Change	Examples of Specific Changes in ACs
Improvement /degradation	- engine reverts to normal operation - engine explodes
increase/decrease, more/less	- engine fails more dramatically or completely very mild, almost imperceptible vibration
Subsystem dependency effects	- vibration causes fuel line to loosen and leak fuel - fuel pump causes fuel starvation
timing—too rapidly/too slowly	- vibration onset very slowly, - thrust loss is large and immediate
repeated elsewhere	- other engine begins to vibrate and make noise

Two examples of how the AC parameters can differ from the base case can be observed in Figures 7 and 8.

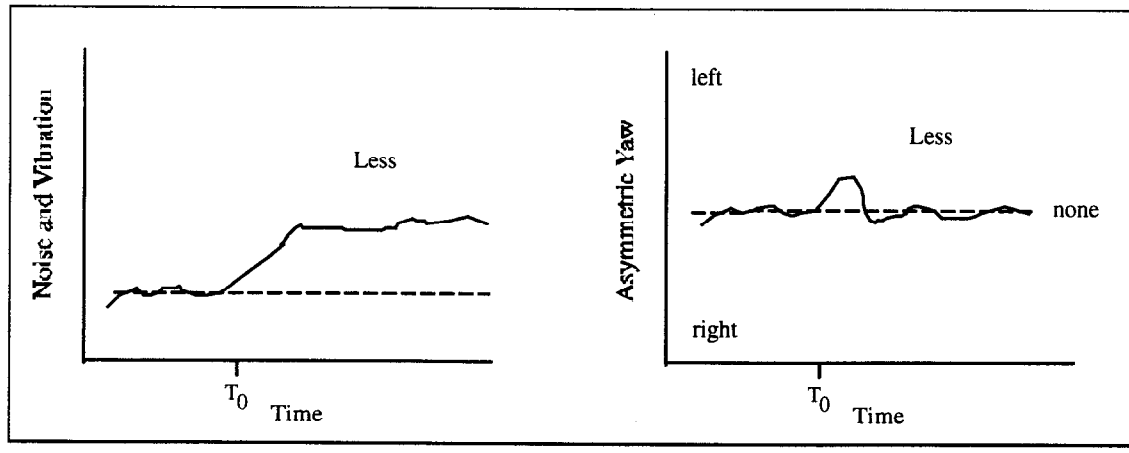

Figure 7. Slow Onset of Noise and Vibration and Low Magnitude Asymetric Yaw

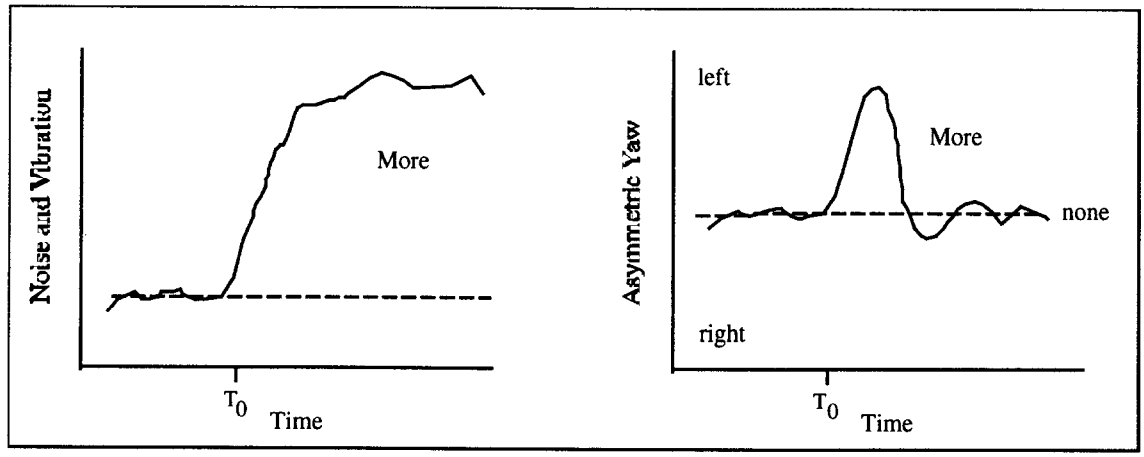

Figure 8. Rapid Onset of Noise and Vibration and High Magnitude Asymetric Yaw

This first pair represents the case where the onset of symptoms is slower and the magnitude smaller. This second pair represents the case where the onset of symptoms is more rapid and of higher magnitude.

6.5 Step 5. Identify Relevant PSFs

At this point, PSFs need to be considered as conditions that may make information-processing or action errors more likely. The PSFs, when combined with the aircraft conditions (ACs) form the error-forcing contexts (EFCs). The PSFs could be based on weather (WX), traffic (TF), operator factors (OFs), design factors (DFs), procedural factors (PFs), and crew-resource-management (CRM) issues. As PSFs and EFCs get identified, they will serve as fertile ground for UAs and CFFFs discussed in the following step.

Because so many PSFs can have negative impacts on human performance, the analyst is advised to attempt to separate out the generic from the specific. The generic, such as fatigue and bad weather, may apply to most aircraft operations, and in this sense may not add valuable insight to the base-case scenario at hand, or to potential mitigating design or procedural fixes. However, to be thorough, the generic PSFs that may apply should probably be listed. Generic PSFs, which apply to virtually all aircraft operations, are listed below in Table 6. The analyst may chose those that seem relevant to the current prospective analysis.

Table 6. Generic PSFs that Apply to Most Aircraft Operations

Class of PSF	Generic PSFs
Weather (WX)	- turbulence affecting stability of aircraft attitude - wind shear affecting vertical stability - precipitation and low temperature – icing conditions - precipitation affecting engine performance - temperature and humidity affecting takeoff and landing performance - ground precipitation affecting runway surface - electrical storm affecting aircraft electrical systems - strong headwind or tailwind affecting flight schedule - wind direction affecting direction of approach/departure - crosswinds affecting takeoff or landing - precipitation or thunder cell affecting route
Traffic (TF)	- congestion near airport, radar down, power outage, ATC problems - unsafe separation/collision potential - light/no traffic affecting expected route conditions
Operator factors (OFs)	- pilot fatigue - pilot training - pilot experience in type/series - pilot management style - pilot knowledge of mechanical design
Design factors (DFs)	- glass cockpit - autothrottle - autopilot - flight management system - aircraft handling characteristics - display features
Procedural factors (PFs)	- emergency procedure/checklist use - radio communication protocol
Crew resource management (CRM)	- delegation of responsibility for fly/fix situations - use of cabin crew in emergencies - pilots' cross-checking process

Specific PSFs are those which are judged to have highly interactive effects with, or significant impacts upon the base-case scenario and COM. Examples of specific PSFs that apply to the base-case scenario outlined in Step 3 are listed below:

Step 5. Identify Specific PSFs	
Class of PSF	**Specific PSFs**
weather (WX)	- icing conditions affecting handling of plane might interfere with handling changes resulting from asymmetric thrust
traffic (TF)	- inability to proceed to diversion of choice, prolonging exposure to reduced thrust
operator factors (OFs)	- knowledge of aircraft air conditioning system - recent simulator exercises involving engine failure - recent experience in model and series - stress effects on diagnostic thinking and problem-solving
Design factors (DFs)	- airborne vibration monitoring (AVM) system displays poorly designed - AVM system's inability to isolate source of vibration - cannot see engines from cockpit
procedural factors (PFs)	- under what conditions will crew shut down an engine - what are engine-diagnosis procedures when ambiguous cues
crew resource management (CRM)	- communication with cabin crew about engine fire - who can diagnose engine failure best

6.6 Step 6. Identify Knowledge-base Vulnerabilities, Relevant Rules, and Tendencies

Not every pilot can be expected to know everything about his aircraft, its systems, their interrelationships, and all symptoms of all possible problems. Chances are, pilots are most knowledgeable and familiar with problems on which they train regularly, recently publicized mishaps, and simple, straightforward, cause-and-effect relationships. This step attempts to identify any relevant gaps in the knowledge base associated with the base-case scenario, the behavior of its systems, relationships among its interacting systems, etc. The analyst will identify these potential knowledge-base vulnerabilities in this step.

In addition, the aviation system uses hundreds of rules to keep it safe. Rules are intended and designed to keep pilots and crews from performing UAs. Rules help to keep pilot's and cockpit crew's behaviors predictable and, hopefully, out of conflict with other crew's behaviors in nearby airspace. Some rules are formalized by an airline or government agency, while others are considered best practices or 'rules of thumb.' Regardless, because rules can be extremely influential in determining pilot behavior, they must be considered within the context of performing UAs. Rules are considered apart from PFs (in the PSFs) because they may or may not be expressed as specific procedures to be followed in particular circumstances.

Tendencies in pilots' behaviors are the most likely courses of action based on experience, knowledge, and rules. A tendency to respond in a particular manner to a situation may at first

seem to be the most natural, comfortable set of decisions and actions. In some cases, the familiar response is so comfortable and automatic, that little R/D/M takes place—as soon as a familiar situation is recognized, an aligned set of responses begins to be executed. Tendencies are analogous to error mechanisms in that they are correctly applied most of the time, and save cognitive processing effort. However, when they are used in the wrong situation, they are considered errors in the R/D/M stage of information processing, and UAs can result. For the base case of single-engine failure, the following list of vulnerabilities, rules, and tendencies applies:

Step 6. Identify Knowledge-base Vulnerabilities, Relevant Rules, and Tendencies

Vulnerabilities

a. Due to infrequency of losing engines and time span since last simulator exercise, pilots may not have the skills necessary to correctly determine which engine failed based on cockpit indications alone. More specifically, vibration indications that are not normally used in everyday operations may be somewhat foreign to pilots and therefore not interpretable.

b. Experience with a given craft may predispose pilots to expect a particular engine to be the one most likely to fail. This could increase chances of not relying on the symptomatic information alone to make the diagnosis.

c. Pilots' incomplete mental model of how the aircraft systems work can affect how they diagnose problems. This may be due to incomplete training or training that was completed long ago, or limited hours in the specific craft, many recent hours in a similar craft, or very few recent hours in the specific craft.

Rules

a. Pilot's tendency to respond immediately to radio contact will interfere with the diagnosis and response to a problem, especially the thought processes that might lead to a complete and correct problem characterization and diagnosis.

b. As a safety measure, pilots learn to shut down broken engines to lessen the likelihood of fire or airframe damage. If errors are made in diagnosis, the drive to shut an engine down quickly can lead to shutting down the wrong engine.

Tendencies

a. Tendency to react quickly to noise/vibration from partial engine failure. Pilots do not wish to take any more time than is absolutely necessary to identify and reduce power to the faulty engine. They can sense asymmetrical power and any imbalances in the engines, especially if engines are on the wings. Pilots don't like vibrations and wish to solve the problem quickly, thereby increasing the likelihood of making a mistake.

b. Respect for the captain may predispose a copilot to agree with a captain's diagnosis, even when the diagnosis is incorrect, especially when the copilot is uncertain.

Step 6. Identify Knowledge-base Vulnerabilities, Relevant Rules, and Tendencies (Cont.)

c. Pilots expect that if power to the failing engine is reduced, the noise/vibration will decrease. Anything they do which decreases the noise/vibration helps to confirm that they've selected the correct engine.

d. Pilots' confidence in their abilities might prevent them from using all of their resources to diagnose engine problems, such as cabin crew and passengers.

e. Pilots may have a tendency to assume that it is relatively easy to unambiguously identify which engine is having problems.

6.6.1 Importance of the EFC

The result of completing Steps 4 through 6 is a thorough description of the EFC for the scenario(s) being considered as deviations from the base case. Recall from Chapter 1 that a philosophical premise of the ASHRAM approach, is that significant human errors occur as a result of a combination of aircraft, airspace, weather, and crew conditions and other factors that trigger error mechanisms in the pilots. As the term EFC suggests, pilots can be tricked into executing UAs, such as bypassing safety features. Exploring how changes in the EFC can lead to deviant scenarios follows from Step 9.

6.7 Step 7. Identify Potential CFFFs and UAs

As discussed earlier, the CFFFs, or critical flight function failures, are failures in the critically needed functions for safe flight (see Table 3). Whereas a CFFF is the loss of a necessary flight function, and for the sake of discussion these are limited to the entries in Table 3, any number of UAs can lead to a CFFF. For example, if loss of thrust is the CFFF, this can be brought about by a number of UAs, including:

- throttle back power to engine
- pull fire extinguisher handle for engine
- turn critical engine fuel pump off
- etc.

6.7.1 Types of UAs

Unsafe actions can come from several sources. First of all, a UA can be defined totally by context, where under one set of circumstances the action is not unsafe, but in another it becomes unsafe. An example is when a pilot changes altitude or heading and compromises airspace separation. Normally this can't happen because ATC is looking out for airspace conflicts and avoiding them when assigning altitudes and headings. Another source can be written procedures that are not 100% correct for all circumstances of use. Here the pilot goes through his procedure/checklist, usually without questioning the steps, and may put the flight in danger.

Another source is taking instructions from another, as when a PIC asks the FO to perform some cockpit action. Three UA source paths can apply here: 1) the instruction is complied with, but is an unsafe action, 2) omitting the action, when it is the correct thing to do, and 3) performing the action incorrectly or incompletely. Although many HRA techniques differentially analyze behavior based on the type of error, as in errors of omission (EOOs) and errors of commission (EOCs), ASHRAM concentrates more on the context and the error mechanisms involved.

6.7.2 Two Paths

ASHRAM is flexible in its process in that it allows the analyst to follow two general paths. The analyst can either generate UAs from variations in the EFC, or study the circumstances that may precipitate a given, pre-defined UA. The former approach is called a 'forward search' because it follows the flowchart in Figure 5 and follows the logic of UAs resulting from an EFC. This process takes full advantage of one of ASHRAM's major strengths, creating scenarios where things can go wrong without pre-defining what the UAS are. This process is discussed a little later in this section, and because no UAs are identified, it is explained in detail in Step 9.

6.7.3 Reverse Search

If the CFFFs and UAs of interest are defined, then the analyst documents them explicitly in this step, and performs a 'reverse search.' This search process consists of finding ACs, PSFs, and knowledge vulnerabilities, rules and tendencies that relate to and precipitate its manifestation. In a sense, the search is for elements of the EFC that in combination set the stage, cause confusion, and entice the pilot(s) to perform unsafe actions. This is done by moving through the cognitive model backwards—that is by beginning in the Action box and moving left to the R/D/M and EP boxes in a search to find what elements within the EFC could lead to error mechanisms that affect perception and reasoning. Before getting into the detailed machinations of this reverse-search process, the UAs of interest need to be defined. The following section presents two alternative means.

6.7.4 Defining UAs of Interest

Our single-engine out example, introduced in Step 1, includes a specific CFFF – that of lost thrust. However, the issue definition does not specifically address UAs. If it did, it might look like this (underlined text indicates differences from original):

1. Define the Issue

Within the past 20 years, there have been several cases where cockpit crews have inadvertently shut down operable engines. Examine the issue of a crew experiencing a partial engine failure and reacting appropriately to conclude the flight safely. In particular, look into ways that crew members might power back engines, reduce fuel flow, or shut them down, thereby eliminating or severely limiting available thrust for safe flight.

a. *Boundaries* – limit analysis to jet airframes that are significantly affected by the loss of one engine – limit to partial loss of one engine, or where cues as to which engine is affected are ambiguous
b. *Goals* – generate plausible scenarios where loss of thrust is inadvertently achieved, and gain an understanding of the potential contributing factors.
c. *Relationships to risk and aviation safety* – analysis may lead to improved designs or safety procedures.

Therefore, the UAs of interest that follow from this example would be:

Critical Flight Function Failures	Possible Unsafe Actions
1. Failure to maintain thrust. This CFFF covers any action or set of actions that might lead to thrust that is less than adequate.	- no throttle back of bad engine may lead to explosion, fire, or structural damage - not following appropriate procedures for engine shut-down - inadvertently reducing needed supplies for engine, such as fuel or hydraulic pressure - the wrong engine may be powered back or shut down.

Issue and scope statements may describe a very specific area of investigation, but fail to call out explicitly the CFFFs and UAs. If this is the case, the analyst may infer the CFFF and UAs of interest from the issue and scope statements and writes them in the appropriate form. The CFFFs and UAs delineated below might result from an analyst's inference of the example Steps 1 and 2, repeated here for convenience:

1. Define the Issue

Within the past 20 years, there have been several cases where cockpit crews have inadvertently shut down operable engines. Examine the issue of a crew experiencing a partial engine failure and reacting appropriately to conclude the flight safely. Investigate deviations and reasonable variations that could lead to UAs.

a. *Boundaries* – limit analysis to jet airframes that are significantly affected by the loss of one engine – limit to partial loss of one engine, or where cues as to which engine is affected are ambiguous
b. *Goals* – identify potential UAs, and associated EFCs and error mechanisms that could lead to loss of thrust or some other CFF
c. *Relationships to risk and aviation safety* – analysis may lead to improved designs or safety procedures.

2. Define the Scope and Initiating Events

a. Scope Limitations:

Engine failure occurs during normal cruise configuration
Engine failure leads to significant loss of thrust and destination diversion
Cockpit crew is functioning normally w/currency requirements fulfilled
Cabin crew is functioning normally w/currency requirements fulfilled

b. Relevant Initiating Events:

Class of Initiating Event	Example Initiating Event
Internal engine failure	Broken fan blade Bearing failure Turbine shaft failure Pump malfunction Fire
Supply failure (indirect)	Electrical Fuel problem Lubrication leak/inadequate reserve
External event	Bird/debris ingestion Collision with another aircraft Weather-hail/snow/rain—flame-out Lightning
Cockpit-initiated	Power-back Fire extinguisher activated inadvertently Fuel pump cut-off switches Etc.
Automated sources	Fuel management system Autopilot-related problem

The following CFFFs and UAs might result from the inference process:

7. Identify Potential CFFFs and UAs:	
Critical Flight Function Failures	**Unsafe Actions**
1. Failure to maintain flight control during reduction of engine thrust. This CFFF covers any action or set of actions that might lead to inappropriate attitude or altitude of the plane while discovery and recovery of engine failure are taking place.	- reverting to manual control mode and not paying attention to primary flight indicators, - flying the plane as a secondary priority, including preoccupation with diagnosis and non-primary flight displays, discussions with cockpit and cabin crew, leaving the flight deck, reading maps, extended visual confirmation of faulty engine, etc.
2. Failure to maintain thrust. This CFFF covers any action or set of actions that might lead to thrust that is less than adequate.	- the wrong engine may be powered back or shut down. - failing to shut down bad engine may lead to explosion, fire, or structural damage - inappropriate procedures for engine shut-down
3. Failure to make appropriate flight plan modification for safe navigation. This CFFF covers the subsequent decisions and actions involved in changing the flight plan in light of the new conditions.	- continuing toward original destination when there are nearer airfields - diverting to a distant field due to economics of repair or shuttling passengers - not paying attention to new symptoms that might indicate a change in engine status - taking too much time in getting plane on the ground

As the issue and scope imply, the explicitly stated CFFFs and UAs (as shown in the table above) are the ones of interest to the prospective analysis, and remain fixed throughout the analysis. Now that specific UAs are identified, the prospective analysis turns to discovering ways in which the UAs can happen. Recall that the primary goal of the prospective analysis is to generate plausible scenarios that can lead to UAs. Assuming competence in the pilots and ATC personnel, this involves looking closely at the EFC for conditions that may precipitate information-processing and action errors.

6.7.5 Reverse Search (continued)

Although Figure 5 gives an accurate depiction of the overall flow of search steps for (at least part of) the 'forward search,' it does not adequately support the 'reverse search' process. Figure 9 outlines the thought process necessary to begin the reverse search method. Taking each UA in turn, the following process applies:

Using the cognitive model for guidance, we first must ask some questions about the nature of the UA:

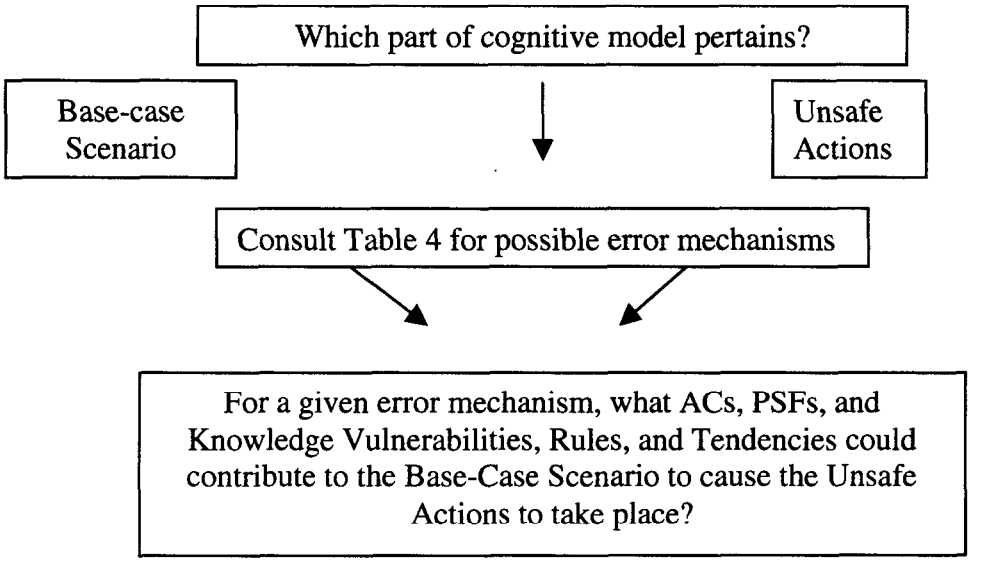

Figure 9. Outline of Reverse Search Process

Is the UA a slip? [Was the intention correct, but the execution wrong?] If so, the third box in the cognitive model, Action, is the focus of interest. Looking at Table 4 *[in Chapter 4]*, we find the error mechanisms that relate to action. From this list we can infer conditions which might contribute to the likelihood of the slip. For example:

UA = pilot pulls fire extinguisher handle and shuts down a good engine

If there is no reasonable explanation for the pilot intending to perform this UA (such as misdiagnosis), it may be an error in execution, or a slip. The pilot may have reached for the correct handle and grasped the wrong one. What factors may have contributed to this slip?

