

CONF-980910--

An Application of Probabilistic Safety Assessment Methods
To Model Aircraft Systems and Accidents¹

G. Martinez-Guridi, R.E. Hall, R. R. Fullwood;
Brookhaven National Laboratory,
Department of Advanced Technology;
Upton, New York 11973-5000

RECEIVED

AUG 17 1998

POST

Keywords: system safety, accident modeling, Probabilistic Safety Assessment

Abstract

A case study modeling the thrust reverser system (TRS) in the context of the fatal accident of a Boeing 767 is presented to illustrate the application of Probabilistic Safety Assessment methods. A simplified risk model consisting of an event tree with supporting fault trees was developed to represent the progression of the accident, taking into account the interaction between the TRS and the operating crew during the accident, and the findings of the accident investigation. A feasible sequence of events leading to the fatal accident was identified. Several insights about the TRS and the accident were obtained by applying PSA methods. Changes proposed for the TRS also are discussed.

Introduction

The safety assessment of an aircraft system typically is carried out using ARP (Aerospace Recommended Practice) 4761 (ref. 1) 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 rarely incorporate the action(s) taken by the operating crew, nor the progression of events during an accident.

Very useful insights can be obtained by modeling aircraft systems in the context of the progression of accidents during which important interactions between the operating crew and the aircraft systems may occur, and the configuration of the aircraft systems may change.

This paper proposes using Probabilistic Safety Assessment (PSA) methods to model aircraft systems by incorporating the progression of events during an accident, including the action(s) taken by the operating crew. PSA, also known as Probabilistic Risk Assessment (PRA), encompasses event-tree analysis (ETA), FTA, and common-cause analysis, among others. PSA is broader than 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 take into account the dynamic behavior (in time) of the airplane as it responds to 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 the 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, the fault tree for a system must be modified so that it adequately models the response of the system during another mission time. In this way, a system can be more accurately and realistically modeled during an accident than by using static methods such as FTA and FMEA.

To illustrate the application of PSA methods, we analyze the thrust reverser system (TRS) in the context of a fatal accident in Thailand on May 26, 1991, involving a Lauda Air Boeing 767-300ER airplane. We also exemplify modeling of accidents by using such methods. This paper summarizes the analyses; a complete explanation

¹ This work was carried out as part of the Federal Aviation Administration (FAA) Research Grant number 95-G-039 and under the auspices of the U.S. Department of Energy.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

is given by Martinez-Guridi et al. (ref. 2). The study is meant to be illustrative of the application of PSA methods, and is not an exhaustive PSA of the TRS nor of the accident.

The paper is divided into four main sections: in the first, we briefly describe the accident; in the second we briefly describe the TRS; in the third section we discuss our application of PSA methods; and, finally, the fourth presents our conclusions.

Description of the Accident

The accident is documented in a report by the Aircraft Accident Investigation Committee, Ministry of Transport and Communications, Thailand (ref. 3), that determined the probable cause of the accident to be uncommanded in-flight deployment of the left engine's thrust reverser, resulting in loss of flight-path control. The specific cause of such deployment was not positively identified. For brevity, we refer to this report as the accident report, and the following description follows the information in it.

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) had 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 was a REV ISLN amber-light on the center pedestal, or an 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 an anomaly between the respective hydraulic isolation valve (HIV) and the associated position of the thrust reverse lever, or an anomaly in the air/ground system.

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 in response to the REV ISLN indication.

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

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 the structural breakup of the airplane.

All 213 passengers and ten crew aboard the airplane died. 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 break away 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; the evidence is inconclusive about whether the left engine thrust reverser could have been restowed. 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

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, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any 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 thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

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

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.

The airplane involved in the accident was a Boeing 767-300ER which is an extended-range model of the 767-300; it was powered by two Pratt & Whitney 4060 high-bypass-ratio turbofan engines which have a nominal (at cruise) bypass ratio of 5:1.

