# Why System Safety Professionals Should Read Accident Reports

**C. M. Holloway*, C. W. Johnson†**

*NASA Langley Research Center, 100 NASA Road, Hampton VA 23681-2199, U.S.A., c.m.holloway@nasa.gov
† Dept. of Computing Science, University of Glasgow, Glasgow, G12 9QQ, johnson@dcs.gla.ac.uk

**Keywords:** accidents, accident prevention, system safety

## Abstract

System safety professionals, both researchers and practitioners, who regularly read accident reports reap important benefits. These benefits include an improved ability to separate myths from reality, including both myths about specific accidents and ones concerning accidents in general; an increased understanding of the consequences of unlikely events, which can help inform future designs; a greater recognition of the limits of mathematical models; and guidance on potentially relevant research directions that may contribute to safety improvements in future systems.

## 1 Introduction

Our experience suggests that few people except accident investigators and lawyers read complete accident reports regularly. This is a shame. People from many different disciplines have much to gain by regularly reading accident reports, particularly reports produced by professional investigatory organizations. This is especially true of system safety professionals, whether they are practitioners or researchers.

Professional investigatory organizations, such as the National Transportation Safety Board in the United States and the Air Accidents and Marine Accident Investigation Branches of the Department for Transport in the United Kingdom, investigate and report on accidents for one primary purpose: to improve safety. System safety professionals share this purpose, and thus it seems appropriate that they should seek to learn from the results of accident investigations. We believe that regularly reading accident reports is an excellent way to do this.

In the remainder of this paper, we discuss four benefits that our experience suggests system safety professionals are likely to obtain from reading accident reports. We have conducted some initial empirical studies into the benefits of reading accident and incident reports. For example, a questionnaire was issued to safety professionals in the United Kingdom and the United States in 1999. The results confirmed that remarkably few engineers ever read complete accident and incident reports [1].

We believe that we have identified some key benefits that might be obtained if more engineers, particularly system safety engineers, read accident reports. We have not yet conducted any experiments or case studies to confirm or deny whether these benefits are real, so this paper should be considered to be simply setting forth hypotheses for the reader's consideration. Also, further work is required to determine why more people do not read accident reports regularly. Our hypothesis is that people do not often read complete accident reports because they do not believe the reports contain information that will be helpful to them, but additional studies are needed to determine the accuracy of this hypothesis.

The paper is organized as follows. Section two explains how reading reports may improve one's ability to separate truth from fiction, reality from myth, regarding accidents. Section three explains the positive effect that regular reading may have on one's understanding of the possible consequences of unlikely events. Section four describes how reading accident reports may improve one's understanding of the limits of mathematical models. Section five suggests ways in which studying accident reports may positively influence research directions. The paper concludes with section six, in which we draw on the previous sections to encourage the reader to cultivate the habit of regularly reading accident reports.

## 2 Dispelling Myths

Perhaps the most obvious benefit that should accrue to those who regularly read accident reports is an improved ability to separate myths from reality in regard to accidents. This ability allows one to learn the lessons that are *really taught* by an accident or group of accidents.

Myths and misunderstandings may be divided into two main categories: those about specific accidents, and those about accidents in general. Examples from both of these categories are discussed below.

### 2.1 Myths about Specific Accidents

Several years of observing presentations given at various conferences and of reading summaries of accidents written in technical papers and popular articles have shown that people's understanding of specific accidents is often incomplete or inaccurate. One symptom of this general problem is the way that electronic mailing lists, such as safety-critical@cs.york.ac.uk, are filled with threads in which respondents trade partial and incomplete accounts of previous failures in order to support points that are only made in

passing within an official report or are not mentioned at all [2].

To illustrate some of the sorts of misunderstandings that exist, we briefly discuss three specific accidents below.

**Cali, Colombia, 1995**

On December 20, 1995, American Airlines flight 965 crashed into mountainous terrain while attempting to land at Cali, Colombia. Of the 155 passengers and 8 crew members aboard the Boeing 757 aircraft, only 4 survived the accident. The complex causal factors leading to this accident [3] have been oversimplified in several different ways, ranging from claiming it as an example of a software error to asserting that the accident report exemplifies the tendency of investigatory agencies to blame the pilot. Only someone who has read the complete accident report is likely to avoid being misled by these oversimplifications.

