ROOT CAUSES OF ENGINEERING COMPLACENCY ON AVIATION AND AEROSPACE SAFETY

by

Alyssa M. Olson, B.S.

THESIS

Presented to the Faculty of

The University of Houston Clear Lake

In Partial Fulfillment

of the Requirements

for the Degree

MASTER OF SCIENCE

THE UNIVERISTY OF HOUSTON-CLEAR LAKE

2011

ROOT CAUSES OF ENGINEERING COMPLACENCY ON AVIATION AND AEROSPACE SAFETY

by

Alyssa M. Olson

APPROVED BY

Ipek Bozkurt, Ph.D., Chair

James Dabney, Ph.D., Committee Member

Jim Helm, Ph.D., Committee Member

Mary Randolph-Gips, Ph.D., Committee Member

Dennis M. Casserly, Ph.D., Associate Dean

Zbigniew J. Czajkiewicz, Ph.D., Dean

ABSTRACT

ROOT CAUSES OF ENGINEERING COMPLACENCY ON AVIATION AND AEROSPACE SAFETY

Alyssa M. Olson, M.S.
The University of Houston Clear Lake, 2011

Thesis Chair: Dr. Ipek Bozkurt

When engineers, maintenance personnel or operators in aviation and aerospace begin to settle into a complacent mindset they inherently accept a greater amount of risk, thus opening the door for the possibility of dangerous events to unfold. If a connection as to why engineers or operators settle into a complacent mindset is made, and consequently how the development of that attitude can be avoided, it is the author's opinion that catastrophic events can be avoided. This thesis identifies possible catalysts, in the form of complacency factors, that can make engineers and operators have high confidence in a system and cause them to accept a higher amount of risk. A total of six complacency factors were identified and include: discounting risk, ignoring warning signs, assuming risk decreases over time, over-reliance on redundancy or automation, unrealistic risk assessments, and ignoring high-consequence low probability events. This investigation into engineering complacency and the root cause of it occurring in aerospace and aviation safety relied on an analysis of historical accident investigation data and the circumstances involved. Case studies were pulled from the aerospace and aviation industry that involve both engineering and operator error. Catastrophic accidents within military aircraft, NASA systems including the Space Shuttles and Satellites, and commercial and private aviation were explored. Analysis was conducted to look at the system safety programs, risk management, and corrective action procedures for each organization. Through case study analysis it was apparent that one or more of the identified complacency factors were present in all cases. Complacency is a substantial risk throughout any human oriented task or engineering centric organization, not just aerospace. Complacency can be evaluated in the oil industry, nuclear industry, manufacturing and everyday tasks such as operating an automobile. Focusing on a particular failure mode in a single organization would allow for concentrated analysis and corporate culture specific trending. Implementation of trending analysis to evaluate failure modes within all of the aforementioned organizations is imperative to identifying areas where complacent factors can occur.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

Complacency or a false sense of security should not be allowed to develop as a result of long periods without an accident or serious incident. An organization with a good safety record is not necessarily a safe organization. — International Civil Aviation Organization, Accident Prevention Manual, 1984.

Complacency is defined by the National Aeronautics and Space Administration, NASA, as a "self-satisfaction that can result in non-vigilance based on an unjustified assumption of satisfactory system state" (Prinzel, 2002). When engineers, maintenance personnel or operators in aviation and aerospace begin to settle into a complacent mindset they inherently accept a greater amount of risk, thus opening the door for the possibility of dangerous events to unfold. It is the opinion of the author and goal of this thesis to show that catastrophic events such as the Challenger and Columbia Space Shuttle accidents, the Colgan Air disaster, and the Mars Climate Orbiter (MCO) Satellite incident could have been avoided had the engineers or operators not become complacent with their respective systems.

Society's current mindset is to produce high quality items quickly and for the lowest possible price. Profit margins and legacy confidence are two of the main factors that have led to system safety engineering complacency (Petroski, 1992). When complacency or the need to cut costs begins to set in, the accepted amounts of risk increase and thus there is a reduction in safety. Often times these accepted amounts of risk increases are small but can be compounded throughout the entire program.

If a connection as to why engineers or operators settle into a complacent mindset is made, and consequently how the development of that attitude can be avoided, would it be feasible to assume that we could avoid major catastrophic events such as the Shuttle accidents? However, the main question is how can you do this and would that be enough? This thesis expects to identify the possible catalysts that make engineers and operators have such high confidence in a system and what triggers them to accept a higher amount of risk. This will be done through analysis of past catastrophic aviation and aerospace accidents as well as questioning the engineering and operator community in both the aviation and aerospace industries, with the ultimate goal to make recommendations on how these programs can identify and avoid complacency.

1.1 PROBLEM MOTIVATING STUDY

The true iniquity of engineering complacency is rooted deep in the increased levels of risk which engineers or operators are willing to accept. Risk acceptance and safety go hand in hand. Often times the residual risk across an entire aviation or aerospace program may be stacked, meaning that there are varying levels of risk accepted throughout different systems in that program. The presence of stacked risk can mean that safety implications can go unrealized without proper system safety engineering involvement. As programs continue to age and budgets are slashed, engineers and operators, as a means to reduce costs, may rely on past mission success rather than addressing the problem in the here and now or qualifying hardware through rigorous testing.

Many military aircraft and government aerospace programs have been long running; some nearly 30 years since their inaugural flight. Many of these organizations have employed safety programs from the beginning stages yet still have experienced catastrophic accidents. Ironically, successful missions are a channel for accidents since it can lead to complacency and cutting of corners or making tradeoffs that increase risk (Leveson, 2001). The idea that successful programs yield complacency and reductions in safety is not a new one. In fact, it can be quite common. Once complacency begins to creep into a program's engineering culture it can be difficult to offset (Petroski, 1992). Programs with deep rooted success in safety can often be plagued by a slow drift towards states of high risk.

Complacency can manifest itself through managerial decisions and/or the decision makers who choose to ignore substantial evidence of risk. Since the safety culture of any organization is a subset of their attitude and approaches to safety and risk management, laxness in technical rigor or risk management processes can result in accidents (O'Connor, 2009). This laxness can be due to overconfidence or project management teams who may be focused primarily on meeting mission objectives for cost and schedule, and with that, scrutiny of risk can fall by the wayside. In turn the amount of acceptable or residual risk increases slowly throughout the lifetime of a program, as long as there is no incident, and continues to go unnoticed by the operators and engineers. The challenge is to identify this drift and set in place safeguards to prevent it prior to an accident occurring (Leveson, 2005).

Complacency can also breed when engineers or operators begin to assume that risk decreases over time. In fact, the opposite actually occurs. The longer a program is successful or the longer someone has been an operator, the chance for complacency and risky behavior increases (Leveson, 2005). Pilots become more brazen with what they believe they or their hardware are capable of (relying on automation) and engineers begin to rely on past success rather than testing and analysis (Prinzel, 2002). Identifying the warning signs of engineer and operational complacency can help companies to boost safety programs and to keep risk in check.

1.2 PURPOSE OF THE STUDY

1.2.1 What is to be Accomplished

This study will look into the risk factors that lead to engineering and operational complacency. The goal is to show that catastrophic accidents such as the Challenger and Columbia Space Shuttle accidents, the Colgan Air disaster, or the Mars Climate Orbiter (MCO) Satellite could have been avoided had the engineers or operators not become complacent with their system. However, before a direct line between aerospace and aviation safety and complacency can be made, it is necessary to generate a concise definition of complacency.

1.2.2 Usefulness of the Study

Analyses completed during this body of thesis work will aide in the identification of the warning signs of engineering and pilot complacency prior to a catastrophic event. This study is useful to the field of Systems Engineering because human factor events should be analyzed for the life cycle of a project in order to develop appropriate work-processes and to identify areas where complacency can develop. The goal of human factors engineering is to design a system so that the human-system interface works safely and so that optimum system performance is achieved. However, the development of automated system aides can lead to complacency with system outputs. Identification of areas for complacency prior to a mission can reduce the threat of catastrophic loss.

2.0 BACKGROUND RESEARCH

In order to understand complacency within the aerospace industry, extensive research was completed on developing a concise definition of complacency and how it falls under the umbrella of the field of human factors. Human factors (or ergonomics), as defined by the International Ergonomics Association, is the scientific discipline concerned with the understanding of interaction among humans and other elements of a system, and the profession that applies theory, principles, data, and other methods to design in order to optimize human well-being and overall system performance (International Ergonomics Association, 2010). The discipline of human factors ergonomics is broken down into three domains of specialization: physical ergonomics, organizational ergonomics, and cognitive ergonomics. The domain of cognitive ergonomics is the primary focus for this body of research because it is concerned with the mental processes as they effect interactions of humans and the elements of a system. This research focuses on decision-making, perception, memory, reasoning, and motor response. The concept of human complacency falls within this domain. The goal of human factors engineering is to design a system so that the human-system interface works safely and so that optimum system performance is achieved. However, as we will see in the body of this research, the development of automated system aides can lead to complacency with system outputs. The field of human factors engineering can be a double-edged sword when it comes to the delicate topic of complacency.

Through extensive research completed on this topic, there appears to be very minimal focus on the subject of complacency in the aerospace industry. However, research has been completed in automation-induced complacency which has been noted as a factor of complacency within the aircraft cockpits. Raja Parasuraman of George Mason University has conducted significant research on automation-induced complacency within the workplace. He and his colleagues have found that an increase in injury and errors occurs when automated functions are introduced into a system, such as automated instrument readouts within a cockpit, and from that research have coined the term "automation-induced complacency". The reliance on automation has led to a rise in errors due to the failure to cross-check or monitor the automated data. Humans rely on the data that is given and sometimes that can lead to catastrophic consequences.

In addition to automation-induced complacency, Nancy Leveson from the Massachusetts Institute of Technology has brushed the very surface of the topic through her research into the NASA Columbia accident. Leveson, when speaking of the Columbia accident, refers to complacency as a common theme in what she describes as NASA's culture of denial where risk assessments are unrealistic and credible risks and warnings are dismissed without appropriate investigation (Leveson, 2004). She does not delve any further than referring to complacency as one of the factors in NASA's culture, focusing more on the decisions of upper management and risk management.

The Columbia Accident Investigation Board (CAIB) also refers to a complacent attitude among NASA engineers within the CAIB Report as a contributing factor to the Columbia accident. However, like

Leveson's study, it is mostly a reference to complacency rather than the factors that generated that attitude. The primary focus was on the risk management process, decisions made by upper management and the silent safety program.

3.0 METHOD

3.1 OVERVIEW

The investigation into engineering complacency and the root cause of it occurring in aerospace and aviation safety will rely on an analysis of historical accident investigation data and the circumstances involved. Case studies were pulled from the aerospace and aviation industry that involve both engineering and operator error. Catastrophic accidents within military aircraft, NASA systems including the Space Shuttles and Satellites, and commercial and private aviation were explored. Analysis was conducted to look at the system safety programs, risk management, and corrective action procedures for each organization. Areas of interest for this trending data will be the U.S Air Force, the U.S Army, NASA and the National Transportation Safety Board (NTSB). These organizations were selected because they represent a large sampling of government aviation and aerospace programs as well as the commercial and private aviation sector. Figure 1 below illustrates visually the method used to complete this study on engineering complacency:

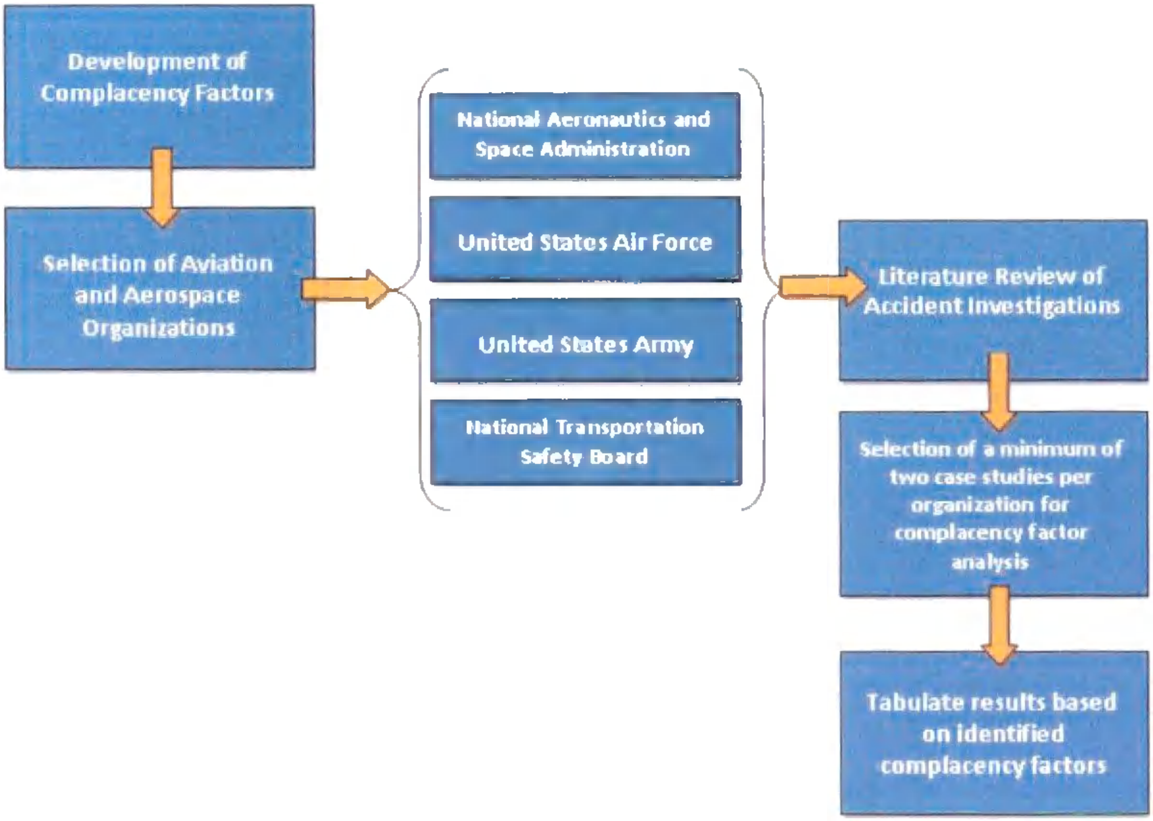

Development of Complacency Factors
Selection of Aviation and Aerospace Organizations
National Aeronautics and Space Administration
United States Air Force
United States Army
National Transportation Safety Board
Literature Review of Accident Investigations
Selection of a minimum of two case studies per organization for complacency factor analysis
Tabulate results based on identified complacency factors

Figure 1: Method Flow Diagram

3.2 RESEARCHED ORGANIZATIONS

3.2.1 Description

The primary subject focus for the body of this research was on aerospace organizations with high expense or losses if a catastrophic event were to occur. A cut off was established for case studies evaluated in this body of work at a level where loss of life or loss of system resulted in costs in excessive of one million dollars. Organizations such as NASA, the U.S. Army, U.S. Air Force, and the commercial and private aviation were the primary focus of data collection. Each of these organizations is subject to catastrophic loss of life or system events.

