RECEIVED

On the Safety of Aircraft Systems: FFR 10 1998
A Case Study OSTI

Prepared for the

**Federal Aviation Administration
Research Grant Number 95-G-039**

by

G. Martinez-Guridi, R.E. Hall, R.R. Fullwood

**Engineering Technology Division
Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 11973**

May 14, 1997

This research was supported by the U.S. Department of Energy:
Contract No. DE-AC02-76CH00016

Disclaimer

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

DISCLAIMER

**Portions of this document may be illegible
electronic image products. Images are
produced from the best available original
document.**

On the Safety of Aircraft Systems: A Case Study

G. Martinez-Guridi, R.E. Hall, R.R. Fullwood

Engineering Technology Division
Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 11973

May 14, 1997

Work carried out as part of FAA Research Grant Number 95-G-039

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

CONTENTS

	<u>Page</u>
List of Figures	iii
List of Tables	iii
Acknowledgments	iv
List of Acronyms	v
Executive Summary	vi
1. Introduction	1
1.1 Information about the Accident	2
1.2 Airplane Information	4
2. Overview of the Boeing 767-300ER	5
2.1 Overview of Turbofan Engines	6
2.1.1 Propulsion and Thrust	6
3. Description of Thrust Reverser System	10
3.1 Functional Description of the Thrust Reverser System	11
4. Analyses of the Accident Contained in the Accident Report	15
4.1 Engineering Simulation of the Accident	15
4.2 Analysis of Failures of the Components of the TRS	16
4.3 Changes in System Design as a Result of the Accident	17
5. Application of Probabilistic Safety Assessment (PSA) Methods	19
5.1 PSA model	19
5.2 Assessment of the Changes in TRS Design	28
6. Conclusions and Future Work	30
6.1 Conclusions	30
6.2 Future Work	31
References	33
Appendix A Details of the Thrust Reverser System	34

Acknowledgments

We would like to acknowledge the support and guidance of Sam Sampath and John LaPointe from the Federal Aviation Administration (FAA) at the William J. Hughes Technical Center. We are indebted to Bob Baitoo, FAA, Long Beach, California, who suggested the study of the thrust reverser system.

We also are grateful to Pranab Samanta, leader of the Risk and Reliability group, for his insightful comments throughout this study.

List of Acronyms

AD	Airworthiness Directive
ARP	Aerospace Recommended Practice (SAE)
CVR	Cockpit Voice Recorder
DCV	Directional Control Valve
DFDR	Digital Flight Data Recorder
EEC	Electronic Engine Control
EICAS	Engine Indicating and Crew Alerting System
ETA	Event Tree Analysis
ETOPS	Extended-range Twin-engine Operations
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HIV	Hydraulic Isolation Valve
LVDT	Linear Variable Differential Transformer(s)
MCS	Minimal Cut Set(s)
NTSB	National Transportation Safety Board
PIMU	Propulsion Interface Monitor Unit
PSA	Probabilistic Safety Assessment
PSSA	Preliminary System Safety Assessment
PSEU	Proximity Switch Electronic Unit
QRH	Quick Reference Handbook
SAE	Society of Automotive Engineers, Inc.
TRA	Throttle Resolver Angle
TRS	Thrust Reverser System

Executive Summary

An airplane is a highly engineered system incorporating control- and feedback-loops which often, and realistically, are non-linear because the equations describing such feedback contain products of state variables, trigonometric or square-root functions, or other types of non-linear terms. The feedback provided by the pilot (crew) of the airplane also is typically non-linear because it has the same mathematical characteristics.

An airplane is designed with systems to prevent and mitigate undesired events. If an undesired triggering event occurs, an accident may progress in different ways depending on the effectiveness of such systems. In addition, the progression of some accidents requires that the operating crew take corrective action(s), which may modify the configuration of some systems.

The safety assessment of an aircraft system typically is carried out using ARP (Aerospace Recommended Practice) 4761 (SAE, 1995) methods, such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA). Such methods may be called *static* because they model an aircraft system on its *nominal* configuration during a *mission time*, but they do not incorporate the action(s) taken by the operating crew, nor the dynamic behavior (non-linearities) of the system (airplane) as a function of time.

Probabilistic Safety Assessment (PSA), also known as Probabilistic Risk Assessment (PRA), has been applied to highly engineered systems, such as aircraft and nuclear power plants. PSA encompasses a wide variety of methods, including event tree analysis (ETA), FTA, and common-cause analysis, among others. PSA should not be confused with ARP 4761's proposed PSSA (Preliminary System Safety Assessment); as its name implies, PSSA is a preliminary assessment at the system level consisting of FTA and FMEA.

A typical application of PSA methods requires developing event trees and fault trees. The event trees model the dynamic behavior (in time) of the airplane as it tries to cope with undesired events; corrective action(s) taken by the operating crew as the accident progresses are incorporated into it. Then, fault trees are developed to model the response of mitigating systems at each stage of the accident's progression depicted in a corresponding event tree. When the configuration of a system changes as an accident progresses, a fault tree for a system has to be modified so that it adequately models the response of the system during *another* mission time. In this way, the non-linearities and complexities of the progression of an accident can be more accurately and realistically modeled.

The objective of this study was to apply PSA methods to incorporate the non-linear behavior of a system (airplane) by modeling the dynamic processes during possible accidents as a function of time. To this end, the thrust reverser system (TRS) is analyzed in the context of a fatal accident that happened in Thailand on May 26, 1991, involving a Lauda Air Boeing 767-300ER airplane powered by two Pratt & Whitney 4060 engines. The objective included developing a PSA model of the TRS during the progression of this accident to illustrate the usefulness of PSA methods in incorporating

non-linear feedback and in treating the interaction between the operation of systems and actions taken by the operating crew.

This work was carried out as part of the Federal Aviation Administration (FAA) Research Grant number 95-G-039. The scope included a review of non-linear feedback, of turbofan engines and thrust concepts, of the TRS and of the accident; a discussion of different approaches for the safety assessment of aircraft systems; and development of a PSA model of the most relevant components of the TRS and of the major factors in the progression of the accident.

A risk model was developed consisting of an event tree with supporting fault trees to represent the progression of the accident. The interaction between the TRS and the operating crew during the accident is modeled, and findings of the accident investigation are incorporated in the model. A feasible sequence of events leading to the fatal accident was identified.

The following major insights were gained during the development of the risk model:

1. In the Boeing 767, the deployment of the TRS of *one* engine versus *two* engines is very critical because the engine in one wing will "push" while the engine in the other wing will "pull", throwing the airplane into a spin (yawing and rolling). This would be the case for any aircraft employing one engine in each wing, and it may also affect airplanes with other configurations of engines when normal (forward) thrust is applied in one wing and reverse thrust is applied in the other.
2. The interaction between the aircraft systems and the crew are very important, and they can be modeled using the integrated approach of PSA methods.
3. The report describing the accident does not give details of the changes proposed by Boeing after the accident, nor how the TRS would operate with the changes implemented. An assessment of the TRS design changes using PSA techniques would require a detailed development of risk models (beyond the scope of this grant), and more detailed information. From the limited evaluation of the TRS, the following insights are applicable:
 - 3.1 By adding a dedicated stow valve, the redundancy provided by two valves to prevent uncommanded TRS deployments would be preserved. Accordingly, this change is expected to reduce the likelihood of an uncommanded in-flight deployment.
 - 3.2 The Directional Control Valve (DCV) of the TRS has some latent failures-modes, identified in the report of the accident, that future changes could take care of. An example is uncommanded deployment of the thrust reverser when the solenoid valve's return-passage internal to the DCV is blocked.

- 3.3 Further guidance can be given in the airplane's Quick Reference Handbook (QRH) about the criticality of an uncommanded in-flight deployment of the TRS of **one** engine.
- 3.4 It seems advisable to review the *support* activities related to the TRS, such as maintenance and troubleshooting. Findings in the accident report, such as the inspections and checks required by airworthiness directive (AD) 91-15-09, indicate that approximately 40 percent of airplane reversers checked had auto-restow position sensors out-of-adjustment. It would be advisable to enhance training and awareness of crew members and support personnel on the potentially catastrophic effects of an uncommanded in-flight deployment of the TRS of **one** engine.
- 3.5 It seems prudent to implement a mechanism that would **definitely** prevent an uncommanded deployment of the TRS of one engine. There are two possibilities:
 - 3.5.1 A mechanism that does not allow the TRS to deploy unless it is commanded by the crew,
 - 3.5.2 A mechanism that does not allow the TRS of one engine (two engines in an airplane with 4 engines, two in each wing) to deploy unless the TRS of the engine in the other wing (the two engines in the other wing) also deploys. This possibility would have to be substantiated by further, more detailed analyses and tests.