ACs = unusual attitude and g forces caused reach and grasp to locate wrong control

DFs = multiple handles are identical in shape, size and color
multiple handles are adjacent to each other
fire alarm displays are adjacent to one another

OFs = pilot trained and has experience in aircraft where handle assignments are reversed
pilot was severely fatigued and could not stabilize his reach

WX = severe turbulence caused reach and grasp to locate wrong control

CRM = copilot was reading procedure and did not confirm correct selection of control

PFs = pilot did not visually confirm his choice of control
unrecoverable actions of high consequence typically require extreme care and precision

Given the EFC elements in the example above, it is a relatively small step to build scenarios around them.

Is the UA a mistake? [Not a slip (distinction is discussed in Appendix C).] If so, the second box of the cognitive model pertains, R/D/M, or reasoning/decision-making. Looking at Table 4, we find the error mechanisms that relate to R/D/M. From this list we can infer conditions which might contribute to the likelihood of the mistake. For example:

UA = pilot pulls fire extinguisher handle and shuts down a good engine

There may be a reasonable explanation for the pilot intentionally pulling the wrong handle. What factors may have contributed to this mistake?

ACs = aircraft was incorrectly wired at factory and wrong alarm display
illuminated alarm system in engine with fire not working or disabled; both alarms sounded, but only one fire in one engine

DFs = pull handle for intended engine is on other side of cockpit from pilot

OFs = pilot trained or has extensive experience in planes that have reversed assignment of controls for engines

PFs = copilot reads shut-down procedure for wrong engine

CRM = pilot and copilot do not confer on which handle is correct

Rules/Tendencies = required speed of response causes pilots to act quickly and choose wrong control

Was the UA a result of erroneous information? If so, the first box of the cognitive model, environmental perception (EP) pertains. Looking at Table 4, we can find the error mechanisms

that relate to EP. From this list we can infer conditions which might contribute to the likelihood of the acquiring erroneous information from the environment. For example:

UA = pilot pulls fire extinguisher handle and shuts down a good engine

If the UA was not a slip, and was not the result of faulty reasoning or decision-making, then we might conclude that the pilot(s) perceive or received erroneous information. This could be due to existing erroneous information in the environment, such as a mis-wired display, or it could be due to an error in sensing or perceiving the information. After finding the potentially applicable error mechanisms in Table 4, we look to elements of the EFC that might contribute.

ACs = aircraft was incorrectly wired at factory and wrong alarm display illuminated
alarm system in engine with fire not working or disabled
both alarms sound, but only one fire in one engine
other engine parameters point to wrong engine

DFs = fire alarm displays do not specify which engine is on fire
fire alarm displays are labeled ambiguously
cannot see engines from cockpit
engines produce thrust despite fire

OFs = extreme fatigue causes pilot to misread displays
previous experience leads pilot to associate display with wrong engine

Given the EFC elements in the example above, it is a relatively small step to build scenarios around them.

6.7.6 Forward Search

As pointed out earlier in this chapter, if the analyst or team prefers to generate UAs from the EFC alone, this can be done by performing a forward search. Unlike many HRA techniques that need the unsafe actions as input to the method, and then identify relevant PSFs, or calculate human error probabilities given known scenarios, ASHRAM is somewhat unique in not only allowing for the generation of scenarios, but also the 'discovery' of UAs. This method has its advantages and disadvantages. On the positive side, it allows for the 'organic' germination of UAs directly from the initial conditions, initiating event, and EFC. This approach has advantages for a team that is talented at (or enjoys) brainstorming potential deviant scenarios. The approach also takes the pressure off of the team to generate all possible outcomes of UAs earlier in the process. This can be a very difficult and somewhat intimidating task. Forsythe and Wenner (Ref. 9.32) have extolled the virtues of this "organic approach" to HRA. They see problems with generating every possible way that operators can make errors, and see advantages in enumerating the system conditions and characteristics that breed human errors. If this

approach is taken, the analyst skips through Steps 7 and 8 in the first iteration of the flowchart in Figure 5, and goes directly to steps 4 through 6 to iterated variations in the EFC. Because no UAs are identified up front, this procedure is covered in detail in Step 9.

6.7.7 Contributory Actions

This term was first introduced in the Retrospective Analysis section. It referred to actions made by operators or ATC controllers that lead to or contribute toward an unsafe action, but in and of itself is not an unsafe action. In this strict interpretation, a faulty diagnosis of a problem, such as identifying which engine is causing vibrations is not an UA, because it does not reduce thrust. However, it contributes significantly to the UA of shutting down a good engine, which fits the definition of an unsafe action by defeating a CFF. ASHRAM does not emphasize contributory actions (CAs) because there is the potential for so many to exist in a scenario event that it would be difficult to list, discuss, and treat all of them. This is not to say that CAs cannot be very important in the analysis of how error mechanisms can lead to UAs.

6.8 Step 8. Identify Recovery Paths

The cyclic process of generating and documenting a plausible deviation scenario needs to include enumerating plausible recovery paths that prevent the scenario from ending in a terminal event. By terminal event, we mean an event that signifies the unsuccessful termination of a flight (see glossary in Appendix F). By recovery path, we mean a set of activities that catches the UA and corrects it, or instigates activities that prevent the UA from leading to a terminal event. Recovery paths are limited to activities that take place after an UA has been committed. Obviously, this step is omitted from base-case scenarios, which have no UAs and, by definition, end with a successful conclusion. For forward searches for deviant scenarios, recovery paths obviously need to be considered after the UAs are identified and full scenarios are scripted.

One of the reasons recovery paths are an important part of the scenario-generation, prospective-analysis process is that the overall likelihood of a deviation scenario proceeding toward a terminal-event conclusion is based on the probability of the unsafe act being committed combined with the probability that recovery does not occur. An 'obvious' UA, such as inadvertently shutting off a critical subsystem function (like a fuel pump), may have ample cues for recovery such as warning lights announcing a decrease in pressure, fuel-starvation symptoms from the engines and the like. The analyst/team needs to consider all of these events and their potential impact on the eventual outcome of the scenarios as they are generated. Finding ways to recover from UAs can be as involved a process or even more involved than finding ways that UAs can occur.

Recovery from unsafe actions almost necessarily implies that the crew is aware of the UA and seeks ways to mitigate an unsafe situation. There are cases where operators or crews are unaware of unsafe conditions and unknowingly avert costly consequences by inadvertently mitigating the unsafe condition. However, for the most part, crews need to be aware that something is wrong before they can have the intent or motivation to recover. Therefore, analysts should be particularly aware of the potential for UAs that are insidious, (that is, difficult to

discern), for these are the most likely to lead to terminal events. Many human error specialists would not even consider a recovery possible or "give credit" for a recovery path if the operators were not aware of an unsafe action that led to an unsafe condition.

In considering the possibilities of recovery paths for a deviation scenario, we look to the ASHRAM cognitive model for the outline of a systematic process of discovery. If there is general knowledge among the crew that an UA has been committed, stages two and three of the cognitive model predominate the approach to recovery. For instance, a pilot in command (PIC) comes into final approach too high and fast, decides to land anyway, and the crew struggles to keep the landing plane from overrunning the length of the active runway. Having made the dubious decision to land, the crew thinks of ways to brake the plane and executes them quickly—stage 2 and 3 processes. However, if there is not general knowledge of an UA, then the crew must rely on stage one processes, environmental perception, to detect the need to recover. For example, a PIC allows the airspeed to drop below safe minimum. He doesn't notice, because if he knew, he would correct for it immediately. The first officer (FO) feels something is strange, scans his instruments, and notices the anomaly—a stage 1 process—environmental perception. The FO then either says something to the PIC or grabs the yoke and throttles and corrects the mistake himself, stage 2 and 3 processes. Thus, the cognitive model can help structure the search for recovery paths.

The process of completing Step 8 is, based on the previous discussion, broken into two major paths—one for known UAs, and one for unknown UAs. Due to potential terminology confusions with the discussion in Step 7 of known and unknown UAs, the term 'intent' will be used here. Step 8 should be completed for each UA and deviation scenario derived in the previous steps.

6.8.1 Intentional Recovery from a UA

When a scenario includes a UA, very often the pilots will realize their slip, mistake, or faulty logic immediately and consider ways to undo their misdeed. If the timeline is such that there is time for the physics to be turned around, as in spooling up an idling turbofan engine, or as in completing some tasks with enough altitude to still land safely, the chances for full recovery are quite good. In fact, in most intentional recovery paths, there is very positive likelihood of a safe outcome, i.e., no terminal event. Several commercial flights are successfully concluded each day thanks to recovery paths that trivialize UAs by quick recognition and rapid response. Those flights that suffer more unfortunate outcomes are most likely limited in their ability to recover from UAs due to one or more of the following:

a. other mechanical/electrical failures
b. not enough altitude
c. inability to ascertain the real problem
d. loss of flight controls
e. etc.

Fortunately, many UAs are recognized immediately from environmental perception at the time of the UA, or some action leading to it, as a contributory action (CA). For example, a pilot

throttles back a good engine during diagnosis and finds that the noise and vibration *don't* abate. A good pilot would throttle back up as soon as possible to maintain thrust and altitude. In the recovery analysis the team needs to consider all possible recovery paths that would nullify a UA and document these along with the scenario.

6.8.2 Unintentional Recovery from UA

As mentioned previously, unsafe conditions need to be detected and identified for recovery to take place. These processes begin with environmental perception. Are there any perceptible cues available as to the nature of the condition?

a. instrument indications: e.g. rate of climb display decreasing
b. visual cues: e.g. ice forming on windshield
c. noises: e.g. a loud thump
d. smells: e.g. raw fuel, smoke
e. kinesthetic: e.g., large G forces, vibrations

Is there knowledge or intent among the crew that would allow them to perceive a discrepancy with the desired state? [This is important, because if no knowledge exists, then a conflict cannot be found, and in all likelihood, the potential for a recovery path does not exist.]

If yes, state the known referent from which there is a departure or discrepancy:

- plane is at cruise, altitude should be stable
- icing is a very hazardous condition
- unexpected loud noises in flight are suspicious
- the smell of raw fuel or smoke is not normal—may have leak or fire
- at cruise, we do not expect G forces or major vibrations

In our single-engine failure example, if the UA of shutting down the good engine takes place, there are several paths to recovery that might be identified using the process outlined above.

Are there any perceptible cues available as to the nature of the condition?

a. instrument indications: airborne vibration monitoring system shows elevated vibration levels compared to normal operating conditions, N1 and N2 (or EPR) instruments indicate lower than normal thrust, EGR shows decrement, fuel flow is lower than normal

b. visual cues: smoke and occasional fire can be seen periodically in engine

c. noises: none

d. smells: occasionally the smell of smoke

e. kinesthetic: above normal vibrations can be felt through the airframe

If yes, state the known referent from which there is a departure or discrepancy:

a. although with only one engine operating it is an absolute judgment, an experienced pilot knows what normal [cruise] operating range is for most of his instruments

b. although the pilots cannot see the engines from the flight deck in most large jets, they have the cabin crew and passengers who can assist

c. the smell of smoke in a plane is never a good thing

d. vibrations felt through the airframe are easily perceived at the onset and cessation, however adaptation can take place quickly and long-term vibrations may not be a salient cue

6.9 Step 9. Search for Deviations from Base Case?

This is a decision node in the bottom half of Figure 5, which calls for the analyst to decide if another deviation is to be searched for by reverting back to Steps 4, 5, and 6 in order to make changes in the EFC. It may be appropriate here to clarify the nature of the relationship between the base-case scenario and deviations. The base-case scenario as described in step 3, is an event that has some history, possibly some documentation, and that relates a problem and a textbook type of set of responses by the crew, or the COM. A deviation is a minor variation in some aspects that is otherwise based upon the base-case scenario. Although a different scenario altogether—complete with UAs, a deviation remains a 'family member' to a base-case scenario. Typically, in a forward search, the team plays "what if?" games to generate deviations in ACs, PSFs, vulnerabilities, rules and tendencies to create changes that could lead to UAs and CFFFs. Refer to information below and to Steps 4 through 6 for guidance on stepping through deviations. Once all the potential deviations to a base-case scenario are exhausted, the analyst proceeds to Step 10.

6.9.1 Forward Search

Typically, the process of searching for deviations assumes that the UAs of interest have not yet been identified and that the search process will help lead to their 'discovery.' As outlined in Step 7, this manner of searching is referred to as 'forward search,' as it progresses through the cognitive model from left to right, from environmental perception to action, or in a 'normal,' forward direction. That is, the analyst or team systematically varies elements of the EFC, looking for combinations that might elicit error mechanisms in perception, reasoning, or action. Figure 7 depicts an outline of the search process using ACs and PSFs, while the text below describes the details.

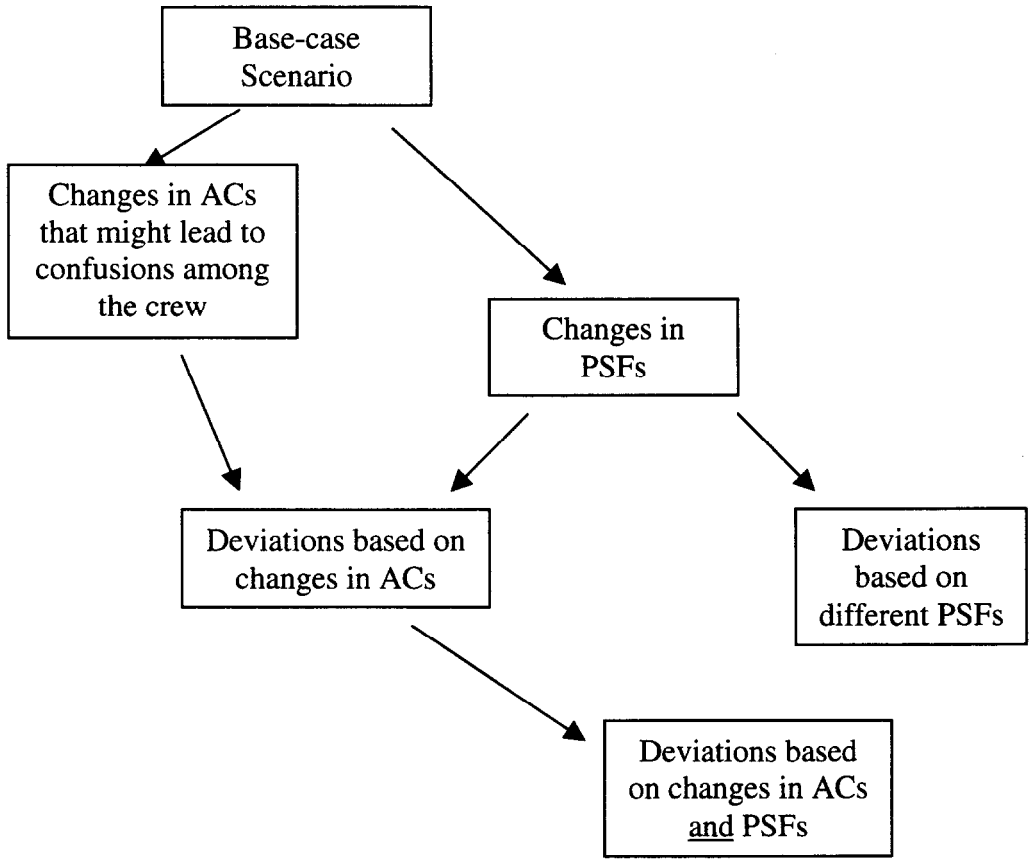

Figure 10. Strategy to Create Deviant Scenarios, Using ACs and PSFs

Go to Step 4 to explore any ACs that fit within the assumptions, limitations, and initiating events specified in Step 2 that might happen differently to cause misperceptions or confusion in the cockpit. Consult Table 5 for classes and examples of variations in aircraft conditions that could generate viable deviant scenarios. Analysts should note that very minor deviations are not of interest, unless they would lead to a variation in scenario outcome. For the partial loss-of-engine example, several possible variations exist; however, we will concentrate on two simple variations for this example. [Note that it would be more desirable to begin with a large number of deviations and to pare down the list to the most viable as the process continues. This approach ensures that good, reasonable, viable (but not necessarily highly probable) deviations do not get overlooked.] First, the onset of symptoms can be extremely gradual, leading to delayed perception and increased ambiguity about what is happening or which engine is having problems. Second, the onset can be much faster and more dramatic, leading possibly to flight-control issues and increased urgency.

Two examples of how the AC parameters can differ from the base case can be observed in Figures 7 and 8, which are repeated below for your convenience.

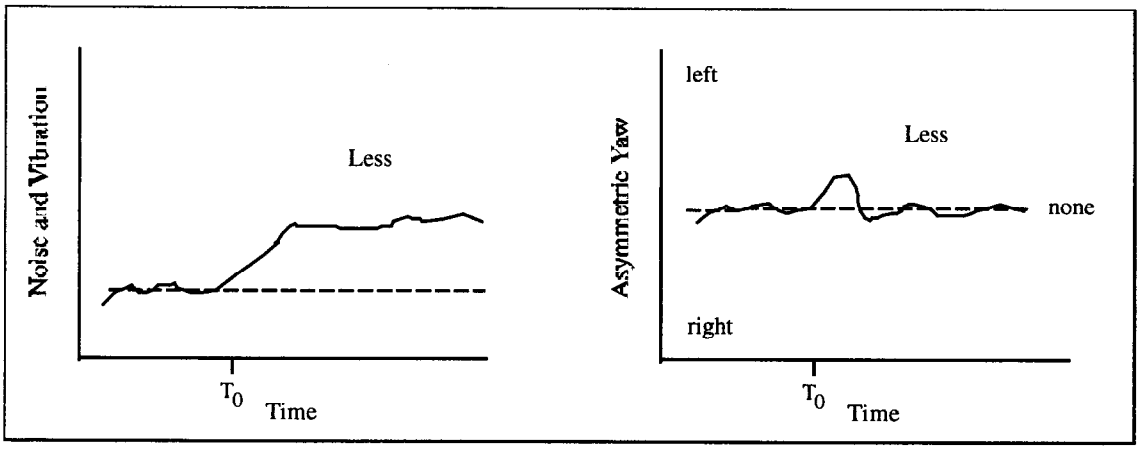

Figure 7. Slow Onset of Noise and Vibration and Low Magnitude Asymetric Yaw

This first pair represents the case where the onset of symptoms is slower and the magnitude smaller.

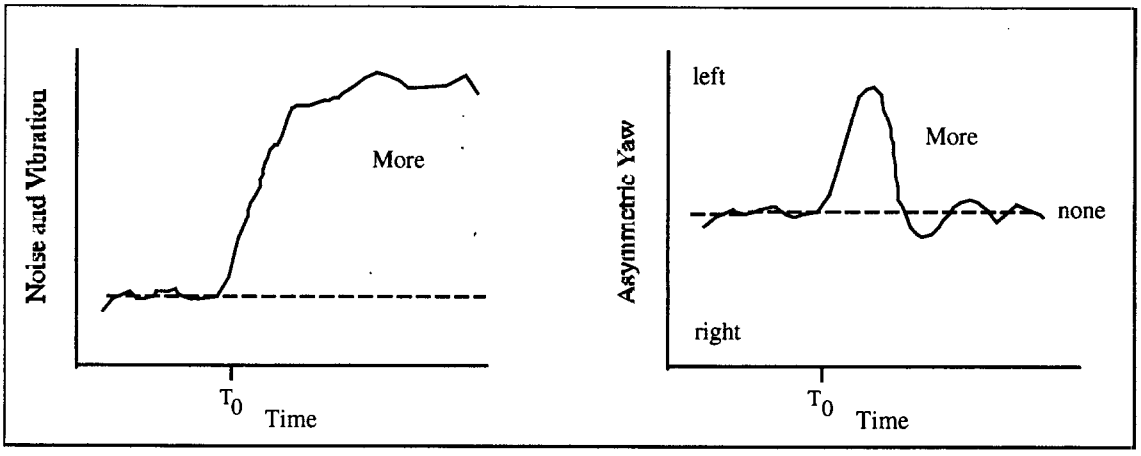

Figure 8. Rapid Onset of Noise and Vibration and High Magnitude Asymetric Yaw

This second pair represents the case where the onset of symptoms is more rapid and of higher magnitude. An example narrative of the two deviant scenarios, composed solely on the difference in AC, and no other EFC elements is shown below.

Minor/Partial Engine Failure. Physical parameters concomitant with engine failure are universally slower in developing and have lower intensity. This leads to the pilots not realizing something went wrong until later in the 'damage timeline.' Instruments do not help, as minimal deviations occur and no alarms sound. Thrust is lost gradually over time and pilots may not even realize the corrections made by the FMS. At some point, a loss in altitude would be noticed, either by the pilots, or the FMS. If this did not occur, the flight may terminate as a CFIT.

If the loss in altitude was noticed, diagnosis would begin, and the pilots would attempt to identify the affected engine. Correct identification of the affected engine is much more difficult than in the base case due to the lack of asymmetric thrust and to the minor differences in instrument readings. Readings of engine pressure ratio (EPR), fuel flow, and vibration would be very similar among the engines, if there were only minor problems. Noise and seat-of-the-pants vibration monitoring might be the strongest cues for the pilots, making diagnosis extremely difficult. If the wrong engine is identified, 'safe practices' may cause pilots to power back and possibly shut down a good engine and eventually fly to a diversion airport on a bad engine.