**Mars Climate Orbiter, 1999**

Mars Climate Orbiter (MCO) was launched by NASA on December 11, 1998. The last signal was received from it on September 23, 1999 following Mars orbit insertion. The spacecraft was presumed lost. The cause of the loss of this spacecraft is usually attributed simply to a "units problem" in the software. While such an attribution is consistent with the root cause determination of the investigation, it ignores crucial factors that led to the units problem occurring, factors that are perhaps more important for system safety engineers to understand than the so-called root cause [4,5]. Someone who has not read the mishap report, and hears only about the use of incorrect units, is likely to dismiss this mishap as the result of simple incompetence.

**Sioux City, Iowa, 1989**

On July 19, 1989, United Airlines flight 232 crashed while trying to make an emergency landing at the Sioux Gateway Airport in Sioux City Iowa. The emergency landing was necessary because of an in-flight engine failure, which so severely damaged the aircraft's hydraulic systems that the control surfaces were unusable. Of the 296 (285 passengers and 11 crew) persons aboard the aircraft, 185 survived the crash, although one of the survivors died 31 days after the accident as a result of his injuries.

A common misunderstanding about this accident does not involve its causes, but rather the details about the survivors. Because this accident has frequently been used to justify the need to change the rules concerning restraining of infants and small children in aircraft, many people think that the survival rate for unrestrained children was lower than that for other passengers. Reading the accident report [6] reveals that this was not the case. Of the four unrestrained children aboard the plane, three survived, yielding a survival rate of 75%. For the remaining 284 people, the survival rate was only 62%. (We are not suggesting that this difference in survival rate means that changing the restraint rules for small children is unnecessary. The NTSB called for such a change in its recommendations stemming from the accident. We use this example simply to illustrate the ease with which one can draw incorrect conclusions unless one reads the full accident reports.)

For each of these examples, and for the many more examples that could be cited, reading the entire official report provides a much more complete picture of what took place than does simply reading or listening to what others say about the accident. Without such a complete picture, it can be easy to draw the wrong lessons from a specific accident. System safety engineers who want to draw the right lessons need to read the full reports.

### 2.2 Myths about Accidents in General

Just as reading the full report about a particular accident should keep one from believing falsehoods about, or having an incomplete understanding of, that accident, so too should regularly reading many accident reports keep one from believing myths about accidents and accident investigations in general. Three such myths are discussed in this section: simplicity of causal determinations, personal invulnerability, and a bias towards blaming individuals.

**Causal Simplicity**

One myth about accident investigations that appears to be believed by some people is that making causal determinations for most accidents is a fairly simple thing to do. Anyone who reads even a few major accident reports should quickly see that this is false. Even relatively simple accidents often involve complex events and interactions, which makes determining why the accidents happened anything but simple.

As an example, consider a school bus accident that took place in Omaha, Nebraska, on October 13, 2001. A 78-passenger bus carrying 31 people ran off the side of the road, flipped over a bridge, and fell 49 feet to land in a shallow creek. Four people were killed as a result.

On the surface, this may appear to be a simple accident, one in which determining the causes would be equally simple. However, the NTSB's report [7] on the accident reveals that it occurred as a result of complex interactions involving a work zone lane shift, narrow lanes, the speed limit, another bus travelling in the opposite direction, lack of median separation, and un-repaired damage to the bridge railing. These interactions were so complex that the Board was unable to reach a unanimous decision about the probable cause statement.

**Personal Invulnerability**

A second general myth that some engineers seem to believe concerning accidents is that accidents only happen to incompetent people, or to systems or equipment designed by incompetent people. This myth is an instantiation of what is

known as the fundamental attribution error, in which people tend to emphasize personal characteristics over situational circumstances as the reason why certain actions or decisions are made. Because few engineers consider themselves to be incompetent, they are inclined to think that accidents will not happen to them or to the systems with which they are involved. The general mentality seems to be this: accidents only happen when someone messes up, and I will not mess up, so no accidents will happen to me or the systems with which I work.