The following major areas can be further explored:

- 1. PSA-based methods to analyze aircraft accidents/incidents. Development of a database of PSA models of systems/accidents.
- 2. Design and procedural improvement of aircraft systems. Application of PSA methods to prioritize resources to enhance aviation safety.
- 3. Modeling interactions of aircraft systems (airplane) and the flight crew
- 4. Comprehensive study of the TRS both before the accident and, especially, after the changes have been implemented.
- 5. Compilation of field failure data to quantitatively evaluate the model.
- 6. Preparation of PSA methods, such as the ones used in this study, as a package of safety tools that can be used by the air transportation industry and the FAA.

These areas are discussed in section 6.2.

1. Introduction

An airplane is a highly engineered system incorporating control- and feedback-loops which often, and realistically, are non-linear because the equations describing such feedback contain products of state variables, trigonometric or square-root functions, or other types of non-linear terms (Grantham and Vincent, 1993). The feedback provided by the pilot (crew) of the airplane also is typically non-linear because it has the same mathematical characteristics.

The safety assessment of an aircraft system typically is carried out for its *nominal* configuration during a *mission time*, and it does not incorporate the dynamic behavior (non-linearities) of the system (airplane) as a function of time.

The objective of this study was to apply Probabilistic Safety Assessment (PSA) methods to help incorporate the non-linear behavior of a system (airplane) by modeling the dynamic processes during possible accidents as a function of time. To this end, the thrust reverser system (TRS) is analyzed in the context of a fatal accident that happened in Thailand on May 26, 1991, involving a Lauda Air Boeing 767-300ER airplane powered by two Pratt & Whitney 4060 engines. This event is documented in a report (Aircraft Accident Investigation Committee, Ministry of Transport and Communications, Thailand, July, 1993) that determined the probable cause of the accident to be uncommanded in-flight deployment of the left engine's thrust reverser, which resulted in loss of flight-path control. The specific cause of such deployment was not positively identified.

The objective included developing a PSA model of the TRS in the context of the progression of this accident to illustrate the usefulness of PSA methods in incorporating non-linear feedback, and in treating the interaction between the operation of systems and actions taken by the operating crew.

Scope

This work was carried out as part of the Federal Aviation Administration (FAA) Research Grant number 95-G-039. The analysis illustrated the ability of PSA methods to analyze a system during the progression of an accident, which may include interactions with the operating crew and non-linear feedback. The scope included a review of non-linear feedback, of turbofan engines and thrust concepts, of the TRS and of the accident; a discussion of different approaches for the safety assessment of aircraft systems; and development of a PSA model of the most relevant components of the TRS and of the major factors in the progression of the accident.

Due to the limited resources available for this work, it is not meant to be an exhaustive PSA of the TRS; furthermore, no quantitative evaluation of the models was carried out.

The only information available to us about the accident and the way in which TRS was implemented in this airplane was the accident report mentioned above. To give the reader a good understanding without having to refer to the original document, we produced a self-contained document with information on the accident and the TRS. In addition, to clarify the operation of this system, we

included figures from a Boeing 737 airplane when they were not available for a Boeing 767; we understand that the corresponding figures for both types of airplanes are similar.

Outline of the Report

The remainder of this chapter gives information about the accident and the airplane involved. Chapter 2 is an overview of a Boeing 767-300ER, turbofan engines, and thrust concepts. The TRS involved in the accident is described in Chapter 3 and Appendix A, and analyses about the accident contained in the accident report are given in Chapter 4. The application of PSA methods to the TRS in the context of the accident is discussed in Chapter 5. Finally, Chapter 6 presents the conclusions obtained and proposes future work.

1.1 Information about the Accident

Lauda Air Flight 004 (NG004) was on a scheduled passenger flight from Hong Kong via Bangkok to Vienna, Austria. NG004 left Hong Kong Airport on May 26, 1991, and made the intermediate landing at Bangkok, Thailand, to unload and load passengers and cargo. The flight left Bangkok Airport at 1602 hours (local time) on May 26, 1991 for the final sector to Vienna, Austria.

All pre-flight, ground, and flight operations appear routine until five minutes and forty-five seconds after the cockpit voice recorder (CVR) recorded the sounds of engine power being advanced for takeoff. At this point, a discussion ensued between the crew members about the illumination of a REV ISLN indication. It is not known whether this indication consisted of either a REV ISLN amber-light illumination on the center pedestal, or a L REV ISLN VAL amber message of the Engine Indicating and Crew Alerting System (EICAS), or both. Here, we refer to this indication as the "REV ISLN indication." It indicates a disagreement between the respective hydraulic isolation valve (HIV) and the associated position of the thrust reverse lever, or an anomaly in the air/ground system. Figure 1 shows the position of the display of EICAS in the Flight Deck of a Boeing 767.

The crew's discussion of this indication was informative and lasted for some four and one half minutes. The co-pilot read information from the Airplane Quick Reference Handbook (QRH) as follows: "Additional systems failures may cause in-flight deployment" and "Expect normal reverser operation after landing." The pilot-in-command stated "...it's not just on, it's coming on and off.", and shortly thereafter stated "...it's just an advisory thing..." No actions were identified as being taken by the crew as a response to the REV ISLN indication.

Ten minutes and twenty seconds into the flight, the co-pilot advised the pilot-in-command of the need for rudder trim to the left. The pilot-in-command acknowledged the co-pilot's statement.

Figure 1 Position of EICAS display in the Flight Deck of a Boeing 767 (reproduced from Wild, 1990)

Fifteen minutes and one second into the flight (i.e., 4 minutes and 41 seconds later), the co-pilot's voice was heard to exclaim "ah reverser's deployed." Sounds similar to airframe shuddering and metallic snaps then were heard on the CVR. Twenty-nine seconds later, the CVR recording ended with multiple bangs, thought to be structural breakup of the airplane.

All persons aboard the airplane died; 213 passengers and ten crew. The airplane was destroyed by in-flight breakup, ground impact, and fire. Evidence indicates that the fire that developed after the breakup resulted from the liberation of the airplane's fuel tanks.

The Digital Flight Data Recorder (DFDR) was damaged by heat, and no useful information could be recovered. Flight conditions were recovered from the best available source, post-accident readout of the non-volatile computer memory within the left Electronic Engine Control (EEC).

The physical evidence at the crash site conclusively showed that the thrust reverser actuators of the left engine (left and right sleeves) were fully deployed. They were not restored to the forward thrust position before impact, and the evidence is inconclusive about whether the left engine thrust reverser could have been restored. The left EEC data indicates that the fuel cutoff switch was probably selected to cutoff within 10 seconds of deployment of the thrust reverser. Examination of the cutoff switch also indicates that it was in the cutoff position at impact.

The EEC data indicated that an anomaly occurred between channel A and B reverser-sleeve-position signals. The accident report concluded that this anomaly was associated with the thrust reverser deployment of one or both sleeves.

At the suspected point of deployment, the EEC readout indicated that the airplane was at a speed of Mach 0.78, and developing climb power.

1.2 Airplane Information

The airplane involved in the accident was a Boeing 767-3Z9ER, which is a Boeing 767-300ER manufactured to the specifications of Lauda Airlines. It was powered by two Pratt & Whitney 4060 engines.

Since August 14, 1990, 13 maintenance actions were logged on the left engine's thrust reverser system, almost always in response to recurring Propulsion Interface Monitor Unit (PIMU) messages of "EEC CH-B REVERSER RNG FAIL" and "EEC CH A/B REV CR-CHK FAIL." Ten of these actions occurred since January 28, 1991. Lauda continued to send the airplane on its regular schedule, troubleshooting after its return to the home station. Dispatch of the airplane with the particular PIMU messages was permitted under a time-limited dispatch condition, outlined in the airline's maintenance planning document. The Boeing Dispatch Deviation Guide cites the Pratt and Whitney Type Certificate Data Sheet E24NE, which permits dispatch for up to 500 operating hours with an EEC maintenance message annunciated.

2. Overview of the Boeing 767-300ER

This section presents an overview of the Boeing 767-300ER, the focus of this study.

Boeing designed the 767 to compete with the Airbus Industrie A-300B, also a twin-engine 230-passenger airplane, built as a combined effort of France, Germany, and Great Britain. The 767 is a twin-engine design sized between the Boeing's 737 and 757, and the 747 and 777 (Figure 2).

Figure 2 Boeing 767, 1982 (reproduced from Shevell, 1983)

The first flight of a 767 was on September, 1981; the 767-300 got under way in September 1983. The 767 was the first airplane to earn an extended-range twin-engine operations (ETOPS) rating, in May 1985, from the Federal Aviation Administration (FAA); it was approved for long-range flights of up to 120 minutes from a suitable airport. In March 1989, the FAA approved the 767 for 180-minute ETOPS. According to Boeing (Internet site, April 1997), the 767 now crosses the Atlantic more often than any other type of airplane; 32 carriers currently operate 767s across the north- and mid-Atlantic.