Dramatic Engine Failure. Physical parameters concomitant with engine failure are universally faster in developing and have higher values. In this scenario, instead of minutes available for reacting, the pilots may have only a few seconds. As the engine fails abruptly, noise and vibration shake the plane violently, the plane yaws toward the affected engine (if on the wing), the nose drops due to reduced thrust, and the pilots must react quickly to keep the plane flying level. Correct control response would be to apply opposite rudder (feet), pull up on the nose, and increase throttle to the remaining engines. Opposite aileron may be necessary if the plane starts to roll in the direction of the affected engine. Power needs to be cut to the affected engine to reduce the probability of airframe damage and fire. If the threat of fire is suspected, or if the fire alarm sounds, the fire handle for the affected engine should be pulled (cutting off flammable fluids and flooding engine nacelle with fire-suppressing foam). If the pilots cannot identify the affected engine by flight dynamics alone, deviations in the instruments would point to the affected engine (reduced EPR, fuel flow, and RPM, and increased vibration). The danger of this scenario is not misdiagnosis, but the possibility of losing control of the craft or sustaining airframe damage due to fire, explosion, or mechanical disintegration. If both of these outcomes can be avoided, the pilots should be able to fly to a diversion airport safely using the remaining engines.

As can be seen from these two deviations in the onset of symptoms, differences in ACs can have a powerful effect on deviation development—and that is why ACs are the first element of the EFC to be modulated in the search process. In the first, emphasis is put on the pilots' perceptual abilities to notice something peculiar about the state of their craft. This concentrates on the information-processing performance early in the cognitive model—environmental perception.

The second scenario, on the other hand, emphasizes quick response and expert motor-control of the aircraft. Obviously, this concentrates on the performance later in the cognitive model—action. These two examples of deviant scenarios demonstrate the powerful influence of the aircraft condition on the nature of the event.

Proceeding to Step 5, we next identify relevant PSFs that could change the process/outcome of our base-case scenario to include error mechanisms and UAs, making it a deviant scenario. This can be done in two phases. Phase one would be different PSFs that might influence the base-case scenario in and of themselves. Phase two would be PSFs that are now relevant due to changes made in ACs in Step 4. We will follow these two branches separately, but the processes are very similar.

6.9.2 Base-case scenario with different PSFs

Given the base-case scenario as a starting point, the analyst must systematically examine how changes in the various forms of PSFs might contribute to the elicitation of error mechanisms and the eventual perpetration of UAs. Referring back to Table 6, generic PSFs need to be considered as potentially contributing elements of the EFC, and the analyst is encouraged to list the most pertinent ones, along with their applicable category (WX, OF, etc.). It may be tempting to resign to the viewpoint that every PSF listed, and even some that are not, are, in fact, pertinent to the analysis. However, the limitations imposed by the scope may help narrow the field and illuminate particular PSFs that are pertinent. Next, consider *specific* PSFs that have particular relevance to the base case. Specific PSFs are those which probably would not apply to other scenarios, but because of some specific relationship, are pertinent to the base case. See the box below as an example of identifying specific PSFs that might apply to the base case.

Step 5. Identify Specific PSFs

Class of PSF	Specific PSFs
Weather (WX)	- heavy precipitation that may further complicate engine problems
Traffic (TF)	- conflicting traffic contributes to inability to proceed to diversion of choice, prolonging exposure to reduced thrust
Operator factors (OFs)	- recent simulator exercises involving engine failure - recent flight experience in model and series - stress effects on diagnostic thinking and problem-solving
Design factors (DFs)	- airborne vibration monitoring (AVM) system displays poorly designed - AVM system's inability to isolate source of vibration - cannot see engines from cockpit
Procedural factors (PFs)	- what are engine-diagnosis procedures when ambiguous cues - what procedure will crew use to shut down an engine—is it able to be restarted?

Step 5. Identify Specific PSFs	
Class of PSF	**Specific PSFs**
crew resource management (CRM)	- communication with cabin crew about engine fire - who can diagnose engine failure best—PIC or FO, while other communicates with ATC and plans diversion

Deviant Scenarios with different PSFs

Next, given that some deviant scenarios have been developed based on different aircraft conditions, PSFs need to be considered again. Generic PSFs are probably no different than those identified for the base case, however, new, specific PSFs need to be identified for the deviant scenarios. Consider the deviant scenario wherein the onset of engine-problem symptoms is much more gradual than in the base case. In this case, any hint of engine trouble would be beneficial to the crew and their situation, in that they could enact extremely vigilant monitoring of engine performance, and ostensibly be ready for any significant reduction of thrust. Here, the team/analyst might first look at factors that might help or hurt the detection of the first signs of engine trouble. This might include other noises, weather conditions that might help to obscure subtle auditory or kinesthetic cues, instrument precision that may not allow the discrimination of the small differences exhibited by minor engine damage or imbalance, or busy radio communication that might keep attention diverted from scanning instruments or listening for abnormal events. Alternatively, regarding the more dramatic engine-failure deviant scenario, the team/analyst needs to consider factors that might help or hurt the initial recovery of the plane's attitude after the sudden onset of significantly reduced thrust. These may include weather, the crew's experience with unusual flight attitudes, the design of the airframe and its inherent handling, the design of the flight instruments (especially roll, pitch, and yaw), and established pilot-copilot procedures for taking manual control of the aircraft in emergency situations. The latter CRM-related factors border on the rules, which are covered in the next step.

Moving to Step 6, the process is similar, in that the knowledge-base vulnerabilities, relevant rules, and tendencies need to be thought of and applied both to the base case and the deviant scenarios. In terms of the base case, the example box in Step 6 applies. As would be expected, knowledge vulnerabilities open up opportunities for UAs. What is more interesting, however, is how the rules and tendencies, obstensively instituted to increase the safety of operations, can work against the crew. For example, the safety practice (rule) of shutting down damaged engines is designed to prevent a bad engine from disintegrating, throwing projectiles, and damaging the wing (or other part of the airframe) on which it is mounted. This rule is beneficial almost all of the time, however this rule, when combined with a faulty diagnosis, was one of the largest contributing factors to the 1989 Kegworth accident. The tendency to respond and do something quickly in the face of threatening symptoms further increases the chances of making errors. Lists similar to the one found in Step 6 can be constructed to support deviant scenarios, with the goal of identifying UAs and generating plausible scenarios. An example follows for the AC deviation of dramatic engine failure:

Step 6. Identify Knowledge-base Vulnerabilities, Relevant Rules, and Tendencies

Vulnerabilities

a. Pilots know that if an engine fails dramatically, the resultant asymmetric yaw will point the nose toward the bad actor. If this is not known, due to training on other topics, or lack of experience, an obvious diagnosis as to which engine is faulty may not be forthcoming.

Rules

a. Pilots learn to fly the plane first, and navigate and communicate after that. A severe loss of thrust will require significant corrective, manual-control responses to keep the plane flying straight and level. As opposite rudder and aileron are applied, and compensating thrust is marshaled for recovery, the PIC is most likely near mental-workload capacity, and probably not available for other tasks, such as diagnosis.

b. As a safety measure, pilots learn to shut down broken engines to lessen the likelihood of fire or airframe damage. If errors are made in diagnosis, the drive to shut an engine down quickly can lead to shutting down the wrong engine.

Tendencies

a. Tendency to react quickly to noise/vibration from partial engine failure. Pilots do not wish to take any more time than is absolutely necessary to identify and reduce power to the faulty engine. They can sense asymmetrical power and any imbalances in the engines, especially if engines are on the wings. Pilots don't like vibrations and wish to solve the problem quickly, thereby increasing the likelihood of making a mistake.

b. Pilots expect that if power to the failing engine is reduced, the noise/vibration will decrease. Anything they do which decreases the noise/vibration helps to confirm that they've selected the correct engine.

6.9.3 Using Error Mechanisms to create Deviant Scenarios

As can be seen in the preceding sections, deviant scenarios can be generated directly from changes in ACs, PSFs, and knowledge vulnerabilities, rules and tendencies. Changes in the EFC can be powerful enough to suggest different operant rules, tendencies, responses and UAs on the part of the crew. An additional source of UAs and deviant scenarios can be garnered from Table 4. The procedure is simple. First, determine the part of the cognitive model that can be associated with the EFC element (AC, PSF, etc.). Then go to that section of Table 4 and search for any error mechanisms that apply. For example, in diagnosing the source of vibration in an airframe, the AVM system displays the magnitude of vibration. This source of information would be valuable in the base case and the slower-developing deviation. We would proceed to Table 4 and look for any error mechanisms that might interfere with the pilots' acquiring this information from the AVM system. Background information about the AVM display tells us

that in many planes, it features an instantaneous digital indication of vibration on a five-point discrete scale. We also learn from engineers and pilots that because vibration is transmitted through rigid bodies, the system cannot clearly discriminate vibrations emanating from the associated engine or another (connected to the same airframe). Looking at Table 4, two entries seem to apply and they are listed below:

Parameter needed is derivative, or a summary of parameter displayed
Stimulus is not believed to be diagnostic or trustworthy, and therefore not sought out or used when perceived

The first error mechanism suggests that problems with perceiving vibration information can be related to the instantaneous nature of the display. If the pilot needs a trend, or cumulative vibration information, he is out of luck. The second suggests that pilots are not going to waste their time looking at displays that do not offer reliable, diagnostic information. Therefore, even if the AVM system *is* giving accurate information, it may not be in usable form, given sporadic or low-level signals. Further, if the AVM system is historically perceived as non-diagnostic, the information may be totally ignored. In the authors' judgment, these factors contributed to the Kegworth accident. Although the error mechanisms do not lead directly to UAs, the lack of information about the aircraft condition contributes directly to a misdiagnosis of the problem.

Similarly, the two remaining sections of Table 4 need to be consulted for potential error mechanisms that could lead to errors in R/D/M and action. One that might apply to the diagnosis portion of engine-out scenarios, is the confirmation bias. This is where the problem-solver develops an hypothesis about the source or nature of the problem and has trouble releasing it, preferring instead to concentrate on data that confirm his original hypothesis.

6.10 Step 10. Select, Prioritize, and Document the Deviant Scenarios

As the cyclic process of iteration from Step 9 up and through Steps 4 - 8 continues, numerous deviant scenarios are accumulated. Prior to this step they are all candidate scenarios. In order for them to be successful in passing through to documentation, they need to pass some fairly simple and straightforward criteria. The criteria can be any set deemed relevant by the team. Several will be suggested here with emphasis on remaining internally consistent with the original purpose of the analysis. Each scenario generated should be compared to the following list of questions.

- Does the scenario fit into the original issue or purpose (Step 1) of the study?
- Does the scenario match the assumptions, limitations, and initiating events specified in Step 2?
- Can the scenario be successfully related to the base-case scenario?
- Is each scenario unique in some way, i.e., non-redundant?

- Is each scenario plausible within the current realms of physics and human behavior?

If for any scenario, the answers to the above cannot all be stated in the affirmative, then the scenario should probably be dropped from this analysis. That is not to say it should be dropped altogether. It might be a seed for another set of related scenarios, with a minor change in scope. If this is the case, after documentation, the analyst/team should consider going to Step 11 and iterating the scope.

6.10.1 Prioritization

Whenever a group of plausible scenarios exists, there is opportunity to organize and prioritize. Organization can be along any of the lines of the EFC elements, stages of the cognitive model, or any other reasonable set of criteria. This can be useful for documentation and presentation purposes. Prioritization, on the other hand, if done at all, should be done with caution. If the analyst or team wants to promote some scenarios as being more desirable than others, the dimension of probability should be omitted from the prioritization. The reason for this advice may not be obvious, but it is due to the fact that the primary goal of ASHRAM is to predict accident scenarios that have not yet occurred. By their very nature, these events are of extremely low probability. Therefore, it makes little sense to downgrade a scenario due to its low probability of occurrence. Nevertheless, if some scenarios are seen as much more likely to occur, they can be highlighted as such in Step 12.

6.10.2 Documentation

For any given deviant scenario, we suggest two alternative means of documentation. First, is writing out the event in narrative format. This approach has the obvious advantages of including as much detail as desired and reading like a story. Unfortunately, if many deviations are forthcoming from a prospective analysis, the writing can get laborious. Deviant scenarios expressed as narratives have been used previously in the text to demonstrate other procedures. A relatively simple format is suggested for those that may not belong to a family of related scenarios:

> *Dramatic Engine Failure.* Physical parameters concomitant with engine failure are universally faster in developing and have higher values. In this scenario, instead of minutes available for reacting, the pilots may have only a few seconds. As the engine fails abruptly, noise and vibration shake the plane violently, the plane yaws toward the affected engine (if on the wing), the nose drops due to reduced thrust, and the pilots must react quickly to keep the plane flying level. Correct control response would be to apply opposite rudder (feet), pull up on the nose, and increase throttle to the remaining engines. Opposite aileron may be necessary if the plane starts to roll in the direction of the affected engine. Power needs to be cut to the affected engine to reduce the probability of airframe damage and fire. If the threat of fire is suspected, or if the fire alarm sounds, the fire handle for the affected engine should be pulled (cutting off flammable fluids and flooding engine nacelle with fire-suppressing foam). If the pilots cannot identify the affected engine by flight
> *Dramatic Engine Failure.* (Cont.)

dynamics alone, deviations in the instruments would point to the affected engine (reduced EPR, fuel flow, and RPM, and increased vibration). The danger of this scenario is not misdiagnosis, but the possibility of losing control of the craft or sustaining airframe damage due to fire, explosion, or mechanical disintegration. If both of these outcomes can be avoided, the pilots should be able to fly to a diversion airport safely using the remaining engines.

An alternative documentation technique is the event-tree style flow chart. Here, several possible deviant scenarios can be outlined in a diagram showing their relationships that are based on decisions made or action taken. The style cannot carry as much detail as the narrative, but its compact efficiency makes it desirable for families of deviations that are all minor variants of each other. Figure 8 is an example of an event-tree style flow chart describing several deviations of the single-engine out base-case scenario.

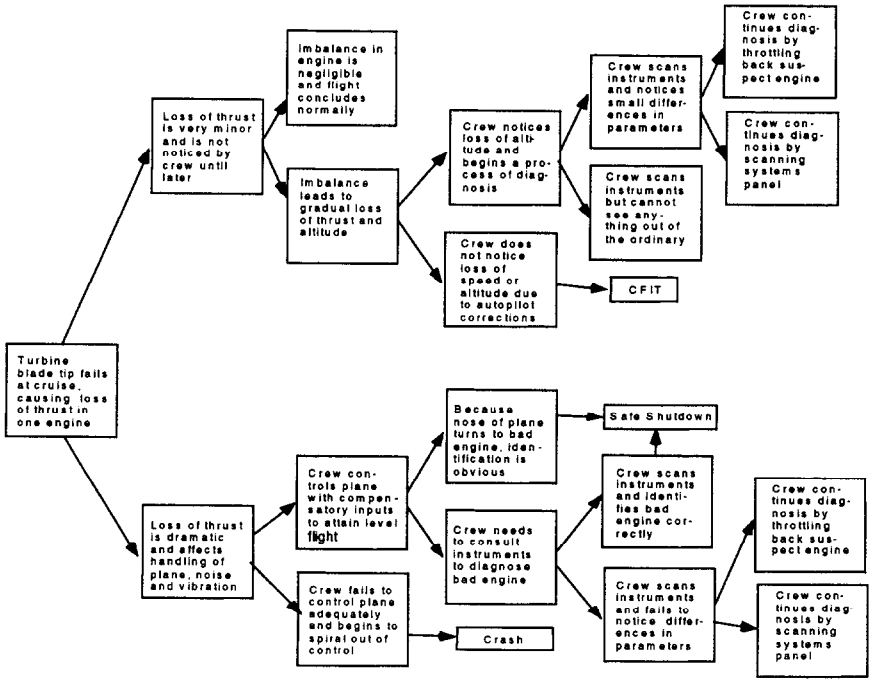

Figure 11. Event-tree Style Flow Chart for Documenting Deviant Scenarios

6.11 Step 11. Change Scope?

Having completed all of the possible deviations of the base-case scenario, there may be a desire to generate additional scenarios based on a shift in scope. Perhaps during the search process a SME made the team aware of a whole family of scenarios possible if one of the assumptions were different, or if the initiating event came from another source. Regardless, the decision here is to either write up some conclusions in step 12, Issue Resolution (below), or to continue to generate scenarios founded on a new base case. If the issue remains consistent, the scope can be altered, a new base-case scenario can be written up, and new families of deviations can be generated. For example, if the team wishes to study single-engine failures on takeoff or landing, this represents a change in scope, but remains within the issue to be resolved. If the issue

changes, then the analyst or team should proceed to Step 12, resolve the current issue, and start afresh with a new one in a new prospective analysis.

6.12 Step 12. Issue Resolution

After all the deviations are generated for all of the base-case scenarios (if more than one), it is time for the analyst/team to take stock and form some conclusions about their work and the products they've created. They may wish to prioritize the scenarios on a criterion, or quantitatively evaluate the relative likelihood of their occurrence. There may be deviations that are of particular concern, and they may wish to highlight or publicize them for the aviation safety community. It may be decided that some of the scenarios generated need a quantitative analysis to estimate absolute risk. There may be some suggestions or recommendations the team would like to make to reduce the likelihood of certain scenarios and their consequences. This is the place in the prospective analysis to do these kinds of things. Like an executive summary of a long report, the Issue Resolution section contains the important findings. Facts, observations, results, conclusions, and recommendations are placed here so that if someone does not have the time to look at the entire prospective analysis, he/she can look here and find enough information to form a conclusion. The format for issue resolution is left up to the analyst/team. The following brief example is included to give the reader an idea of the content and tone of issue resolution:

12. Issue Resolution

The xyz team studied commercial-airline, single-engine jet failures during cruise, assuming the initiating event was a single blade tip failure, leading to partial loss of thrust. The team studied several variations of the speed of the failure, ranging from virtually negligible symptoms, through significant noise and vibration, to an instantaneous, significant loss of thrust. In the case of very minor initial damage, the team found that current information made available to pilots is inadequate to diagnose engine trouble when only minor engine imbalances are present. Further, the team found that with the sudden onset of major thrust reduction, good CRM is necessary to safely control the airplane and make appropriate responses. The team recommends research and development be conducted to design or apply improved engine-health monitoring sensors, processors, and displays. Additionally, the team suggests training programs include scenarios of dramatic single-engine failure and consider CRM rules of thumb to handle the other cockpit tasks.

6.12.1 Quantification

As noted above, individuals performing an ASHRAM analysis may decide that it is necessary or beneficial to quantify the probability that a particular unsafe actions or CFFF could occur given an identified EFC. The need for quantification may be because the analysis is being performed as part of probabilistic risk assessment (PRA). Alternatively, there may simply be a need to provide estimates of the likelihood of particular events in order to provide input into decisions

about where and how limited resources might be applied to address potential problems. Regardless of the reasons for the need for quantification, there exists a number of possible options for a quantification process. However, the approach most directly consistent with the ASHRAM analysis is the approach described in ATHEANA (Ref. 9.1).

Quantification in both ATHEANA and ASHRAM requires the evaluation of the probabilities of the specific EFCs identified in the accident scenarios and then requires evaluating the conditional likelihood of the unsafe actions occurring, given the occurrence of the EFC. Finally, the probability of not recovering from the initial UA must be considered in order to determine the overall likelihood of an event that could lead to the loss of a CFF and a resulting an airplane crash. The quantification approach outlined in ATHEANA is directly adaptable to ASHRAM (with the CFFFs in ASHRAM being comparable to human failure events (HFEs) in ATHEANA) and this approach is recommended. In addition, the guidance in ATHEANA describes how quantified UAs and HFEs (CFFFs) can be incorporated into PRAs.

From the ATHEANA perspective, there are three types of conditions that can determine how the probability of an unsafe action is estimated:

1. The EFC is so compelling that the occurrence if the UA is virtually certain.
2. The EFC is so non-compelling that there is no significant likelihood of the UA occurring
3. The extent to which the EFC is compelling lies somewhere in between

ATHEANA provides specific guidance for determining the potential for the conditions described in items one and two immediately above. In addition, ATHEANA recommends the use of existing quantification approaches such as HEART (Ref. 9.7), SLIM-MAUD (Ref. 9.4), or expert elicitation approaches (such as that advocated by the developers of MERMOS (Ref. 9.10) for cases where the EFC cannot be determined to be particularly strong or weak (conditions described in item 3).

However, when it is necessary to use other approaches for quantification of UAs, such as HEART, SLIM-MAUD or an expert elicitation approach, analysts are cautioned to be sure to use the approach selected in such a way that the impact of the EFC and the potential for recovery is reasonably captured in determining the human error probabilities. At a minimum, ATHEANA provides the guidance necessary for considering the issues and factors relevant to appropriate quantification, and review of Section 10 in ATHEANA is highly recommended for those wishing to quantify unsafe actions (and accident scenarios) identified using ASHRAM.

7. RESOURCES

Fill-in Forms

In addition to the explanatory text and supporting tables and examples, the analyst/team has several blank forms to assist with the analysis. The blank forms can be copied out of this report and filled in during the analysis. Electronic copies of the forms may be obtained by contacting the authors. Using the text as a step-by-step guide, the following forms may be used to complete the retrospective and prospective analyses. The first set pertains to a retrospective analysis. The set following after these pertain to the prospective analysis.