Regular reading of accident reports should effectively shatter this myth. Although *some* accidents happen as a result of incompetence, most do not. Rather accidents often happen despite the best efforts of very competent people to prevent them from happening. Recognizing this should provide strong motivation to system safety engineers to be extra careful in their work, being especially diligent to consider the types of accidents that might happen, and working to design systems in such a way as to prevent accidents from happening.

**Blaming an Individual**

A third general myth about accidents, and perhaps the most commonly believed one, is the notion that accident investigators are inclined to blame human operators at the expense of conducting thorough examinations into organizational and other systemic factors. Such a notion is perhaps not surprising, given the discussion in the previous section concerning attribution error. The notion is manifested in statements such as, "75% [or some other high percentage] of accidents are blamed on human error," which are repeated often at conferences and in the literature.

We recently conducted several studies to examine whether this oft repeated statement is supported by the evidence. These studies were prompted by intuition gained through reading many, many accident reports, which suggested to us that the conventional wisdom might well be wrong. Our results served to confirm our intuition.

The initial studies examined aviation accident reports produced by the National Transportation Safety Board (NTSB) in the United States [8] and by the Transportation Safety Board in Canada [9]. The follow-up study examined the major accident reports in all transportation modes published by the NTSB from 1996 – 2004 [10]. The results of these studies confirmed our intuition. We discuss briefly, and in simplified form, the latter study below. Readers interested in the full details should consult the reference.

In the all-modes study, we analyzed the 114 major accident reports adopted by the NTSB during the selected time period, distributed across the various transportation modes as follows: aviation – 30; rail – 28; highway – 21; marine – 16; pipelines – 11; and hazardous materials – 8. Table 1 shows a composite view of part of the results from our analysis.

| General Category | By Causes | By Reports |
|---|---|---|
| Individuals | 31% | 62% |
| Organizations | 50% | 80% |
| Equipment | 16% | 43% |
| Other | 3% | 10% |

Table 1: Attribution of causes in all reports.

The first column, General Category, lists the four general categories into which we eventually grouped the causal factors identified in the accident reports. The Individual category includes all those causal factors in which the actions or inactions of an individual were cited. The Organizations category includes those causal factors citing matters dealing with company or regulator actions, inactions, policies, or procedures. Causal factors involving equipment design or failures are included in Equipment. Finally, the Other category includes those causal factors that could not be placed in one of the other three categories, with weather-related factors being the most common of these.

The second column, By Causes, shows the percentage (rounded) of the total number of identified causes falling into this category. For example, of all the causes identified in the 114 reports, one-half of them involved Organizations, while only 31% involved Individuals. The third column, By Reports, shows the rounded percentage of the total number of reports in which at least one causal factor from the category was cited. Thus, 80% of the 114 reports cited at least one Organizational cause, and 63% of the reports cited at least one Individual cause.

Additional results from the study included the following. Considered by total causes cited, individuals accounted for a smaller percentage of causes than organizations for all modes. Considered by reports, individuals were cited in a smaller percentage of reports than organizations for every mode except aviation. And for aviation, the percentage of citations of individuals was only marginally larger than that of organizations. Also, more than twice as many reports cited organizational issues without citing any individual human errors, as cited individual human errors without also citing any organizational issues. These results demonstrate conclusively that as far as major accidents investigated by the National Transportation Safety Board in 1996-2004 are concerned, it is not true to claim that the investigations seek to blame individuals, at the expense of a thorough look into organizational factors. As mentioned previously, it was as a result of intuition gained through reading of many accidents that we were motivated to conduct the studies to debunk the myth of individual blame.

## 3 Understanding Consequences

Another benefit that we believe may come from the regular reading of accident reports is that it may provide a more

realistic understanding of the potential consequences of 'improbable' occurrences. We explain briefly what we mean by this below.