With a maximum range of 10,990 km (6,830 miles), the 767-300ER is an extended-range model of the 767-300; Table 1 lists some of their characteristics. These airplanes are powered by two high-bypass-ratio turbofan engines, selected by the airline customer: Pratt & Whitney PW4000, General Electric CF6-80C2, and Rolls-Royce RB211-524G/H. The 767 brought high-bypass-ratio engine technology to this size of airplane.

Table 1 Characteristics of the 767-300 and 767-300ER

Wing Span	47.6 m (156 feet 1 inches)
Overall Length	48.5 m (159 feet 2 inches)
Fuselage Length	47.2 m (155 feet)
Passengers	181 (three classes) 224 (two classes) Up to 285 (charter)
Cargo Volume	86.9 cubic meters (3,070 cubic feet)

2.1 Overview of Turbofan Engines

2.1.1 Propulsion and Thrust

All propulsion is based on Newton's third law: To every action there is an equal opposed reaction. If body A exerts a force on body B, body B exerts an equal but opposite force on body A. An airplane's engine (the propulsion unit) pushes on air, and air pushes back on the engine, creating thrust. Quantitatively, the thrust produced is equal to the time-rate of change of momentum of air.

A turbofan engine (Figure 3) uses an aircraft gas-turbine, a device in which freestream air is taken in through a carefully designed inlet, compressed in a rotating compressor, heated in a combustion chamber, and expanded through a turbine. The gas then leaves through a nozzle at a velocity greater than freestream. The turbine absorbs power in excess of that required to drive the compressor; a turbofan engine uses this excess power to drive a fan in an auxiliary duct, usually annular, around the primary duct. The flow through the outer part of the fan may be five or six times the flow through the engine's core. The engine produces

Figure 3 Diagram of a Turbofan Engine
(reproduced from Docherty, 1992)

part of the fan may be five or six times the flow through the engine's core. The engine produces

thrust both from the hot jet leaving the main nozzle (called here "hot flow"), and from acceleration of the cold bypass flow outside the engine's core (called here "cold flow").

The thrust equation for a turbofan engine can be derived from the general form of Newton's second law (i.e., force equals the time-rate of change of momentum), $\tau = d(mv)/dt$. Figure 3 illustrates the inlet and exhaust flows of the turbofan. The negative thrust due to bringing the freestream air almost to rest just ahead of the engine is called momentum drag or ram drag. The net thrust is given by equation 1:

$$\text{Net thrust } \tau = \text{gross thrust} - \text{momentum drag} \quad (1)$$

or,

$$\text{Net thrust } \tau = \text{momentum thrust} + \text{pressure thrust} - \text{momentum drag} \quad (2)$$

For subsonic engines, the pressure thrust is about 1 to 2%. If we neglect the pressure term, we get:

$$\text{Net thrust } \tau = \text{momentum thrust} - \text{momentum drag} \quad (3)$$

Since both the cold and hot flows contribute to the total thrust, equation (3) must be applied separately to each stream. For the cold flow, we have:

$$\tau = \frac{dm_{iC}}{dt} (v_{eC} - v) \quad (4)$$

where dm_{iC}/dt = cold airflow rate,
 v_{eC} = cold airflow exit velocity
 v = aircraft speed.

Taking into account the rate of fuel flow, application of (3) to the hot flow yields:

$$\tau = \left(\frac{dm_{iH}}{dt} + \frac{dm_f}{dt} \right) v_{eH} - \frac{dm_{iH}}{dt} v \quad (5)$$

where dm_{iH}/dt = hot airflow rate,
 dm_f/dt = fuel flow rate,
 v_{eH} = hot airflow exhaust velocity.

The total thrust from a turbofan is obtained by adding the thrust created by each of the airflows, i.e., by adding the right-hand terms of equations (4) and (5):

$$\tau = \left(\frac{dm_{iH}}{dt} + \frac{dm_f}{dt} \right) v_{eH} - \frac{dm_{iH}}{dt} v + \frac{dm_{iC}}{dt} (v_{eC} - v) \quad (6)$$

The ratio of the cold flow that bypasses the compressor and burners to the hot flow that passes through them is called the bypass ratio, β .

Since the fuel flow-rate is considerably smaller than the airflow rate (typically, it is about 2%), we can neglect its contribution and express (6) as:

$$\tau = \frac{dm_{iH}}{dt} (v_{eH} - v) + \frac{dm_{iC}}{dt} (v_{eC} - v) \quad (7)$$

The product of thrust and flight velocity, τv is sometimes called thrust power. One measure of the performance of a propulsion system is the ratio of this thrust power to the rate of production of propellant (air) kinetic energy. This ratio is commonly known as the propulsion efficiency:

$$\eta = \frac{\tau v}{dE/dt} \quad (8)$$

It is clear from this definition that the less the kinetic energy per unit time left in the exhaust gases, the greater will be the efficiency. From (7), this energy is given by:

$$\frac{dE}{dt} = \frac{dm_{iH}}{dt} \frac{v_{eH}^2 - v^2}{2} + \frac{dm_{iC}}{dt} \frac{v_{eC}^2 - v^2}{2} \quad (9)$$

Thus, from (7) and (9), for a specified momentum imparted to the air each second, the kinetic energy will be less for a higher air flow rate and a lower exhaust velocity. Turbofans do exactly that, adding a lower velocity increment to a larger flow rate of air, compared to a turbojet in which the available energy in the exhaust gases is converted to the kinetic energy of the jet.

Fan air is compressed to a much lower pressure than primary air and exits at a lower velocity. As bypass ratio is increased, i.e., as more energy is extracted by the turbine to drive the fan, the exit velocity of the primary gas is reduced. Higher bypass ratios lead to lower exit velocities and higher

efficiency, which, in turn, result in a lower fuel consumption than a turbojet. Another important gain from high-bypass-ratio turbofans is the reduction in noise from the exhaust jet which varies as the eighth power of the relative exhaust velocity, i.e., the velocity of the exhaust gases with respect to the freestream. Finally, another important feature of the turbofan engine is that its aerodynamics can be satisfactorily controlled, even with flight Mach numbers as high as 0.85, because the fan is enclosed in a duct. The turbofan has become the engine of choice for high-speed (subsonic) commercial aircraft.

The Lauda Air 767 used two Pratt & Whitney PW4000 series turbofan engines (Figure 4). The engine thrust is in the range of 222 to 289 kN (50,000 to 65,000 lb_f¹). It has a nominal (at cruise) bypass ratio of 5:1.

Figure 4 Pratt & Whitney PW4000 Turbofan Engine
(reproduced from Hill & Peterson, 1992)

¹kN means 10³ Newtons; lb_f means pound force.

3. Description of Thrust Reverser System

A Thrust Reverser System (TRS) in the engine of an aircraft achieves the following objectives:

- 1 It enables the aircraft to be brought quickly to a halt, even on wet or icy runways.
- 2 It can reduce the runway lengths required by the aircraft. It is increasingly difficult for conventional disk brakes to stop high-speed, high-gross-weight aircraft in short landing distances.
- 3 It greatly reduces wear on the tires and brakes, and so reduces costs when the aircraft is used regularly in short-haul service with frequent stops.

Two types of TRS are mechanical-blockage ones and aerodynamic-blockage ones (Lombardo, 1993). The thrust reversers installed on the PW4000 engines on the Boeing 767 are of the second type, and reverse only the (cold, bypass) fan airflow, while the (hot) primary flow remains in the normal (forward) direction. Thrust reversal is achieved by means of left- and right-hand translating fan sleeves containing blocker doors that block the fan flow, redirecting it through stationary cascade vanes (Figure 5). The translating sleeves are hydraulically actuated.

Figure 5 Thrust Reverser Operation (of a 737 engine)
(reproduced from reference 2)

The description of the TRS of the PW4000 engines on the Boeing 767 is based on Appendix C of the accident report, "Thrust Reverser System General Description", which was excerpted from Boeing document D926T302-2, Rev A, Thrust Reverser Description and Failure Mode and Effects Analysis-767/PW4000. That Appendix does not appear to contain the Failure Mode and Effects Analysis part of the Boeing document.

The use of reverse thrust is restricted to ground operation only, providing an additional retarding force on the airplane during landings and refused takeoffs.