7.1 ASHRAM Retrospective Analysis

---

1. EVENT IDENTIFIER –

Event Name:
Aircraft Type:
Date & Time:
Problem:
Unsafe Acts:
Outcome:
Sources:

---

2. ANALYSIS PERFORMED BY:

Name(s):

Organization(s):

Contact information:

Dates:

3. EVENT SUMMARY:

EVENT SUMMARY (continued)

4. SIGNIFICANCE OF EVENT:

ASHRAM SUMMARY

5. CRITICAL FLIGHT FUNCTION:

6. MOST NEGATIVE INFLUENCES:

7. MOST POSITIVE INFLUENCES:

8. KEY FLIGHT PARAMETER/CREW STATUS

Phase:
Altitude:
Location:
On Board:
Mechanical:
Air Frame hrs.
Fuel on board:
Cockpit crew:

Cabin crew:

9. INITIATING EVENT:

Initiator	Progression	Termination
0:00		

Timeline Events

Event	*Time*	*Description*
	0:00	

10. ISSUES FOR PROSPECTIVE ANALYSIS

7.2 ASHRAM Prospective Analysis

Analysis Performed by:

Name(s):

Organization(s):

Contact information:

Dates:

1. Define the Issue

a. Boundaries

b. Goals

c. Relationships to risk and aviation safety

2. Define the Scope and Initiating Events

a. Scope limitations:

b. Relevant Initiating Events:

Class of Initiating Event	Specific Initiating Event

3. Describe the Base Case Scenario

a. *Assumed initial conditions, including aircraft conditions:*

b. *Assumed causes:*

c. *Expected sequence of events (outline) including COM*

d. *Full description of base-case/COM scenario*

Time Frame	Major Occurrences	Influences on/by Pilots
Initial conditions		
Initiating event 0- sec.		

4. Define Aircraft Conditions:

Class of AC Change	Specific Changes in ACs
Improvement /degradation	
Increase/decrease, more/less	
Subsystem dependency effects	
Timing—too rapidly/too slowly	
Repeated elsewhere	

5. Identify Specific PSFs

Class of PSF	Specific PSFs
Weather (WX)	
Traffic (TF)	
Operator factors (OFs)	
Design factors (DFs)	
Procedural factors (PFs)	
Crew resource management (CRM)	

6. Identify Knowledge-base Vulnerabilities, Relevant Rules, and Tendencies

a. Knowledge-base Vulnerabilities

b. Rules

c. Tendencies

7. Identify Potential CFFFs and UAs:

Critical Flight Function Failures	Unsafe Actions
1.	
2.	
3.	
4.	
5.	

8. CONCLUSIONS

8.1 What We Have

Now that we have finished creating either a retrospective or prospective analysis (or both), let us consider what we have. In the case of a retrospective analysis, we have summarized the event and several aspects of the event in terms of ASHRAM terminology and the cognitive model. We have also identified the CFF violated, identified the UA, and inferred back from the UA to an information-processing error. This was then used to look for an appropriate error mechanism and associated segment of the cognitive model. This process was completed to relate the UA to conditions in the environment that conspired to construct an error-forcing context for the operators. This approach goes far beyond the "human error" attribution to aviation accidents so prevalent in our reporting systems. Understanding the EFC is important for gaining an appreciation for how to avoid recreating similar circumstances in the future and for redesigning aspects of the aviation system to avoid these EFCs altogether. This is the primary strength of the ASHRAM retrospective analysis. It is to understand, enumerate, and document, the conditions and factors that did contribute to an EFC that precipitated an unsafe action. From this understanding, we can project into the future to appreciate as-yet unexperienced circumstances and conditions that could lead to unsafe actions. One method is to provide an issue or UA for use in a prospective analysis.

In the case of the prospective analysis, we have used the procedure to identify the COM, or textbook operator responses, and systematically varied all of the circumstantial conditions to explore what UAs could occur. If the UAs were previously identified, we worked backward to find what conditions may contribute to them. If UAs were left unidentified, the discovery process teased them out by creating a variety of EFCs and using resources such as the error-mechanisms table to generate plausible UAs and scenarios. This is the primary strength of the prospective analysis—to create plausible scenarios of events that have not as yet occurred.

8.2 What We Don't Have

Any HRA technique cannot be all things to all people. Tradeoffs need to be made. Often a sound and complete HRA analysis needs to combine several techniques to compile the entire picture. ASHRAM's strength is not in developing probabilities for specific human actions. Other techniques have been developed that provides guidance for quantifying estimates of human error probabilities and these methods can be used in conjunction with ASHRAM (see Section 6.12.1). ASHRAM also has no systematic technique to develop cut sets or rank order scenarios according to their likelihood of occurrence. Other techniques have been developed for this purpose. ASHRAM presupposes no taxonomy for categorizing human errors into similar groups, such as errors of omission, commission, etc. It also does not prescribe models to relate the PSFs and other aircraft/airspace conditions to the likelihood of certain errors, but it does provide guidance to facilitate this process and offers a framework into which others' models can be imported and used.

8.3 Where Do We Go From Here?

This report is a first cut at a new process. A similar process is currently undergoing testing and evaluation in the nuclear-power arena. As more is learned about its capabilities, it is being modified. In order to become a valid tool for HRA, ASHRAM also needs extensive peer review, testing, and appropriate modification. It would be a mistake to oversell the technique as a tool ready for wide-scale implementation prior to systematic validation. The authors encourage other government agencies or contractors to assist in taking ASHRAM to the next level. We think the current framework and approach has the potential, with additional validation and development, to discover and predict air disasters of the future before they become realities.

8.4 Contact the Authors

The authors hope ASHRAM can help provide another tool in the arsenal of the aviation-safety professional. If you have read this report and have impressions, reactions, commentary, suggestions, or would like electronic copies of the forms, please contact the authors at the following locations:

Dwight Miller, Ph.D., CPE
Sandia National Laboratories
Systems Reliability Dept. 6411
MS0746
Albuquerque, NM 87185-0746
(505) 845-9803
dpmille@sandia.gov

John Forester, Ph.D.
Sandia National Laboratories
Risk and & Reliability Analysis Dept. 6413
MS0748
Albuquerque, NM 87185-0746
(505) 844-0578
jafores@sandia.gov

9. REFERENCES

9.1 U.S. Nuclear Regulatory Commission, *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624, Rev. 1, U.S. Nuclear Regulatory Commission, September 1999.

9.2 M.T. Barriere, W.J. Luckas, J. Wreathall, S.E. Cooper, D.C. Bley and A.M. Ramey-Smith, *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis*, NUREG/CR-6265, Brookhaven National Laboratory, Upton, NY, August 1995.

9.3 A.D. Swain and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque, NM, August 1983.

9.4 D.E. Embrey, P. Humphreys, E.A. Rosa, B. Kirwan and K. Rea, *Slim-Maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment*, Vols. 1-2, NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, DC, March 1984.

9.5 G.W. Hannaman, A.J. Spurgin, & Y.D. Lukic, *Human Cognitive Reliability Model for PRA Analysis*. (NUS-4531). Plao Alto, CA: Electric Power Research Institute, 1984.

9.6 R.E. Hall, J.R. Fragola, and J. Wreathall, *Post-Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, NUREG/CR-3010, Brookhaven National Laboratory, Upton, NY, November 1982.

9.7 J. C. Williams, "A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance," paper presented at 1988 IEEE Fourth Conference on Human Factors and Power Plants, IEEE, 1988.

9.8 Dougherty, E.M., Jr. and J.R. Fragola, *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, John Wiley and Sons: New York, 1988.

9.9 Parry, G.W., et al, *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*, EPRI TR-100259, Licensable, Electric Power Research Institute, Palo Alto, CA, June 1992.

9.10 C. Bieder, P. Le-Bot, E. Desmares, J-L Bonnet, F. Cara, "MERMOS: EDF's new advanced HRA method," in *Probabilistic Safety Assessment and Management (PSAM 4)*, A. Mosleh and R.A. Bari (eds), Springer-Verlag, New York, 1998.

9.11 O. Strater and H. Bubb, "Assessment of human reliability based on evaluation of plant experience: requirements and implementation," *Reliability Engineering and System Safety*, **63**: 199-219, 1998.

9.12 P.C. Cacciabue, F. Decortis, B. Drozdowicz, M. Masson, J.P. Nordvik, "COSIMO: A cognitive simulation model of human decision making and behavior in accident management of complex plants," *IEEE Transactions on Systems, Man and Cybernetics*, **22**(5): 1058-1074, 1992.

9.13 P. C. Cacciabue, Cojazzi, and P. Parisi, "A dynamic HRA method based on a taxonomy and a cognitive simulation model," in *Probabilistic Safety Assessment and Management*, P.C. Cacciabue and I.A. Papazoglou (eds.): Springer-Verlag, London, 1996.

9.14 D.I. Gertman, H.S. Blackman, L.N. Haney, K.S. Seidler, H.A.Hahn, *INTENT: A Method for Estimating Human Error Probabilities for Errors of Intention*, EGG-SRE-9178, Rev. 1. 1990, Idaho National Engineering Laboratory, Idaho Falls, ID

9.15 J.A. Julius, E.J. Jorgenson, G.W. Parry, A. M. Mosleh, "A procedure for the analysis of errors of commission in a Probabilistic Safety Assessment of a nuclear power plant at full power," *Reliability Engineering and System Safety*, **50**: 189-201, 1995.

9.16 J.A. Julius, E.J. Jorgenson, G.W. Parry, A.M. Mosleh, "A procedure for the analysis of errors of commission during non-power modes of nuclear power plant operation," *Reliability Engineering and System Safety*, **53**: 139-154, 1996.

9.17 A. Macwan and A. Mosleh, *Methodology for Analysis of Operator Errors of Commission During Nuclear Power Plant Accidents with Application to Probabilistic Risk Assessments*. MDNE-93-001. 1993, Department of Materials and Nuclear Engineering, University of Maryland, College Park.

9.18 Hollnagel, E., *Cognitive Reliability and Error Analysis Method (CREAM)*. York: Elsevier Science, New York, 1988.

9.19 F. Monseron-Dupin, B. Reer, G. Heslinga, O. Strater, V. Gerdes, G. Saliou, W. Ullwer, "Human-centered modeling in human reliability analysis: some trends based on case studies," *Reliability Engineering and System Safety*, 58: 249-274, 1997.

9.20 D.D. Woods, H.E. Pople and E.M. Roth, *The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability*, USNRC, NUREG/CR-5213, Washington DC, 1990.

9.21 A.D. Swain, *Comparative Evaluation of Methods for Human Reliability Analysis*, GRS-71, April 1989.

9.22 B. Kirwan, "Human error identification techniques for risk assessment of high-risk systems – Part 1: review and evaluation of techniques," *Applied Ergonomics*, **29**(3): 157-177, 1998.

9.23 E. Hollnagel, *Cognitive Reliability and Error Analysis Method: Cream*, Elsevier: Oxford, 1998.

9.24 B. Reer, O. Strater, V.N. Dang and S. Hirschberg, *A Comparative Evaluation of Emerging Methods for Errors of Commission Based on Applications to the Davis-Besse (1985) Event*, PSI Bericht Nr.xx-xx, Paul Scherrer Institute, Gesellschaft fur Anlagen- und Reaktorsicherheit, Germany, November 1999.

9.25 S.H. Shen, C. Smidts and A. Mosleh, "A methodology for collection and analysis of human error data based on a cognitive model: IDA," *Nuclear Engineering and Design*, **172**: 157-186, 1997.

9.26 K.M. Corker and B. R. Smith, "An architecture and model for cognitive engineering simulation analysis application to advanced aviation automation," in *Proceedings of the AIAA Computing in Aerospace 9 Conference*, San Diego, CA, 1993.

9.27 D.D. Woods, L.J. Johannesen, R.I. Cook and N.B. Sarter, *Behind Human Error: Cognitive Systems, Computers, and Hindsight*, Crew System Ergonomics Information analysis Center (CSERIAC), Ohio State University, Wright-Patterson Air Force Base, Columbus, OH, December 1994.

9.28 D.D. Woods and E.S. Patterson, "How unexpected events produce an escalation of cognitive and coordinative demands," in P.A. Hancock and P.A. Desmond (eds.), *Stress Workload and Fatigue*, Lawrence Erlbaum: Hillsdale, NJ, 2000.

9.29 E.M. Roth, R.J. Mumaw, and P.M. Lewis, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, NUREG/CR-6208, Westinghouse Science and Technology Center, Pittsburgh, PA, July 1994.

9.30 R.J. Mumaw and E.M. Roth, "how to be more devious with a training simulator: Redefining scenarios to emphasize cognitively difficult situations," in *1992 Simulation MultiConference: Nuclear Power Plant Simulation and Simulators*, 1992.

9.31 J. Reason, *Human Error*, Cambridge, England: Cambridge University Press, 1990.

9.32 C. Forsythe and C. Wenner, "Surety of human elements of high consequence systems: an organic model," in *Proceedings of the HEA 2000/HFES 2000 Congress*, pp. 3:839-3:842, 2000.

9.33 L.V. Rigby, "The nature of human error," in *Annual Technical Conference Transactions of the ASQC*, pp. 457-466. American Society for Quality Control, Milwaukee, WI, May 1970.

9.34 J.W. Senders and N.P. Moray, *Human Error: Cause, Prediction, and Reduction.* Hillsdale, NJ: Lawrence Erlbaum Associates, 1991.

9.35 K. S. Park, "Human Error," in G. Salvendy, *Handbook of Human Factors and Ergonomics*, pp. 150-173, John Wiley & Sons: New York, 1997.

9.36 D.A. Norman, *The Psychology of Everyday Things*, Basic Books: New York, 1988.

9.37 M.R. Endsley, "Design and evaluation for situation awareness enhancement," in *Proceedings of the Human Factors Society 32nd Annual Meeting*, pp. 97-101, Santa Monica, CA: Human Factors and Ergonomics society, 1988.

9.38 N.B. Sarter and D.D. Woods, Situation awareness: "A critical but ill-defined phenomenon," *International Journal of Aviation Psychology*, **1**: 45-57, 1991.

9.39 M.J. Adams, Y.J. Tenney and R.W. Pew, "Situation awareness and the cognitive management of complex systems," *Human Factors*, **37**(1): 85-104, 1995.

9.40 J.M. Flach, "Situation awareness: Proceed with caution," *Human Factors*, **37**(1): 149-157, 1995.

9.41 K. Smith and P.A. Hancock, "Situation awareness is adaptive, externally directed consciousness," *Human Factors*, **37**(1): 137-148, 1995.

9.42 C.E.J. Hartel, K. Smith and C. Prince, "Defining aircrew coordination: Searching mishaps for meaning." Paper presented at the Sixth International Symposium on Aviation Psychology, Columbus, OH, 1991.

9.43 M.R. Endsley, "Toward a theory of situation awareness in dynamic systems." *Human Factors*, **37**(1): 32-64, 1995.

APPENDIX A: RETROSPECTIVE ANALYSIS OF KEGWORTH CRASH USING ATHEANA FORMAT

1. EVENT IDENTIFIER – Kegworth Crash

Event Name:	Kegworth Crash
Aircraft Type:	B737 Series 400
Event Date/Time:	01/08/89, 20:24
Event Type:	Engine vibration and fire, followed by shutdown of wrong engine
Secondary Event:	Crew shut down other engine, leading to a crash with 47 fatalities
Data Sources:	SkyNet-special report, Air Accidents Investigation Branch Aircraft Accident Report No: 4/90 (EW/C1095)
Data Input By:	Dwight Miller, Sandia National Laboratories, 505-845-9803

2. EVENT SUMMARY

Event Description: A British Midland Airways Boeing 737 Series 400 aircraft, while climbing through FL283 on its flight from London to Belfast, experienced moderate to severe vibration, shuddering, or rattling, accompanied by the smell of fire in the cockpit. Although the airborne vibration monitoring (AVM) system indicated elevated vibration levels there was no warning of fire on the flight deck. [Both the commander and the first officer survived the crash; the former remembered seeing and smelling air conditioning smoke, the latter remembered only a strong smell of burning.] The commander took control of the aircraft and disengaged the autopilot. Both pilots remembered that they could not diagnose which engine had suffered damage by means of their engine instruments. The commander asked the first officer which engine was causing the trouble and the latter responded "it's the le...it's the right one." At 19 seconds after the onset of the vibrations the commander requested the first officer to "throttle it [#2] back." [According to the FDR, the #2 engine (on the right side) had steady indications, but engine #1 (on the left side) showed strong vibrations, elevated exhaust gas temperatures, increased fuel flow, and a reduction in speed. What the pilots did not know, was that engine #1 had lost one tip of a turbine blade and was running out of balance.] During the 11 seconds that elapsed between the disengagement of the autopilot and the throttle reduction in engine #2, the aircraft rolled slowly to the left through 16 degrees, however no corrective action was taken. Within 2 seconds of throttling back engine #2, the aircraft rolled level again. [This airframe response is consistent with reduced thrust from the left side being equalized by a reduction of thrust on the right.]

After the initial responses made above, the first officer reported the situation to London air traffic control (ATC) as an apparent engine fire. At 43 seconds after initiation, the commander ordered the first officer to "shut it [engine #2] down." The execution was delayed when the commander said, "Seems to be running alright now. Let's see if it comes in." After additional radio conversation addressing alternate landing sites, the first officer said he was about to start the engine failure and shutdown checklist, saying "seems we have stabilized...we still got the smoke." After additional radio conversation, and 2 minutes 7 seconds after initial vibration, the

fuel shutoff valve for engine #2 was closed, and the engine was shut down. The crew directed the airplane to East Midlands for an emergency landing.

In the cabin, flight attendants and passengers heard unusual noises, felt vibrations, and smelled burning. They also saw signs of fire (torching, sparks) from the left (#1) engine, and some saw light smoke in the cabin. After the commander made an announcement about trouble in the right engine and shutting it down, several passengers were puzzled by the discrepancy but failed to alert the flight attendants, who had not heard the commander's reference to the right engine.

About 13 nautical miles (nm) from touchdown, ATC advised a right turn. Power was increased to the operating engine (#1) and the FDR recorded a maximum vibration again. One minute later at 900 ft. and 2.4 nm from touchdown, there was an abrupt decrease in power from the #1 engine. Despite attempts to restart the #2 engine, the airplane crashed short of the runway, killing 47 of its 118 passengers.

Event Surprises:

- Engine instrumentation was ineffective in identifying the affected engine for two pilots. Despite an airborne vibration monitoring (AVM) system, and displayed output via indicators on the secondary EIS, both crew members had no recollection of seeing an indication of above normal vibration in engine #1, despite the FDR record of a properly functioning AVM. [Report states that in the event that the vibration signal achieves maximum at 5.25, the display disappears under the assumption that an error has occurred. All indications are that this was not the case, and the AVM level indicators were functioning.]
- Commander prematurely ordered engine #2 to be shut down. This was not necessary, especially with no fire alarms active.
- Airframe dynamics, in the form of vibration and roll, were not perceived as being diagnostic of a problem in the left engine.
- When thrust was reduced from engine #2 and roll was negated, no one noticed—or at least it was misinterpreted as restoring normalcy instead of counteracting asymmetrical thrust.
- Vibration was perceived as being reduced when engine #2 was throttled back, but vibration sensors recorder on the FDR dispute that claim. May have been due to restored level flight, or a reduction in aerodynamic drag.
- First officer's response to the commander used the terms "right one," may not be significant, but "right" can also mean correct, and "one" can also mean #1.
- Commander knew that engine #2 contributed air conditioning to the cabin and inferred from the apparent cabin smoke that engine #2 might be the affected engine. He even used the term "air conditioning smoke."
- Despite several passengers and flight attendants having seen fire symptoms from the left engine, no one overtly questioned the commander's announcement that the situation had been mitigated.
- It may not be significant, but the commander had only 23 hours on the series 400 B737, while the first officer had only 53 hours.
- Despite a fire in the outboard section of #1 engine for 24 minutes prior to final approach, its fire alarm did not sound until 36 seconds prior to impact.

Safety Recommendations:

a. The Civil Aviation Authority (CAA) consider increasing engine inspections and health monitoring on B737/300 and B737/400 until causes of failures are established.
b. Examine fire/overheat and AVM circuitry for left/right engine sense.
c. CAA and engine manufacturer consider inspection of fan stage of CFM56 engines.
d. Review advice in B737 maintenance manual about excessive heat generated by grinding tools in blending operations.
e. CAA advise pilots about fan tip failure and associated smoke possible from A/C system.
f. Review attitude of pilots to current engine vibration indicators, and possible improvements.
g. CAA should require pilot training for AVM-equipped aircraft.
h. Regulatory requirements should be amended to include a standard way of assessing the effectiveness of such displays in transmitting pertinent information to the flight crew.
i. Modify the EIS on B737-400s to include attention-getting features when vibration meets maximum levels.
j. Boeing should amend flight manuals to include what actions should be taken when high vibration and smell of smoke occurs.
k. CAA ensure that crew currency training in simulators includes practice reprogramming of flight management systems or others that control key approach and landing display format during unplanned diversions.
l. CAA review current guidance to ATC on offering a discrete RT frequency to commercial pilots in emergencies.
m. CAA review training requirements to ensure pilots are familiarized with electronic flight displays before flying public transport aircraft so equipped.
n. Training exercises for pilots and cabin crew should introduced to improve coordination in emergencies.
o. CAA review current training to restore balance in technical appreciation of aircraft systems.
p. Gas turbine engines type certification should include instrumented flight tests to demonstrate freedom from damaging vibratory stresses at all X altitude conditions and powers.
q. Potential for fuel and oils system leakage in the fan case of such engines should be reviewed.
r. Review JARs concerning fuel tank protection from landing gear and engine detachment during ground impact.
s. CAA should look into providing visual status information to the flight crew via external and internal closed circuit television monitoring.
t. FDRs which use buffering techniques made non-volatile and hence recoverable after loss of power.
u. CAA should consider increasing engine vibration sampling rate from every 64 seconds to every second.
v. CAA should actively seek improvement in JARs, and not be constrained by FAA requirements.

w. JAR 35.561 and .562 loading and dynamic testing requirements should be applied to new and registered aircraft.
x. JARs should be modified to ensure seating is safety engineered to minimize occupant injury on impact.
y. CAA should research passenger seat design for effective torso restraint and aft-facing seats.
z. Cabin floor designs of new aircraft types should take into account dynamic impulse and distortion.
aa. CAA should research feasibility of increasing cabin floor toughness beyond current levels.
bb. CAA should require infants and young children be placed in child seats for T/O, landing, and turbulence.
cc. CAA expedite publication of as specification for child seat designs.
dd. Certification requirements of cabin stowage bins and other items of mass should be improved for retention when subjected to dynamic crash pulses beyond current static load factors.
ee. Overhead stowage bins should receive better latches.