The National Aeronautics and Space Administration, NASA, was formed in July 1958 with the Congressional adoption of the National Aeronautics and Space Act, commonly referred to as the "Space Act". The Space Act was enacted to provide for research into problems of flight within and outside the earth's atmosphere, and for other purposes (NASA, 1985). Since then, NASA has been among the leading innovators in human spaceflight and satellite development.

The United States Army is a branch of the United States Armed Forces which is responsible for land-based military operations. As one of the oldest branches of the U.S. military, their primary mission is to "provide necessary forces and capabilities... in support if the National Security and Defense Strategies (United States Army, 2006)." The modern Army gets its roots from the original formation of the Continental Army on June 14, 1775 to meet the demands of the Revolutionary War, but the Army as we know it today was officially created by the Congress of the Confederation on June 3, 1784. The U.S. Army operates several aircraft in support of their operations (United States Army, 2010). While they operate a few fixed-wing aircraft, their primary operated aircraft include rotorcraft such as the AH-64 Apache attack helicopter, the OH-58D Kiowa Warrior armed reconnaissance/light attach helicopter, the UH-60 Black Hawk utility tactical support helicopter and the CH-47 Chinook heavy-lift transport helicopter.

The United States Air Force is a branch of the United States Armed Forces which is primarily responsible for aerial warfare. Initially part of the U.S. Army, the Air Force was formed as a separate branch of the military September 18, 1947 (United States Air Force, 2010a). The mission statement of the Air Force is "fly, fight, and win" in air, space and cyberspace (United States Air Force, 2010b)The U.S. Air Force is broken down into core functions. These functions include Nuclear Deterrence Operations, Special Operations, Air Superiority, Global Integrated ISR, Space Superiority, Command and Control, Cyberspace Superiority, Personnel Recovery, Global Precision Attack, Building Partnerships, Rapid Global Mobility and Agile Combat Support (United States Air Force, 2010b). The U.S. Air Force operates a large majority of fixed-wing aircraft and rotorcraft. The active fixed-wing aircraft include the C-17 Globemaster III cargo transport, the B-52H Stratofortress bomber, and the F-22 Raptor Fighter.

The National Transportation and Safety Board, NTSB, was formed in 1967 to operate as an independent government agency responsible for civil transportation accident investigation. The NTSB investigates and reports on aviation accidents, certain types of highway crashes, ship and marine accidents, pipeline accidents and railroad accidents (NTSB, 2006). While they investigate a broad range of transportation related incidents, for the purpose of this thesis investigation the focus will be on air accidents. The majority of commercial and private aviation research for the purpose of this thesis will come from NTSB investigation material.

3.2.2 Selection

These organizations were selected based on their prominence in the aerospace industry and the fact that each has long running programs where complacency is more likely to be present. NASA has programs such as the Space Shuttle which has been in service since the early 1980's and the Army and Air Force have aircraft such as the Apache Helicopter, operating since 1982, and the KC-135, operating since 1950; respectively.

3.3 DATA COLLECTION

As part of this thesis investigation a lengthy literature review was necessary to gather the datum for making educated recommendations on how to combat complacency in the aviation and aerospace community. Data collection for this thesis was completed by reviewing Journal Articles, Symposium data, and accident investigation reports from the NTSB, NASA, U.S. Air Force and U.S. Army as the primary focus this review.

4.0 ANALYSIS AND RESULTS

As stated earlier in this thesis, in order to gauge whether or not a program is succumbing to complacency, one must first define what exactly complacency means to the body of this work. This is important to the body of this research because without it, contributing factors to catastrophic engineering events might be mistaken or never identified as complacency. What exactly is complacency? Numerous industry definitions exist but they all seem to converge to one common idea, the idea that complacency is an attitude. It is an attitude that governs how engineers and operators respond to certain incidents to a given set of circumstances. Complacency and human factors go hand-in-hand. In fact, complacency is described as one of the "dirty dozen", a term coined by Canadian safety specialist Gordon Dupont to describe the twelve most common causes of human error in the aviation world (Dupont, 1997). The aerospace and aviation industries are very repetitive in nature and with that they breed complacency (Dupont, 1997).

During historical research of catastrophic events for the body of this work, the following question was asked throughout the investigation to aide in developing a clear definition of complacency: Are safety philosophies and processes that are established to evade catastrophic events being given a low priority in the systems engineering process? From this question there are several subcategories that were identified that can be reviewed to further determine if complacency is an issue within a program. These include:

- Failure or Problem Reporting Methods: Were they not recording detailed information for escapements or failures and or incorrectly evaluating that data?
- Sedimentary Mind-set: Was the company in a "why change" mind-set? Being satisfied with the status quo or being too lazy to seek out and recognize improper operating conditions.
- Monotony: Was there a lack of interest – Not feeling challenged by a long running or seemingly easy program? Having a mindset that we don't need to learn much else. Ignoring small operational problems.

Asking this overall arching question during the investigation helped to determine reoccurring factors that categorize complacency.

While researching different aerospace and aviation accidents there were clear factors that became reoccurring themes across all programs investigated. While not all factors were present in every instance analyzed, at least two or more of the factors in Figure 2 were present in catastrophic accidents. Figure 2 on the following page was created for this paper to show a visual representation of the six factors that can lead to complacent behavior:

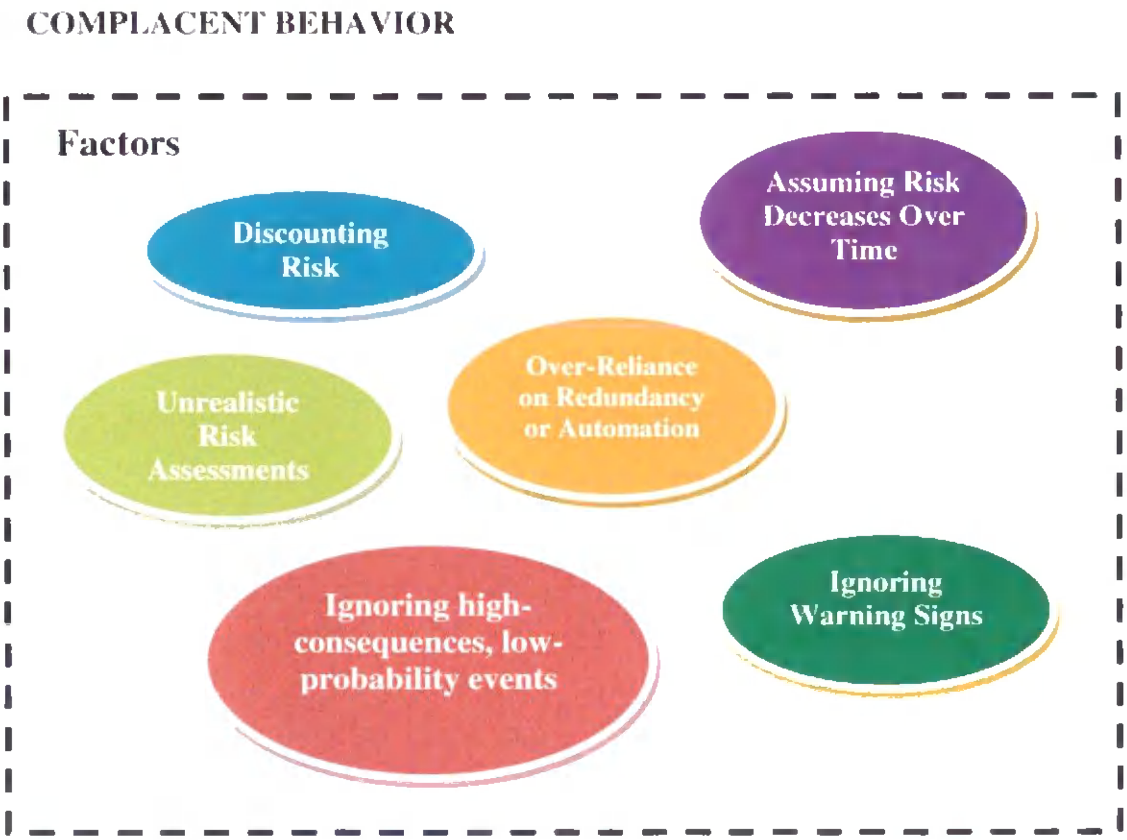

COMPLACENT BEHAVIOR
Factors
Discounting Risk
Assuming Risk Decreases Over Time
Unrealistic Risk Assessments
Over-Reliance on Redundancy or Automation
Ignoring high-consequences, low-probability events
Ignoring Warning Signs

Figure 2: Factors of Complacent Behavior

The above complacency factors were generated through research done by Nancy G. Leveson of the Massachusetts Institute of Technology. Her categorization of the factors found in complacency-based events was a jumping-off point for this body of research. It is important to understand each factor individually and how it might be viewed within an engineering situation. Understanding what cues or human response to these factors was imperative in recognizing those factors within the case studies analyzed within the aerospace communities.

Discounting of risk within a program is a human tendency. Most catastrophic accidents in well-designed systems involve two or more low-probability events occurring in the worst possible combination. When engineers or operators attempt to predict risk, they explicitly or implicitly multiply events with low probability, assuming independence, and come out with impossibly small numbers, when the events are actually dependent (Leveson, 2002). This dependence between events has been coined the Titanic Coincidence by Machol (Machol, 1975). A number of coincidences contributed to the catastrophic Titanic disaster and subsequent loss of life, such as the captain was going too fast for the weather conditions, there was not a proper watch for icebergs, and the ship did not have enough lifeboats for the passengers on board. These failures seem independent, however when given the overconfidence of the Titanic engineers and operators the actual risk was severely underestimated (Machol, 1975). This shows us that the magnitude of a catastrophic event can be reduced to the extent that engineers and operators believe that the event cannot occur. If engineers and operators were to realize the true risk and not discount it, that cost of taking action in advance to prevent a catastrophic event would be inconsequential in comparison to loss if no action was taken.

It seems intuitive that redundancy within a system should make it more reliable and safe; however, this is not always the case. While redundancy within a system is a good safety measure, often engineers over-rely on redundancy. In some accidents there are common cause failures in which redundant systems are both affected by the same failure mode. There is a paradox in engineering that providing more redundancy leads to a safer vehicle when in reality it may lead to complacency and defeats the purpose of the redundancy. Latent failures within electrical components, sneak circuits[1] or bad lots may cause a common cause failure mode which engineers or operators did not foresee.

For the commercial, military, or private pilot advancements in cockpit automation technology have transitioned pilots from active participants to process supervisors. While this technology advancement has created efficient flying conditions, unfortunately it has opened the door to pilot complacency. The introduction of automated cockpits may lead pilots to "become complacent because they are overconfident in and uncritical of the automation, and fail to exercise appropriate vigilance, sometimes to the extent of abdicating responsibility to it [which can] lead to unsafe conditions (Reserach Integration, 2007)." This implies that the complacency occurs when the automation supervisor, or the pilot, is unaware of the current or impending actions of the machine. Sometimes this pilot complacency can lead to catastrophic results.

[1] A sneak circuit is defined as a designed in signal or current path that causes unwanted functions or modes of operation to occur or that inhibits a desired function from occurring (Ericson II, 2005).