3.1 Functional Description of the Thrust Reverser System

To (intentionally) command the TRS to deploy, a pilot must lift the reverse-thrust lever, located in the control stand inside the flight deck (Figure 6). When this lever is lifted more than 10 degrees, the

Figure 6 Control Stand (of a 737 airplane)
(reproduced from reference 2)

Hydraulic Isolation Valve (HIV) switch closes, which completes the circuit that opens the hydraulic isolation valve admitting hydraulic fluid to the thrust reverser system. The isolation valve ports hydraulic fluid to the directional control valve (DCV) and also through the retract restrictor tee to the rod end of the actuators. Further movement of the thrust lever (29 degrees of its travel) closes the DCV switch, thus allowing the DCV to port hydraulic fluid sequentially to the lock on the center actuator. Build-up of hydraulic pressure causes the lock piston to move and engage the lock-lever pivot arm. Further motion of the piston separates the locking discs, and fluid is ported directly to the head ends of the locking and non-locking actuators. Linear movement of the actuator piston rotates the high-lead acme screw that drives a gear train connected to the upper-

and lower-actuators via flex-drive shafts, thus translating the reverser halves to the deploy position. Upon leaving the stowed position, the reverser's in-transit indication REV (amber) is illuminated on the Engine Indicating and Crew Alerting System (EICAS).

Figure 7 is a diagram of the 767 PW4000 TRS showing both the design used by the airplane involved in the accident, and the "new" design incorporating Boeing's changes after that event. Our description applies to the former.

Figure 7 767 PW4000 Thrust Reverser (from the accident report, reference 1)

The thrust reverser is actuated by hydraulic power from three linear actuators attached to each translating sleeve; the actuators are synchronized by a flexible cable system contained within the hydraulic supply tubing. Supply and control of the hydraulic fluid to the actuators is achieved by means of a hydraulic isolation valve, a directional control valve, and two flow-restrictor orifice "T" connectors. These three components are installed in the engine's support strut. Hydraulic power is supplied to each reverser actuation system associated with the engine upon which the reverser is mounted.

Normal operation of the thrust reverser requires that the airplane must be on the ground to close the air/ground switch with both the main landing gear out of the tilt position, and the forward thrust lever in the idle stop position.

Stow and Auto Restow

To stow the reverser, the reverse thrust lever is returned to the fully down position, thus opening the DCV switch which ports the actuator head end fluid to the return system. Although the isolation-valve switch on the thrust lever is also returned to the off (stow) position, auto-restow switches (proximity sensors) operated by each reverser half of the reverser's translating sleeve remain closed and electrically hold the hydraulic isolation valve open until both halves are stowed. Since the reverser hydraulic power must remain available until the reverser is fully stowed during the stow cycle, a 5-second delay following the sensed reverser-stowed position is incorporated in the Proximity Switch Electronic Unit (PSEU) logic for the restow circuit. The auto-restow circuit is automatically de-energized after this delay.

The proximity sensors are adjusted to close when the reverser sleeve moves from the fully stowed position. The stow relay is energized to complete an electrical circuit to the isolation valve.

Indication of TRS position

Two reverser positions and one system condition are indicated by Engine Indicating and Crew Alerting System (EICAS). Reverser unlock is indicated by "REV" in amber. In full deploy, "REV" changes to green. An isolation valve condition is indicated by L(R) REV ISLN VAL in amber, and a repeater amber light (labeled REV ISLN) on the P10 panel.

The L(R) REV ISLN VAL light and EICAS caution indicate a disagreement exists between the air/ground relays, the reverser system is pressurized in flight, or the reverser system fails to pressurize on command on the ground. A disagreement between pressure and the voltage to the isolation valve or to the reverser control switch or to the air/ground switch will cause a detect relay to release and provide a ground to the REV ISLN light and EICAS after a 2-second delay to remove nuisance warnings.

Reverser Unlocked Indication

The reverser unlocked indication is activated by either of two proximity switches located one on each lock-housing of the center actuators. The "REV" amber indication occurs anytime either lock is unlocked.

The components of the TRS are described in detail in Appendix A of this document.

4. Analyses of the Accident Contained in the Accident Report

4.1 Engineering Simulation of the Accident

Airplanes with wing-mounted engines, such as the DC-8, DC-10, Boeing 707, and Boeing 747, have experienced in-flight reverse thrust, and according to Douglas Airplane Company, all models of the DC-8 (including those airplanes retrofitted with high-bypass fan engines) were certificated for using reverse thrust on the inboard engines in flight. However, differences in wing/engine geometry, reverser design, and the number of engines are all factors in the flight performance of an airplane experiencing reverse thrust.

By the time the accident happened, there had been several in-service, unwanted thrust-reverser deployments on Boeing 747s and other airplanes at moderate- and high-speeds with no reported controllability problems. The Boeing 747 has 4 engines.

Although the Boeing 747 has wing-mounted engines, it also has longer engine pylons which place the engines farther ahead and below the leading edge of the wing compared to the Boeing 767. In-service data suggests that the farther the engine is from the wing, the less likely it is that its reverse-thrust plume will significantly disrupt airflow around the wing.

The Boeing 707 has wing-mounted engines; however, its reverser system is located in the rear of the engine, below and behind the wing's leading edge, also making it less likely to affect wing lift. In the case of in-flight reverse thrust on large three- or four-engine airplanes, each engine produces a smaller percentage of the total thrust required for flight; this results in less thrust/drag asymmetry. Based on engineering judgement, the lower proportion of thrust and the resultant airflow affects a smaller percentage of the wing, and therefore, the effect of reverse thrust is less significant on a three- or four-engine airplane than on a two-engine one.

The mechanical design and type of engine is also important in the event of in-flight reverse thrust. The Boeing 767's engines are high-bypass ratio turbofans, with reverser systems which employ blocker doors and cascades to redirect airflow from the N1 compressor² fan blades. On large twin-engine transport airplanes, the thrust-reverser cascades are slightly below and in front of the wing. At high thrust levels, the plume of thrust from the reverser produces a yawing moment and significantly disrupts airflow over the wing, resulting in a loss of lift over the affected wing. This loss produces a rolling moment which must be promptly offset by coordinated flight-control inputs to maintain level flight. The yaw is corrected by the rudder. If corrective action is delayed, the roll rate and bank angle increase, making recovery more difficult.

² N1 compressor is the low-pressure compressor, consisting of several stages. It is driven by the turbine (Kroes et al., 1990).

For the conditions that existed when the thrust reverser deployed during the accident, wind-tunnel tests showed approximately a 25% loss in lift for an engine at maximum climb power, dropping to approximately 13% as the engine spooled down to idle thrust.

Assuming that the simulator tests with a 25% lift loss are a valid model of the accident conditions, simulated flights piloted by Boeing's Chief Boeing 767 Test Pilot indicated that recovery could not be accomplished unless the flight crew of the Lauda Boeing 767 took full corrective action within 4- to 6-seconds of the reverser's deployment. The use of full authority of the flight controls in this phase of flight is not part of a normal training programme. Further, correcting the bank attitude is not the only obstacle to recovery in this case, as the simulated flight shows that the airplane would rapidly accelerate in a steep dive. The event was uncontrollable for a flight crew that was not expecting it. The criticality of an in-flight thrust reverser deployment was not recognized and, therefore, the flight crew had no operational guidance.

4.2 Analysis of Failures of the Components of the TRS

The examinations and tests of components of the TRS are reported in the accident report. The insights gained are as follows:

1. The inspections and checks required by airworthiness directive (AD) 91-15-09, which might have included several types of airplanes, indicated that approximately 40 percent of airplane reversers checked had auto-restow position sensors out-of-adjustment. Such improper adjustment can result in an auto-restow signal.
2. Testing a DCV showed that contamination in its solenoid valve can produce internal blockage, which, in combination with hydraulic pressure available to the DCV (HIV open), can result in its uncommanded movement to the deploy position. Contamination of the DCV solenoid valve is a latent condition that may not be detected until it affects operation of the thrust reverser.
3. Tests disclosed that uncommanded deployment of the thrust reverser was possible with blockage of the solenoid valve's return passage internal to the DCV, or with total return blockage in the return line common to the reverser cowls.
4. The investigation of the accident disclosed that certain hot-short conditions involving the electrical system could potentially command the DCV to move to the deploy position. The electrical circuits involved are protected against short circuits to ground by installing current-limiting circuit breakers into the system. These circuit breakers should open if their rated capacity is exceeded for a given time. The DCV electrical circuit also has a grounding provision for hot-short protection.

Testing and analysis indicated that a minimum voltage of 8.2 V DC was required to actuate one of 599 DCV solenoids tested. The worst case hot-short threat identified within the thrust

reverser's wire bundle would provide 22.6 V DC to the DCV solenoid for 1.0 seconds. The extent of the thrust reverser's movement in response to a momentary hot-short with a voltage greater than 8.2 V DC could not be determined, nor the ability of the thrust reverser to return to the stowed position after tripping the circuit breaker associated with the source of the hot-short.