ATHEANA Summary:

Most Negative Influences

- The #1 engine, which lost a fan blade tip, could continue to run at over 90% power. If the engine blew up completely instead of being partially disabled, the crew could have determined the source of the vibration with higher reliability – **aircraft condition**
- The captain had received training he remembered that taught him that the air conditioning system to the cabin was fed through the right (#2) engine. This **training (PSF)** had created a strong belief that the smell of smoke in the cockpit resulted from smoke in the aft cabin coming from the A/C system and the right engine. This belief further confirmed the erroneous hypothesis that the right (#2) engine was damaged and should be shut down.
- The design of the AVM display was such that neither pilot could infer from the instrumentation which engine was causing the initial vibration – **human-system interface (PSF).**
- At no time did the first officer challenge the commander's hypothesis that the vibration was coming from engine #2—**crew resource management**
- At no time did the cabin crew, who were busy cleaning up the cabin, hear or challenge the commander's hypothesis that the vibration was coming from engine #2— **crew resource management**
- The unfortunate coincidence of the vibration ceasing when the crew throttled back engine #2 led the crew to believe they were acting appropriately – **aircraft condition**

Most Positive Influences (that could have prevented or otherwise mitigated the event)

- Some of the passengers noticed the inconsistency of the fire in the left engine and the commander reporting the problem with the right engine was essentially solved, but none alerted the crew – **communication (PSF)**

- The commander tried to review the cockpit crew's actions when there was time to on initial approach to make sure they got it right, but the only running engine lost power and interrupted his train of thought – **aircraft condition**
- The aircraft was equipped with an airborne vibration management system (AVM) that is designed to inform the cockpit of engine vibration problems. However, the implementation of the displays of the information was less than adequate (LTA) to call attention to or convey the information to the cockpit crew - **human-system interface (PSF)**

Significance of Event:
This event never had to happen. With proper cockpit instrumentation, or a fire management system that worked, or better communication with the cabin crew, this aircraft could have easily flown home on the one 100% good engine and the second at reduced power (or shut down).

Extreme or unusual conditions: Perceived vibration cessation when the wrong engine was throttled back
Contributing pre-existing conditions: Design of AVM instrumentation or crew training/experience LTA. Fire management system LTA.
Misleading or wrong information: State of health of engine #1 LTA'ly displayed to pilots.
Information rejected or ignored: Cabin passengers did not communicate concerns over engine confusion, pilots did not perform visual confirmation of engine conditions
Multiple hardware failures: Loss of turbine blade tip and fire with no fire alarms;
Similar to other events:? Review other accidents???

KEY FLIGHT PARAMETER STATUS

Conditions Immediately Prior To Initiating Event

Phase: Climbing to cruise altitude, 295 kts. CAS
Altitude: Climbing through 28,300 ft.
Location: 13 minutes into flight from London to Belfast
On Board: 8 crew, 118 passengers
Mechanical: All systems normal
Air Frame hrs. 521
Fuel on board: 9281 lbs.
Cockpit crew: Commander – male, 43, 763 hrs. in 737, 23 in Series 400, 12 hrs. last 28 days
First Officer – male, 39, 192 hrs. on 737, 53 in Series 400, 37 hrs. last 28 days
Cabin crew: Six attendants with cumulative B737 experience of 2 years 5 months

AIRCRAFT STATUS	
Initial Aircraft Conditions & Configurations	**Accident Conditions & Consequences**
Configuration: 1. Nominal climbing power conditions **Noteworthy Pre-existing Conditions:** 1. Limited flying hours of cockpit crew in the B737 Series 400 aircraft 2. Minimal service hours of cabin crew in B737 aircraft **Initiator** 1. Loss of turbine blade tip in engine #1, leading to compressor stalls, vibration, and eventually fire	**Automatic Responses:** 1. none **Failures:** 1. Fire management system did not sense fire in engine #1 2. AVM worked as designed, but did not effectively communicate vibration level in engine #1 to crew **Consequences:** 1. Crew throttled back and shut down good engine (#2) by mistake, relied on bad engine to fly home, crashed when bad engine lost thrust

3. ACTION SUMMARY

Event Timeline:

Initiator			Event Progression					Event Termination		
20:05.05		05.24	07.12	07:xx	08:xx	12.28	23.49	23.xx	24.43
^	^	^	^	^	^	^	^	^	^	^
E1	E2	R1	R2	U1	U2	U3	R3	E3	R4	T

Unsafe Actions and Other Events:

Key: U = unsafe actions
E = equipment failures (significant to the event)
H = non-error (non-recovery) actions
R = recovery actions
T = terminal event

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
E1	Loss of turbofan blade tip in engine #1, onset of vibration and slight loss of thrust
E2	Despite fire in engine #1, no fire alarms sounded until 36 seconds prior to crash (no apparent hardware failure—system functioned as designed)
R1	Commander and first officer check instruments to diagnose problem
R2	Upon Commander's order, first officer throttles back engine #2
U1	In response to Commander's order (05:48), first officer shuts down engine #2
U2	Conferred with cabin crew about smoke, but did not discuss suspect engine
U3	Cabin crew members saw that engine #1 was on fire but never confirmed w/Commander
R2	Cockpit crew reviews incident by discussing sequence of events
E3	Engine #1 loses thrust when called on for more power in approach turn
R3	First officer attempts to restart engine #2
T	Crash short of runway

HUMAN DEPENDENCIES		
Actions	**Dependency Mechanism**	**Description**
U1-U2	Based on hypothesis that engine #2 was affected, commander's bias led to conclusion that correct actions were being taken when vibration subsided with throttle back of engine #2.	Commander believed that smell of smoke from cabin implied engine #2 creating a bias that engine #2 was damaged
U2-U3	Based on the assumption that the cockpit crew had made a correct decision to shut down engine #2, no passengers nor cabin crew questioned the sparks emanating from engine #1	Passengers and cabin crew believed that cockpit crew had the situation under control

Unsafe Actions Analysis

U1 EOC, In response to commander's order, first officer shuts down engine #2

Error Forcing Context

Aircraft Conditions	Performance Shaping Factors	Failures of Information Processing
Systems Status: 1) Engine #1 was the source of the vibrations, as it had lost a fan blade tip. Engine #2 was in nominal condition at time of shutdown. 2) AVM system was operational and did indicate higher than normal vibrations in engine #1 from the onset. 3) No fire alarms sounded on either engine, despite smell of burning metal and signs of smoke in fuselage. *Flight Impact:* 4) If engine #2 was running at reduced power instead of being shut down, it may have helped avoid the crash when #1 lost power on final approach.	*Displays:* 5) The high vibrations of engine #1 were displayed on the EIS by the AVM. 6) Concomitant engine parameter anomalies were also displayed (e.g. exhaust gas temp., fuel flow), however the status of the engines' respective vibration levels, nor the anomalous engine parameters were conveyed successfully to the pilots. *Training:* 7) Training on the air conditioning (A/C) system led commander to believe that smell of smoke coming from cabin was due to A/C system in engine #2. 8) Low hours on the series 400, or lack of recent training with the AVM displays may have contributed to unfamiliarity w/displays. *Organizational Factors:* *9)* The first officer did not question the commander's decision to shut engine #2 down. *Stress and Weather:* 10) The initiating event happened during routine flight activities. *11)* Feedback of 'reduced vibration' and smoke "confirmed" diagnosis of engine #2.	*Situation Assessment:* 12) Cockpit crew failed to assess which engine was malfunctioning from panel indicators, although several had anomalous readings. 13) Cockpit crew failed to consider left roll of 16 degrees as a sign that engine #1 had lost thrust, and later failed to realize that the wing-leveling effect of reducing power to engine #2 was consistent with engine #1 being compromised. 14) Reduction in vibration and smell of smoke reinforced notion that correct action was being taken in reducing power level of engine #2. *Error Mechanisms:* Confirmation Bias—Commander searched for verification that engine #2 was bad instead of looking for falsification that engine #1 was bad Hypothesis Fixation—Commander's initial hypothesis that engine #2 was affected was held, and failed to update the hypothesis when other conflicting information presented itself

U2 EOO, Conferred with cabin crew about smoke, but did not discuss suspect engine

Error Forcing Context

Aircraft Conditions	Performance Shaping Factors	Failures of Information Processing
Indications: 15) Having shut down engine #2, all evidence of smell and smoke cleared from the flight deck. 16) Power was further reduced to engine #1, which exhibited no signs of unserviceability other than a higher than normal level of indicated vibration, which continued a further 3 minutes and fell progressively until it reached a steady reading of 2 on a scale of 5. 17) In the cabin, the smell of smoke had dissipated by the time the commander made his announcement about shutting down engine #2	*Organizational Factors:* 18) The commander, during two separate conversations, never bothered to ask the cabin crew if they had seen any signs of fire in either engine. This may be due to the pecking order, or a fear of admitting lack of complete awareness on the part of the commander. *Environment:* 19) Reduction of apparent vibration and smell of smoke in cockpit and cabin helped to reinforce the notion that the correct engine had been shut down, and that further confirmation was not necessary.	*Cockpit Resource Management:* 20) Cockpit crew failed to utilize the cabin crew as an added resource to assess which engine was malfunctioning from direct observations. *Error Mechanism:* Self-Centered Bias—Commander acted as if his own judgement was centralized as being the most important in this scenario

U3 EOO, Cabin crew saw that engine #1 was on fire but never confirmed w/Commander

Error Forcing Context

Plant Conditions	Performance Shaping Factors	Failures of Information Processing
21) *Same as directly above*	*Organizational Factors* 22) The cabin crew, assumed the cockpit crew had complete situational awareness. This may be due to the pecking order, or a fear of challenging the commander's knowledge or judgement. 23) Similarly, passengers did not overtly question the cockpit crew's diagnosis, possibly due to the apparent authority role of the crew.	*Error Mechanisms:* Defensive Avoidance—Cabin crew and passengers underestimated the likelihood of the undesired outcome of the cockpit crew being wrong Delegate Risky Decisions—Cabin crew and passengers may have delegated the risky decisions of identifying the bad engine to the cockpit crew, as they did not want the responsibility of major losses

4. ACCIDENT DIAGNOSIS LOG

Time	Event Progression	Details of Responses
20:05.05	Approx. 20 NM SSE of East Midlands Airport and climbing through FL283, engine #1 of the B737 series 400 experienced a blade tip failure, causing compressor stalls, fluctuations of the engine parameters, airframe shuddering, and ingress of smoke and fumes to the flight deck (**E1**). No fire alarms sounded (**E2**).	The commander took control, disengaged the autopilot, and began to canvass the instruments for signs of trouble. The first officer also began to study the instruments (**R1**). The plane rolled to the left 16 degrees after the autopilot was disengaged. The commander then asked the first officer which engine was causing the trouble, to which he replied "it's the le…it's the right one". The commander responded by saying "OK, throttle it back."
20:05.24	First officer throttles back engine #2 (**R2**).	Within 2 seconds the aircraft rolled level. The fluctuations in lateral and longitudinal accelerations ceased, the #1 fan speed settled at 3% below its previous stable speed, the EGT stabilized at 50' C above its previous level, and these parameters remained steady until the commander reduced power on that engine for descent, about a minute later. Indicated vibration remained at maximum (5 out of 5). The commander later recalled that the smell/visual signs of smoke were reduced with the throttling back of engine #2, and the vibration had ceased.
20:05.48	Commander requests first officer to shut down engine #2	The execution was delayed when the commander said "seems to be running alright now…let's see if it comes in..." Radio communication ensued, picking out an alternate destination. The first officer then told the commander that he was starting the engine failure and shutdown checklist and "seems we have stabilized…we've still got smoke…". More radio communication ensued.
20:07.12	First officer finishes engine shut-down procedures by closing the fuel cock to engine #2 and starting the auxiliary power unit (**U1**).	The commander later recalled that after engine #2 was shut down, all evidence of smell and smoke cleared the flight deck, convincing him that the appropriate action had been taken. Shortly afterwards, power

Time	Event Progression	Details of Responses
		was further reduced to engine #1, which continued to operate without any signs of unserviceability other than a higher than normal level of indicated vibration and increased fuel flow. This high level of vibration continued for a further 3 minutes and then fell progressively until it reached a level of 2 units, still higher than normal.
20:07:xx	Commander calls flight service manager (FSM) to the flight deck to ask about smoke in cabin, but does not confirm diagnosis of engine #2 (**U2**).	Commander asked FSM, " Did you get smoke in the cabin back there?" The FSM said, "We did, yes." The commander then instructed the FSM to clear up the cabin and pack everything away. About one minute late the FSM returned to say, "Sorry to trouble you...the passengers are getting very very panicky." The commander then broadcast to the passengers on the cabin address system that there was trouble with the right (#2) engine, which had produced some smoke in the cabin, that the engine was now shut down, and that they could expect to land at East Midlands in about ten minutes.
20:08.xx	Cabin crew had direct knowledge of fire in left engine (#1), but did not confer with cockpit crew (**U3**).	The cabin crew, who saw signs of fire on the left engine, later stated that they had not heard the commander's reference to the right engine in his address to the passengers. Passengers, who had noticed the discrepancy between the commander's address and what they could see out their windows did not point it out to the cabin crew.
20:12.28	Commander attempts to review the incident and actions taken with the first officer (**R2**), but was interrupted by radio communication.	Commander said "Now what indications did we actually get (it) just rapid vibrations in the airplane – smoke..." ATC communications concerning radar heading and approach control frequency interrupted discussion. Then first officer began to read the one-engine inoperative descent and approach checklist. Additional radio

Time	Event Progression	Details of Responses
		Interruptions distracted crew from continuing the review discussion.
	The aircraft struck the ground with a nose-high attitude on level ground just east of the M1 highway (**T**), killing 47 passengers.	Ground witnesses who saw the final approach saw clear evidence of fire associated with the left engine—yellow/orange fire, flames streaming from the aft of the nacelle, pulsating in unison with thumping noises. Metallic rattling was also heard, and flaming debris was seen falling from the aircraft.

APPENDIX B: ATHEANA SEARCH PROCESS FOR AVIATION TEST CASE

1. Define the Issue

Examine the issue of a crew experiencing a partial engine failure and reacting appropriately to conclude the flight safely. Investigate deviations and reasonable variations that could lead to HFEs and UAs.

a. Boundaries – limit analysis to jet airframes that are significantly affected by the loss of one engine – limit to partial loss of one engine.
b. Goals – identify potential HFEs, UAs, PSFs, associated EFCs, and situations that may lead to improved designs or safety procedures.
c. Relationships with PRA – none

2. Define the Scope of Analysis

a. Scope Limitations:
   Engine failure occurs during normal cruise configuration
   Engine failure leads to significant loss of thrust and destination diversion
   Cockpit crew is functioning normally w/currency requirements fulfilled
   Cabin crew is functioning normally w/currency requirements fulfilled

b. Relevant Initiating Events:

Table B.1 Classes and Examples of Potential Initiating Events

Class of Initiating Event	Example Initiators
Internal engine failure	Broken fan blade Bearing failure Turbine shaft failure Pump malfunction Fire
Supply failure (indirect)	Electrical Fuel problem Lubrication leak/inadequate reserve
External event	Bird/debris ingestion Collision with another aircraft Weather-hail/snow/rain—flame-out Lightning
Cockpit-initiated	Power-back Fire extinguisher activated inadvertently Fuel pump cut-off switches Etc.
Automated sources	Fuel management system Autopilot-related problem

c. Resources available:
    No PRA available
    Aircraft accident report no: 4/90 (EW/C1095)
    Appendix B. Summary of event
    Aircraft operating procedures
    Aircraft emergency checklists
    Simulator runs
    Training scenarios
    Pilot interviews

d. Priorities on scenarios:
    Use fan blade failure first
    Partial engine failure w/minor display deviations

3. Describe the Base Case Scenario

a. Assumed initial conditions:
    level cruise altitude, wings level, trimmed pitch
    all systems operational
    current, legal, rested crew
    passengers are onboard
    enough time to deal with problem
    pilot and copilot, minimum
    good flight weather, IFR conditions
    instrumentation is fully operational
    adequate fuel onboard

b. Assumed causes:
    turbine fan blade failure that leads to partial, but perceptible loss of power in the affected engine

c. Expected sequence of events (COM):
    onset/increase of noise/vibration from somewhere
    pilots notice (if perceptible) and make control changes necessary to maintain flight level
    pilots begin diagnosis of situation
        engine or some other source of vibration?
    pilots decide it is an engine problem
        which engine?
        how bad is it?
        shut down affected engine?
        route diversion options—fuel/time availability?
    pilots decide to shut down affected engine
        power back affected engine
        make control adjustments—power increase to good engines
        shut off fluids to affected engine

pilots report situation to radar control/company
decide on best route diversion option
make changes in flight controls to change course heading, altitude, etc.
pilots report situation to cabin crew and passengers
pilots conduct remainder of flight to diversion airport

d. Full description of base-case/COM scenario:

The plane is cruising at altitude in IFR conditions, with legal, unexpired, unfatigued crew, in an otherwise fully operational airframe, when a turbine fan blade fails. The blade exits the rear of the engine but the imbalance imposed on the turbine shaft continues to cause progressive damage over time. This event causes an immediate decrease in engine RPM, a 10 percent decrease in thrust, noise (audible in cockpit), and noticeable airframe vibrations. The flight attitude is immediately affected in the following way: observable asymmetric yaw and slight roll towards the affected engine, slight nose-down, decrease in airspeed.

The first response of the pilot in command (in this case we'll assume it's the first officer) is to turn off the autopilot, apply opposite rudder, level the wings using the ailerons, and to grab the throttle controls to confirm power settings. The pilots begin to diagnose the apparent failure by scanning the instruments and looking for external visual cues as to the cause of the symptoms. As time progresses, the vibrations get stronger and eventually smoke is smelled on the flight deck. Due to experience with simulator training, the pilots' initial thought is that an engine has failed, and that a decrease in power to that engine might reduce the vibration and noise (and certainly reduce the likelihood of uncontrolled fire or airframe damage). As the first officer flies the plane level, the captain examines the engine pressure ratio (EPR), fuel flow, and vibration indications fed by the airborne vibration monitor (AVM) system to see if one engine demonstrates any anomalies. He notices a slight decrease in EPR and fuel flow, and a non-zero indication of vibration for engine 2. He looks out the windshield to see if there are any visible signs of smoke or fire. Not seeing any, he looks back to the other instruments to find another possible source of the noise and vibration. Satisfying himself that it must be engine 2, he asks the first officer to confirm his hypothesis. When the flying first officer confirms, the captain throttles back engine 2, and power is increased to the other engines. Noise and vibration begin to abate, but flight attitude anomalies get stronger. Convinced that correct source of problem has been identified, the captain announces to the first officer that he will proceed with shutting down engine 2. Because no fire alarms have sounded, the captain chooses not to pull the fire extinguisher T-handle, and proceeds with a checklist-based shutdown procedure. As the affected engine winds down, noise and vibration continue to decrease, as airspeed drops, and asymmetric attitudes require increasing opposite control inputs. Trim settings are readjusted by the first officer, as the captain remains vigilant for any signs of fire in engine 2.

Once the situation is stabilized, the pilots confer on diversion options and communicate with radar control for vectors to the nearest suitable diversion airfield. The pilots then make a change in heading to expedite safe arrival and reprogram the FMS with new data. At their first opportunity, the flight deck reports the situation to the cabin passengers and crew. The crew continues to fly safely to the diversion airfield.

4. Define Human Failure Events (HFEs) and Unsafe Actions (UAs):

a. HFE 1: Failure to maintain flight control during reduction of engine thrust. This HFE covers any action or set of actions that might lead to inappropriate attitude or altitude of the plane while discovery and recovery of engine failure are taking place. UAs would include reverting to manual control mode and not paying attention to primary flight indicators, thereby allowing the plane to assume unsafe attitudes or altitude. Any action that would put flying the plane as a secondary priority, including preoccupation with diagnosis and non-primary flight displays, discussions with cockpit and cabin crew, leaving the flight deck, reading maps, extended visual confirmation of faulty engine, etc.

b. HFE 2: Failure to maintain thrust. This HFE covers any action or set of actions that might lead to thrust that is less than adequate. If the degree of thrust lost is underestimated and recovery actions are eliminated or postponed, the safety of the plane would be at risk. If the location of the thrust trouble is not identified, the wrong engine may be powered back or shut down. UAs would include misreading the symptoms and associated displays, engaging faulty mental models of how the plane's systems operate, not following safe procedures for engine shut-down, shutting down the unaffected engine, not including cabin crew in location diagnosis, not using passengers as a resource, etc.

c. HFE 3: Failure to make appropriate flight plan modification. This HFE covers the subsequent decisions and actions involved in changing the flight plan in light of the new conditions. UAs would include not diverting the flight plan, diverting to a distant field due to economics of repair or shuttling passengers, not paying attention to new symptoms that might indicate a change in engine status, taking extra time in getting plane on the ground, etc.