Overview of TRS

The Thrust Reverser System(s) in the engine(s) of an aircraft enables the aircraft to be brought quickly to a halt, even on wet or icy runways. The use of reverse thrust is restricted to ground operation only, providing an additional retarding force on the airplane during landings and refused takeoffs.

Thrust reversal on the PW4000 engines on the Boeing 767 is achieved by means of left- and right-hand translating fan sleeves containing blocker doors that block the fan's flow, redirecting it through stationary cascade vanes. The translating sleeves are hydraulically actuated.

To (intentionally) command the TRS to deploy, a pilot must lift the reverse-thrust lever, located in the control stand inside the flight deck, by more than 10 degrees. Then, the 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); further movement of the thrust lever (29 degrees of its travel) closes the DCV switch, thus opening the DCV. When both valves have opened, the hydraulic fluid will translate 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 1 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.

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. Auto-restow switches (proximity sensors) are adjusted to close when the reverser sleeve moves from the fully stowed position. When they close, they open the hydraulic isolation valve until both halves of the TRS are stowed.

Probabilistic Safety Assessment Model

Typically, event trees and fault trees for a highly engineered device, such as an aircraft, are developed before an accident has happened to assess the adequacy of the device's response to postulated accidents, i.e., the integrated mitigating systems and corrective actions taken by the operating crew. In this study, we applied these methods to an accident that had already happened. Modeling the TRS during the progression of this accident illustrates the importance of analyzing the interactions between the operation of systems, the response of the aircraft, and the actions taken by the operating crew.

Figure 2 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: down represents failure or the onset of an undesired event, and up means success or the undesired event did not occur.