For example, American Airlines Flight 965 succumbed to complacency when the crew failed to crosscheck the aircraft's automated activity during a flight over Columbia in December 1995. Failure to crosscheck the automated altitude measurement resulted in a controlled flight into terrain and the death of all passengers and crew (Aeronautica Civil of the Republic of Columbia, 1995)

Unrealistic assessment of risk can send a program spiraling into a catastrophic event. Unrealistic risk assessments that show positive margins create a sense of complacency. Under schedule pressure engineers or upper management can succumb to a culture of denial where risk assessment is unrealistic and risk that are credible are dismissed without a full investigation (Leveson, 2004). Under this culture, managers are prone to listen to those engineers who can provide confirmed evidence for the story or outcome that they wanted to hear. For example, during the NASA Columbia accident, the Mission Management Team leaders made decisions to reenter the Earth's atmosphere based on data and conclusions from a thermal tile expert, not an expert on the Shuttle wing leading edge tiles, rather than focusing on the negative data and concerns from the Debris Assessment Team that was tasked with evaluating the damage (Gehman, 2003). Management and engineers can be overrun with conflicting data or excessive data with no convenient way to sort through it. This may lead to ignoring factors or discounting risk factors that should have been evaluated further.

Another factor that appears to go hand in hand with complacency is the tendency of engineers to ignore high-consequence, low probability events. The effective evaluation of high-consequence, low probability events in complex systems can be difficult to achieve and thus can lead to complacency on the part of management and engineers to accept questionable data as valid. Obtaining objective data for these types of events can be difficult. The data is often times collected using subjective methods such as "expert opinions, extrapolated data, [and] deductive analysis (Bryson, 1984)." The reliance on expert opinion can also be further complicated by the fact that not all "experts" agree on the data. This can lead to conflicting ideas, making effective evaluation of the datum an even more tedious task. The perception of one "expert" versus another can cloud the decision process of management further, leading to the discounting of these high-consequence, low probability events.

The assumption that risk decreases over time can lead to overconfidence and complacency within engineers and operators and, unfortunately, loss of life. Unexamined faith in a program's fail-safe nature can lead to complacency and a false sense of security in which individuals are lulled into not taking other necessary precautions. This was a very prominent occurrence during both aforementioned Space Shuttle accidents. Important decisions were made based on flawed risk assessments and over-confidence in the vehicle. In the Kraft Report released in February 1995, a NASA advisement team evaluated the presumed risk and overall success of the Space Shuttle program since the Challenger accident. In reading the report it is evident that the advisory committee fully buys into the idea that risk decreases over time. The executive summary of the Kraft report specifically states, "with over 65 successful launches, operations [for the Space Shuttle program] have become quite reliable (Kraft, 1995)." The committee continues on to make recommendations based on the maturity of the vehicle as well as the continued success since the initial Space Shuttle Challenger accident. Lulling the NASA community into a false sense of security based on previous success, it is apparent that the Kraft report was detrimental to the Space Shuttle program. Working on the assumption that risk decreases over time, employees became more confident in the hardware's abilities, ultimately discounting ever-present risk and leading to another catastrophic tragedy, Columbia.

While the catastrophic result of the assumption that risk decreases over time can be easily seen in the Space Shuttle program, it is not just the NASA community who has fallen victim to this complacency factor. Military and private pilots can also succumb to time-based risk acceptance events. Pilot overconfidence due to extensive experience or the "been there, done that" attitude can lead to errors of omission or impulse due to their altered mental state. An example of pilot overconfidence can be seen in the U.S. Air Force C-17A crash in Richardson, Alaska during practice on July 28, 2010 for an upcoming airshow. After the initial climb out and left turn after takeoff, the pilot executed what the data categorizes as an aggressive right turn. As the C-17A banked, the stall warning system activated to alert the crew of an impending stall. In the U.S. Air Force accident investigation report it was noted that the pilot made the conscious decision to continue the turn as planned, ignoring the warning and the need to begin stall recovery procedures. At this point, the aircraft entered a stall from which recovery was not possible. When the pilot did eventually attempt to recover the aircraft, incorrect procedures were used and there was insufficient altitude to regain controlled flight. The aircraft impacted wooden terrain, was destroyed, and all four members of the crew were killed on impact (U.S. Air Force Accident Investigation Board, 2010). The accident investigation board found sufficient evidence that the "crew ignored cautions and warning and failed to respond various challenge and reply items (U.S. Air Force Accident Investigation Board, 2010)." The board specifically describes the crew's actions within the report as "overconfidence" and "expectancy". The pilot had been quoted as "wanting to put on a good airshow" and had consistently planned and operated the aircraft with the stall warning during the 260-degree maneuver. Further review of the accident report for this thesis found that the report is really missing the overarching cause of this accident: complacency. The subfactors to the crew's complacency could be their overconfidence and expectancy, but in actuality the crew had become complacent with the operation of the aircraft and the particular maneuver they were conducting.

Another complacency factor in the C-17A crash is that they were ignoring warning signs. The pilots blatantly dismissed stall warnings and continued down a path that put them in line for a catastrophic accident. Ignoring warning signs can take only a moment or can be a gradual process where the pilot or engineer builds confidence in their system based on the idea that nothing happened last time. The Space Shuttle Challenger, launch 51-L, explosion is another example of ignoring warning signs. The overarching cause of the Challenger accident was determined by the Rogers Commission to be a failure in the joint between the two lower segments of the right Solid Rocket Motor (SRM), a component of the Solid Rocket Booster (SRB); this joint is also often referred to as the O-ring seal. The intended purpose of these seals in to prevent hot gases from leaking through the joint during ignition and burning of propellant of the rocket motor. The joint in question was recognized by both NASA and Morton Thiokol, the SRB contracted developers, to be an insufficient design and in need of a redesign. Morton Thiokol engineers had developed a position on the need for a redesign by stating that "the condition is not desirable but acceptable (NASA, 1987)." NASA management did not accept the judgment of its engineers that the condition was unacceptable, and as the joint issues grew in number they were minimized in management briefing and reports (NASA, 1987). The joints had been shown to be failing for numerous flights and there was ample time available for redesign and manufacturing of new joints, but constraints to meet flight schedules and cut program costs were given a higher priority than safety.

Management at Morton Thiokol failed to inform upper NASA management with the written concerns of their design engineers, ultimately ignoring warning signs and putting the safety of the Challenger and crew in grave jeopardy. One of the major findings of the Rogers Report was that Morton Thiokol management reversed its position and recommendation for the launch of 51-L. This was at the urging of Marshall Space Flight Center and was contrary to the views of the SRB engineers. Management was trying to appease their primary customer and with that they ignored very apparent warning signs.

The identified, reoccurring factors played an important role in determining whether or not a catastrophic accident was caused in full or in part from engineering complacency. It is apparent that one or more of these factors are present in all cases where some form of human error, not specifically complacency, was identified as a contributing factor by the organization it affected. However, in instances where an accident analysis focuses solely on the engineering or mechanical aspects of a failure it can be seen that a complacency hole exists. This hole in the data may be from lack of testing on legacy parts for a new use, failure to properly report problems and implement corrective actions, or certification gaps. Table 1 on the following page provides an overview of the identifying qualities of the complacency factors discussed above.

Table 1: Overview of Identifying Qualities of Complacency Factors

OVERVIEW OF IDENIFYING QUALITIES OF COMPLACENCY FACTORS	
Factors:	**Identifying Qualities:**
Discounting Risk	• Risk calculations based on independence when they are dependent.
Unrealistic Risk Assessments	• Risk-based decisions made on incorrect or unreliable data. • Decision made based on schedule rather than risk. • Overrun with conflicting or excessive data for risk-based decision purposes.
Assuming Risk Decreases Over Time	• Overconfidence in system performance. • Risk decisions made based on previous recorded success. • "Been there, done that" mentality.
Over-Reliance on Redundancy or Automation	• Discounting probability of common cause failures. • Failure to crosscheck automated functions. • Assumption that automated data is correct.
Ignoring high-consequence, Low probability Events	• Achieving objective data is difficult in these scenarios. • Reliance on expert opinion, which can vary between experts.
Ignoring Warning Signs	• Continuing an operation even when caution or warning light is illuminated or annunciated. • Ignoring or not correlating reoccurring failures in risk-based decisions. • Idea that we survived it before, we can survive it again.

During case study analysis, Table 1 was used to determine whether a complacency factor existed. Accident investigations were thoroughly reviewed for the identifying qualities of the six complacency factors. For example, interviews or data from an accident investigation might point to the fact that an engineer or aviator continued with a mission even though a warning light or unmitigated failures had occurred. Then, referring to Table 1, it can be seen that this type of behavior would fit under the factor of ignoring warning signs. The behaviors or events identified that led to the identification of a particular complacency factor were then discussed in detail for the case study.

4.1 NASA: REOCCURRING COMPLACENCY

NASA has had a reputation as the leader in innovative technology and at the forefront in aerospace technology. Recently NASA's catastrophic hardware failures and monetary issues have cast a black shadow over their great achievements. Several satellite and Space Shuttle accidents and the exorbitant costs associated with those failures have placed the NASA community in a position where complacency must be questioned. Many of their programs are long running, the Space Shuttle's inaugural flight occurred on April 12, 1981, and are often in long periods of development; the Hubble Space Telescope was funded in the 1970's with a proposed launch date in 1983 only to eventually and faultily launch in 1990. NASA engineers seem to go through dips and waves of complacency. After a disaster, safety and checks and balances are ramped up, only to have them dip down due to budget concerns prior to another catastrophic accident.

Within the NASA community when catastrophic accidents occur, they often result in the complete destruction of the vehicle and loss of life; thus is the case for the Challenger and Columbia Space Shuttle Accident (Gehman, 2003). Before delving into the Challenger and Columbia disasters, it is important to understand the Space Shuttle System. The Space Shuttle is part of the national Space Transportation System designed to accommodate not only NASA's scientific research needs but also those of the Department of Defense and commercial payload sponsors. The Shuttle was coined as the first reusable launch vehicle and was comprised of three systems: the Orbiter, an expendable fuel tank carrying liquid propellants for the Orbiter's engines, and two recoverable Solid Rocket Boosters (NASA, 1986). The Shuttle was designed to launch like a rocket and land like an airplane. It is the only reusable spacecraft in the world capable of simultaneously putting a multiple-person crew and heavy cargo into orbit, of deploying, servicing, and retrieving satellites, and of returning the products of on-orbit research to Earth (Gehman, 2003). Figure 3 on the following page depicts an artist representation of the Space Shuttle System in its launch configuration (NASA, 1986).

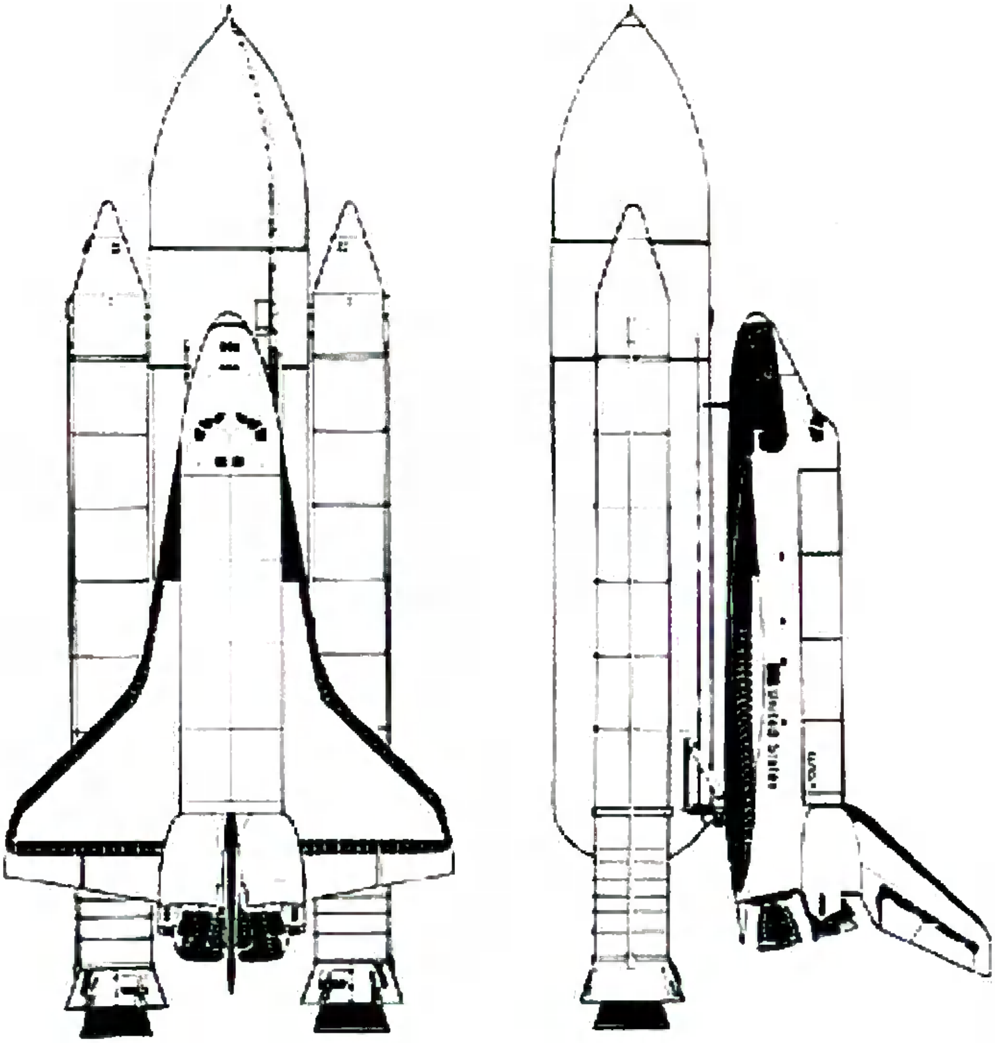


Figure 3: Space Shuttle System in Launch Configuration

4.1.1 Case Study 1: Space Shuttle Challenger Disaster

Challenger, the first of the Shuttle Accidents occurred on January 28, 1986. At this point, the Space Shuttle Program had launched 24 prior successful missions and all within a 57-month period (NASA, 1986). In fact, NASA was in the process of ramping up the number of Shuttle missions, originally contemplating an eventual rate of one mission a week, but quickly realized that was an unlikely scenario and set a goal in 1985 for an annual rate of 24 flights by 1990. With this ambitious goal a huge emphasis was placed on schedule and the Roger's Commission Report found that with the rapid succession of flights the current Shuttle Program requirements did not ensure that critical anomalies occurring during one flight are identified and addressed appropriately before the next flight. Complacency in ignoring these warning signs would be the downfall of Challenger and its crew.