5. Identify Potential Vulnerabilities in the Operators' Knowledge Base

a. Tendency to *react quickly* to noise/vibration from partial engine failure. Pilots do not wish to take any more time than is absolutely necessary to identify and reduce power to the faulty engine. They can sense asymmetrical power and any imbalances in the engines, especially if engines are on the wings. Pilots don't like vibrations and wish to solve the problem quickly, thereby increasing the likelihood of making a mistake.

b. Due to *infrequency* of losing engines and time span since last simulator exercise, pilots may not have the skills necessary to correctly determine which engine failed based on cockpit indications alone. More specifically, vibration indications that are not normally used in everyday operations may be foreign to pilots and not interpretable.

c. Pilots expect that if power to the failing engine is reduced, the noise/vibration will decrease. Anything they do which *decreases the noise/vibration helps to confirm* that they've selected the correct engine.

d. Prior *history with a given craft* may predispose pilots to expect a particular engine to be the one most likely to fail. This could increase chances of not relying on the symptomatic information alone to make the diagnosis.

e. Pilots' incomplete *mental model* of how the aircraft systems work can affect how they diagnose problems. This may be due to incomplete training or training that was completed long ago, or limited hours in the specific craft, many recent hours in a similar craft, or very few recent hours in the specific craft.

f. Pilot's tendency to *respond immediately to radio contact* will interfere with the diagnosis and response to a problem, especially the thought processes that might lead to a complete and correct problem characterization and diagnosis.

g. As a safety measure, pilots learn to *shut down broken engines* to lessen the likelihood of fire or airframe damage. If errors are made in diagnosis, the drive to shut an engine down quickly can lead to shutting down the wrong engine.

h. Respect for the captain may *predispose a copilot to agree with a captain's* diagnosis, even when the diagnosis is incorrect, especially when the copilot is uncertain.

i. Pilots' *confidence* in their abilities might prevent them from using all of their resources to diagnose engine problems, such as cabin crew and passengers.

j. Pilots may have a tendency to *assume that it is relatively easy* to unambiguously identify which engine is having problems.

Table B.2 Time Frames of Interest for Base Case Scenario

Time Frame	Major Occurrences	Influences on/by Pilots
Initial conditions	Normal cruise conditions	Routine, pilots in supervisory mode
Source event 0-5 sec.	Onset of vibrations, loss of thrust, possibly change in pitch and yaw	Pilots alert and begin to react by correcting any change in attitude via flight controls, disengage autopilot
Situational appraisal 5-20 sec.	Vibrations continue and probably continue to worsen, possibly additional cues such as smell of smoke, etc.	Pilots search for cues in environment that would suggest nature of problem, airframe, engines, subsystems, etc.
Preliminary diagnosis 15-35 sec.	Problem may stabilize or continue to degrade	Pilots have narrowed possibilities and have agreed on probable source of problem—engine
Response plan 35-50 secs.	Problem may stabilize or continue to degrade	Pilots agree on action strategy to confirm preliminary diagnosis or to mitigate problem—power back one engine
Execute Response Plan 50-90 secs.	Vibration may diminish if engine speed is reduced	Pilots power back suspected engine and appraise any change in symptoms

Time Frame	Major Occurrences	Influences on/by Pilots
Situation communicatio n 40-100 secs.	Problem may stabilize, or continue to degrade	Pilots report situation to radar control or ATC
Response confirmation 60-120 secs.	Either a change in vibrations occurs or does not	Change in symptoms or instrument readings would confirm preliminary diagnosis and lead to safe shutdown of bad engine, no change would suggest it may be something else
Diversion plan 100-200 secs.	If craft has a disabled engine, a diversion should be sought after	Pilots look at maps and confer ATC to coordinate best diversion plan
Execute diversion plan	Regardless of problem stabilization, crew needs to divert soon as possible	Pilots attempt to get plane on ground as quickly as possible

Operator Tendencies and Informal Rules:

Table B.3 Table Relating Critical Functions and Informal Rules

Critical Flight Functions	Emergency Situation	Pilot Action Tendencies
Thrust	Reduced	Compensate quickly for to maintain altitude
Flight controls (cruise)	Upset attitude	Make yoke and trim adjustments to regain level flight
Airframe integrity	Threatened by explosion or fire	Eliminate potential for explosion or fire at the source as quickly as possible (shut down faulty engine)
Navigation	Diversion	Find nearest airfield that can accommodate craft and navigate to it immediately; maintenance facility would be an advantage, but tendency is to get plane down

Step 6. Search for Deviations from Base Case Scenario

Step 6.1. Search for Initiator and Scenario Progression Deviations

The initiating even in the base case scenario is a broken turbine fan blade that causes some internal engine damage, indicated by noise and vibration, followed by a gradual power decrease over time. The COM case is moderate damage/noise/vibration, leading to a fairly obvious diagnosis (Figure 1). Physical deviations of parameters in the 'more/less' dimension would definitely affect the salience of the perceptual cues to the pilots and affect subsequent diagnosis and quickness of response. More damage/noise/vibration (Figure 2) would cause a quicker, possibly more drastic response, whereas less damage/noise/vibration (Figure 3) might lead to a much delayed response or no response to the problem. When an engine loses significant thrust, thrust becomes asymmetric, potentially causing the plane to yaw in the direction of the affected

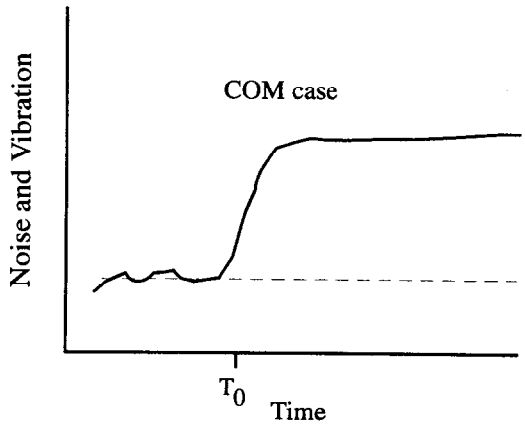

Figure 1.

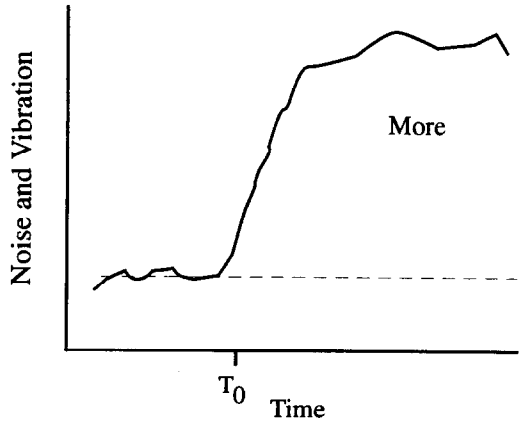

Figure 2.

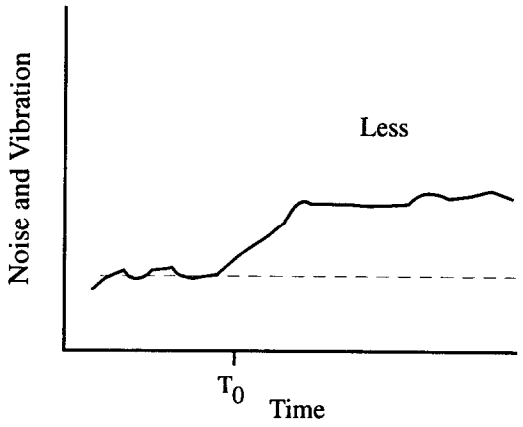

Figure 3.

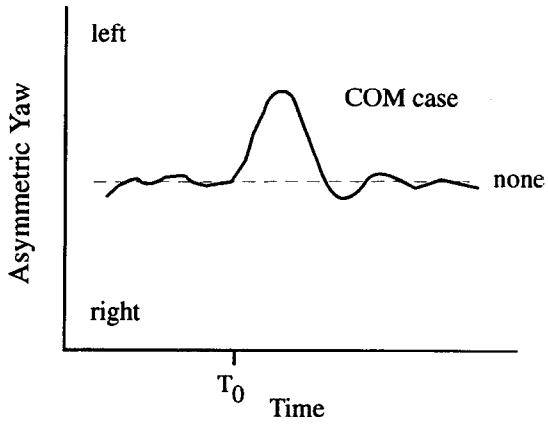

Figure 4.

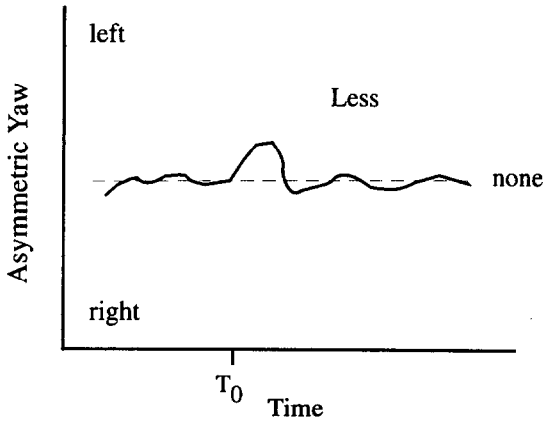

Figure 5.

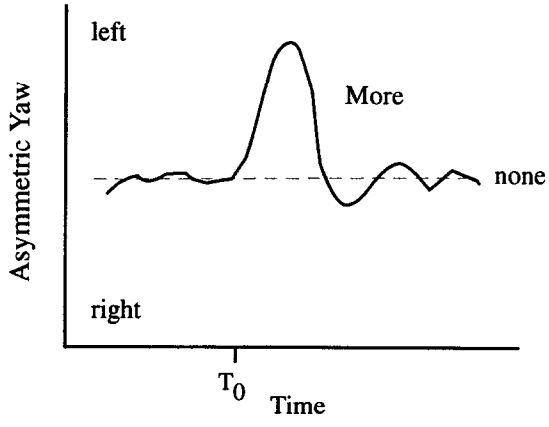

Figure 6.

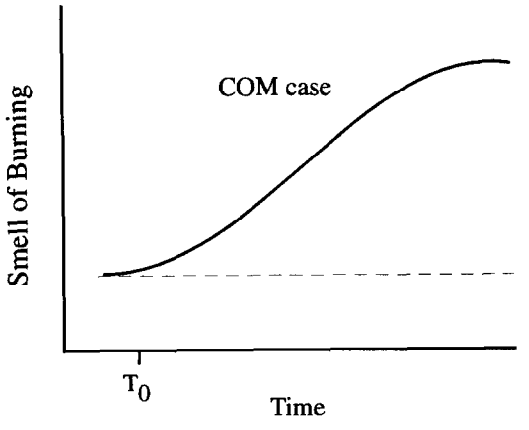

Figure 7.

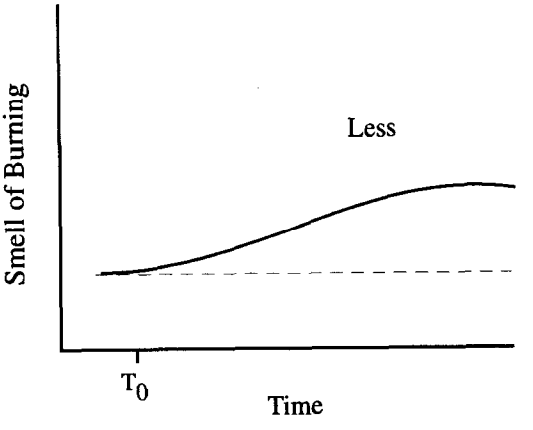

Figure 8.

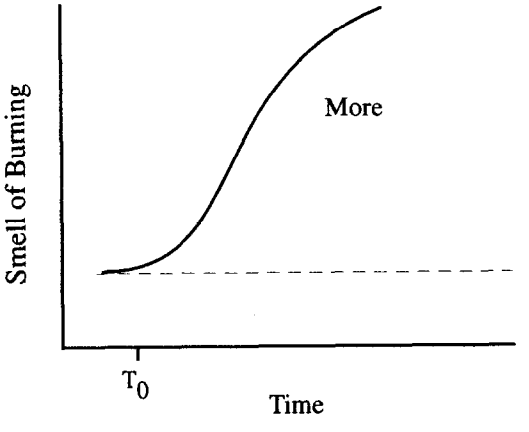

Figure 9.

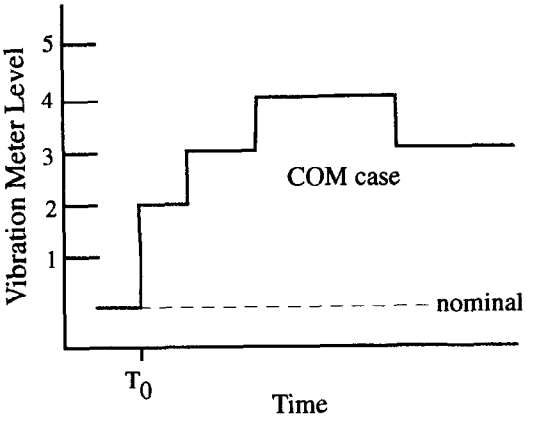

Figure 10.

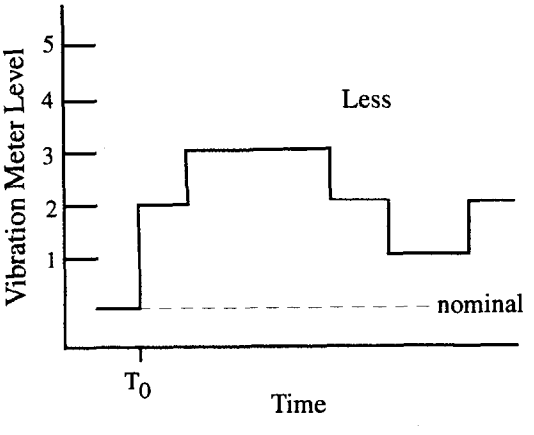

Figure 11.

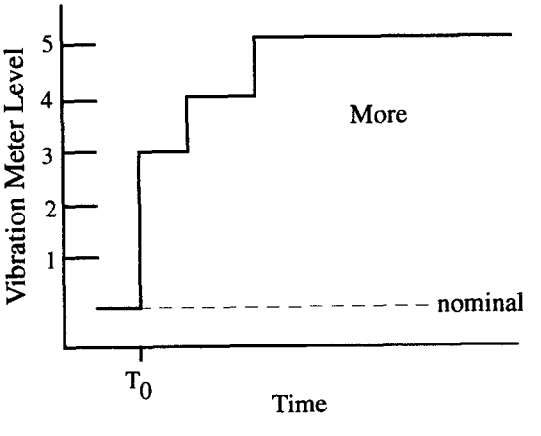

Figure 12.

engine (Figure 4). The rise followed by the immediate fall indicates a rapid response made by either the pilot or the autopilot to bring about coordinated flight. When the damage/noise/ vibration has a milder onset, virtually no asymmetric yaw occurs (Figure 5). Conversely, when damage/noise/vibration has a stronger onset (Figure 6), asymmetric yaw will be much more noticeable, and contribute to identification of the affected engine, but conceivably also to higher stress levels. Concomitant variables such as the smell of burning (Figures 7-9), and vibration meter level (Figures 10-12) act in similar ways to give the pilots additional information about the progression of the situation. In every case, however, higher levels of the parameter would lead to both higher stress levels and urgency, but also more diagnostic cues as to the source of the problem, i.e., which engine is failing.

Following the procedure outlined in 9.6.3 of NUREG 1624, Tables 9.16a and 9.16b were consulted for the two cases of 'more' and 'less.' In the case where there is a small change in parameters (less), two types of error can occur: lack of awareness, and application of incorrect procedure, due to misdiagnosis. In the case where larger changes in parameters occur (more), the error types listed in the tables don't seem to apply to the aviation scenario. If the parameters were dramatically increased over the COM levels, stress and workload probably would increase, but identification of which engine was failing would probably be much easier and faster. Controlling the plane with increased asymmetric yaw and keeping the plane at altitude with a significant loss in power would increase workload to a level that could negatively affect pilot performance. If it were affected severely, loss of control and HFE1 would occur. See Tables B.4 and B.5 at the end of this appendix for summaries of the results of this deviation analyses.

Step 6.2 Search for Relevant Rules:

Unlike nuclear power plant emergency operating procedures, which give detailed information on how to respond to accident scenarios, pilots must rely on training, instruments, and knowledge of the systems to diagnose what is happening and how best to respond. The following list is a partial list of rules of thumb that most pilots fly by in responding to in-flight emergencies:

1. Solve problem quickly or divert ASAP

2. Use available altitude as a safety net

3. Isolate failure so it does not creep and cause others, i.e. if an engine failure is identified, shut down the affected engine to reduce the chances of airframe damage or an uncontrollable fire.

4. Use a checklist, if appropriate, and if time

5. Report problem to ATC as soon as practicable

6. Divert to closest field with appropriate runways

7. Have faith in your instruments, but if in doubt, check redundant indicators

8. Involve cabin crew only if necessary

9. Keep the plane flying safely while solving any problems

10. Keep engines matched in operational parameters. In the partial loss of engine COM scenario, most rules support safety in flying. However, in the deviation involving 'less than' changes in physical parameters, rules 1, 7, and 8 can have deleterious effects on overall crew performance and flight safety. With less salient cues about the nature of the problem and which engine is affected, the rules of thumb push the pilots toward rapid resolution and increase the likelihood of a misdiagnosis and possibly shutting down a good engine. If cues are undetectable, then the rules above do not apply. If cues are 'more' salient, then the situation is even more dire than the COM and the rules support flight safety.

Step 6.3 Search for Support System Dependencies:

Table B.6 Primary Dependency Matrix for Turbofan Engine in Flight

System	Back-up	Engine	Pneumatic	Hydraulic	Electrical	APU and Batteries	Navi-gation
Pneumatic	2X	^					
Hydraulic	3X	^	^				
HVAC	2X		^				
Electrical	APU	^		v			
APU/Batteries	Is one		^		<>		
Flight Controls	Manual			^	^		
Navigation	2X		^		^		
Fuel	Multiple	v			^	v	
Instruments	Multiple	^	^		^		^
Computers	3X				^		
Suppl. Ox	Is one						

A>B = A is dependent upon B

The dependency table (Table B.6) shows that four major subsystems are (primarily) dependent upon the engines for their viability; pneumatics, hydraulics, electrical, and some instruments. Because of the back-ups and redundancy built into these subsystems, and the overabundance of power provided by the engines (some of these subsystems can operate normally with only one engine operating), it is not likely that the failure of an engine will first be communicated to the flight deck via the failing of, or sub-optimal performance of, a dependent subsystem. In other words, if the pilots noticed a sudden drop in hydraulic pressure, they probably would not initially infer that an engine has lost power.

If we look at secondary dependencies, several subsystems are dependent upon the electrical system, which is in turn, primarily dependent upon engine power. However, there are several back-up subsystems (the Auxiliary Power Unit, or APU, and a battery storage system), further

limiting the dependence of subsystems on the electrical system, fed by engine power. The dependencies of interest lie in the subsystems on which the engines depend, such as fuel and lubrication. The fuel systems have multiple redundancies and reconfiguration capabilities, and can be adjusted for minor blockages or pump failures. The lubrication system is part of the engine itself, and is fairly simple and robust. Nevertheless, pilots need to be aware of any glitches in the subsystems upon which the engines depend to anticipate and avoid any cascading-failures effect through the system architecture.

The partial engine failure COM could originate from internal engine failures, such as fan blades, shaft disintegration, bearing failures, etc. or from support-system problems, such as fuel starvation or lubrication failure. Normal flight-deck diagnosis for an initiating source would 'interrogate' these lines of reasoning, and would lead to checking instruments relating to the supporting subsystems.

Step 6.4 Search for Operator Tendencies and Error Types

Tables 15 and 16 from ATHEANA (NUREG 1624, REV. 1) were scanned for any error types that could relate to the HFEs of interest, and the following were found to apply:

HFE1: 1. Reduced attention paid to other parameters
2. Stress over concern of dramatic engine failure
3. Failure to recognize serious situation in time

HFE2: 1. Act too soon to shut down engine and make error in selection
2. Generation of false theories to explain coincidental changes
3. Delay in response while searching for common explanation
4. Defer action due to small changes in parameters

HFE3: 1. Develop a faulty response plan
2. Delay turning to diversion field, increasing risk

Step 6.5 Develop Descriptions of Deviation Scenarios

*A. **Minor/Partial Engine Failure.*** Physical parameters concomitant with engine failure are universally slower in developing and have lower intensity. This leads to the pilots not realizing something went wrong until later in the 'damage timeline.' Instruments do not help, as minimal deviations occur and no alarms sound. Thrust is lost gradually over time and pilots may not even realize the corrections made by the FMS. At some point, a loss in altitude would be noticed, either by the pilots, or the FMS. If this did not occur, the flight may terminate as a CFIT.

If the loss in altitude was noticed, diagnosis would begin, and the pilots would attempt to identify the affected engine. Correct identification of the affected engine is much more difficult than in the base case due to the lack of asymmetric thrust and to the minor differences in instrument readings. Readings of engine pressure ratio (EPR), fuel flow, and vibration would be very similar among the engines, if there were only minor problems. Noise and seat-of-the-pants

vibration monitoring might be the strongest cues for the pilots, making diagnosis extremely difficult. If the wrong engine is identified, 'safe practices' may cause pilots to power back and possibly shut down a good engine and eventually fly to a diversion airport on a bad engine.