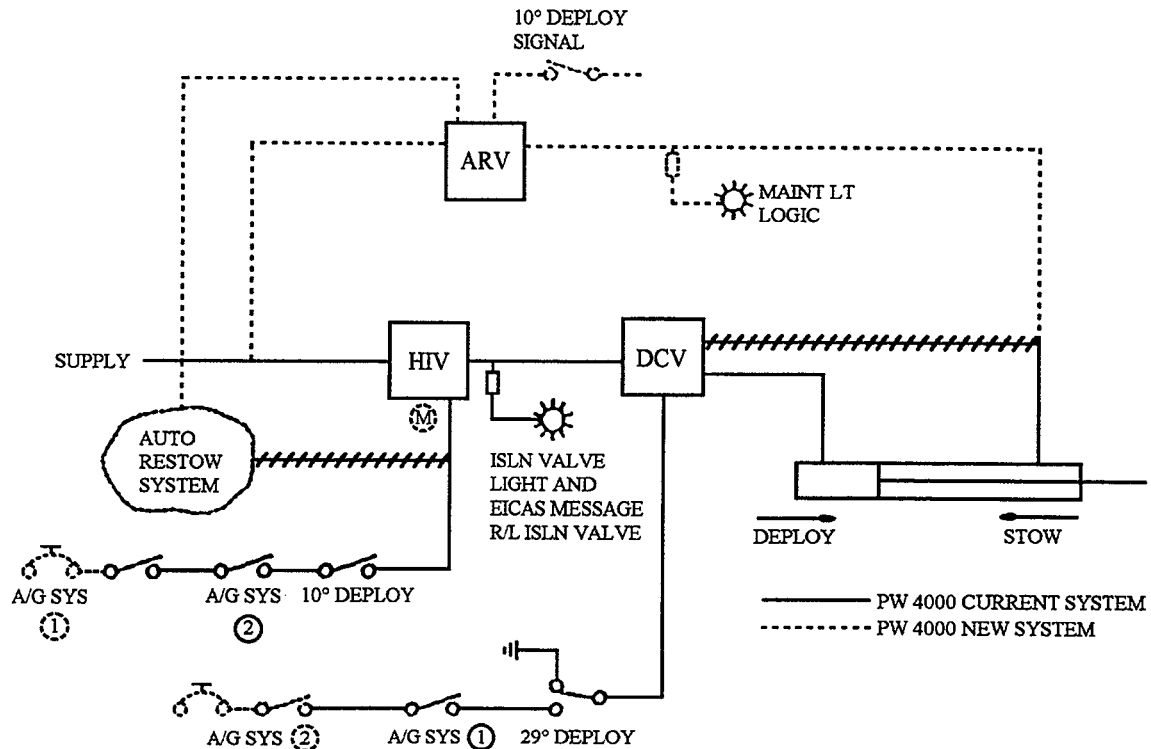


Figure 1 - 767 PW 4000 Thrust Reverser (from the accident report)

A sequence of events may lead to loss of the aircraft or to a successful recovery. The outcome of each sequence is shown in figure 2 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 from the EEC data that indicated 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 had auto-restow position sensors out-of-adjustment.

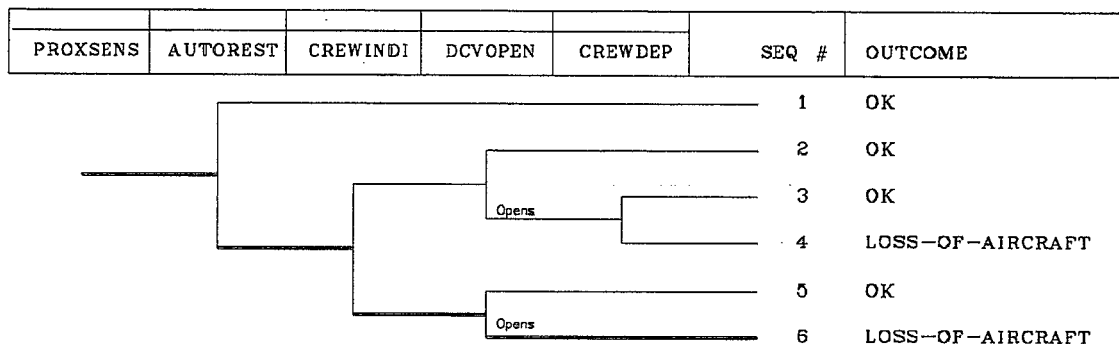


Figure 2 - Event Tree for the Triggering Event "Proximity Sensors Out of Adjustment"

Since improper adjustment of the auto-restow sensor 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 the restow. The REV ISLN light illuminates for this period, after the first 2 seconds. The associated EICAS message appears 2 seconds later.

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, as 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 occurs, 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. By design, the main thrust of an engine with a high-bypass-ratio is due to the fan's airflow that may be five or six times more than the flow through the engine core. By reducing

the power of the engine, the fan's airflow is reduced, and so could substantially reduce the thrust in the opposite direction that the aircraft experiences 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 747s (4 engines) and other airplanes at moderate- and high-speeds with no reported problems with controllability. In the 767, the in-flight deployment of the TRS of *one* of the *two* engines is very critical because the engine in one wing will "push" while the engine in the other wing will "pull", causing asymmetric thrust. If the operating crew does not implement recovery actions promptly after this condition is reached, the airplane will experience yawing and rolling, which may have been the major contributor to the breakup of the airplane of the fatal accident. 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 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).

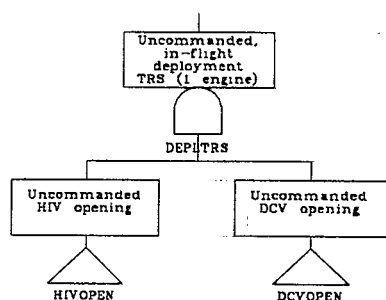


Figure 3 - Top Level of Fault Tree

For the TRS to deploy, both, HIV and DCV, have to be open to allow hydraulic pressure to 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)." Figure 3 shows the top level of such a fault tree.

The logic in figure 3 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. We used these mechanisms to develop the branch "uncommanded DCV opening" of the top level fault tree (figure 3). Such development is shown in figure 4. 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.