The consensus of the Roger's Commission and other investigating agencies was that the Challenger disaster was caused by a failure of the joint between the two lower segments of the right Solid Rocket Motor at a mere 73 seconds into the flight. The joint failure was specifically caused by the destruction of the seals that are intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor. Evidence collected during the investigation showed that no other element of the Space Shuttle system contributed to the disaster (NASA, 1986). The Solid Rocket Booster is comprised of 7 subsystems: structure, thrust vector control, range safety, separation, electrical and instrumentation, recovery, and the Solid Rocket Motor. Figure 4 below shows an exploded view of the Solid Rocket Booster system (NASA, 1986):

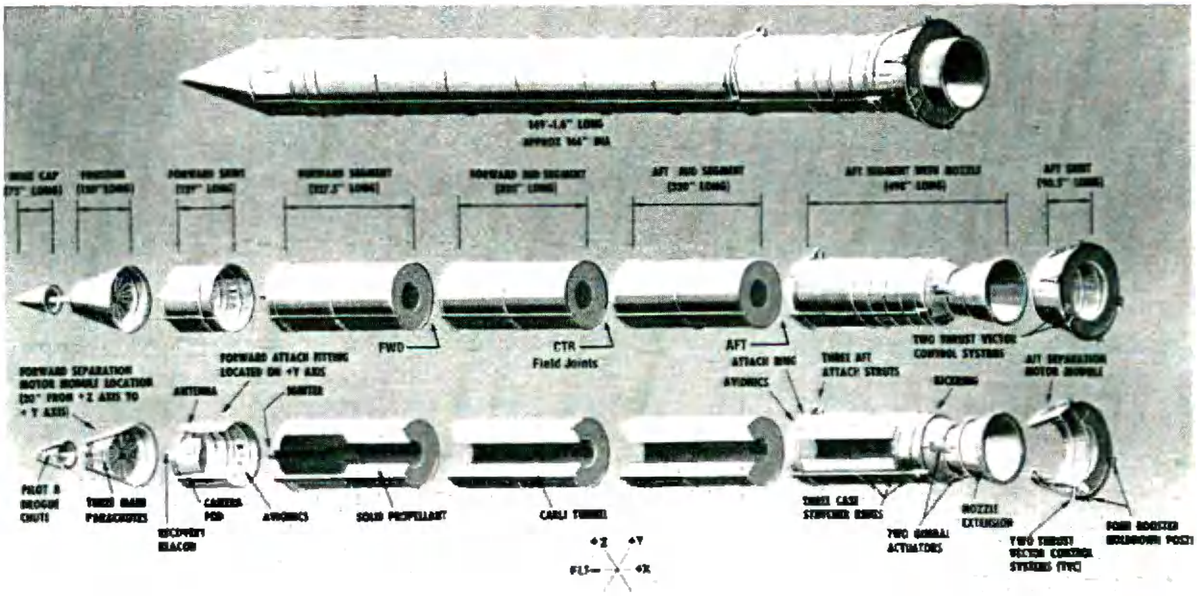
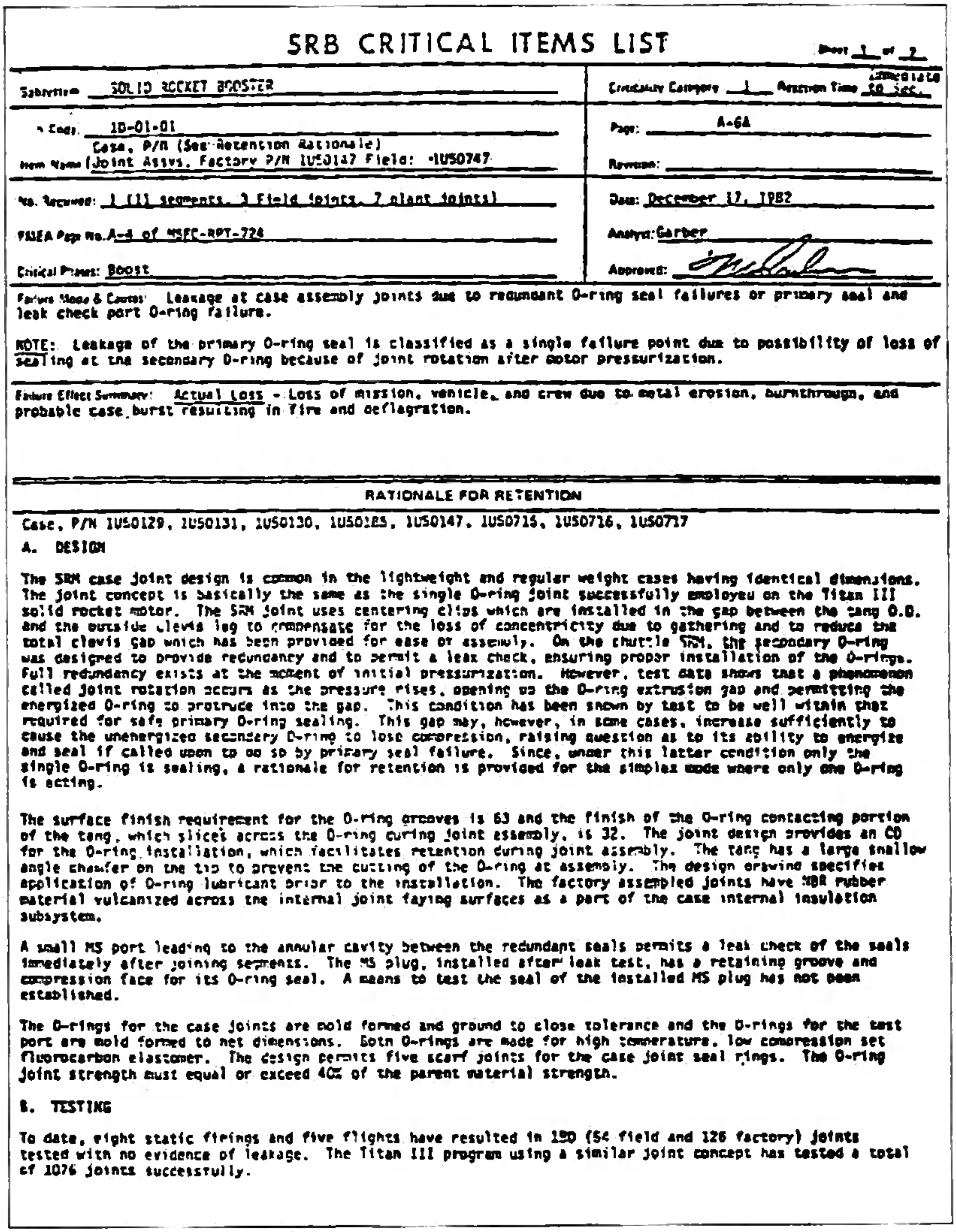


Figure 4: Exploded view of Solid Rocket Boosters

4.1.1.1 Factor 1: Unrealistic Risk Assessments

Reviewing technical data and eye witness accounts about the Challenger disaster it is very evident that the Space Shuttle Program was succumbing to complacency at the time of the accident; although complacency is never directly stated as a cause in the accident in the Roger's Commission Report. Several of the factors of complacency identified earlier are present and the first of these factors to be discussed is NASA and their contractor's generation of unrealistic risk assessments. While at the time of the accident, the SRB system was technically listed as a criticality 1, meaning loss of life or vehicle could occur if the system should fail, all problem reporting documentation from Morton Thiokol and NASA Marshall Space Flight Center listed the system as a criticality 1R, meaning that the system contained redundant components that if both were to fail could result in loss of life or vehicle (NASA, 1986). Figure 5 on the following page shows NASA's Critical Items List (CIL) of the SRB system representing the system as a criticality of 1 (NASA, 1986).



SRB CRITICAL ITEMS LIST

Sheet 1 of 2

Subsystem SOLID ROCKET BOOSTER

Criticality Category 1 Reaction Time Immediate 10 Sec.

Item Code 10-01-01

Page: A-6A

Item Name Case, P/N (See Retention Rationale) Joint Assys, Factory P/N 1U50147 Field: 1U50747

Revision:

No. Required: 1 (11 segments, 3 Field joints, 7 plant joints)

Date: December 17, 1982

FMEA Page No. A-4 of MSFC-RPT-724

Analyst: Garber

Critical Phase: Boost

Approved:

Failure Mode & Causes: Leakage at case assembly joints due to redundant O-ring seal failures or primary seal and leak check port O-ring failure.

NOTE: Leakage of the primary O-ring seal is classified as a single failure point due to possibility of loss of sealing at the secondary O-ring because of joint rotation after motor pressurization.

Failure Effect Summary: Actual Loss - Loss of mission, vehicle, and crew due to metal erosion, burnthrough, and probable case burst resulting in fire and deflagration.

RATIONALE FOR RETENTION

Case, P/N 1U50129, 1U50131, 1U50130, 1U50185, 1U50147, 1U50715, 1U50716, 1U50717

A. DESIGN

The SRM case joint design is common in the lightweight and regular weight cases having identical dimensions. The joint concept is basically the same as the single O-ring joint successfully employed on the Titan III solid rocket motor. The SRM joint uses centering clips which are installed in the gap between the tang O.D. and the outside clevis leg to compensate for the loss of concentricity due to gathering and to reduce the total clevis gap which has been provided for ease of assembly. On the shuttle SRM, the secondary O-ring was designed to provide redundancy and to permit a leak check, ensuring proper installation of the O-rings. Full redundancy exists at the moment of initial pressurization. However, test data shows that a phenomenon called joint rotation occurs as the pressure rises, opening up the O-ring extrusion gap and permitting the energized O-ring to protrude into the gap. This condition has been shown by test to be well within that required for safe primary O-ring sealing. This gap may, however, in some cases, increase sufficiently to cause the unenergized secondary O-ring to lose compression, raising question as to its ability to energize and seal if called upon to do so by primary seal failure. Since, under this latter condition only the single O-ring is sealing, a rationale for retention is provided for the simplex mode where only one O-ring is acting.

The surface finish requirement for the O-ring grooves is 63 and the finish of the O-ring contacting portion of the tang, which slices across the O-ring during joint assembly, is 32. The joint design provides an OD for the O-ring installation, which facilitates retention during joint assembly. The tang has a large shallow angle chamfer on the tip to prevent the cutting of the O-ring at assembly. The design drawing specifies application of O-ring lubricant prior to the installation. The factory assembled joints have NBR rubber material vulcanized across the internal joint faying surfaces as a part of the case internal insulation subsystem.

A small MS port leading to the annular cavity between the redundant seals permits a leak check of the seals immediately after joining segments. The MS plug, installed after leak test, has a retaining groove and compression face for its O-ring seal. A means to test the seal of the installed MS plug has not been established.

The O-rings for the case joints are mold formed and ground to close tolerance and the O-rings for the test port are mold formed to net dimensions. Both O-rings are made for high temperature, low compression set fluorocarbon elastomer. The design permits five scarf joints for the case joint seal rings. The O-ring joint strength must equal or exceed 40% of the parent material strength.

B. TESTING

To date, eight static firings and five flights have resulted in 180 (54 field and 126 factory) joints tested with no evidence of leakage. The Titan III program using a similar joint concept has tested a total of 1076 joints successfully.

Figure 5: Solid Rocket Booster CIL

This divide in criticality assumption produced the illusion that there was redundancy in the SRB system and therefore, may have lead to unrealistic risk based decision by management to launch Challenger. But where did this disconnect in actual criticality and perceived criticality assessment come from? The major problem with the Challenger SRB risk assessment is that it was apparent that neither NASA nor Thiokol fully understood the mechanism by which the joint sealing action of the SRB took place. The original criticality assessment of the solid rocket booster in 1980 was a criticality 1R; NASA fully believed that the secondary O-ring in the joint was a redundant component that would pressurize the SRB should the primary O-ring not seal. The 1980 criticality 1R solid rocket booster CIL specifically states:

"Redundancy of the secondary field joint seal cannot be verified after motor case pressure reaches approximately 40 percent of maximum expected operating pressure. It is known that joint rotation occurring at this pressure level with a resulting enlarged extrusion gap causes the secondary O-ring to lose compression as a seal. It is not known if the secondary O-ring would successfully reseal if the primary O-ring should fail after motor case pressure reaches or exceeds 40 percent of maximum expected operating pressure (NASA, 1986)."

The phrasing from the CIL directly shows that NASA was basing their flight readiness off of unrealistic risk assessments. They were operating under the assumption that the secondary O-ring would seal the solid rocket booster, even though they were unable to verify this phenomenon through testing. This unrealistic risk assessment carried out until November 1982, or through the first 5 Shuttle flights, when the CIL was updated to reflect that the system was in fact not redundant and had a criticality 1 function. Although an update in the CIL documentation had been made, the NASA community continued to represent the solid rocket joint O-ring seals as a redundant system.