B. Dramatic Engine Failure. Physical parameters concomitant with engine failure are universally faster in developing and have higher values. In this scenario, instead of minutes available for reacting, the pilots may have only a few seconds. As the engine fails abruptly, noise and vibration shake the plane violently, the plane yaws toward the affected engine (if on the wing), the nose drops due to reduced thrust, and the pilots must react quickly to keep the plane flying level. Correct control response would be to apply opposite rudder (feet), pull up on the nose, and increase throttle to the remaining engines. Opposite aileron may be necessary if the plane starts to roll in the direction of the affected engine. Power needs to be cut to the affected engine to reduce the probability of airframe damage and fire. If the threat of fire is suspected, or if the fire alarm sounds, the fire handle for the affected engine should be pulled (cutting off flammable fluids and flooding engine nacelle with fire-suppressing foam). If the pilots cannot identify the affected engine by flight dynamics alone, deviations in the instruments would point to the affected engine (reduced EPR, fuel flow, and RPM, and increased vibration). The danger of this scenario is not misdiagnosis, but the possibility of losing control of the craft or sustaining airframe damage due to fire, explosion, or mechanical disintegration. If both of these outcomes can be avoided, the pilots should be able to fly to a diversion airport safely using the remaining engines.

C. Onset of Symptoms During Takeoff. Here, the engine begins to disintegrate just when maximum power is needed, accelerating the damage and increasing the urgency of response. Assuming the power decrease is significant, the pilots must respond quickly and appropriately if they are to survive. The nose would have to come down to avoid a stall, and a much more gradual rate of ascent (or if enough altitude, level flight) would normally be attempted. The crew would most likely attempt to return to the same field, assuming that it is closest. Diagnosis and identification of the affected engine may not be critical to this scenario, as even a crippled engine may add to the thrust needed to land the plane quickly. Here is a dilemma situation at lower altitudes—if the engine is powered back, the flight may not have enough thrust to make the field, if not, the airframe may be damaged from fire or disintegration. This scenario, being very different from the base case, may deserve its own analysis.

D. Something else happens while responding to engine failure: This scenario compounds an engine failure with some other event, which could be interpreted as being either related to the engine failure, or as unrelated. An example would be a warning alarm that hydraulic pressure is down. This could be due to an engine-driven pump (related) or an electric pump (unrelated). This scenario may deviate significantly enough from the base case to deserve its own base-case treatment.

Step 7. Identify and Evaluate Complicating Factors and Links to PSFs

PSFs that Apply to the EFC:

1. Training – Traditional pilot training for engine-out response stresses speedy response to obvious perceptual cues. Upon engine-out diagnosis, rapid shut-down and compensation are the

rule. When cues are ambiguous, the pilots will be uncertain, stress will increase, and pilots will be forced to look for additional information to aid in their diagnosis and decision-making. In an ambiguous engine-failure context, lack of awareness of the vibration meters and how to interpret could be deadly, especially if the wrong engine is throttled back and eventually shut down. We do not have knowledge of level of training on AVM indicators.

2. Human-System Interface – The AVM indicators in some aircraft are comprised of five indicator lights that encircle the secondary engine instrument system (EIS) display. As vibration rises above nominal levels, the lights begin to illuminate in order, cumulatively, so that the number of lights illuminated indicates the vibration level on a five-point scale. For example, a level 3 would be indicated by the first three lights being illuminated. As vibration level varies, so does the number of lights illuminated, with little damping or lag. When a pilot looks at the meter, he/she is getting an instantaneous readout, not an average over some time period. Implications are that a pilot may look at the meter during a series of varied indications up and down the scale and not get a reasonable interpretation of the overall level of vibration. Depending on the sampling of indications, the interpretation may be too high or too low. 'Too high' may not affect things negatively, but a 'too-low' interpretation would lead to confusion if the pilot is attempting to compare a good engine with a bad one (both readings would be low). A better solution would be a trend indicator, which displays a time-averaged reading over a period of minutes, so that minor increases or major variations in vibration level can be captured and the history communicated to the pilots.

3. Communication – I don't know if this is a 'PSF', but crew communication can be critical in both the crisis-mode reaction to an abrupt, major engine failure (who is flying, who is shutting down bad engine?), or an ambiguous situation, where the crew must coordinate diagnosis and decision-making behaviors. Communication also relates to the cabin crew when needing additional input to diagnosing ambiguous cues. If communication between the flight deck and cabin crews is not a regular practice, valuable information can be lost.

4. Fatigue – We have made the assumption in this example that fatigue is NOT a factor. Obviously, it could be a negative factor in any incident/accident scenario. Fatigue has been shown to impair reasoning skills, decision-making, and problem-solving. When combined with stress, fatigue can make otherwise simple problems lead to disasters.

5. Stress – In some of the deviant scenarios, the urgency of the situation and workload could cause the pilots to feel that they may not be able to perform adequately to avoid failure. This response to environmental and contextual factors is called stress. If the time available is extremely limited, or the tasks required are too difficult to perform, or both, moderately high to extreme levels of stress can occur. In some cases, stress can actually trigger exceptional performance, as when adrenaline contributes to the strength or speed of a physical response (fight and flight). Fortunately, or unfortunately, most of our systems have engineered out requirements of great physical strength, so unless power assists fail, adrenaline-boosted physical strength may have limited utility. Stress normally has a negative influence on cognitive behaviors, even in well-trained operator populations, such as airline pilots. Stress can impair perceptual tasks, interpretation of information, accessing memory, reasoning skills, decision-making, and problem-solving. Routine scenarios, that have been anticipated and trained for, can

become nightmares quite easily, if the pilots' response to stressors is high, and it impairs cognitive skills significantly. This stress response can be assumed, given that equipment failures during flight are not that frequent, and that the consequences are dire.

6. Organizational Factors – Occasionally, airlines base decisions on economics rather than safety. If the airline of the affected plane asked the crew to divert to a field based on the availability of maintenance services or spare planes rather than proximity, HFE3 would be more likely.

Additional Physical Conditions:

Any additional failures during the primary event has already been discussed in Table B.6.

Step 8. Evaluate the Potential for Recovery

A. Minor/Partial Engine Failure. At some point, a loss in altitude would be noticed with a high likelihood, either by the pilots, or the FMS, and the faulty engine could be identified and shut down. If the wrong engine is shut down, flying on the bad engine could eventually make itself evident, and if at an adequate altitude, the good engine could be restarted for a safe landing. However, this is probably less likely than flying the bad engine into the ground.

B. Dramatic Engine Failure. The danger of this scenario is not misdiagnosis, but the possibility of losing control of the craft or sustaining airframe damage due to fire, explosion, or mechanical disintegration. If both of these outcomes can be avoided, the pilots should be able to fly to a diversion airport safely using the remaining engines.

C. Onset of Symptoms During Takeoff. Here is a dilemma situation at lower altitudes—if the engine is powered back, the flight may not have enough thrust to make the field, if not, the airframe may be damaged from fire or disintegration. Probability of recovery below about FL80 is very slim.

D. Something Else Happens while responding to engine failure: Recovery from this scenario is obviously less than just the engine failure alone, but the amount depends on the nature of the additional failure and its timing.

Table B.4. Partial Loss of Engine: Scenario Deviation Considerations

Guide Word	Physical Deviation	Significance	Analyze?
No/not/never	Initiator - sounds like engine failure but is not Scenario – real problem gets worse as pilots react to engines	Initiator – here, a sound and vibration is perceived as an engine failure, when it is really something else, power may be cut back Scenario – if something else is going bad, and pilots think it's the engine, problem-solving can be delayed, and plane can be power-deprived for a while, but good engines can be used to fly home	No. Pilots would most likely check engine instruments and diagnose that it is not engines – plane has power, is OK
Less, slower, part of	Initiator – very minor engine problem with no apparent attitude changes Scenario – problem continues to get worse	Initiator – a very minor problem in the engine may not develop into engine failure, or might cause failure later on – onset is not very abrupt, or is imperceptible, which can be insidious, may be picked up with constant surveillance of instruments by pilots or FMS. Scenario – once a problem is noticed, due to the subtle symptoms, it may be difficult to see differences in engine parameters and identify which engine is having problems, little asymmetric yaw, etc.	Yes. This case can lead to disaster if engine failure is not recognized by crew, or if identification of bad engine done incorrectly.
More, faster	Initiator – very abrupt onset of engine problems with thrust deficit and flight attitude change	Here, there is no question as to something going wrong very quickly and the pilots' reaction is assumed to be in very high stress mode. Pilots must recover safe flight attitude, make a quick diagnosis of which engine has failed, shut down that engine, increase thrust of available engines and divert.	Yes. Although different skills are required, and training should help, pilots still can fail at this set of tasks.
Reversed	Initiator – engine problem symptoms Scenario – symptoms go back to normal	Here, the pilots begin to respond to an engine failure and then realize that the symptoms (noise, vibration, smell of smoke) subside, and they are led to believe everything is normal again. Good pilots would assume that some problem still exists and perform diagnostics.	Yes. This case can lead to disaster if the engine is really failing but they are no longer reacting to it.
Late/early	Initiator – onset of symptoms occurs on T/O or landing Scenario –	The COM assumes cruise configuration. The tasks and associated workloads increase dramatically if the loss of engine occurs either on takeoff or landing phases.	Yes. Obviously, these deviations are extremely dangerous – may require its own COM analysis.
Inadvertent/as well as	Initiator – something else happens Scenario – while responding to engine, something else happens	In either case, the scenario becomes more complex, and the tasks and associated workloads become more difficult to complete without error. For instance, a fire breaks out in an engine nacelle, the alarm sounds, and the T-handle is pulled. If this is the affected engine, it could help identification, if not, it could increase scenario complexity.	Yes. Obviously, these deviations from the COM are extremely dangerous.

Table B.5. Results of Partial Engine Failure Source Event/Scenario Deviation Analysis

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Information Processing	Potential Error Types	Further Analysis?
Minor engine problem with no apparent attitude changes, problem continues to get worse, but with gradual changes, even when discovered, identification of exact nature is difficult	Limited discrimination – imperceptible or gradual change in display or flight attitude given demands Expectation bias - although pilots don't expect engine problems, they are sensitive to any change in sound or vibration. However, the last thing they want to hear is an engine glitch, so may be cognitively resistant to an imminent engine failure. Recency bias – pilots have experienced operational engines for many previous missions Apathy, lack of urgent consideration of changes Reluctance to change behaviors	Lack of awareness that parameters are changing – no action taken Failure to a response plan to a serious problem in time, and/or miss a decision point to take preventive actions or divert to alternate dest. Aware of problem, but little diagnostic information to base response-planning decisions upon – can lead to inappropriate responses and unsafe conditions	Yes. This kind of scenario can lead to major confusion in the cockpit, making response errors likely
Abrupt onset of major engine problems with thrust deficit and flight attitude change	Tunnel vision – perceptual narrowing due to high stress and compelling nature of perceptual cues Fixation - preoccupation with solving immediate problem obscures any others that may occur Overeagerness – pilots' intense need to stabilize situation may lead to unnecessary actions	Over-respond and put plane in dangerous attitude Lose awareness of/disregard other cues Unneeded or unsafe actions may be taken if pilots panic	? Don't know – probably not errors that ATHEANA is interested in
Engine problem symptoms, then go back to normal	Incredulity – pilots may not believe in the reversal of parameters, as mechanical systems do not usually fix themselves Fixation - preoccupation with solving immediate problem obscures any others that may occur, including reversal of symptoms	Disbelief would lead to a conservative approach and probably a safe outcome	No. This is not a realistic scenario.
Onset of symptoms occurs early or late -- on T/O or landing	Expectation bias - although pilots don't expect engine problems, they are sensitive to any change in sound or vibration. However, the last thing they want to hear is an engine glitch, so may be cognitively resistant to an imminent engine failure. Tunnel vision – perceptual narrowing due to high stress and compelling nature of perceptual cues Fixation - preoccupation with solving immediate problem obscures any others that may occur	With engine speeds changing more often and less need for power in landing phase, an engine problem may be less perceptible. Landing is a high-workload task, and if loss of power is not known until a correction is made to lengthen landing or go-around, a disaster could happen. In T/O phase, the opposite is true and	Yes. These are interesting deviations and the probability for human error would be very high, given the stress and need for quick action in these scenarios.

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Information Processing	Potential Error Types	Further Analysis?
	Overeagerness – pilots' intense need to stabilize situation may lead to unnecessary actions	the "pucker factor" will be the highest – losing power on T/O is a pilot's worst nightmare come true. One small mistake or delayed response could cause the loss of the already small opportunity to recover.	
Something else happens while responding to engine. A good example might be a sudden decrease in hydraulic pressure that is nearly simultaneous with engine failure. It would be ambiguous as to the relationship between the two – they could very well be related, or totally unrelated.	The 'something else' can be either supportive, or related to the initial problem, and help the detection and identification process, or can be unrelated and therefore distracting and competing. If supportive, the following may apply: Tunnel vision – perceptual narrowing due to high stress and compelling nature of perceptual cues Fixation - preoccupation with solving immediate problem obscures any others that may occur Overeagerness – pilots' intense need to stabilize situation may lead to unnecessary actions If competing, the following may apply: Cause attribution – the pilots may infer that due to the simultaneity of the symptoms, they must be related. This can lead to misdiagnosis problems. Incredulity – pilots may not believe that something else has gone bad. Expectation bias – pilots would not expect an unrelated problem to occur simultaneously and may not respond. Multiple lines of reasoning are created – conflicting choices, double binds, dilemmas, etc.	***If supportive, there should be less probability of human error, however the tunnel vision, preoccupation, or eagerness to do something may be enhanced as regards other problems that may arise.*** If competing, the probability of errors should rise substantially. The two problems would compete for pilots' attention and increase workload.	Yes. These are interesting deviations and the probability for human error would be very high, given the stress and need for quick action in these scenarios.

APPENDIX C: DISCUSSION OF THE TERM "HUMAN ERROR"

Human error is a term intentionally avoided in this treatment for two reasons. First, it does not contribute to the discussion in any constructive way. Secondly, the implied aspect of assigning blame detracts from the discussion by making people respond defensively. Human error is traditionally defined as: "any member of a set of actions that exceeds some limit of acceptability" (Rigby, Ref. 9.33). Senders and Moray (Ref. 9.34) wrote a book about the nature of human error, that reflected the thinking of 22 of the world's preeminent authorities on the subject, who met for a week on the subject in Bellagio, Italy, in 1983. The consensus was that an error means that "something has been done which: was not intended by the actor; was not desired by a set of rules or an external observer; or that led the task or system outside its acceptable limits." Park (Ref. 9.35) mentions that human errors are typically "manifested as failure to perform a required action; or its performance in an incorrect manner, out of sequence, or at an incorrect time." These types of errors are typically referred to as (respectively), errors of omission, errors of commission, sequence errors, and timing errors.

The distinction between mistakes and slips, made by Reason and Norman (Refs. 9.31 and 9.36) is perhaps more useful than the term error. They define a mistake as an incorrect plan or intention, whereas a slip has the correct goal state in mind, but the action or execution is not congruent with the goal. Examples would be:

> *mistake*—a pilot decides to divert to an airport 10 miles further because it has repair facilities, when he only has enough altitude to make it to the closest airport.
>
> *slip*—a pilot decides to switch gyro input to his artificial horizon display, but reaches up to turn the switch and inadvertently turns the control for the copilot's display.

For ASHRAM, the terms mistake and slip may be useful in assigning the erroneous behavior to a particular stage of processing—generally, mistakes to R/D/M and slips to Actions. Following this logic, error mechanisms would lead to mistakes, but not slips.

APPENDIX D: DISCUSSION OF THE TERM "SITUATION AWARENESS"

Many articles and reports have been written about situation awareness (SA) recently, and especially in relation to aviation operations. Endsley defines SA as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" (Ref. 9.37). Sarter and Woods (Ref. 9.38) define SA as "the accessibility of a comprehensive and coherent situation representation which is continuously updated in accordance with the results of the recurrent situation assessments." Adams, Tenny, and Pew (Ref. 9.39) refer to SA as the "up-to-the-minute cognizance required to operate or maintain a system." Although the term has definite intuitive appeal and has received much recognition since the later 1980s, Flach (Ref. 9.40) warns against creating circular reasoning by treating SA as anything more than a second-level abstraction for describing a set of environmental perception processes. Smith and Hancock (Ref. 9.41) describe SA as adaptive, externally directed consciousness.

Pilots and flight crews, perhaps more than any other group of system controllers, need to be aware of their location, vector through space, and condition to remain flying safely. In a study of military aircraft accidents, Hartel, Smith, and Prince (Ref. 9.42) found that problems with SA were found to be the leading cause. Looking at accidents among major commercial carriers, Endsley (Ref. 9.43) found that 88% of accidents involving human error could be attributed to problems with SA. These results may not be unexpected, given the rather broad interpretation of SA and its inherent constituent processes. Commercial pilots need to be aware of the flight plan, geographical location, positions of other aircraft, approach and airport peculiarities, current altitude, heading, velocity, weather, applicable flight rules, and the operational conditions of dozens of systems and subsystems that sustain their crafts. Military pilots additionally need to be aware of tactical goals and the capabilities and locations of enemy aircraft. Maintaining a high level of awareness of all of these things can be a challenge. Not only is the pilot maintaining awareness, but he/she is also flying the plane, making decisions, communicating with crew members and ATC, consulting maps, and performing other tasks. The SA needs to take place in parallel with the other tasks, assisting them, not interfering with them. How does a pilot maintain SA while performing other tasks?

In complex tasks, where much active, relevant information needs to be readily accessible, working memory is easily overloaded. One explanation for compensating for this deficit is the development of an internal construct of the current environment. When confronted with indications of an abnormal occurrence, people actively try to construct a coherent, logical explanation to account for their observations. Situation assessment involves developing and updating a mental representation of the factors known, or hypothesized, to be affecting plant state at a given point in time. The mental representation resulting from situation assessment is referred to as a *situation model.* The situation model is the person's understanding of the specific current situation. As can be gleaned from the definitions of SA offered above, the model is constantly updated as new information is received. This constant updating and implied rehearsal of the unchanged portions of the model make it suitable for registry in long-term memory, thereby relieving working memory of the burden of maintaining the model.

Many authors ascribe to the notion of an updateable internal model of the external world, but no one has experimentally proven its existence, located it in relation to other accepted processes and constructs (such as long-term memory), or has given a detailed account of how it works. Furthermore, although the internal model is an attractive and comprehensible concept, no one has explained if we have multiple models running in parallel for all of the systems we operate or comprehend during the day, or if we have one comprehensive world model. The concept also suffers from the inevitable fate of growing too responsible for cognition, thereby making it virtually impossible to test for validity.

APPENDIX E: EXAMPLE OF AN ASHRAM RETROSPECTIVE ANALYSIS

ASHRAM Retrospective Analysis

1. EVENT IDENTIFIER – Kegworth Crash

Event Name: Kegworth Crash
Aircraft Type: B737 Series 400
Date & Time: 01/08/89, 20:24
Problem: Engine vibration and fire
Unsafe Acts: Crew shut down good engine
Outcome: Crash with 47 fatalities
Sources: SkyNet special report, Air Accidents Investigation Branch Aircraft Accident Report No: 4/90 EW/C1095

2. ANALYSIS PERFORMED BY:

Name(s): Dwight Miller
Organization(s): Sandia National Laboratories
Contact information: Systems Reliability Dept. 6411
MS 0746
Albuquerque, NM 87008
dpmille@sandia.gov, (505) 845-9803

Dates: March 12-25, 1999

3. EVENT SUMAMRY:

A British Midland Airways Boeing 737 Series 400 aircraft, while climbing through FL283 on its flight from London to Belfast, experienced moderate to severe vibration, shuddering, or rattling, accompanied by the smell of fire in the cockpit. Although the airborne vibration monitoring (AVM) system indicated elevated vibration levels there was no warning of fire on the flight deck. [Both the commander and the first officer survived the crash; the former remembered seeing and smelling air conditioning smoke, the latter remembered only a strong smell of burning.] The commander took control of the aircraft and disengaged the autopilot. [Both pilots remembered that they could not diagnose which engine had suffered damage by means of their engine instruments.] The commander asked the first officer which engine was causing the trouble and the latter responded "it's the le...it's the right one." At 19 seconds after the onset of the vibrations the commander requested the first officer to "throttle it [#2] back." [According to the FDR, the #2 engine (on the right side) had steady indications, but engine #1 (on the left side) showed strong vibrations, elevated exhaust gas temperatures, increased fuel flow, and a reduction in speed.

What the pilots did not know, was that engine #1 had lost one tip of a turbine blade and

was running out of balance.] During the 11 seconds that elapsed between the disengagement of the autopilot and the throttle reduction in engine #2, the aircraft rolled slowly to the left through 16 degrees, however no corrective action was taken. Within 2 seconds of throttling back engine #2, the aircraft rolled level again. [This airframe response is consistent with reduced thrust from the left side being equalized by a reduction of thrust on the right.]

After the initial responses made above, the first officer reported the situation to London air traffic control (ATC) as an apparent engine fire. At 43 seconds after initiation, the commander ordered the first officer to "shut it [engine #2] down." The execution was delayed when the commander said, "Seems to be running alright now. Let's see if it comes in." After additional radio conversation addressing alternate landing sites, the first officer said he was about to start the engine failure and shutdown checklist, saying "seems we have stabilized...we still got the smoke." After additional radio conversation, and 2 minutes 7 seconds after initial vibration, the fuel shutoff valve for engine #2 was closed, and the engine was shut down. The crew directed the airplane to East Midlands for an emergency landing.

In the cabin, flight attendants and passengers heard unusual noises, felt vibrations, and smelled burning. They also saw signs of fire (torching, sparks) from the left (#1) engine, and some saw light smoke in the cabin. After the commander made an announcement about trouble in the right engine and shutting it down, several passengers were puzzled by the discrepancy but failed to alert the flight attendants, who had not heard the commander's reference to the right engine.

About 13 nautical miles (nm) from touchdown, ATC advised a right turn. Power was increased to the operating engine (#1) and the FDR recorded a maximum vibration again. One minute later at 900 ft. and 2.4 nm from touchdown, there was an abrupt decrease in power from the #1 engine. Despite attempts to restart the #2 engine, the airplane crashed short of the runway, killing 47 of its 118 passengers.