Often engineers, managers, and researchers think of safety in terms of a risk matrix, similar to what is shown in Figure 1. Such a matrix combines the severity of potential consequences with the likelihood of these consequences occurring. Boxes with the same colour are typically considered to contain hazards that are basically equivalent, requiring the same level of attention. This attention may range from hazards that must be eliminated entirely (dark grey boxes), to those that should be eliminated if practicable or controlled otherwise (medium grey), to those that should be controlled if cost-effective (light grey), to those that may be permitted to remain without control (white).

| | | Severity of Consequence | | | |
|---|---|---|---|---|---|
| | | Catastrophic | Critical | Marginal | Negligible |
| Likelihood | Frequent | | | | |
| | Probable | | | | |
| | Occasional | | | | |
| | Remote | | | | |
| | Improbable | | | | |

Figure 1: A Typical Risk Matrix

Several decades of experience has suggested that the use of matrices such as this can be quite helpful in improving system safety. That is not to say that people are not aware of possible problems in the use of these matrices; they are. For example, a paper by the U.S. Food and Drug Administration notes the following: "There can be inconsistency in risk assessments because there are at least two dimensions of subjectivity involved in the use of the risk assessment matrix. Interpretations of exposure, severity and probability may be different based on experience. This can be reduced by group discussions and averaging the ratings of several individuals. Remember the goal is to ultimately identify all risks in order of importance in order to prioritize risk control efforts." [11]

We believe that system safety engineers who make a habit of reading accident reports are likely to have a clear understanding of the potential pitfalls with these matrices, and to view them in slightly different ways than engineers who do not. The primary way in which we think this is true involves the approach to handling hazards with remote likelihood but potentially catastrophic and critical consequences, for example hazards that could lead to loss of life or of multiple lives. Traditional application of the risk management principles embodied in a risk matrix would typically permit either of two main approaches to be taken to such hazards: eliminate them, or reduce the likelihood of their occurrence to improbable. Regular reading of accident reports may well lead an engineer confronted with choosing between these two approaches to choose the former, if at all possible.

We believe this to be the case because many accidents suggest a tendency on the part of system designers and operators to underestimate the likelihood of very improbable, undesirable events. The potential consequences are often recognized, but their likelihood is thought to be quite a bit lower than it turns out to be. Examples of such accidents include the following:

- Space Shuttle *Challenger*: the consequences of complete O-ring failure were understood, but the likelihood of this failure occurring was not well understood [12].

- Space Shuttle *Columbia*: the consequences of a breach in the thermal protection on the leading edge of a wing were understood, but the likelihood of foam shedding from the external tank causing such a breach was thought to be much smaller than it turned out to be [13].

- Collision between U.S. Navy Submarine *USS Greeneville* and Japanese Motor Vessel *Ehime Maru*: the consequences of the submarine surfacing at a high rate of speed underneath a surface vessel were known, but the likelihood that there was a nearby vessel was not understood [14].

- American Airlines flight 587: the consequences of exceeding the ultimate design loads on the vertical stabilizer were known, but the likelihood of a pilot causing the airplane to exceed these loads was underestimated by both pilot and the airframe manufacturer (although in different ways) [15].

- United Airlines flight 585 and USAir flight 427: the consequences of a rudder reversal at low altitude and speed were understood, but the likelihood of it happening was not [16,17].

System safety engineers who read these reports, and the many others that show the same thing, may decide that system safety would be better served if designers focused more of their efforts on eliminating or mitigating the consequences of severe system hazards, rather than on attempting to further reduce the likelihood of occurrence of these hazards. This does not mean that engineers should not think about probabilities, only that perhaps the balance might be off. This seems particularly true within the system safety research community, where the opportunity often exists to consider alternate designs, techniques, and architectures that might be able to eliminate entire categories of adverse consequences, rather than simply reducing the probability of these consequences happening.

## 4 Recognizing Limits of Math Modelling

Still another benefit to be gained by system safety engineers from a regular reading of accident reports is a greater recognition of the limits of mathematical models. Mathematical modelling is applicable across many areas, in many different ways. In some areas, its full potential is rarely

realized, particularly within the United States. Analysis of software / hardware algorithm correctness via formal methods is one such area [18]. Also, various forms of mathematical modelling are often used in accident investigations: detailed simulations and performance analysis are two examples. However, mathematical modelling is not without its limits. Regular reading of accident reports can help to highlight two areas in which limits exist: understanding complex interactions, and causal description.