5. Tests showed uncommanded deployment of one thrust-reverser cowl when the HIV was energized porting fluid to the rod end of the actuator (stow commanded) with the piston's head seal missing and the bronze cap separated from the actuator piston head. These details may have been overlooked in the original failure mode and effects analysis.
6. Approximately 9 months after the accident, the DCV was returned to the Department of Aviation in exchange for a reward by persons not associated with the accident investigation. The condition of the valve indicated that they had partially disassembled and reassembled it. This DCV showed no anomalies, except that a metal plug, identified as a case-relief valve plug used elsewhere in the engine accessory section, was installed "finger tight" in the retract port of the DCV. Such a plug would have prevented retraction of the thrust reverser cowls on the left hand engine.
7. Lauda maintenance records indicate that the thrust-reverser actuators had been replaced and re-rigged.
8. There is no indication on the CVR that the crew initiated reverse thrust.

4.3 Changes in System Design as a Result of the Accident

After the accident, the following design changes were proposed by Boeing and mandated by FAA AD for all PW4000-series powered airplanes:

1. Replacing the solenoid-operated Hydraulic Isolation Valve (HIV) with a motor-operated Hydraulic Isolation Valve.
2. Adding a dedicated stow valve.
3. Adding new electric wiring from the electronics bay and flight deck to the engine strut. Isolation and protective shielding for critical wires is now required.
4. Adding a new reverser test/reverser system-maintenance-indication panel in the cockpit.
5. Replacing existing reverser-stow proximity targets with improved permeability material to reduce nuisance indications.
6. Adding a thrust-reverser deploy pressure switch.

With exception of the figure of the TRS, reproduced here as Figure 7, the accident report does not provide any information about how the system works with the changes implemented.

5. Application of Probabilistic Safety Assessment (PSA) Methods

This study applied Probabilistic Safety Assessment (PSA) methods to incorporate the non-linear behavior of a system (airplane) by modeling the dynamic processes during possible accidents as a function of time. The thrust reverser system (TRS) was analyzed in the context of the accident described in the accident report.

Probabilistic Safety Assessment (PSA), also known as Probabilistic Risk Assessment (PRA), has been applied to highly engineered systems, such as aircraft and nuclear power plants (Fullwood and Hall, 1988, and SAE, 1995: ARP 4761). PSA includes a wide variety of methods, such as event tree analysis (ETA), fault tree analysis (FTA), and common-cause analysis. PSA should not be confused with ARP (Aerospace Recommended Practice) 4761's proposed PSSA (Preliminary System Safety Assessment); as its name implies, PSSA is a preliminary assessment at the system level consisting of FTA and Failure Mode and Effects Analysis (FMEA).

A highly engineered machine, such as an aircraft, is designed with systems to prevent and mitigate undesired events. If an undesired triggering event occurs, an accident may progress in different ways depending on the effectiveness of such systems. In addition, the progression of some accidents requires that the operating crew take corrective action(s), which may modify the configuration of some systems. The automatic response(s) of mitigating systems and the corrective action(s) taken by the operating crew also may introduce non-linear feedback to the aircraft. FTA and FMEA typically are carried out for the *nominal* configuration of the mitigating systems and, therefore, they are *static* models of the systems. They do not fully incorporate the dynamic progression of an accident, the action(s) taken by the operating crew, and hence, the non-linear feedback.

A typical application of PSA methods to a nuclear power plant requires developing event trees and fault trees. The event trees model the dynamic behavior (in time) of the plant as it tries to cope with undesired events; corrective action(s) taken by the operating crew as the accident progresses are incorporated into it. Then, fault trees are developed to model the response of mitigating systems at each stage of the accident's progression depicted in a corresponding event tree. Event trees model the *dynamic* progression of accidents; fault trees are *static* models that model the response of a system *during a certain mission time*. When the configuration of a system changes as an accident progresses, a fault tree for a system has to be modified so that it adequately models the response of the system *during another mission time*. In this way, the non-linearities and complexities of the progression of an accident can be more accurately and realistically modeled.

5.1 PSA model

The event trees and fault trees for a nuclear power plant are developed *before* an accident has happened to assess the adequacy of the plant's response to postulated accidents, i.e., the integrated mitigating systems and corrective actions taken by the operating crew. Such development requires considerable resources. In this study, we applied these methods to an accident that had *already* happened.

Figure 8 shows an event tree for the triggering event "Proximity Sensors Out of Adjustment" (PROXSSENS). The accident is initiated by this event and progresses from left to right. For each heading in the tree, such as AUTOREST and CREWINDI, there is a branching point: up means success or the undesired event did not occur, and down represents failure or the undesired event.

The development of the event tree considered the following:

1. We assumed that the only way in which a non-intentional opening of the HIV would occur was due to an auto-restow operation. In reality, other failure modes may have led to opening.
2. We did not include so-called "errors of commission" which are human actions exacerbating the progression of the accident.

A sequence of events may lead loss of the aircraft or to a successful recovery. The outcome of each sequence is shown in Figure 8 under the heading OUTCOME; OK means that the crew prevented the loss of the aircraft.

The possibility that the auto-restow sensors were actually out-of-adjustment (PROXSSENS) is supported by the post-accident finding that the EEC data indicated that an anomaly occurred between channel A and B reverser-sleeve-position signals. In addition, the inspections and checks required by airworthiness directive (AD) 91-15-09 showed that approximately 40 percent of airplane reversers checked had auto-restow position sensors out-of-adjustment.

Since improper auto-restow sensor adjustment may cause an auto-restow signal, the second heading in the tree, AUTOREST, models such possibility. In the event tree, up means there is no signal to auto-restow, and down means there is such a signal, and, as a result, the HIV opens. The down path has two relevant characteristics:

1. The HIV *does not fail*; it performs its design function. However, by opening, the redundancy to prevent an uncommanded in-flight deployment of the TRS is reduced to only the DCV.
2. When the auto-restow function is required, system pressure to close the sleeves is applied during restow. The REV ISLN light illuminates for this period, except for the first 2 seconds. The associated EICAS message appears 2 seconds after the REV ISLN light illuminates.

Two observations suggest that an auto-restow operation (AUTOREST) actually took place:

1. Interpretation of the crew's comments about the REV ISLN indication, "coming on and off" suggests that they may have been observing cycling of the auto-restow system. This interpretation was proposed in the accident report.
2. EEC data indicated that an anomaly occurred between channel A and B reverser-sleeve-position signals.

If an anomaly or an auto-restow operation occurred, the crew would receive indication by either a REV ISLN amber light illumination on the center pedestal, or a L REV ISLN VAL amber message of the Engine Indicating and Crew Alerting System (EICAS), or both. The crew may then decide to take precautionary measures, such as reducing the power of the engines, or even landing in an airport to have the TRS checked. In a twin-engine airplane with high-bypass-ratio turbofan engines, a reduction in power might reduce the severity of the phenomena due to an in-flight deployment of the TRS. As shown in section 2.1.1, the thrust of a turbofan is approximately given by:

$$\tau = \frac{dm_{iH}}{dt} (v_{eH} - v) + \frac{dm_{iC}}{dt} (v_{eC} - v) \quad (10)$$

where the second term in the right-hand side is the thrust contribution from the (bypass) fan airflow. By design, engines with a high-bypass-ratio have a fan airflow that may be five or six times the flow through the engine core. Thus, a very substantial part of the total thrust of the engine is produced by the second term in the right-hand side of (10). As mentioned in section 2.1.1, the Pratt & Whitney PW4000 series turbofan engine has a nominal (at cruise) bypass ratio of 5:1.

By reducing the power of the engine, the fan airflow is reduced, and so could substantially reduce the thrust in the opposite direction that the aircraft would experience when the TRS deploys. This argument is based on theoretical principles, and a more detailed analysis is required to substantiate it; the point we are making is that the crew might be able to take mitigative actions, or even land the plane before a catastrophic event occurs.

There are two indications during the accident suggesting that appropriate importance was not given to an in-flight deployment of the TRS of one of the engines:

1. The Airplane Quick Reference Handbook (QRH) does not give mitigative actions, and
2. The pilot-in-command's comment about the REV ISLN indication, "...it's just an advisory thing..."

Seemingly, not enough importance was given to in-flight deployment of the TRS because there had been several in-service unwanted thrust-reverser deployments on Boeing 747 (4 engines) and other airplanes at moderate- and high-speeds with no reported problems with controllability. In the 767, the deployment of the TRS of *one* engine versus *two* engines is very critical because the engine in one wing will “push” while the engine in the other wing will “pull”, throwing the airplane into a spin (yawing and rolling). Such spin may have been the major contributor to the breakup of the airplane. This would be the case for any aircraft employing one engine in each wing, and it may also affect airplanes with other configurations of engines when forward thrust is applied in one wing and reverse thrust is applied in the other.

The conversation about the REV ISLN indication among the crew members was informative, and it appears that no mitigative action was taken. Therefore, the accident actually followed the down path in the event tree for the heading representing mitigative actions taken by the crew (CREWINDI).