NASA engineers and contractors were complacently accepting past risk assessments of criticality 1R as fact when evaluating flight readiness. It seems that NASA wasn't effectively communicating its updates in criticality so that the engineers and decision making management were educated. Testimony taken during the Roger's Commission interviews support the theory that NASA was evaluating mission readiness based on complacent, unrealistic risk analysis. For example, an interview with a Thiokol engineer, Howard McIntosh, after the Challenger accident went as follows (NASA, 1986):

Commission Question: [After the Criticality I classification], what did you think it would take to make [the joint seal] 1R?

Mr. McIntosh: I thought it was already 1R. I thought that after those tests that would have been enough to do it.

Commission Question: Well, you knew it was 1 but you were hoping for 1R?

Mr. McIntosh: Yeah, I was hoping for 1R, and I thought this test data would do it, but it didn't.

Even Marshall Solid Rocket Motor program management had the idea that they were operating with redundancy except for within exceptional cases. Dr. Judson Lovingood, manager of Marshall Solid Rocket Motor division told the Commission during post accident interviews (NASA, 1986):

" . . . [T]here are two conditions you have to have before you don't have redundancy. One of them is what I call a spatial condition which says that the dimensional tolerances have to be such that you get a bad stackup, you don't have proper squeeze, etc. On the O-ring so that when you get joint rotation, you will lift the metal surfaces off the O-ring. All right, that's the one condition, and that is a worst case condition involving dimensional tolerances.

"The other condition is a temporal condition which says that you have to be past a point of joint rotation, and of course, that relates back to what I just said.

"So first of all, if you don't have this bad stackup, then you have full redundancy. Now, secondly, if you do have the bad stackup, you had redundancy during the ignition transient up to the 170 millisecond point, whatever it is, but that is the way I understand the [Critical Items List]."

The biggest point to take away from these two separate interviews of both NASA management and Thiokol engineers is that both were working under the assumption that the system would be redundant based on design and not testing. Testing was not completed or had been unable to show that the Solid Rocket Booster seals were actually redundant in nature. However, some members of the NASA community, especially those in risk evaluation and decision making positions, were making uneducated launch decisions. Neither NASA nor Thiokol fully understood the mechanism by which the joint sealing action took place. This is seen through interviews with engineers who believed that they had a redundant system. Had the appropriate qualification testing been completed a better understanding of the non-redundant system could have been achieved. The Roger's Commission determined that overall the joint test and certification program was inadequate. Requirements to test the motor in flight configuration did not exist and with that, the motors were never tested in their vertical launch position but only in a static horizontal position. Early testing in the horizontal position showed that the joint performed in the exact opposite effect than what engineers at Thiokol had predicted, the joint was actually opening rather than closing. Although these initial findings were reported to the NASA program office, it was believed by Marshall that this wasn't really evidence of joint rotation and so the Solid Rocket Booster program continued as planned with no additional testing required. It wasn't until a 1980 Space Shuttle Verification/Certification Committee appointed by NASA for evaluation of flight worthiness was the inadequate testing given a second look. The Verification Committee discovered that the qualification of the joint testing was inadequate. From that, a recommendation was made to conduct full-scale tests to verify the field joint integrity and additionally perform the original hydroburst tests with one O-ring removed to verify redundancy. NASA program's final response on the matter was that initial testing (the testing which showed joint opening) was adequate and further testing was not required. Certification and testing aside, had the NASA community paid close attention to the hardware performance history, they would have clearly seen the correlation of O-ring damage to low launch temperatures.

4.1.1.2 Factor 2: Ignoring Warning Signs

The Challenger accident was shrouded by complacency. In addition to operating under unrealistic risk assessments, NASA and Morton Thiokol were also complacently ignoring the warning signs from previous flights and motor tests. The phenomenon of O-ring erosion and joint blow by which doomed the Challenger was nothing new to NASA with the launch of 51-L. As discussed previously, early tests showed the exact opposite of what engineers expected from the Solid Rocket Booster joint. Sealing of the joint is provided by two rubber O-rings that are installed during motor assembly. The O-ring static compression during and after assembly is determined by the gap between the tang and clevis of the joint. This gap at any location after assembly is influenced by the size and shape of the segments as well as their associated loads. Zinc chromate putty is applied to the composition rubber insulation face prior to installation. This putty was intended to act as a thermal barrier to prevent gases coming into contact with the O-rings. It was also intended that the O-rings be actuated and sealed by combustion gas pressure displacing the putty into the gap between the tang and clevis; a process known as pressure actuation (NASA, 1986). NASA and Morton Thiokol assumed that this pressure actuation process would occur, although they were unable to recreate in testing, and the gap opening was severely influenced by the external loads and joint dynamics; ultimately dooming the Challenger. Figure 6 on the following page shows the joint configuration of the solid rocket motor joint (NASA, 1986):

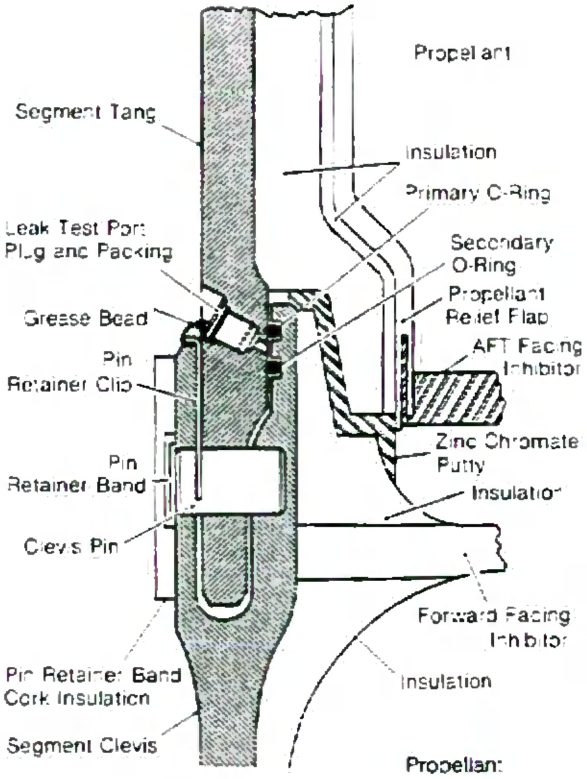


Figure 6: Solid Rocket Motor cross section shows positions of tang, clevis and O-rings. Putty lines the joint on the side toward the propellant

Issues with the joint separation and letting in hot gases wasn't something just seen during testing or limited to one motor or vehicle, it was a wide spread issue throughout the Shuttle fleet. Table 2 shows flight and test data of the Solid Rocket motors and the associated failures experienced (NASA, 1986).

Table 2: Flight and Test Data from Solid Rocket Booster Motors

Flight or Motor	Date	(Solid Rocket Booster)	Joint/O-Ring	Pressure (psi)		Erosion	Blow-by	Joint Temp °F
				Field	Nozzle			
DM-1	7/18/1977	-	-	NA	NA	-	-	84
DM-2	1/18/1978	-	-	NA	NA	-	-	49
DM-3	10/19/1978	-	-	NA	NA	-	-	61
DM-4	2/17/1979	-	-	NA	NA	-	-	40
QM-1	7/13/1979	-	-	NA	NA	-	-	83
QM-2	9/27/1979	-	-	NA	NA	-	-	67
QM-3	2/13/1980	-	-	NA	NA	-	-	45
STS-1	4/12/1981	-	-	50	50	-	-	66
STS-2	11/12/1981	(Right)	Aft Field/Primary	50	50	X	-	70
STS-3	3/22/1981	-	-	50	50	NA	NA	80
STS-4	6/27/1982	Unknown: hardware lost at sea		50	50	NA	NA	80
DM-5	10/21/1982	-	-	NA	NA	-	-	58
STS-5	11/11/1982	-	-	50	50	-	-	68
QM-4	3/21/1983	-	Nozzle/Primary	NA	NA	X	-	60
STS-6	4/4/1983	(Right)	Nozzle/Primary	50	50	-1	-	67
		(Left)	Nozzle/Primary	50	50	-1	-	67
STS-7	6/18/1983	-	-	50	50	-	-	72
STS-8	8/30/1983	-	-	100	50	-	-	73
STS-9	12/28/1983	-	-	100	100	-	-	70
STS 41-B	2/3/1984	(Right)	Nozzle/Primary	200	100	X	-	57
		(Left)	Forward Field/Primary	200	100	X	-	57
STS 41-C	4/6/1984	(Right)	Nozzle/Primary	200	100	X	-	63
		(Left)	Aft Field/Primary	200	100	-3	-	63
		(Right)	Igniter/Primary	NA	NA	-	X	63

STS 41-D	8/30/1984	(Right)	Forward Field/Primary	200	100	X	-	70
		(Left)	Nozzle/Primary	200	100	X	X	70
		(Right)	Igniter/Primary	NA	NA	-	X	70
STS 41-G	10/5/1984	-	-	200	100	-	-	67
DM-6	10/25/1984	-	Inner Gasket/Primary	NA	NA	X	X	52
STS 51-A	11/8/1984	-	-	200	100	-	-	67
STS 51-C	1/24/1985	(Right)	Center Field/Primary	200	100	X	X	53
		(Right)	Center Field/Secondary	200	100	-4	-	53
		(Right)	Nozzle/Primary	200	100	-	X	53
		(Left)	Forward Field/Primary	200	100	X	X	53
		(Left)	Nozzle/Primary	200	100	-	X	53
STS 51-D	4/12/1985	(Right)	Nozzle/Primary	200	200	X	-	67
		(Right)	Igniter/Primary	NA	NA	-	X	67
		(Left)	Nozzle/Primary	200	200	X	-	67
		(Left)	Igniter/Primary	NA	NA	-	X	67
STS 51-B	4/29/1985	(Right)	Nozzle/Primary	200	100	X	-	75
		(Left)	Nozzle/Primary	200	100	X	X	75
		(Left)	Nozzle/Primary	200	100	X	-	75
DM-7	5/9/1985	.	Nozzle/Primary	NA	NA	X	-	61
STS 51-G	6/17/1985	(Right)	Nozzle/Primary	200	200	X5	X	70
		(Left)	Nozzle/Primary	200	200	X	X	70
		(Left)	Igniter/Primary	NA	NA	-	X	70
STS 51-F	7/29/1985	(Right)	Nozzle/Primary	200	200	-6	-	81
STS 51-I	8/27/1985	(Left)	Nozzle/Primary	200	200	X7	-	76
STS 51-J	10/3/1985		-	200	200	-	-	79
STS 61-A	10/30/1985	(Right)	Nozzle/Primary	200	200	X	-	75

		(Left)	Aft Field/Primary	200	200	-	X	75
		(Left)	Center Field/Primary	200	200	-	X	75
STS 61-B	11/26/1985	(Right)	Nozzle/Primary	200	200	X	-	76
		(Left)	Nozzle/Primary	200	200	X	X	76
STS 61-C	1/12/1986	(Right)	Nozzle/Primary	200	200	X	-	58
		(Left)	Aft Field/Primary	200	200	X	-	58
		(Left)	Nozzle/Primary	200	200	-	X	58
STS 51-L	1/28/1986	.	.	200	200	.	.	31

Dash (-) denotes no anomaly.

NA denotes not applicable.

1 On STS-6, both nozzles had a hot gas path detected in the putty with an indication of heat on the primary O-ring.

2 On STS-9, one of the right Solid Rocket Booster field joints was pressurized at 200 psi after a destack.

3 On STS 41-C, left aft field had a hot gas path detected in the putty with an indication of heat on the primary O-ring.

4 On a center field joint of STS 51-C, soot was blown by the primary and there was a heat effect on the secondary.

5 On STS 51-G, right nozzle has erosion in two places on the primary O-ring.

6 On STS 51-F, right nozzle had hot gas path detected in putty with an indication of heat on the primary O-ring.

7 On STS 51-I, left nozzle had erosion in two places on the primary O-ring.

Looking at the flight data above it can be seen that there was an increasing trend in O-ring failures. NASA and Morton Thiokol personnel failed to see the warning signs of their hardware. A research into the flight history of the solid rocket motor would have shown the engineers that there was a problem with performance of the O-rings. Instead NASA and Morton Thiokol just began to accept that O-ring blow back was an acceptable and unavoidable flight risk. Complacency in problem reporting and corrective action may have been one of the factors that led to this type of failure being an acceptable risk. Ineffective problem reporting for analysis purposes can wreak havoc on the efficiency with which engineers and program management are able to evaluate mission risk.

With the lack of evaluation of post flight failures or anomalies prior to the next mission, it is apparent that NASA was experiencing difficulties with their problem reporting methods. At the time of the Challenger accident NASA did not have a concise problem reporting method. It was broken up in several documents and there was little agreement between sites to which method was the correct philosophy. Complacency in requirements development for problem reporting left a gaping hole for failures and anomalies to go, not unnoticed, but unevaluated appropriately for risk purposes. A cursory view of the data in a tabulated format (see Table 2) quickly shows a trend that failure of the solid rocket motor O-ring failures were increasing and engineers should have been reacted. Development of trend data between reported failures is a standard practice that is an expected function of a successful system safety program. In 1984, the Shuttle Program began to see a large upturn in the number of O-ring anomalies reported; going from one in nine missions prior to 1984 to more than a fifty percent occurrence rate after that date. Wiley Bunn, director of Reliability and Quality Assurance at Marshall, when interviewed for the Roger's Commission Report all but says the word "complacency" when talking about their lack of trending and risk-based failure analysis: "I agree with you from my purview in quality, but we had that data. It was a matter of assembling that data and looking at it in the proper fashion. Had we done that, the data just jumps off the page at you (NASA, 1986)." This laxness in problem reporting data evaluation should have been one of the first red flags that the Space Shuttle Program was slipping into a complacent nature. Ultimately, Challenger and several of the other missions prior should not have been launched without the proper evaluation into the reoccurring O-ring failures.