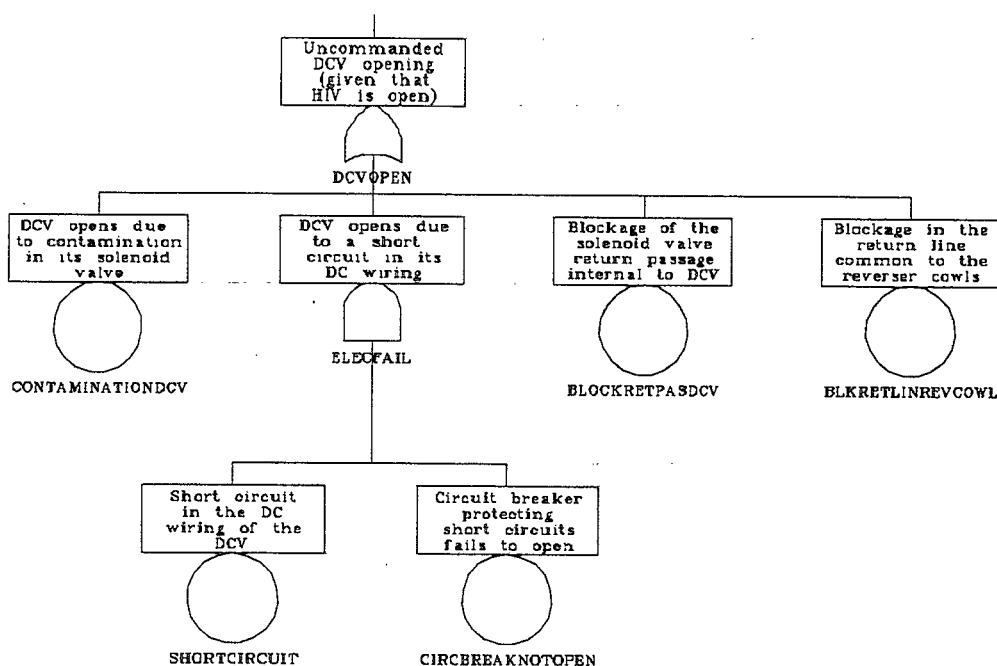


Figure 4 - Fault Tree for Uncommanded DCV Opening

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 of the crew controlling 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 are only 4- to 6-seconds to apply full corrective actions. Time 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.

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. The cutoff switch 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 2): Improper auto-restow sensor adjustment (PROXSSENS), resulting in auto-restow (AUOREST) 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 4. 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, they could not reasonably recover from the phenomena that followed deployment.

As shown in figure 2, sequences of events numbered 1, 2, 3, and 5 result in an adequate

control of the aircraft. For example, sequence 2 consists of the following events: Auto-restow sensors are improperly adjusted (PROXSSENS), and as a result, auto-restow takes place (AUOREST). The REV ISLN indication is observed by the crew who take appropriate, mitigative actions (CREWINDI). The DCV does not open as a result of one of the failure mechanisms identified (DCVOPEN), and the TRS is not deployed.

Insights from the PSA Modeling and Analyses:

As discussed above as part of the PSA, in airplanes with two engines mounted on the wings, like the Boeing 767, the in-flight deployment of the TRS of one of the two engines is very critical because the resulting asymmetric thrust causes the airplane to yaw and roll if no prompt recovery actions are implemented by the operating crew. Loss of an aircraft due to forward thrust applied in one wing and reverse thrust applied in the other may also occur in other airplanes with different configurations of engines mounted on the wings, for example, one with two engines on each wing. Therefore, independently of the design of the TRS, the basic event to be avoided is reverse thrust in one wing while forward thrust is applied in the other. Accordingly, a mechanism preventing an uncommanded in-flight deployment of the TRS of the engine(s) can be considered a desirable enhancement. A more detailed analysis would be required to study the feasibility of such mechanism.