### 4.1 For understanding complex interactions

In the previous section we listed several accidents in which the likelihood of certain events occurring was not well understood. Both of the space shuttle accidents also illustrate limits on the use of mathematical models to help understand complex interactions. In both cases, there existed mathematical models used to simulate aspects of the systems which ultimately contributed to the accidents, and in both cases these models turned out to be inadequate.

Another example of the limits of mathematical models comes from the report on the loss of the Mars Polar Lander [19]. Mars Polar Lander (MPL) was launched on January 3, 1999, and arrived at Mars eleven months later. MPL lost contact with mission control approximately ten minutes before its expected landing, and was presumed crashed into the Martian surface. The mishap investigation board included the following observations concerning the use of mathematical modelling (analysis) in the MPL development: "... many of the findings are related to the propulsion system, which employed analysis as a substitute for test in the verification and validation of total system performance. Therefore, the end-to-end validation of the system through simulation and other analyses was potentially compromised in some areas when the tests employed to develop or validate the constituent models were not of an adequate fidelity level to ensure system robustness."

### 4.2 For causal description and analysis

The use of mathematical modelling for causal analysis and description is also limited. Although formal definitions for 'cause' exist, these definitions have significant limitations [20]. One limitation is that they are not easy for non-logicians to use effectively or correctly. This limitation alone might relatively minor; however, other limitations exist that are more serious.

In particular, counterfactually-based definitions of cause, which are the primary type that have been proposed, are both too narrow and too broad. They are too narrow in that they tend to eliminate as causal factors many of the organizational factors that are typically, and correctly, identified as causal in accidents. On the other hand, these formal definitions are too broad in that they often lead to difficulty in making necessary distinctions between causes and conditions, both of which may be shown to be counterfactually necessary.

## 5 Setting Directions

A final benefit of regular reading of accident reports is the prospect that doing so will help provide guidance on potentially relevant research directions. This possible guidance may lead in two directions: towards areas of likely safety improvements, and away from areas unlikely to affect safety.

One of the main ways in which guidance towards areas of likely safety improvements may be obtained is by carefully reading and understanding the recommendations made in individual accident reports. Many of the recommendations involve changes in procedures, training, or regulations, for which research is unnecessary; but some recommendations also involve matters for which research is needed. Examples of research matters mentioned in recent NTSB recommendations include the following: crew alertness and fatigue [21], minimum frictional quality standards for commercial tires on wet pavement [22], effectiveness of colour vision test protocols at screening out pilot applicants with impairing colour vision deficiencies [23], techniques for determining actual aircraft weight and balance data [24], and methods for converting non-frangible structures to frangible ones [25].

Another way in which guidance towards areas of likely safety improvements may be obtained is by considering broad classes of accidents that appear across many reports. For example, much research concerning fatigue, terrain warning, collision avoidance, and anti-lock brakes was motivated by trends noticed in accident reports. Careful consideration of accident trends may also provide guidance away from areas of research that are unlikely to improve safety significantly.

There are some caveats to kind in mind, however, when seeking guidance for research directions from accident reports. One of the most important caveats is the need to watch for a tendency to 'fight the last war'; that is, to conduct research that addresses issues that are no longer as important as they once were. A rather old, but nevertheless illustrative, example of this comes from 1970 in NASA. During a brief period shortly after his historic landing on the moon, Neil Armstrong served as the deputy associate administrator for aeronautics within the Agency. When a proposal came to him for research into automated aircraft flight controls using analog computers, he rejected it, telling the proposal writers that digital flight controls were the way to go [26].

Another important caveat is the need to be mindful of biases that might affect ones judgement. Two particularly dangerous biases are hindsight bias (which can lead you to think you have solved a problem when you do not even really understand it), and technology bias (which immediately assumes that accident causes can be solved by different technology, particularly the technology in which you have a vested interest). The effect of these two biases can often be readily seen in the aftermath of some recent accidents, where a multiple of different researchers produced papers and

presentations explaining how their particular techniques would have prevented the accident from happening. The Ariane 5 flight 501 explosion [27] and the Mars Polar Lander loss are two such accidents for which this has happened.