4.1.1.3 Factor 3: Assuming Risk Decreases Over Time

The assumption that risk decreases over time or the opinion "well we got away with it last time" is one of the factors of complacency and was present up to the Challenger accident. It is quite possible that one of the reasons that proper failure investigation and corrective action was not taken through the problem reporting process is because engineers had settled on the mindset that risk decreases over time. In the case of Challenger, NASA and Thiokol continued to accept escalating risk because with each incident prior to Challenger they had a successful launch. Commissioner Feynman, a member of the Roger's Commission, stated in the report that NASA was operating the Space Shuttle as "a kind of Russian roulette…[The Shuttle] flies [with O-ring erosion] and nothing happens. Then it is suggested, therefore, that the risk is no longer so high for the next flights. We can lower our standards a little bit because we got away with it last time…. You got away with it but it shouldn't be done over and over again like that (NASA, 1986)." The striking part of this quote is not just that the Commissioner calls them out on assuming that their risk decreased because they "got away with it" but that he calls them out for continually applying that philosophy. When flights are continually flawless or hardware continues to perform without incident engineers begin to become complacent with the capabilities of their systems. NASA and Morton Thiokol may have built up the capabilities of the Solid Rocket Motor system too much and eventually became complacent that they would be capable of a safe launch each mission.

4.1.1.4 Factor 4: Ignoring high-consequence, low-probability events

In January 1985, when STS 51-C returned with significant O-ring damage, engineers recognized that there was a need to collect and study data on the relationship between cold temperatures and o-ring erosion (Gehman, 2003). STS 51-C remained on the launch pad for three straights days in uncharacteristically freezing Florida temperatures prior to launching. Upon its return, it was noticed that the damage had blown by the primary O-ring and there was evidence of heat effect on the secondary. While engineers recognized the need to study cold effect on the joint, this study was thought of as a low priority because at the time the O-ring was still, incorrectly, viewed as a redundant system. Furthermore, engineers also believed that a reappearance of freezing temperatures was a low probability event (Gehman, 2003).

A need to evaluate temperatures and recurring O-ring damage was recognized by engineers and subsequently ignored or given extremely low probability. Even though O-ring erosion was deemed a catastrophic event, improper fault tolerance categorization left engineers complacent with the way in which their system was operating. Ignoring high-consequence, low-probability events such as launch in low temperatures and subsequent O-ring degradation can lead to catastrophic events such as the Challenger disaster. In hindsight, the engineers recognized the need to test but when the time came to evaluate launch of STS 51-L, the data had yet to be analyzed and management was forced to make an uninformed risk-based decision to launch.

4.1.1.5 Results

Seven lives were lost the day that Challenger exploded just 73 seconds into its launch from Cape Canaveral. While the NASA community has not come and blatantly said that the Challenger accident was caused by complacency, evidence collected from interviews and information provided by NASA shows that it was. Unrealistic risk assessments, ignoring warning signs, and assuming that risk decreases with each occurrence fed into the complacency that engineering and management were exuding. After the accident NASA pledged to learn from their mistakes and make a beef up to their system safety program. While this did occur and a scrub of all the Failure Modes and Effects Analysis did occur, how long can a complacent nature be subdued if a constant attention to combating complacency is not made? Table 3 on the following page provides an overview of the discussed factors of complacency and the associated events of those factors.

Table 3: Overview of Challenger Case Study Complacency Factors and Events

CHALLENGER COMPLACENCY FACTORS AND EVENTS		
Factors:	**Events:**	**Outcome:**
Unrealistic Risk Assessments	• SRB system criticality was treated as a criticality 1R, meaning redundancy, even though it was analyzed and recorded in a FMEA as a criticality 1 system. • NASA failed to effectively communicate change in criticality from 1R to 1. • Problem Reporting reports were not reviewed effectively for the SRB joint. Numerous failures were reported and that data was not correlated or used for launch decisions. • Qualification of the joint testing was inadequate	• NASA management made the decision to launch with flawed risk assessment data.
Ignoring Warning Signs	• O-rings were to be actuated and sealed by a process known as pressure actuation. NASA and Morton Thiokol assumed that this pressure actuation process would occur, although they were unable to recreate in testing. • O-ring erosion had occurred on previous flights prior to 51L. • Lack of evaluation of post flight failures or anomalies prior to the next mission. A correlation to O-ring erosion and cold temperatures was missed.	• Ineffective problem reporting for analysis purposes created insufficient data for engineers and program management to evaluate mission risk.
Assuming Risk Decreases Over Time	• SRB system continued to operate in an unacceptable state (o-ring erosion) even though the phenomenon was known. • Continued mission success supports the "we got away with it last time" mentality of engineers and management.	• Proper failure investigation and corrective action was not taken through the problem reporting process is because engineers had settled on the mindset that risk decreases over time. • Ineffective problem reporting for analysis purposes created insufficient data for engineers and program management to evaluate

		mission risk.
Ignoring high-consequence, Low probability Events	• In January 1985, engineers recognized that there was a need to collect and study data on the relationship between cold temperatures and o-ring erosion but this was placed on the low priority list. • Engineers believed that a reappearance of freezing temperatures, which were thought to be the trigger to O-ring erosion, was a low probability event.	• Engineers did not complete the O ring cold temperature study. • When the time came to make launch decisions for STS 51L, there was a lack of data for making the risk-based choice to launch.

4.1.2 Case Study 2: Space Shuttle Columbia Disaster

In 1995 NASA, at the request of Administrator Chris Kraft, formed a review team for the Space Shuttle Program to propose a new management system that could significantly reduce operating costs; the technical report generated from this review team would eventually be known as the Kraft Report. The review team was composed of a group of people "with broad and extensive experience in spaceflight and related areas" and the major idea formed from this review was that the "shuttle [had] become a mature and reliable system, and-in terms of a manned rocket-propelled space launch system-is about as safe as today's technology will provide (Kraft, 1995)." In the author's opinion, the assumptions from the Kraft report set the stage for a complacent mindset to develop within the NASA community. The Kraft report makes the assumption that the shuttle is a mature and reliable system, thus lulling engineers into the "why change" mentality. Why improve a system design or add redundancy if you have determined that you are "as safe as technology will provide"?

While there was dissent to the claims in the Kraft report, the NASA community had begun to slack since the Challenger accident and was spiraling toward another catastrophic accident, Columbia. In 2001, just a couple years prior to the Columbia accident, then Deputy Associate Administrator for Space Flight William Readdy indicated the assumptions of safety that NASA was operating under at that time by saying:

"The Space Shuttle has made dramatic improvements in the capabilities, operations and safety of the system. The payload-to-orbit performance of the Space Shuttle has been significantly improved – by over 70 percent to the Space Station. The safety of the Space Shuttle has also been dramatically improved by reducing risk by more than a factor of five. In addition, the operability of the system has been significantly improved, with five minute launch windows – which would not have been attempted a decade ago – now becoming routine. This record of success is a testament to the quality and dedication of the Space Shuttle management team and workforce, both civil servants and contractors (Readdy, 2001)."

This shows another example of the implied safety of the space shuttle program through citing of mission success and reduction in risk. These generalizations are made with no true data to back them up other than an accident has not occurred; mission success cannot be used as the sole factor in determining a safe program. Review after the Columbia accident revealed several holes within NASA's safety assessments. Ultimately the CAIB report determined that one of the major factors leading to the Columbia accident was that NASA's safety culture had become "reactive, complacent, and dominated by unjustified optimism (Gehman, 2003)."

The Space Shuttle Columbia, STS-107, was launched on January 16, 2003 and broke apart on re-entry on February 1, 2003. The cause of the Columbia Accident, per the Columbia Accident Investigation Board (CAIB) review, was a breach in the Thermal Protection System on the leading edge of the left wing. The breach was initiated by a piece of insulating foam that separated from the left bipod ramp of the External Tank and struck the wing in the vicinity of the lower half of Reinforced Carbon-Carbon (RCC) panel 8 at 81.9 seconds after launch on January 16, 2003. During re-entry, the breach in the Thermal Protection System (TPS) allowed superheated air to penetrate the leading edge of the wing and melt the aluminum structure. This resulted in a weakening of the structure until increasing dynamic forces cause a loss of control scenario, failure of the wing, and subsequent breakup of the Orbiter (Gehman, 2003).

During re-entry the Orbiter is subjected to temperatures as high as 3,000 degrees Fahrenheit. In order to protect the crew and Orbiter aluminum structure during these extreme superheated temperatures, the Orbiter is covered by various materials which make up the TPS. The TPS system is made up of heat resistant tiles, blankets, and RCC panels on the wing and nose leading edge. The RCC panels, which protect those areas susceptible to the highest heat, are comprised of special graphite cloth that is molded to specific shapes for Orbiter placement (NASA KSC, 2006).

While the tragic demise of the Columbia seemed to occur very quickly over the short re-entry period, it was just the culmination of several weeks of complacent engineering evaluations on the Orbiter TPS. As is standard with previous flights prior to STS-107, high resolution video footage of the liftoff was evaluated the following day. This video footage showed that Columbia had experienced a debris strike to the left wing at 81.9 seconds after launch from an object off the External Tank. Those who evaluated the video were concerned by the objects large size and apparent momentum and with that believed that Columbia may have sustained damage that could not be seen on the limited footage available from launch. Based on their concerns the launch photo review team prepared a report and video clip and sent them to the Mission Management Team, Mission Evaluation Room, and engineers at United Space Alliance and Boeing. This was NASA's first chance to properly evaluate the risk associated with the debris strike for re-entry; however senior NASA officials refused to further image Columbia tile damage based on previous flight history success. And thus began the last, of many, complacent acts on the part of engineers and management that would lead to the demise of Columbia.

4.1.2.1 Factor 1: Unrealistic Risk Assessments

It was a series of low probability, high risk failures that led to the demise of the Columbia. Engineers based assumptions off of unrealistic risk assessment and discounted the multiplied risk associated with these occurrences, thus not fully understand the implications of External Tank foam shedding. While the probability of foam shedding from the External Tank was nothing new to engineers at NASA, the risk of damage due to it was still considered a low probability event. Engineers believed that aerodynamic drag generated during launch made it so that any debris expelled from the vehicle would pull away from Orbiter striking distance. Even so, engineers believed that if a debris strike were to occur the likelihood of catastrophic damage would be minimal (Gehman, 2003). This idea was based off of TPS tile analysis conducted using a modeling program referred to as Crater. Crater predicted damage depth by using a specially developed algorithm; however, this mathematical software was developed for smaller size pieces of debris, not 20 inch by 10 inch by 6 inch pieces of debris as was estimated for Columbia. Prior to the Columbia accident, Crater was used to evaluate small debris strikes such as ice shed from the External Tank during launch. The use of this program to assess the foam strike during STS-107 was the first use of the model while a mission was on orbit (Gehman, 2003). The biggest flaw in using this program to buy off risk was that engineers used it inappropriately to evaluate debris 640 times larger in volume that what the model was calibrated for (Gehman, 2003). Figure 7 gives a visual representation of the size disparity when analyzing the Columbia foam debris (Gehman, 2003):

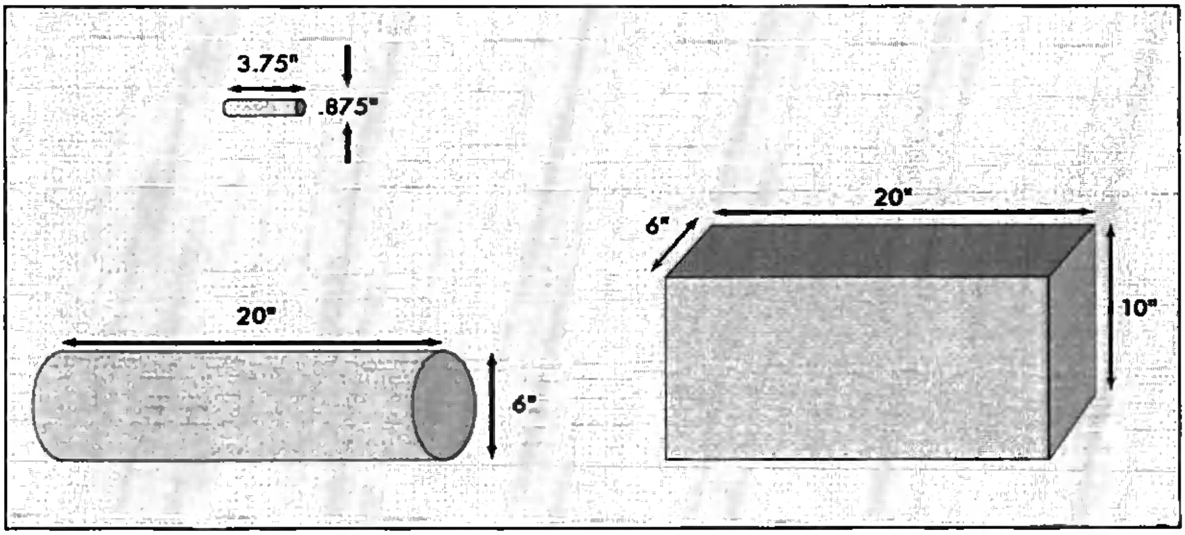


Figure 7: The small cylinder at top illustrates the size of debris Crater was intended to analyze. The larger cylinder was used for the STS-107 analysis; the block at right is the estimated size of the foam.