For the particular design of the TRS involved in the accident in Thailand, we can use the risk model developed in this study, consisting of an event tree with supporting fault trees, to suggest improvements to the design and operations of the TRS to reduce the likelihood of such accidents. The event tree (Figure 2) has two accident sequences, 4 and 6, whose outcome is loss of the aircraft. Each of the five headings of this tree, such as PROXSSENS and CREWDEP, are failures comprising at least one of these two accident sequences; see, for example, the description of sequence 6, above. Therefore, a reduction in the likelihood of occurrence of these headings should reduce the frequency of loss of aircraft due to an uncommanded in-flight deployment of the TRS. The headings are discussed in rough order from left to right in the event tree:

1. 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 had auto-restow position sensors out-of-adjustment. Improving maintenance and troubleshooting of the auto-restow position sensors would decrease the frequency of the postulated initiating event of the event tree, PROXSSENS, so directly lowering the frequency of all accident sequences.

2. After the accident, several design changes were proposed by Boeing and mandated by the FAA AD for all PW4000-series powered airplanes. One change suggested by Boeing is to add a dedicated stow valve (we assume it is the valve labeled ARV in Figure 1); then, 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. The PSA analysis presented here supports this modification since the criticality of two events identified in the event tree would be substantially reduced:

A) 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.

B) Auto-restow operation because proximity sensors are out-of-adjustment (AUTOREST) would not cause the HIV to open.

3. In this analysis (see event tree), two actions by the operating crew are considered relevant: CREWINDI (response of the crew to the REV ISLN indication) and CREWDEP (response of the crew to the uncommanded deployment of the TRS of one engine). There are two potential ways to decrease the probability of occurrence of these failures:

A) 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.

B) Give further guidance in the airplane's QRH about the criticality of an uncommanded in-flight deployment of the TRS of one engine.

4. Efforts to reduce the probability of the DCV failures modes, as identified by the accident report and depicted logically in Figure 4, can be useful since such modes impact the heading DCVOPEN of the event tree. An example of these modes is opening of DCV when the solenoid valve's return-passagage internal to the DCV is blocked.

These insights are directed toward decreasing the likelihood of an uncommanded deployment of the TRS. These improvements are not expected to affect the intended function of this system, for example, deploying when commanded during landing. However, we recommend a comprehensive study to assure that the proposed improvements do not impair its intended function.

Conclusions

By using a PSA method called event tree analysis, the dependencies and interactions during an accident are modeled, including the interaction between systems and corrective actions taken by the operating crew. To illustrate the usefulness of PSA methods, we presented a case study modeling the thrust reverser system (TRS) in the context of a fatal accident of a 767-300ER. The risk model consists of an event tree with supporting fault trees. The interaction between the TRS and the operating crew during the accident is modeled, incorporating the findings of the accident investigation.

By using the PSA model developed in this study, we obtained the following insights:

1. A feasible sequence of events leading to the fatal accident was identified: Improper auto-restow sensor adjustment, resulting in auto-restow and the consequent opening of the hydraulic isolation valve (HIV). The REV ISLN indication was observed by the

crew (indicating a disagreement between the respective HIV and the associated position of the thrust reverse lever, or an anomaly in the air/ground system), but no mitigative actions were taken. The directional control valve (DCV) opened due to one of its failure mechanisms, resulting in an uncommanded, in-flight deployment of the left engine TRS, leading to loss of the aircraft.

2. Improvements to the design and activities related to the TRS are examined. A reduction in the probability of occurrence of the events involved in accident sequences, having as outcome the loss of aircraft due to in-flight uncommanded deployment of the TRS of one engine, should decrease the overall frequency of this accident. These changes include

- A) reviewing the support activities related to the TRS, such as maintenance and troubleshooting, to decrease the frequency of auto-restow position sensors out-of-adjustment,
- B) adding a dedicated stow valve (suggested by Boeing) to prevent the HIV from opening as a result of an auto-restow signal,
- C) enhancing 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, and providing further guidance in the airplane's QRH about the criticality of such deployment,
- D) reducing the probability of some failures modes of the DCV, one of the valves in the TRS.