Technology bias also appears in a general form, when the assumption is made that every causal factor in an accident is likely to have a technological solution. One of the most dangerous and ubiquitous forms of this type of technology bias today is the assumption that increasing automation is always a good thing, an assumption that appears to shared by quite a few people [28].

A final important caveat to remember is that research alone does not improve safety. Insertion of the positive results of the research into practice is necessary for real improvements to happen. Theoretical results that are not used in system development and certification do not improve safety.

Within the system safety community, perhaps more so than within any other community, a close, mutually respecting relationship is essential between system safety practitioners and researchers. Without such a relationship, researchers are unlikely to produce anything useful in real systems, and practitioners are unlikely to make any improvements over the current state-of-the-practice. Perhaps a shared understanding of the results of previous accidents, based on careful and regular reading of accident reports, might help improve this relationship.

## 6 Concluding Remarks

This paper has proposed four benefits that are likely to accrue to system safety professionals from the regular reading of accident reports: an improved ability to separate myths from reality; an increased understanding of the consequences of unlikely events; a greater recognition of the limits of mathematical models; and guidance on potentially relevant research directions. Our basis for asserting the existence of these benefits is personal experience and observation. We encourage readers of this paper to conduct your own case studies to see if you obtain the benefits we believe you will.

## Acknowledgments

We are happy to acknowledge the constructive comments and criticisms made by the reviewers and by our colleagues. Specific thanks go to Kelly Hayhurst at NASA Langley Research Center and Billy Greenwell at the University of Virginia for their participation in discussions upon which much of this paper is based.

## References

[1] P. Snowdon, ; C. W. Johnson: "Results of a Preliminary Survey into the Usability of Accident and Incident Reports", in *People in Control: An international conference on human interfaces in control rooms, cockpits and command centres*, J. Noyes and M. Bransby, editors, Bath, UK, 21-23 June 1999, pp. 258-262.

[2] See for example the discussion thread concerning Ariane 5 and Commercial-Off-The-Shelf software archived on the web at <http://www.cs.york.ac.uk/hise/safety-critical-archive/2005/0341.html>, visited 17 March 2006.

[3] Aeronautica Civil Of The Republic Of Colombia: "Aircraft Accident Report: Controlled Flight Into Terrain American Airlines Flight 965, Boeing 757-223, N651AA, Near Cali, Colombia, December 20, 1995", Aeronautica Civil Of The Republic Of Colombia. [Web version at <http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/ComAndRep/Cali/calirep.html> visited 13 March 2006.]

[4] National Aeronautics and Space Administration: "Mars Climate Orbiter Mishap Investigation Board Phase I Report", November 10, 1999.

[5] C. W. Johnson: "The Natural History of Bugs: Using Formal Methods to Analyse Software Related Failures in Space Missions", edited by J.S. Fitzgerald, I.J. Hayes, and A. Tarlecki, *Lecture Notes in Computing Science Number 3582*, Heidelberg, Germany, 2005, pp. 9-25.

[6] National Transportation Safety Board: "Aircraft Accident Report: United Airlines Flight 232, McDonnell Douglas DC-10-10, Sioux Gateway Airport, Sioux City, Iowa, July 19, 1989", NTSB/AAR-90/06.

[7] National Transportation Safety Board: "Highway Accident Report: School Bus Run-off-Bridge Accident, Omaha, Nebraska, October 13, 2001", NTSB/HAR-04/01, Notation 7610.

[8] C. M. Holloway; C. W. Johnson: "Distribution of Causes in Selected U.S. Aviation Accident Reports Between 1996 and 2003", *Proceedings of the 22nd International System Safety Conference*, Providence, Rhode Island, 2-6 August 2004. Electronic version available on the web at <http://shemesh.larc.nasa.gov/ssse/issc05-cmhcwj-ntsbanalysis.pdf>

[9] C. W. Johnson; C. M. Holloway: "'Systemic Failures' and 'Human Error' in Canadian TSB Aviation Accident Reports between 1996 and 2002", *Proceedings of HCI in Aerospace 2004*, Toulouse, France, 29 September - 1 October 2004.