For the TRS to deploy, both the HIV and the DCV have to be open to allow hydraulic pressure to

Figure 9 Top Level of Fault Tree

move the sleeves. A fault tree can be developed to model this condition. The top event of the fault tree (undesired event) can be defined as “uncommanded, in-flight deployment of the TRS of one engine (due to opening of these two valves)”. The top level of such fault tree is presented in Figure 9.

The logic in Figure 9 means that it is necessary to have both a failure leading to opening of the HIV and a failure leading to opening of the DCV for an uncommanded, in-flight deployment of the TRS of one engine.

Since the “Uncommanded HIV opening” was developed as part of the event tree, now it is only necessary to develop the other branch of the fault tree for the “Uncommanded DCV opening”. The accident report identified several failure mechanisms leading to an uncommanded (non-intentional) opening of the DCV; see section 4.2, “Analysis of Failures of the Components of the TRS”. We used these mechanisms to develop the branch “Uncommanded DCV opening” of the top level fault tree (Figure 9). Such development is shown in Figure 10. Some failure mechanisms require the HIV to be open, others do not. The uncommanded (non-intentional) opening of the DCV is a critical event in the progression of the accident, and it is included in the event tree with the heading DCVOPEN.

Figure 10 Fault Tree for Uncommanded DCV Opening

When the HIV has opened as a result of an auto-restow operation, and the DCV has also opened due to one of the mechanisms mentioned above, the TRS will deploy. Then, the crew will attempt to control the airplane, which is modeled by the heading CREWDEP in the event tree. The up path means that the crew can control the airplane after the uncommanded deployment, and the down path means they cannot. The possibility that the crew may be able to control the airplane after the uncommanded deployment depends on several factors, including whether they took corrective action when they saw the REV ISLN indication. Simulation of the accident (following the accident report) shows that there is only 4- to 6-seconds to apply full corrective actions after the TRS deploys. This period is so short that the event is uncontrollable. For this reason, the branching for the heading CREWDEP only occurs if the crew had successfully taken mitigative actions when they saw the REV ISLN indication.

In the accident, it appears that an emergency action taken by the operating crew to try to lessen the severity of the phenomena triggered by the deployment of the TRS of the left engine was to actuate the fuel cutoff switch to cutoff within 10 seconds of deployment. As mentioned in section 1.1, examination of the cutoff switch indicated that it was in the cutoff position at impact. Cutting fuel to the engine reduces the reverse thrust by cutting power to the engine's fan.

The evidence and findings support the possibility that the accident followed the sequence of events depicted in sequence 6 of the event tree (highlighted in Figure 8): Improper auto-restow sensor adjustment (PROXSSENS), resulting in auto-restow (AUTOREST) and the consequent opening of the HIV. The REV ISLN indication was observed by the crew but no mitigative actions (CREWINDI) were taken (the QRH did not provide them). The DCV opened (DCVOPEN) as a result of one of the failure mechanisms shown in the fault tree of Figure 10. Because of this sequence of events, there was an uncommanded, in-flight deployment of the left engine TRS, leading to loss of the aircraft. Since only 4- to 6-seconds were available to the crew to take full corrective actions, the crew could not reasonably recover from the phenomena that followed such deployment.

Sequences 1 to 5 in the event tree represent other possible ways in which events may happen; each of them is described next.

Sequence 1. Auto-restow sensors are improperly adjusted (PROXSSENS), but not sufficiently to generate a signal for auto-restow to take place. The outcome is OK.

Sequence 2. Auto-restow sensors are improperly adjusted (PROXSSENS), and as a result, auto-restow took place (AUTOREST). The REV ISLN indication was observed by the crew who took appropriate, mitigative actions (CREWINDI). The DCV does not open as a result of one of the failure mechanisms identified. The TRS is not deployed. The outcome is OK.

Sequence 3. Auto-restow sensors are improperly adjusted (PROXSSENS), and as a result, auto-restow took place (AUTOREST). The REV ISLN indication was observed by the crew who took appropriate, mitigative actions (CREWINDI). The DCV opened (DCVOPEN) due to one of the failure mechanisms shown in the fault tree of Figure 10. As a result, there was an uncommanded, in-flight deployment of the left engine TRS, but the crew managed to control the airplane. The outcome is OK.

Sequence 4. Auto-restow sensors are improperly adjusted (PROXSSENS), and auto-restow took place (AUTOREST). The REV ISLN indication was observed by the crew who took appropriate, mitigative actions (CREWINDI). The DCV opened (DCVOPEN) as a result of one of the failure mechanisms shown in the fault tree of Figure 10. This sequence of events caused an uncommanded, in-flight deployment of the left engine TRS, and the crew could not control the airplane. The outcome is loss of aircraft.

Sequence 5. Auto-restow sensors are improperly adjusted (PROXSSENS), and as a result, auto-restow took place (AUTOREST). The REV ISLN indication was observed by the crew, but no mitigative actions (CREWINDI) were taken. The DCV does not open as a result of one of the failure mechanisms identified. The TRS is not deployed. The outcome is OK.

The two sequences leading to loss of the aircraft can be more finely resolved in terms of the basic failure mechanisms leading to the failure of the headings of the event tree by integrating the event tree and the fault tree(s) into a single, unified safety-model. The solution of such model yields *minimal*

cut sets (MCSs), which are the unique ways in which an accident sequence may occur in terms of basic failures of equipment and human errors. This process was carried out for sequences 4 and 6, and the results are given in Table 2. An example is MCS 1 of sequence 6: auto-restow sensors are improperly adjusted (PROXSSENS), auto-restow because proximity sensors are out-of-adjustment causes the HIV to open (AUTOREST), crew does not take adequate action after REV ISLN indication (CREWINDI), and blockage in the return line common to the reverser cowl causes the DCV to open (BLKRETLINREVCOWL).

If a probability of occurrence is assigned to each of the components (basic failures) of a MCS, then a probability of occurrence of each MCS and of the loss of aircraft can be obtained. The MCS then can be sorted in descending order of probability. The MCSs in Table 2 are sorted by their size, i.e., the number of basic failures in each.

Insights about the criticality of each of the failures in the MCSs of sequences 4 and 6 to the occurrence of a loss of aircraft due to an uncommanded in-flight deployment of the TRS of one engine can be obtained from qualitative observations, even without a quantitative evaluation. Auto-restow sensors are improperly adjusted (PROXSSENS), the triggering event of the event tree, and consequently, of each sequence, appears in every MCS and therefore, it is very critical. A reduction (or elimination) in its frequency or probability of occurrence correspondingly reduces the frequency or probability of loss of aircraft. Similarly, auto-restow because proximity sensors are out-of-adjustment (AUTOREST) appears in every MCS and also is very critical. The same argument about a reduction (or elimination) in its frequency or probability applies. Failures may be critical for one particular sequence; crew fails to control the aircraft after TRS deployment (CREWDEP) appears in all MCSs of sequence 4, and crew does not take adequate action after REV ISLN indication (CREWINDI) appears in all MCSs of sequence 6. A reduction in the human error probability of either of these actions will reduce the frequency or probability of its corresponding sequence.

Finally, one of the methods proposed by ARP 4761, Markov Analysis, can, in principle, model the dynamic behavior of an accident, but its capability is not fully exploited. In addition, Markov Analysis does not yield directly the sequences and MCSs leading to failure of the system/occurrence of the accident. ARP 4761 does not address the treatment of human errors, and the interaction between them and the progression of an accident.