In addition, a mechanism to prevent an in-flight uncommanded deployment of the TRS of the engine(s) could be considered. These suggested changes are based on the limited PSA of the TRS and the accident; we did not analyze their impact on the intended functions of the TRS, such as commanded deployment during landing. Finally, a simplified analysis of the thrust of a turbofan engine, such as those engines used by the Boeing 767, shows that for this type of

aircraft in-flight deployment of the TRS of one of the two engines is very critical when no prompt recovery actions are implemented by the operating crew because the consequent asymmetric thrust causes the airplane to yaw and roll, and may result in loss of control and breakup of the airplane. This would be the case for any aircraft employing one engine in each wing, and might 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.

Acknowledgments

We acknowledge the support and guidance of Dr. S. Sampath from the FAA. We also are grateful to Dr. G. Lyddane, FAA's National Resource Specialist for Flight Management, and to our colleague, Dr. P. Samanta, at Brookhaven National Laboratory, for their insightful reviews of this study. We are indebted to Mr. R. Baitoo, FAA, Long Beach, California, who suggested the study of the thrust reverser system.

References

1. 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.
2. G. Martinez-Guridi, R.E. Hall, R.R. Fullwood, "On the Safety of Aircraft Systems: A Case Study", report BNL-64946, May 1997.
3. 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.

Biography

Gerardo Martinez-Guridi, M.Sc., Brookhaven National Laboratory, Building 130, Upton, New York 11973-5000, telephone - 516 344-7907, facsimile - 516-344-4512, e-mail - martinez@bnl.com.

Mr. Martinez-Guridi is currently a Research Engineer I, and a member of the Risk and Reliability Group at BNL. He has been a Principal Investigator for projects for the U.S. Nuclear Regulatory Commission, the Federal Aviation Administration, and the New York State Department of Transportation. He has more than 15 years of experience on the application and development of safety methods for nuclear, chemical, and aviation systems. He has more than 50 technical publications on Probabilistic Safety Assessment (PSA) and related topics. He has developed computer codes for PSA, and was a consultant to the International Atomic Energy Agency on software development for PSA. Also, he was a visiting scientist in Riso National Laboratory, Denmark.

Robert E. Hall, Brookhaven National Laboratory, Building 130, Upton, New York, 11973-5000, telephone - 516-344-2144, facsimile - 516-344-3957, e-mail: rehall@bnl.gov.

Mr. Hall heads the Engineering Technology Division at Brookhaven National Laboratory and as a researcher support in the development and application of new techniques in quantitative risk and safety assessment. He has over 100 publications in this and related fields of

engineering and is co-author of the college text: Probabilistic Risk Assessment in the Nuclear Power Industry - Fundamentals and Applications, Pergamon Press, 1988. Mr. Hall is Vice-Chair of IEEE's Nuclear Power Engineering committee, has served on the IEC TC45, and has been active in international standards development for risk, reliability, and human performance.

Dr. Ralph R. Fullwood, Brookhaven National Laboratory, Building 130, Upton, New York 11973-5000, telephone - 516-344-2180, facsimile - 516-344-4512, e-mail - fullwood@bnl.com.

An original participant in the Rasmussen Study, Dr. Fullwood has performed PRA for light water, heavy water, liquid metal, and gas cooled reactors, fuel cycle facilities, waste disposal, process chemistry, and aviation. He was author with R.E. Hall of Probabilistic Risk Assessment in the Nuclear Power Industry, Pergamon, 1988. Presently, he is completing Probabilistic Safety Assessment by Government and Industry, which is both an up-date of the previous book and extension to process chemistry. Previously, Fullwood was an Associate Professor at RPI, an experimental physicist at LANL, and Assistant Vice-President at SAIC; he has over 200 publications.