[10] C. M. Holloway; C. W. Johnson: "On the Prevalence of Organizational Factors in Recent U.S. Transportation Accidents", *Proceedings of the 23rd International System Safety Conference*, San Diego California, 22-26 August 2005.

[11] Department of Health and Human Services, US Food and Drug Administration, Center for Food Safety and

Applied Nutrition: “Food Safety and Security: Operational Risk Management Systems Approach”, November 29, 2001. [Available on the web at <http://www.dhs.ca.gov/fdb/PDF/Food%20Safety%20and%20Security11-29.PDF> visited 17 March 2006.]

[12] Government Printing Office: *Presidential Commission on the Space Shuttle Challenger Accident*, Washington, D.C., June 6, 1986.

[13] Government Printing Office: *Columbia Accident Investigation Board, Report Volume 1*, August 2003.

[14] National Transportation Safety Board: “Collision between the U.S. Navy Submarine *USS Greeneville* and Japanese Motor Vessel *Ehime Maru* Near Oahu, Hawaii, February 9, 2001”, NTSB/MAB-05/01.

[15] National Transportation Safety Board: “In-Flight Separation of Vertical Stabilizer, American Airlines Flight 587, Airbus Industrie A300-605R, N14053, Belle Harbor, New York, November 12, 2001”, NTSB/AAR-04/04.

[16] National Transportation Safety Board: “Uncontrolled Descent and Collision with Terrain, United Airlines Flight 585, Boeing 737-200, N999UA, 4 Miles South of Colorado Springs, Municipal Airport, Colorado Springs, Colorado, March 3, 1991”, NTSB/AAR-01/01.

[17] National Transportation Safety Board: “Uncontrolled Descent and Collision with Terrain, USAir Flight 427, Boeing 737-300, N513AU, Near Aliquippa, Pennsylvania, September 8, 1994”, NTSB/AAR-99/01.

[18] Jonathan P. Bowen; Michael G. Hinchy: “Ten Commandments of Formal Methods … Ten Years Later”, *IEEE Computer*, Volume 39, Number 1, January 2006, pp. 40-48.

[19] Jet Propulsion Laboratory, JPL Special Review Board, “Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions”, JPL D-18709, March 22, 2000.

[20] C. W. Johnson; C. M. Holloway: “A Survey of Logic Formalisms to Support Mishap Analysis”, *Reliability Engineering and Systems Safety*, Volume 80, Issue 3, pp. 271-291, June 2003.

[21] National Transportation Safety Board: Collision with Trees and Crash Short of Runway, Corporate Airlines Flight 5966, British Aerospace BAE-J3201, N875JX, Kirksville, Missouri, October 19, 2004, NTSB/AAR-06/01.

[22] National Transportation Safety Board: Motorcoach Median Crossover and Collision with Sport Utility Vehicle, Hewitt, Texas, February 14, 2003, NTSB/HAR-05/02.

[23] National Transportation Safety Board: Collision With Trees on Final Approach Federal Express Flight 1478, Boeing 727-232, N497FE, Tallahassee, Florida July 26, 2002, NTSB/AAR-04/02.

[24] National Transportation Safety Board: Loss of Pitch Control During Takeoff Air, Midwest Flight 5481, Raytheon (Beechcraft) 1900D, N233YV, Charlotte, North Carolina, January 8, 2003, NTSB/AAR-04/01.

[25] National Transportation Safety Board: Runway Overrun During Landing, American Airlines Flight 1420, McDonnell Douglas MD-82, N215AA, Little Rock, Arkansas, June 1, 1999, NTSB/AAR-01/02.

[26] James R. Hansen: *First Man: The Life of Neil A. Armstrong*, Simon & Schuster, 2005.

[27] Report by the Inquiry Board: “Ariane 5 Flight 501 Failure”, Paris, 19 July 1996.

[28] Kelly J. Hayhurst; C. Michael Holloway: “Visions of Automation and Realities of Certification”, *Infotech@Aerospace*, Arlington, Virginia, 26-29 September 2005.