Table 2 Minimal Cut Sets for Sequences 4 and 6

Cut No.	Size	Sequence 4: Minimal Cut Sets
1	4	PROXSSENS, AUTOREST, BLKRET LINREV COWL, CREWDEP
2	4	PROXSSENS, AUTOREST, BLOCKRETPASDCV, CREWDEP
3	4	PROXSSENS, AUTOREST, CONTAMINATIONDCV, CREWDEP
4	5	PROXSSENS, AUTOREST, SHORTCIRCUIT, CIRCBREAKNOTOPEN, CREWDEP

Cut No.	Size	Sequence 6: Minimal Cut Sets
1	4	PROXSSENS, AUTOREST, CREWINDI, BLKRET LINREV COWL
2	4	PROXSSENS, AUTOREST, CREWINDI, BLOCKRETPASDCV
3	4	PROXSSENS, AUTOREST, CREWINDI, CONTAMINATIONDCV
4	5	PROXSSENS, AUTOREST, CREWINDI, SHORTCIRCUIT, CIRCBREAKNOTOPEN

Description of Events in Minimal Cut Sets

Event	Description
AUTOREST	Auto-Restow because proximity sensors out-of-adjustment causes HIV to open
BLKRET LINREV COWL	Blockage in the return line common to the reverser cowl causes DCV to open
BLOCKRETPASDCV	Blockage of the solenoid-valve return passage causes DCV to open
CIRCBREAKNOTOPEN	Circuit breaker protecting short circuits fails to open
CONTAMINATIONDCV	DCV opens due to contamination in its solenoid valve
CREWDEP	Crew fails to control the aircraft after TRS deployment
CREWINDI	Crew does not take adequate action after REV ISLN indication
PROXSSENS	Proximity (Auto-Restow) sensors are out-of-adjustment
SHORTCIRCUIT	Short circuit in the DC wiring of the DCV

5.2 Assessment of the Changes in TRS Design

The accident report does not describe in detail the changes proposed by Boeing after the accident, nor how the TRS would operate with the changes implemented. An assessment of the TRS design changes mentioned in section 4.3 using PSA techniques would require a detailed development of risk models (and more detailed information), which is beyond the scope of the grant. From the limited evaluation of the TRS in this chapter, the following insights are applicable:

1. By adding a dedicated stow valve (we assume it is the valve labeled ARV in Figure 7), an auto-restow signal would not result in a command to the HIV to open. In this case, the redundancy provided by the HIV and DCV to prevent uncommanded TRS deployments would be preserved. In terms of the PSA analysis, the criticality of two events identified above would be substantially reduced:
 - 1.1 Auto-restow sensors are improperly adjusted (PROXSSENS), the triggering event of the event tree, would still lead to an auto-restow signal, but the command is directed to the ARV, and the HIV would remain closed.
 - 1.2 Auto-restow operation because proximity sensors are out-of-adjustment (AUTOREST) would not cause the HIV to open.

Accordingly, this change is expected to reduce the likelihood of an uncommanded in-flight deployment of the TRS.

2. The DCV has some latent failures modes, identified by the accident report and depicted graphically in Figure 10, that future changes could take care of. An example is uncommanded deployment of the thrust reverser when the solenoid valve's return-passage internal to the DCV is blocked.
3. Further guidance could be given in the airplane's QRH about the criticality of an uncommanded in-flight deployment of the TRS of **one** engine.
4. It seems advisable to review the *support* activities related to the TRS, such as maintenance and troubleshooting. This is suggested by findings in the accident report, such as the inspections and checks required by airworthiness directive (AD) 91-15-09 indicating that approximately 40 percent of airplane reversers checked had auto-restow position sensors out-of-adjustment. It is advisable to enhance the training and awareness of crew members and support personnel on the potentially catastrophic effects of an uncommanded in-flight deployment of the TRS of **one** engine.
5. A mechanism that would **definitely** prevent an uncommanded deployment of the TRS of one engine could be implement . We suggest two possibilities:

- 5.1 A mechanism that does not allow the TRS to deploy unless it is commanded by the crew,
- 5.2 A mechanism that does not allow the TRS of one engine (two engines in an airplane with 4 engines, two in each wing) to deploy unless the TRS of the engine in the other wing (the two engines in the other wing) also deploys. This possibility would have to be substantiated by further, more detailed analyses and tests.

6. Conclusions and Future Work

6.1 Conclusions

This study applied Probabilistic Safety Assessment (PSA) methods to incorporate the non-linear behavior of a system (airplane) by modeling the dynamic processes during accidents as a function of time. The thrust reverser system (TRS) was analyzed in the context of the accident described in the accident report.

The safety assessment of an aircraft system typically is carried out using ARP 4761 methods such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA). Such methods may be called *static* because they model an aircraft system on its *nominal* configuration during a *mission time*, and they do not incorporate the dynamic behavior (non-linearities) of the systems (airplane) as a function of time, nor the interaction between the systems and corrective actions taken by the operating crew as the accident progresses. One of the methods proposed by ARP 4761, Markov Analysis, in principle, can model the dynamic behavior of an accident, but such capability is not fully exploited in ARP 4761. ARP 4761 does not address human errors, nor the interaction between such errors and the progression of an accident.

In contrast, by using a PSA method called event tree analysis, we modeled the dynamic behavior of an accident, the interaction between the mitigating systems and corrective actions taken by the operating crew as the accident progresses, and hence, treated the effect of non-linearities on the aircraft. Other safety analysis methods, such as FTA and FMEA, are linked with the event trees to obtain an integrated, dynamic model of the response of an aircraft to postulated accidents.

A risk model consisting of an event tree with supporting fault trees was developed to represent the progression of the accident. The interaction between the TRS and the operating crew during the accident is modeled, and findings of the accident investigation incorporated in the model. A feasible sequence of events leading to the fatal accident was identified.

The following major insights were gained during this study:

1. Insufficient importance was placed on the in-flight deployment of the TRS because there had been several in-service unwanted thrust-reverser deployments on other airplanes at moderate- and high-speeds with no reported problems with controllability. The deployment of the TRS of one engine in the Boeing 767 is very critical, and, as described in section 5.1, could throw the airplane into a spin, resulting in its breakup.
2. The interaction between the aircraft systems and the crew are very important; they can be modeled using the integrated approach of PSA methods.
3. The accident report does not describe in detail the changes proposed by Boeing after the accident, nor how the TRS would operate with the changes implemented. An assessment of

the TRS design changes using PSA techniques would require a detailed development of risk models, and more detailed information. Given our limited evaluation of the TRS, the following insights are applicable:

- 3.1 By adding a dedicated stow valve, the redundancy provided by two valves to prevent uncommanded TRS deployments would be preserved, and would reduce the likelihood of an uncommanded in-flight deployment of the TRS.
- 3.2 The accident report identified some latent failures modes of the Directional Control Valve (DCV) of the TRS. An example is uncommanded deployment of the thrust reverser when the return line common to the reverser cowls has total return blockage. It is advisable to review these failure modes.
- 3.3 Further guidance could be provided in the airplane's Quick Reference Handbook about the criticality of an uncommanded in-flight deployment of the TRS of **one** engine.
- 3.4 The *support* activities related to the TRS could be reviewed, such as maintenance and troubleshooting. Also, enhanced training and awareness of crew members and support personnel on the potentially catastrophic effects of an uncommanded in-flight deployment of the TRS of **one** engine is advisable.
- 3.5 A mechanism is suggested that would **definitely** prevent an uncommanded deployment of the TRS of one engine:
 - 3.5.1 It does not allow the TRS to deploy unless it is commanded by the crew, or
 - 3.5.2 It does not allow the TRS of one engine to deploy unless the TRS of the engine in the other wing also deploys.

6.2 Future Work

The insights gained from the limited application of PSA-based methods to an aircraft accident and specifically to a particular system, the Thrust Reverser System (TRS), can be used to conduct useful research that will address and can improve aircraft safety. There are several areas related to this particular study:

1. PSA-based methods to analyze aircraft accidents/incidents

The method used here can be broadened to analyze accidents and incidents that occur in the aviation industry. This will allow a better risk-perspective of different accidents, and also, the lessons learned can be used to improve safety of the industry. A database of PSA models of systems/accidents can be developed.

2. Design and procedural improvement of aircraft systems

The analysis presented of the TRS in this report provided important input based on probabilistic considerations. These inputs can be combined with those deemed desirable based on engineering/deterministic considerations. Such a process can make the changes needed cost-effective and, at the same time, will result in improvements in safety and performance. The approach used needs to be broadened, and applied to different aircraft systems. Specific design changes and procedure improvements can be defined to address significant failure causes and their effects, thereby preventing accidents.

3. Modeling interactions of aircraft systems (airplane) and the flight crew

As studied in this report, PSA-based tools, such as the integrated event and fault trees, are very powerful in modeling the interaction of the pilots and the complex systems they operate. Developing a safety model for an aircraft system will be very useful to analyze different actions taken by the crew and their implications. This can be used to enhance procedures and crew training, and can provide input for improvements in design. In general, PSA methods can be applied to prioritize resources and enhance aviation safety. For example, training, maintenance, and inspections can be ranked according to their impact on safety.

There are several other fields that can be further explored:

1. Comprehensive study of the TRS both before the accident and especially after the changes have been implemented. Detailed fault trees/event trees can be developed to more accurately and realistically model the system/accident.
2. Compilation of field failure-data to quantitatively evaluate the model.
3. Preparation of PSA methods, such as the ones used in this study, as a package of safety tools for the air transportation industry and FAA.