4. SIGNIFICANCE OF EVENT

This event never had to happen. With proper cockpit instrumentation, or a fire management system that worked, or better communication with the cabin crew, this aircraft could have easily flown home on the one 100% good engine and the second at reduced power (or shut down). It also demonstrates how a normally good safety practice (shutting down a malfunctioning engine) can lead to a disaster.

5. CRITICAL FLIGHT FUNCTION

Departure, climb to cruise - Thrust

6. MOST NEGATIVE INFLUENCES:

- The #1 engine, which lost a fan blade tip, could continue to run at over 90% power. If the engine blew up completely instead of being partially disabled, the crew could have determined the source of the vibration with higher reliability – **(AC)**
- The unfortunate coincidence of the vibration ceasing when the crew throttled back engine #2 led the crew to believe they were acting appropriately – **(AC)**
- The design of the AVM display was such that neither pilot could infer from the instrumentation which engine was causing the initial vibration – **(DF).**
- Despite a fire in the outboard section of #1 engine for 24 minutes prior to final approach, its fire alarm did not sound until 36 seconds prior to impact **(DF)**
- The captain had received training he remembered that taught him that the air conditioning system to the cabin was fed through the right (#2) engine. This had created a strong belief that the smell of smoke in the cockpit resulted from smoke in the aft cabin coming from the A/C system and the right engine. This belief further confirmed the erroneous hypothesis that the right (#2) engine was damaged and should be shut down. **(OF)**
- Airframe dynamics, in the form of vibration and roll, were not perceived as being diagnostic of a problem in the left engine **(OF)**
- The commander had only 23 hours on the series 400 B737, while the first officer had only 53 hours **(OF)**
- At no time did the first officer challenge the commander's hypothesis that the vibration was coming from engine #2—**(CRM)**
- At no time did the cabin crew, who were busy cleaning up the cabin, hear or challenge the commander's hypothesis that the vibration was coming from engine #2— **(CRM)**

Most Positive Influences: (that could have prevented or otherwise mitigated the event)

- Some of the passengers noticed the inconsistency of the fire in the left engine and the commander reporting the problem with the right engine was essentially solved, but none alerted the crew – **(CRM)**
- The commander reported that he tried to review the cockpit crew's actions when time permitted on initial approach to make sure they got it right, but the only running engine lost power and interrupted his train of thought – **(AC)**
- The aircraft was equipped with an airborne vibration management system (AVM), which is designed to inform the cockpit of engine vibration problems. – **(DF)**

7. KEY FLIGHT PARAMETER/CREW STATUS

Phase: Climbing to cruise altitude, 295 kts. CAS
Altitude: Climbing through 28,300 ft.
Location: 13 minutes into flight from London to Belfast
On Board: 8 crew, 118 passengers
Mechanical: All systems normal
Air Frame hrs. 521
Fuel on board: 9281 lbs.

Cockpit crew: Commander – male, 43, 763 hrs. in 737, 23 in Series 400, 12 hrs. last 28 days

First Officer – male, 39, 192 hrs. on 737, 53 in Series 400, 37 hrs. last 28 days

Cabin crew: Six attendants with cumulative B737 experience of 2 years 5 months

8. INITIATING EVENT:

20.05.05 Loss of turbine blade tip in engine #1, leading to compressor stalls, vibration, and eventually fire

9. EVENT TIMELINE

Initiator			Event Progression						Termination	
0:00		+0:19	+0:43	+2:07		+3:xx	+7:23		+18:44	+19:38
^	^	^	^	^	^	^	^		^	^
E1	E2	C1	C2	U1	R1	R2	R3		E3/R4	T

Unsafe Actions and Other Events:

Key: U = unsafe actions
C = contributory actions
E = equipment failures (significant to the event)
R = recovery actions
T = terminal event

10. EVENT LOG

Event	*Time*	*Description*
E1	0:00	Loss of turbo fan blade tip in engine #1, onset of vibration and slight loss of thrust
E2	0:xx	Despite fire in engine #1, no fire alarms sounded until 36 seconds prior to crash (no apparent hardware failure—system functioned as designed)

Event	*Time*	*Description*
CA1	+0:19	Upon Commander's order, first officer throttles back engine #2
CA2	+0:43	Commander requests first officer to shut down engine #2
UA1	+2:07	First officer finishes shutting down engine #2
R1	+2:xx	Conferred with cabin crew about smoke, but did not discuss suspect engine
R2	+3:xx	Cabin crew members saw that engine #1 was on fire but never confirmed w/Commander
R3	+7:23	Cockpit crew reviews incident by discussing sequence of events
E3/R4	+18:44	Engine #1 loses thrust when called on for more power in approach turn. At the request of the Commander, first officer attempts to restart engine #2
T	+19:38	Crash short of runway

11. UNSAFE ACTION ANALYSIS

UA Identification

The loss of thrust (CFFF) was caused by the crew shutting down engine #2 (UA). The crew shut down engine #2 for two reasons: 1) it was incorrectly diagnosed as being problematic, and 2) safe flying practices dictate that disabled engines be shut down to prevent possible fire and/or airframe damage.

EFC Description

1. ***Which aircraft-related events or conditions helped to create confusion about the actual status of the plane?***

   Minor decrease in thrust from affected engine made diagnosis ambiguous
   - Minor roll induced by asymmetric thrust
   - Instrument values did not unambiguously indicate which engine was in trouble

   Vibration decreased when engine #2 was throttled back, confirming erroneous hypothesis
   Smell of smoke seemed to be coming from cabin A/C vents, suggesting engine #2

2. ***What aircraft design issues contributed to either poor environmental perception or interfered with appropriate control of the aircraft or its systems.?***

   Airborne vibration monitoring (AVM) displays were not adequately designed and historically are not trusted by pilots to give useful information
   Functioning engine fire alarm system did not sound for 24 minutes

3. ***Which operator or crew factors contributed to insufficient environmental perception, faulty reasoning and decision-making, or inadequate response actions?***

   Both Pilot In Command (PIC) and First Officer (FO) had minimal hours in Series 400 B737
   Both PIC and FO had low hours (12 and 37) in previous 28 days

PIC had systems knowledge of A/C system, which he used to diagnose smell of smoke coming from the wrong engine
Both PIC and FO did not have familiarity with AVM displays, or may have mistrusted them
Inability of PIC or FO to infer engine trouble from other instruments
Assumption that reducing thrust on bad engine alone would reduce vibrations

4. ***What rules or procedural factors contributed to the accident?***
Procedure of reducing thrust to diagnose which engine is faulty
Safe-operating rule of shutting down faulty engine

5. ***What weather factors contributed to the accident?***
None that we know of

6. ***What traffic states or events contributed to the accident?***
None that we know of

7. ***What CRM issues factored in the accident?***
PIC had pretty strong hypothesis that engine #2 was affected and may have biased FO in his diagnosis
Cabin crew did not feel responsible to take an active role in assisting cockpit crew

All of these factors had a negative influence on the situation, leading the crew to the UA of shutting down a good engine. These factors, when combined in this manner, make up the EFC for the UA.

Cognitive Model Stages and Error Mechanisms
For the UA of shutting down engine #2, we know that it was an intentional act, and that no errors were made in its execution. Therefore, no errors were committed in the Action stage. We know however, that the pilots could not ascertain from their instruments which engine was exhibiting vibration and diminished thrust. These are problems in environmental perception. We also know that there was some faulty reasoning in diagnosing which engine was problematic. Therefore, there were errors committed in the R/D/M stage.

Environmental Perception:	Lack of familiarity with display stimuli prevents comprehension
Reasoning/ Decision-Making	Primacy bias – tendency to give more significance to early information, hypotheses and conclusions than later
	Expectation or Confirmation bias – operator gives more significance to information that confirms beliefs than to information which contradicts beliefs
	Cause/effect relationship assumption – tendency to assume a cause-effect relationship between or among events that occur simultaneously

12. RECOVERY ANALYSIS (after UA of shutting down wrong engine)

1. No fire alarm for affected engine until final approach
2. No observance of worse-than-typical engine performance from instruments for remainder of flight
3. Passengers and cabin crew looking out window at engine fire did not contact cockpit crew
4. Review of actions by Commander interrupted by radio contact
5. Attempt to restart good engine on final approach

13. SAFETY IMPROVEMENTS (from source documentation)

a. Examine fire/overheat and AVM circuitry for left/right engine sense.
b. CAA advise pilots about fan tip failure and associated smoke possible from A/C system.
c. Review attitude of pilots to current engine vibration indicators, and possible improvements.
d. CAA should require pilot training for AVM-equipped aircraft.
e. Regulatory requirements should be amended to include a standard way of assessing the effectiveness of such displays in transmitting pertinent information to the flight crew.
f. Modify the EIS on B737-400s to include attention-getting features when vibration meets maximum levels.
g. Boeing should amend flight manuals to include what actions should be taken when high vibration and smell of smoke occurs.
h. CAA ensure that crew currency training in simulators includes practice reprogramming of flight management systems or others that control key approach and landing display format during unplanned diversions.
i. CAA review current guidance to ATC on offering a discrete RT frequency to commercial pilots in emergencies.
j. CAA review training requirements to ensure pilots are familiarized with electronic flight displays before flying public transport aircraft so equipped.
k. Training exercises for pilots and cabin crew should introduced to improve coordination in emergencies.
l. CAA review current training to restore balance in technical appreciation of aircraft systems.
m. CAA should look into providing visual status information to the flight crew via external and internal closed circuit television monitoring.
n. FDRs which use buffering techniques made non-volatile and hence recoverable after loss of power.
o. CAA should consider increasing engine vibration sampling rate from every 64 seconds to every second.
p. JARs should be modified to ensure seating is safety engineered to minimize occupant injury on impact.
q. CAA should research passenger seat design for effective torso restraint and aft-facing seats.
r. Cabin floor designs of new aircraft types should take into account dynamic impulse and distortion.
s. CAA should research feasibility of increasing cabin floor toughness beyond current levels.
t. CAA should require infants and young children be placed in child seats for T/O, landing, and turbulence.
u. CAA expedite publication of as specification for child seat designs.

14. ISSUE SOURCE

a. Diagnosis of single-engine failure during cruise
b. ATC radio communications as interruptions of cockpit activities and procedures
c. Interaction of cockpit and cabin crews in diagnosing airframe and subsystem conditions.

APPENDIX F: GLOSSARY OF TERMS USED IN ASHRAM

Action: The third step in the ASHRAM cognitive model that includes taking specific control actions required to perform a task. It may involve taking discrete actions (e.g., flipping a switch) or it may involve continuous control activity (e.g., keeping the wings level). An action may be performed by a single person, or it may require communication and coordination among multiple individuals.

Aircraft Conditions (ACs): The aircraft state defined by combinations of its physical properties and equipment conditions, including the measurement of parameters. This includes not only the states of major systems (engines) and supporting subsystems (fuel pumps), but the attitude and vector of the craft in the airspace (airspeed, pitch, roll, yaw, altitude, rate of climb, etc.).

ATHEANA: A technique for human event analysis, or ATHEANA was developed by the US Nuclear Regulatory Commission's (NRC) Office of Nuclear Regulatory Research, in cooperation with SNL, Brookhaven National Laboratories and various other contractors in the late 1990s. It is an HRA modeling process that can accommodate and represent the human performance found in real nuclear power plant events, and can be used with probabilistic risk assessments (PRAs) or other safety perspectives to resolve safety questions (see NUREG-1624, Rev.1).

Availability Heuristic: The tendency of individuals to base interpretations or judgements on the ease with which relevant information can be recalled or with which relevant instances or occurrences can be imagined. Availability can be influenced by factors such as the recency and salience of the individual's own experiences.

Base-case scenario: A nominal, well-understood, successful scenario that is used as a reference, or seed event for the ASHRAM prospective analysis. It comprises a set of assumptions, initial conditions, an initiating event, and 'textbook' responses by the crew, referred to collectively as the consensus operator model (COM).

Circumvention: A deliberate, deviation from rules and practices that has the intention of maintaining safe and/or efficient operations.

Crew Resource Management (CRM): The ability of a crew to manage and delegate responsibilities, tasks, and activities of its crew members effectively so that all tasks required for safe flight are accomplished.

Cognitive Activity: Cognitive activity is the thought process associated with the operator's (1) environmental perception, (2) reasoning and decision-making, and (3) actions.

Confirmation Bias: The tendency of individuals to seek or interpret indications in ways that confirm expectations. The result can be a failure to appropriately revise opinions or interpretations in light of new, conflicting information.

Consensus Operator Model (COM): The COM is the consensus set of appropriate pilot responses to the situations posited in the base-case scenario.

Contributory Action (CA): An action performed by a crew member or ATC controller that leads to or contributes toward an unsafe action, but in and of itself is not an unsafe action.

Critical Flight Functions (CFFs): The fundamental functions required for conducting a safe flight.

Critical Flight Function Failures (CFFFs): Failure in fundamental, functions required for conducting a safe flight.

Design Factors (DFs): Performance shaping factors that could contribute to an error-forcing context from the particular aircraft design, instruments, etc.

EGT: Exhaust gas temperature

Environmental Perception: This is the first stage of the ASHRAM cognitive model, which includes all perceptual modalities and the receiving of all information from the environment (both inside and outside the aircraft). The division between this stage and latter stages of the model, and the amount of active cognitive functioning (as in selective attention and memory retrieval) is the subject of continuous debate among theorists, and will not be resolved here.

Error-Forcing Context (EFC): The situation that arises when particular combinations of *performance shaping factors* and *aircraft/airspace conditions* create an environment in which unsafe actions are more likely to occur.

Error of Commission (EOC): An unsafe action, that, when taken, leads to a change in aircraft configuration, with the consequence of a degraded safety state. Examples include setting an inappropriate navigation frequency, taking the plane to an unauthorized flight level, and landing on a closed runway,

Error of Omission (EOO): An unsafe action resulting from a failure to take a required action, that leads to an unchanged or inappropriately changed aircraft configuration with the consequence of a degraded safety state. Examples include failures to maintain altitude and omitting an important action step in the landing checklist.

Error Mechanism: A cognitive process that can cause a particular *unsafe action* and is triggered by particular combinations of *performance-shaping* factors and *aircraft conditions*. Error mechanisms are often not inherently bad behaviors, but represent mechanisms by which people often efficiently perform skilled work. However, in the wrong context, these mechanisms may lead to inappropriate human actions that have unsafe consequences.

Expectation Bias: The tendency for people to give more significance to information that confirms their beliefs than to information that contradicts their beliefs.

Event: Generic term used in discussion of both base-case scenarios and deviation scenarios that refers to the collective scenario activities that take place after an initiating event.

Frequency Bias: Frequently occurring events are often recalled more easily than scarce events. This can lead to a tendency in people to interpret in-coming information about an event in terms of events that occur frequently, rather than infrequently occurring or unlikely events.

Fixation Error: A failure to appropriately revise the assessment of a situation as new evidence is introduced.

Human Error: In the PRA community, the term 'human error' has often been used to refer to human-caused failures of a system or component. However, in the behavioral sciences, the same term is often used to describe the underlying psychological failures that may cause the human action that fails the equipment. Therefore, in ASHRAM, the term 'human error' is only used in a very general way, with the terms *unsafe action* and *error mechanism* being used to describe more specific aspects of human errors.

Human Failure Event (HFE): A basic event that is modeled in the logic models of a PRA (event and fault trees), and that represents a failure of a function, system, or component that is the result of one or more *unsafe actions*. A human failure event reflects the PRA systems' modeling perspective.

Human Reliability: The probability of successful performance of the human activities necessary for either a reliable or an available system. More specifically, the probability that a system-required human action, task, or job will be completed successfully within a required time period, as well as the probability that no extraneous human actions detrimental to system reliability will be performed (Swain and Guttmann, 1983).

Human Reliability Analysis (HRA): A method by which human reliability is estimated.

Initial Conditions (ICs): In scenario descriptions, initial conditions describe the pertinent states of the aircraft, weather, traffic, and crew at the point of departure from routine flight conditions, or when the initiating event occurred.

Initiating Event (IE): A discrete event that happens during a flight that perturbs the steady-state, nominal, or expected operation of the flight, that challenges airplane control and creates a unique context for potential UAs. If no discrete event can be identified, as in a slow drifting off-course, the analyst may choose an arbitrary point during the continuous event, or the next identifiable, discrete event following the continuous event as the initiating event.

Information Processing: A theoretical approach to cognitive psychology, popular from the 1960s through the present that emphasizes discrete, identifiable, testable, stages of processing of information, from perception to response.

Information Processing Model: A general description of the range of human cognitive activities required to respond to abnormal or emergency conditions. The model used in ATHEANA considers actions in response to abnormalities as involving three steps (1) environmental perception, (2) reasoning and decision-making, and (3) actions.

Mental Model: Mental representations that integrate a person's understanding of how systems and plants work. A mental model enables a person to mentally simulate plant and system performance in order to predict or anticipate plant and equipment behavior.

N1 and N2: These readings indicate the air pressures before (N1) and after (N2) the compressor stages of a turbofan engine.

Operator factors (OFs): Performance shaping factors that exist within the operator or crew member, including knowledge, experience, intelligence, stress, fatigue, skills, etc.

Performance Shaping Factors (PSFs): A set of influences on the performance of a crew resulting from the characteristics of the aircraft, the airspace, and the crew. For ASHRAM, the PSFs include, weather, traffic, aircraft design (including human-factors aspects of the displays and controls), procedures, operator factors, and crew-resource management.

Primacy Bias/Effects: The tendency in people to give more significance to the data they first see (and may draw conclusions from) than to later data. When judgments or decisions are required, initial information is sometimes more easily recalled than later occurring information.

Probabilistic Risk Assessment/Analysis (PRA): A PRA is an analytical process that quantifies the potential risk associated with the design, operation, and maintenance of aviation infrastructure to the health and safety of the public.

Procedural Factor (PF): A performance-shaping factor that comes from procedural issues, such as checklists, sequences of tasks, required steps

Reasoning and Decision-Making (R/D/M): The second stage of the cognitive model used by ASHRAM, which includes all cognitive functions between environmental perception and taking action. R/D/M includes interpretation, logic, evaluation, reasoning, using rules, problem solving, consideration of alternatives, decision-making, and response planning.

Recency Bias/Effects: Events that happened recently are recalled more easily than events that occurred a long time ago. In attempting to understand in-coming information about an event, people tend to interpret the information in terms of events that have happened recently, rather than relevant events that occurred in the more distant past.

Recovery Path: An action or set of actions that catches the UA and corrects it, or instigates actions or outcomes that prevent the UA from leading to a terminal event.

Representativeness Heuristic: The tendency to misinterpret an event because it resembles a "classic event" which was important in past experience or training, or because there is a high degree of similarity between the past event and the evidence examined so far.

Rules: Rules are the guidance pilots follow in carrying out activities in the operation of a flight. Rules can be either formal or informal in nature. *Formal rules* are specific written instructions and requirements provided to pilots and authorized for use by the FAA, and company management. *Informal rules* sources include training programs, discussions among pilots, experience, past practices, and best practices.

Salience Bias: The tendency to give closer attention or to weight more heavily information or indications that are more prominent, (e.g., the most visible, the loudest, or the most "compelling" instrument displays.)

Satisfying: The tendency in people (under some circumstances) to stop looking for a solution when an acceptable, but not necessarily optimal one, is found.

Simplifying: People tend to disregard complex aspects of data (e.g., interaction effects, and give more significance to aspects of the data they understand). This is analogous to searching for a lost item under the lamppost because that is where the light is.

Subject Matter Experts (SMEs): SMEs are people involved in the ASHRAM analyses that have particular knowledge, skills, or experience that contribute to factual information, judgment, and anticipation involved in analyzing events.

Terminal Event: The event which signifies the unsuccessful termination of a flight. This is usually a crash with fatalities (doubly terminal), but could also be a ground collision, aborted takeoff, a semi-successful crash landing, or any other ending event which is considered an incident or accident.

Traffic Conditions (T): These performance-shaping factors are traffic conditions, either local or remote, aloft or ground, that in some manner affect the flight event being analyzed.

Tunnel Vision: The tendency in people to concentrate only on the information that is related to their prevailing hypothesis, neglecting other important information

Unsafe Action (UA): Actions inappropriately taken, or not taken when needed, by crew members that result in a degraded safety condition.

Weather Conditions (WX): These performance-shaping factors are weather conditions, either local or remote, that in some manner affect the flight event being analyzed.

Distribution

MS0185	Dorothy Stermer, 1317
MS0428	Dave Carlson, 12300
MS0615	Roger Hartman, 6252
MS0615	Richard Perry, 6252
MS0612	Review & Approval Desk, 9612 for DOE/OSTI
MS0736	Thomas E. Blejwas, 6400
MS0739	John Guth, 6415
MS0746	Robert Cranwell, 6411
MS0746	Dwight Miller, 6411 [9]
MS0746	Hugh Whitehurst, 6413
MS0746	Donnie Whitehead, 6413
MS0747	Allen L. Camp, 6410
MS0747	Vincent Dandini, 6410
MS0747	Felicia A. Durán, 6410 [2]
MS0747	Gregory Wyss, 6410
MS0748	Robert Waters, 6413
MS0748	John A. Forester, 6413 [9]
MS0780	Sabrina Jordan, 05838
MS0829	Chris Forsythe, 12323
MS0829	Karen Wenner, 12323
MS0839	Elaine Raybourn, 16000
MS0839	Gerry Yonas, 16000
MS0899	Technical Library, 9616 [2]
MS1137	John Ganter, 6535
MS1188	John Wagner, 15334
MS1202	LeAnn Miller, 5902
MS1221	Russ Skocypec, 15002
MS9018	Central Technical Files, 8945
MS9201	Howard Hirano, 16000