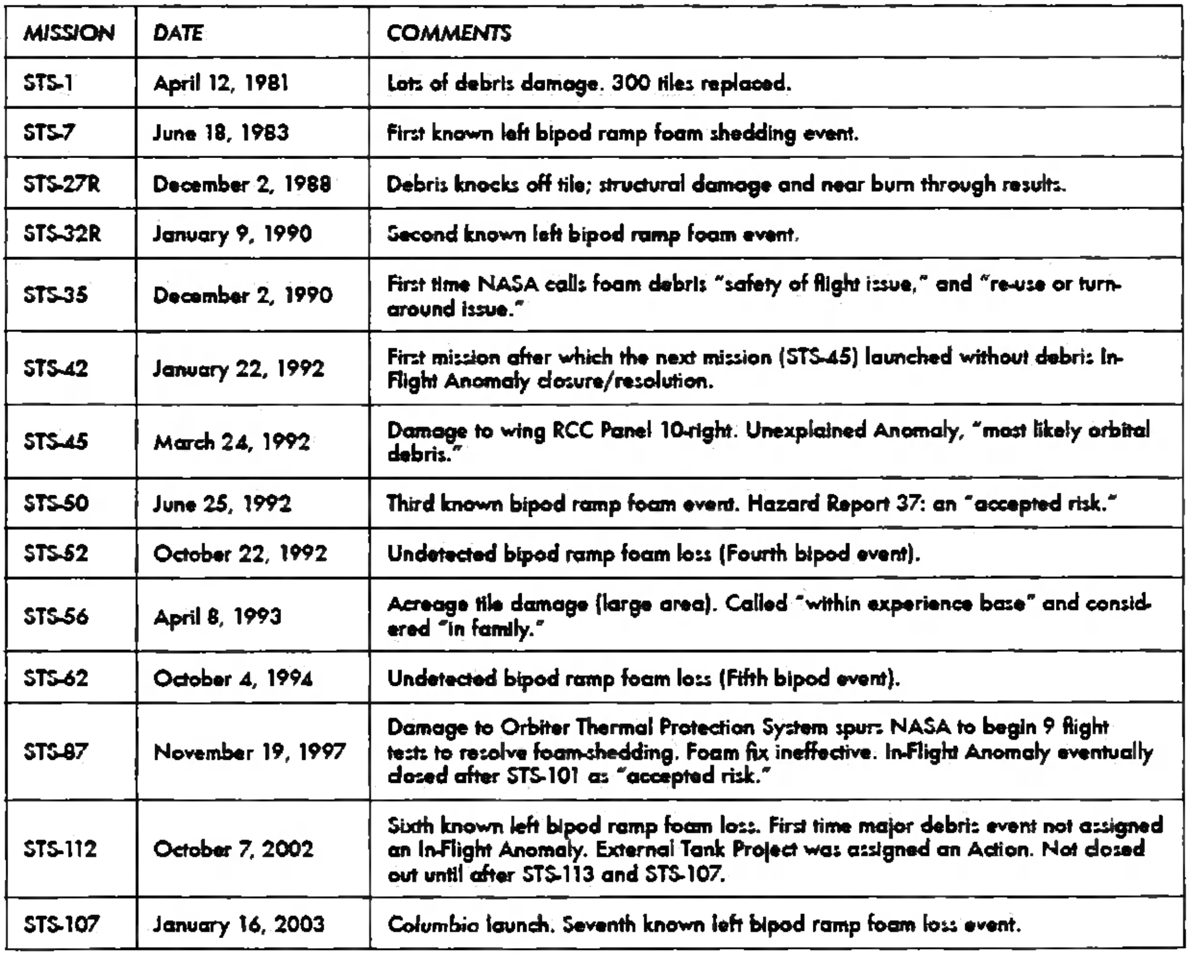
Comparing the specimen size used for Crater calculation versus the estimated debris size, it was clear that the NASA Debris Assessment Team engineers were not able to accurately depict Orbiter damage, leading to unrealistic risk assessments. The Crater system predicted that damage to the Orbiter tile would be thicker than that of the tile thickness. This indicates that the debris that struck Columbia would have exposed the aluminum structure beneath the tile, creating a dangerous entry point for hot gases or burn through during re-entry (Gehman, 2003). However, the engineers assigned to assess the Crater data discounted the possibility of burn through for two reasons. First, the results of calibration tests with small projectiles that Crater typically predicted a deeper penetration than would actually occur. Second, the Crater algorithm did not take into account that the tile contained a lower "densified" layer, which is considerably stronger than the tile skin (Gehman, 2003). It is evident that the engineers assessing the damage to Columbia were in over their heads. Investigation proceedings from the CAIB point out that "Crater was designed for "in-family" impact events and was intended for day-of-launch analysis of debris impacts. It was not intended for large projectiles like those observed on STS-107. Crater initially predicted possible damage, but the Debris Assessment Team assumed, without theoretical or experimental validation, that because Crater is a conservative tool – that is, it predicts more damage than will actually occur – the debris would stop at the tile's densified layer, even though their experience did not involve debris strikes as large as STS-107's." This shows that risk assessments were unrealistic. Engineers were using tools not designed for their specific type of anomaly and were complacently relying on incorrect tools and inexperience to make risk-based decisions.

4.1.2.2 Factor 2: Ignoring Warning Signs

Like discussed with the Challenger disaster, NASA had a resurgence of the complacency factor of ignoring warnings signs ahead of the Columbia accident. The shedding of foam debris during launch was not a new phenomenon to NASA officials; it had actually been seen on 80 percent of the 79 missions for which launch imagery was available (Gehman, 2003). With the echoes of Challenger less than twenty years prior, why would engineers again ignore the warning signs that a catastrophic event may be on the horizon? Like with Challenger, engineers involved with the STS-107 accident were dealing with an inefficient problem reporting system. Although significant changes in problem reporting methodology had been accomplished since 1986, the new database systems used were cumbersome and made evaluating risk difficult. The biggest issue, again echoes of Challenger, was that the various NASA centers were not all using the database uniformly and could not all access each other's data (Gehman, 2003). This made trending of the External Tank debris shedding and External Tank foam anomalies difficult to accomplish. The database itself was also found to be very incomplete as far as TPS strikes. Only strikes that were declared "In-Flight Anomalies" were added to the problem reporting database which masked the true extent of debris strikes to the TPS system and made trending difficult (Gehman, 2003). Adding to a lack in trending capability for risk analysis, the CAIB found that a large number of the hazard statement for the anomalies or failures in the database contained subjective and qualitative judgments such as "believed" and "based on experience from previous flights this hazard is an Accepted Risk (Gehman, 2003)." It should be noted that problem reporting inefficiencies is a reoccurring theme within the NASA community and within their programs which have experienced catastrophic failures. Problem reporting and the way in which those failures are analyzed and relayed to management, is one of the critical components of a successful safety program. NASA's failure to correct their reporting inefficiencies after Challenger ultimately reared its ugly head again in Columbia. Complacency in accepting failure data as "in-family", failing to record failures, or lack of trending leads to missed opportunities for safety measures and risk reduction.

One area in particular caused the most issues with regards to external tank foam shedding; the bipod ramp. The bipod ramp is the area in which the external tank attaches to the underbelly of the Orbiter. In this area, foam is sprayed by hand and then it is manually shaved into a ramp shape once it has fully cured. Although this area was given special attention for foam application, it became the most likely point of foam shedding during Orbiter disconnect. Of the known foam debris strikes, 7 of those were as a result of foam shedding from the bipod ramp. Table 4 below shows the missions which had what was deemed significant thermal protection damage due to debris strikes and the associated NASA comments on that debris (Gehman, 2003).

Table 4: Missions with Thermal Protection System damage or Significant Foam Loss



MISSION	*DATE*	*COMMENTS*
STS-1	April 12, 1981	Lots of debris damage. 300 tiles replaced.
STS-7	June 18, 1983	First known left bipod ramp foam shedding event.
STS-27R	December 2, 1988	Debris knocks off tile; structural damage and near burn through results.
STS-32R	January 9, 1990	Second known left bipod ramp foam event.
STS-35	December 2, 1990	First time NASA calls foam debris "safety of flight issue," and "re-use or turn-around issue."
STS-42	January 22, 1992	First mission after which the next mission (STS-45) launched without debris In-Flight Anomaly closure/resolution.
STS-45	March 24, 1992	Damage to wing RCC Panel 10-right. Unexplained Anomaly, "most likely orbital debris."
STS-50	June 25, 1992	Third known bipod ramp foam event. Hazard Report 37: an "accepted risk."
STS-52	October 22, 1992	Undetected bipod ramp foam loss (Fourth bipod event).
STS-56	April 8, 1993	Acreage tile damage (large area). Called "within experience base" and considered "in family."
STS-62	October 4, 1994	Undetected bipod ramp foam loss (Fifth bipod event).
STS-87	November 19, 1997	Damage to Orbiter Thermal Protection System spurs NASA to begin 9 flight tests to resolve foam-shedding. Foam fix ineffective. In-Flight Anomaly eventually closed after STS-101 as "accepted risk."
STS-112	October 7, 2002	Sixth known left bipod ramp foam loss. First time major debris event not assigned an In-Flight Anomaly. External Tank Project was assigned an Action. Not closed out until after STS-113 and STS-107.
STS-107	January 16, 2003	*Columbia* launch. Seventh known left bipod ramp foam loss event.

While there were numerous foam shedding events, the debris strike damage of STS-107 was foreshadowed by that of Atlantis (STS-27R) launched in December of 1988. The Atlantis had a large debris strike of its TPS occur 85 seconds into launch similar to that of Columbia. However, the way in which these two similar events were handled is a prime example of complacency on the part of Columbia engineers and how they ignored warning signs. When the debris strike was discovered on STS-27R engineers asked that the flight crew inspect for damage to Atlantis on flight day 2 with a camera mounted on the Shuttle robotic arm. Mission Commander R.L. Gibson described the damage he as looking "like it had been blasted by a shotgun (Gehman, 2003)." The Atlantis had lost one complete tile and had 707 dings, 298 of which were greater than an inch in diameter. The extent of the damage was concentrated where the liquid oxygen umbilical line connects prior to launch, which, was an area that had been better reinforced with thick aluminum structural plates. If not for the aluminum plate, based on engineering analysis a burn through would occur. STS-27R re-entered the Earth's atmosphere safely but engineers were "surprised by the damage" and post-mission inspections deemed it "the most severe of any mission yet flown (Gehman, 2003)."

In contrast to STS-27R, Columbia engineers and management never directed the crew to examine the damage. This may have been in part to the mission objectives and the fact that a robotic arm was not installed on this flight. STS-107 was a scientific mission which meant that it was at an orbit of 39 degrees without access to the International Space Station and without an installed robotic arm. It may have been the fact that the robotic arm was not installed this mission that engineers did not push for immediate crew imaging, or maybe it was that they were complacently comfortable with the results from STS-27R's successful re-entry. Either way, the debris strike and resulting damage on STS-27R was a significant warning sign to what debris impact could do to the vehicle.

4.1.2.3 Factor 3: Ignoring high-consequence, low-probability events

While debris impact from external tank foam shedding had been seen on previous flights, it was believed that the likelihood of catastrophic damage due to that debris shedding was a low probability event. Of the known bipod foam shedding occurrences, when STS-112 returned from orbit in October 2002 engineers were shocked at the extensive damage that the orbiter experienced from a single piece of external tank foam. Even though the extent of the damage was concerning to engineers it was concluded that the STS-112 foam hit was not a threat to flight safety (Gehman, 2003). This was based on the logic that while the foam debris was large and there was damage, no serious consequences occurred. Engineers became complacent with the foam debris as a "nagging issue" and concluded that a hit as large as the one that occurred on STS-112 was a low-probability event. To further add to the complacency even though STS-112 had suffered the most extensive damage to date, it was the first major debris event to not be assigned an In-flight anomaly which would require risk analysis and closure prior to the launch of the next vehicle. NASA took no immediate action to improve the launch imagery and also no actions to reduce the risk of foam shedding from the bipod ramp; that is, until after the Columbia disaster.

Ignoring high-consequence, low-probability events such as large debris strikes can lead to catastrophic disasters. That is true of Columbia. Flight Readiness Reviews and managerial buy-offs were taken on a case by case basis and the probability of a large debris impact was considered remote. The idea that a large debris impact was remote was based on flawed imagery data and the fact that mission success had occurred even with large debris damage.

4.1.2.4 Results

The second catastrophic Shuttle accident claimed an additional seven lives with the loss of the Columbia. NASA fell back into their complacent behaviors after several successful missions post Challenger. Resurgence in unrealistic risk assessment, ignoring warning signs, and ignoring high-consequence low-probability events led NASA engineers down the same path that they experienced in 1986. While the events of Columbia and Challenger are different, the complacency factors are strikingly similar. Table 5 on the following page provides an overview of the discussed factors of complacency and the associated events of those factors.