References

1. Aircraft Accident Investigation Committee, Ministry of Transport and Communications, Thailand, "Lauda Air Luftfahrt Aktiengesellschaft, Boeing 767-300ER, Registration OE-LAV, Ban Dan Chang District, Suphan Buri Province, 26 May B.E. 2534 (A.D. 1991)", July 21, 1993, NTSB File No. DCA 91 RA 037.
2. Boeing, "Boeing Commercial Airplanes - 737 Systems".
3. Boeing Internet site, www.boeing.com, April 1997.
4. Docherty, P., Project Editor, "The Visual Dictionary of Flight", Dorling Kindersley, New York, NY, 1st. Edition, 1992.
5. Fullwood, R. R., Hall, R. E., "Probabilistic Risk Assessment in the Nuclear Industry", Pergamon Press, New York, NY, 1988.
6. Grantham, W. J., Vincent, T. L., "Modern Control Systems Analysis and Design", John Wiley & Sons, Inc., New York, NY, 1993.
7. Hill, P., Peterson, C., "Mechanics and Thermodynamics of Propulsion", Addison-Wesley Publishing Company, Inc., Second Edition, New York, NY, 1992.
8. Kroes, M. J., Wild, T. W., Bent, R. D., McKinley, J. L., "Aircraft Powerplants", McGraw-Hill Publishing Company, Inc., Sixth Edition, New York, NY, 1990.
9. Lombardo, D., "Advanced Aircraft Systems", TAB Books, Blue Ridge Summit, PA, 1993.
10. Shevell, R. S., "Fundamentals of Flight", Prentice Hall, Englewood Cliffs, N. J., 1983.
11. Society of Automotive Engineers, Inc. (SAE), "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", ARP 4761, Draft # 14, October 12, 1995.
12. Wild, T. W., "Transport Category Aircraft Systems", Jeppesen Sanderson, Inc., New York, NY, 1990.

Appendix A Details of the Thrust Reverser System

This appendix describes in detail the most relevant components of the Thrust Reverser System of the PW4000 engines on the Boeing 767. This description is based on Appendix C, "Thrust Reverser System General Description", of the accident report, which was excerpted from Boeing's document D926T302-2, Rev A, Thrust Reverser Description and Failure Mode and Effects Analysis-767/PW4000.

Hydraulic Isolation Valve (HIV)

The Hydraulic Isolation Valve (HIV) is a hydraulic servo valve with an arming spool actuated by a solenoid-operated pilot valve. When the solenoid is energized, the pilot valve is opened and fluid is ported to one end of an arming valve spool. This spool is spring-biased to the closed position. A pressure buildup of 750 to 900 psid is required to produce flow through the valve. A check valve in the return port prevents pressure surges from propagating back into the reverser's return system.

Directional Control Valve (DCV)

The Directional Control Valve (DCV) is dual-staged, with a solenoid-operated pilot valve (first stage) and a hydraulic-operated main valve (second stage). The DCV solenoid is powered through the DCV deploy switch. With the DCV solenoid de-energized (stow mode) and the HIV solenoid de-energized, the DCV main spool is spring- and pressure-biased to the stow mode and hydraulic pressure is applied to the rod end of the actuators only; the head end of the actuators are vented to return. The actuators are maintained in the retracted (stowed) position.

At 29 degrees of travel of the reverse-thrust lever, the DCV switch is closed to deploy, thus energizing the DCV solenoid and allowing hydraulic fluid to pass through the first-stage pilot valve. Hydraulic pressure acting on a differential spool area then overcomes the spool's spring force and shuttles the main-valve spool to the deploy mode. In this valve position, hydraulic pressure is applied to the head and rod end of the actuators, unlocking the locks, and allowing the thrust-reverser actuators to be driven to the extended (deployed) position.

Flow Control System (Orifice Tees)

The flow control system divides the incoming flow from the DCV to operate the two reverser sleeves on each engine as separate mechanisms operating simultaneously. To accomplish this, the system incorporates flow-restrictor tees in the extend and retract passages. Incoming flow is ported from the DCV to the PRESS A port for extension. Incoming flow to the PRESS B port for retraction is controlled by the isolation valve.

When the reverser is extended, flow is routed through the extended restrictor tee to the actuator head ends. Equal pressure is developed in both head- and rod-end cavities of the actuators. The reverser

is extended by having a two-to-one actuator-piston area differential favoring extension. The returning flow from the actuator rod ends is routed through the retract restrictor tee and ports to the PRESS B port of the directional control valve.

Actuators

The six hydraulically-powered actuators operate each engine's thrust reverser sleeves. Their movement in the extend direction is produced by connecting both head- and rod-end cavities to the source of flow, thus providing an extension force equal to the supply pressure acting over the difference between head- and rod-end areas. Actuator movement in the retract direction is produced by connecting the rod-end cavity to supply, and the head-end cavity to return. The linear movement of the actuator piston rotates an acme screw installed concentrically within the piston rod. The piston rod is prevented from rotational motion relative to the actuator body by the gimbal mount of the actuator and pinned attachment of the rod end. Rotation of the acme screw drives the synchronization gear-train. The synchronization gear-trains of adjacent actuators are connected by flexible cables encased within the hydraulic tubing that connects the head-end cavities of these actuators. A square end-drive on each end of the flexible cables inserts into the worm gear of the synchronization gear-train to complete the mechanical connection.

As the actuators extend, fluid flow to the head ends is provided by one-half of the volume coming from the fluid source and the other half coming from the restrictor tee of the flow-control system and returning to port PRESS B of the DCV.

Locking Actuators

Each half-sleeve for each engine reverser is translated with three hydraulic linear actuators. The center actuator on each half-sleeve incorporates a locking mechanism that engages two serrated discs. This engagement directly prevents rotation of the synchronizing gear-train that mechanically interconnects the three actuators.

One disc is keyed to the acme screw in the actuator and rotates when the actuator is translating. The other disc is non-rotating, splined to the actuator barrel, and is actuated linearly along the spline by a helical spring to engage the two discs, and by the locking piston through the lock lever pivot arm to separate them.

As the center actuator nears the stowed position during retraction, the helical lock-spring becomes compressed forcing the splined, non-rotating disc against the rotating disc. This causes the two discs to ratchet until the actuator piston bottoms. The center actuator is locked against extension by serration engagement, which prevents the acme screw from rotating, and hence, the piston from moving.

During retraction, the return flow from the actuator's head-end bypasses the lock piston through a check valve and the preload spring holds the lock piston in the locked position. The spring bias of

the preload spring also prevents pressure surges from inadvertently unlocking the serrated disks while the reverser is stowed.

Thrust Reverser Position Feedback System

The thrust-reverser feedback system provides the EEC with an indication of the thrust-reverser's sleeve positions as measured at the center locking actuators. The EEC uses the thrust-reverser position for thrust-lever interlock command and to determine allowable engine power settings (forward and reverse).

The thrust-reverser-position feedback system consists of the two center-locking actuators and two dual-linear variable differential transformers (LVDTs), one mounted on each locking actuator. The dual LVDT is essentially two electronically independent LVDTs packaged within one unit. There are two separate electrical inputs, outputs, moveable armatures, and so on. The two movable armatures are joined together and driven by a single mechanical input.

Electrical Control System

The reverser's electrical control system consists of eight switches and two solenoids for each thrust reverser.

Six switches must all be closed to obtain hydraulic flow in the reverser system for normal operation. Three switches must be closed to complete the circuit to the isolation valve. They are (1) a fire switch in the normal position, (2) an air/ground switch that allows reverser operation (pressurization) only when the plane is on the ground, (3) an isolation-valve switch that allows flow to the isolation valve only when the reverse-thrust lever is lifted. Likewise, to complete the circuit to the directional control valve, a fire switch, an air/ground switch, and a directional-control valve switch must be closed. Either one of two auto-restow sensors, independent of the preceding six switches, initiate or maintain reverser operation any time either reverser half is not stowed. Reverser operation is initiated by energizing the solenoid that opens the isolation valve.

Fire Switches

Operating the fire switches removes electrical power from the isolation valve and the directional control valve solenoids.

Air/Ground Switches

The air/ground switches are relays that are activated by the proximity switch system. When both landing gears move out of the tilted position, the air/ground relays are energized to the ground mode.

Full Reverse Indication

The full reverse indication is controlled by two proximity switches which are connected so that the "REV" green indication occurs only when both reverser halves reach the fully deployed position. If amber and green are signaled simultaneously, the amber signal prevails.

Electronic Engine Control

The Electronic Engine Control (EEC) is a dual-channel micro-processor-based electronic unit and is the core of the engine control system on the PW4000 engine. The EEC has thrust-limiting logic which uses Throttle Resolver Angle (TRA) input via dual position resolvers along with reverser position input via Linear Variable Differential Transformers (LVDTs) to determine engine thrust as a function of reverser position. When the throttle position indicates that reverse thrust has been commanded, the control will limit thrust to idle if the reverser sleeves are less than 70% deployed.

When the throttle position indicates that forward thrust has been commanded, the EEC, via thrust-limiting logic, will assume that the reverser has been commanded stowed and will limit thrust to idle if the reverser is more than 15% deployed. When the reverser is 75% stowed, the thrust-limiting function changes to permit 90% of the maximum forward thrust.