Table 5: Overview of Columbia Case Study Complacency Factors and Events

COLUMBIA COMPLACENCY FACTORS AND EVENTS		
Factors:	**Events:**	**Outcome:**
Unrealistic Risk Assessments	• NASA Debris Assessment Team engineers were not able to accurately depict Orbiter damage.	• Inadequate debris damage leads to unrealistic risk assessments
Ignoring Warning Signs	• Shedding of foam debris during launch was not a new phenomenon to NASA officials; it had actually been seen on 80 percent of the 79 missions for which launch imagery was available. • Lack in trending capability for risk analysis. • Columbia engineers and management never directed the crew to examine the damage.	• Failure to accurately evaluate problems and implement corrective actions for foam shedding leads to lax approach to Columbia debris damage assessments.
Ignoring high-consequence, Low probability Events	• STS-112 foam hit deemed not a threat to flight safety based on the logic that while the foam debris was large and there was damage, no serious consequences occurred. • Idea that a large debris impact was remote was based on flawed imagery data and the fact that mission success had occurred even with large debris damage.	• NASA took no immediate action to improve the launch imagery and also no actions to reduce the risk of foam shedding from the bipod ramp; that is, until after the Columbia disaster.

4.1.3 Case Study 3: Satellite Programs, Mars Polar Lander

NASA not only has had catastrophic events in the Manned Space Flight Program but also throughout their satellite programs. In a report generated by Professor Nancy G. Leveson for the Massachusetts Institute of Technology for AIAA, software-related accidents of four different NASA satellites (Ariane 5, Mars Climate Orbiter, Mars Polar Lander, and the Titan IV/Milstar) are examined to create an accident model and look for root causes for software failures. Of the three main common root causes determined for the four accidents (flaws within the safety culture, ineffective organizational structure and communication, and ineffective or inadequate technical activities), each has an underlying contributing factor of overconfidence and complacency (Leveson, 2001). For the purpose of this thesis the focus will be on the Mars Polar Lander.

The Mars Surveyor '98 program was comprised of two separated spacecraft, the Mars Climate Orbiter (MCO) and the Mars Polar Lander (MPL). These two missions were designed to study the weather, climate, and water and carbon dioxide content on Mars. This was being done in order to understand the Martian planet as well as search for evidence of long-term and episodic climate changes (NASA JPL, 2000). The MPL was supposed to land on the southern polar layer, near the Martian south pole, but all telemetry on December 3, 1999 was lost upon atmospheric entry. While the exact cause of the communication loss of the MPL is not known, investigation following the loss concluded that the cause was most likely a software error that mis-identified vibrations caused by the deployment of the Lander's legs as the vehicle touched down on the Martian surface. This software failure resulted in spacecraft shutting down the vehicle's decent engines while still 40 meters above the surface (NASA JPL, 2000).

4.1.3.1 Factor 1: Ignoring Warning Signs

The software failure that was the demise of the MPL was actually a known phenomenon amongst the software engineers. Although the false indication during the deployment leg was known prior to launch, software engineering analysis and design did not account for the phenomenon. The warning sign for a catastrophic failure of the spacecraft was in front of the engineers on the MPL project the entire time; they knew that a false indication existed. Was it complacency in their ability to produce aircraft that made them ignore this particular warning sign? With the known design flaw, the loss of the MPL must stem from an inadequate control over the development process. Risk was not adequately managed in the design and implementation processes. The Jet Propulsion Laboratory (JPL) investigation committee that convened post MPL loss, noted in their investigation that the system level requirements document did not specifically state the failure modes that the requirement was protecting against (for example a sensor failure) and therefore they speculate that the software designers or one of the reviewers might have discovered the missing software requirement had they been made aware of the rationale underlying the system requirement (NASA JPL, 2000).

4.1.3.2 Factor 2: Assumption that Risk Decreases over time

The complacency shown on the Mars Surveyor program can be considered a combination of two major factors: ignoring warning signs and assuming that risk decreases over time. The assumption that risk decreases over time is seen in the fact that corners were cut during the development of system level requirements; ultimately setting the program up for failure. NASA had launched many successful satellite programs and why should they believe that the MPL should be any different. NASA had become complacent in their requirements development process and with that ignored the warning sign that a potential issue existed within the software. For all accounts, the MPL system worked exactly as it had been designed and without failure, it was the complacent omission of proper risk assessments that allowed this to occur.

A very superficial hazard analysis had been conducted for the software portion of the MPL. The JPL report identifies the only software hazard identified for the program was "Flight software fails to execute properly" and this is labeled as common through all phases of flight; problem is, the software performed just as it was designed. This hazard provides no useful information to the software engineers when developing. Obviously they want the software to execute properly, but what if operating properly means causing irreversible or catastrophic damage to the system? For hardware hazard analysis purposes it would be more common to see more specific hazards such as "line rupture" and a hazard such as "hardware fails to operate properly" would never be an acceptable analysis. Why does it not function properly? Is it because of a propellant line rupture or a premature commanding of engine shutoff? From the JPL failure report, it is apparent that the engineers did not perform proper hazard analysis and develop software fault trees past "software fails to execute properly." This appears to be commonplace for satellite systems because companies often times reuse script from previous programs and tailor those to meet their new requirements; following the philosophy, we have been successful before and will be again. If a proper fault tree had been completed, not one where software is defined as a base event which requires no further analysis, it is possible that the missing software requirements may have been identified. For example, instead of saying simply that the software must work properly, the analysis should have talked to scenarios that must not occur (i.e. the software will not allow premature termination of the engines).

4.1.3.3 Results

Complacently accepting software or hardware without proper risk analysis can lead to catastrophic results, thus was the case for the Mars Polar Lander. Use of the existing software script without proper requirement analysis led to a known false indication. However, if a proper fault tree analysis or software hazard assessment were conducted it would have been understood that the known "false" indication could result in loss of vehicle. Table 6 on the following page provides an overview of the discussed factors of complacency and the associated events of those factors.

Table 6: Overview of MPL Case Study Complacency Factors and Events

MPL COMPLACENCY FACTORS AND EVENTS		
Factors:	**Events:**	**Outcome:**
Ignoring Warning Signs	• The false indication caused by vibrations during the deployment leg was a known phenomenon prior to launch; however, software engineering analysis and design did not account for this. • Inadequate control over the development process: Risk was not adequately managed in the design and implementation processes.	• Missing software requirement leads to a loop hole where software inadvertently shuts down engines too soon.
Assuming Risk Decreases Over Time	• Existing software script from a previous mission was tailored for MPL use. • Corners were cut during the development of system level requirements, thus missing an imperative software requirement. • Superficial hazard analysis had been conducted for the software portion of the MPL because of history of successful flights. • No software centric fault trees created.	• Missed software requirement allowed for premature termination/shutdown of MPL engines resulting in mission failure.

4.2 MILITARY AIRCRAFT

NASA is not been the only organization to succumb to engineering complacency, the armed forces aviation programs have many long running programs and with that, often times, comes areas where complacency may creep in. The Department of Defense (DoD) established a comprehensive guide for the evaluation of accidents or mishaps with respect to human factors. The Department of Defense Human Factors Analysis and Classification System, DoD HFACS, is an analysis tool and model that focuses on human error from four main divisions: acts, pre-conditions for unsafe acts, supervision, and organization influence. Figure 8 on the following page illustrates the human factors model as developed by the DoD (Department of Defense, 2005).

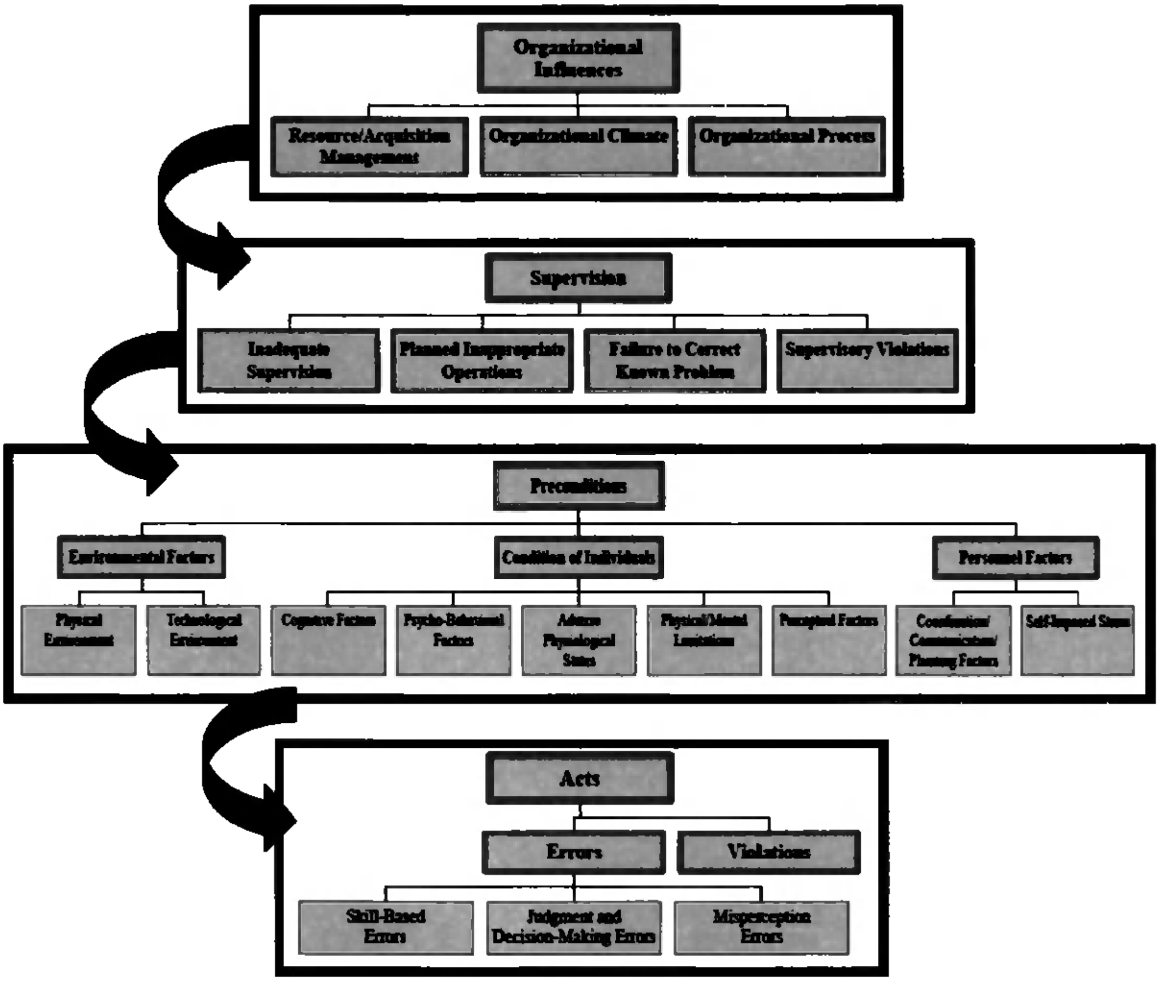


Figure 8: DoD Human Factors Accident Investigation Model

The portion of this model that we are particularly interested in with respect to this body of research is the box containing preconditions for unsafe acts and the underlying psycho-behavioral factors that make up that division. The DoD defines those underlying psycho-behavioral factors as the following (Department of Defense, 2005):

- Pre-Existing Personality Disorder
- Pre-Existing Psychological Disorder
- Pre-Existing Psychosocial Problem
- Emotional State
- Personality Style
- Overconfidence
- Pressing

- Complacency
- Inadequate Motivation
- Misplaced Motivation
- Overaggressive
- Excessive Motivation to Succeed
- Get-Home-Itis/Get-There-Itis
- Response Set
- Motivational Exhaustion (Burnout)

Most important to note is they specifically recognize complacency as a factor that could lead to accidents. The DoD defines complacency as "a factor when the individual's state of reduced conscious attention due to an attitude of overconfidence, undermotivation or the sense that others "have the situation under control" leads to an unsafe situation (Department of Defense, 2005)." It is this definition that will be used while evaluating military accidents for complacency.

4.2.1 U.S. ARMY

The U.S. Army operates helicopters and Unmanned Aerial Vehicles (UAVs) in support of many Army missions which include air assault, scouting or intelligence, troop transport and resupply. Helicopters such as the Apache Longbow, Chinook, Blackhawk, and Kiowa Warrior support ground troops by gathering enemy data, transporting soldiers and supplies, and providing firepower from above.

With long running aircraft programs, the U.S. Army developed an accident investigation program as a reaction to prior incidents. This process is used to learn from accidents in order to make improvements to aircraft and circumvent common cause failures. The Army determined that complacency is a factor that can lead to accidents. Consequently, they defined a specific code listed for overconfidence or complacency as a cause of an accident. This is referred to as Code 16 and it states:

Overconfidence/complacency in abilities. Overconfidence is a temporary state of mind that becomes a root cause when an accident is caused by a person's unwarranted reliance on their own ability to perform a task, the ability of someone else to perform a task, the performance capabilities of equipment or other material (United States Army, 2009).

With a specific code dedicated to complacency, it is apparent the Army believes that complacency is a genuine concern. The Army provides a flow chart with questions that accident investigators should consider as they evaluate a system failure. Figure 9 on the following page shows the flow chart and the questions used to gauge human error and complacency.

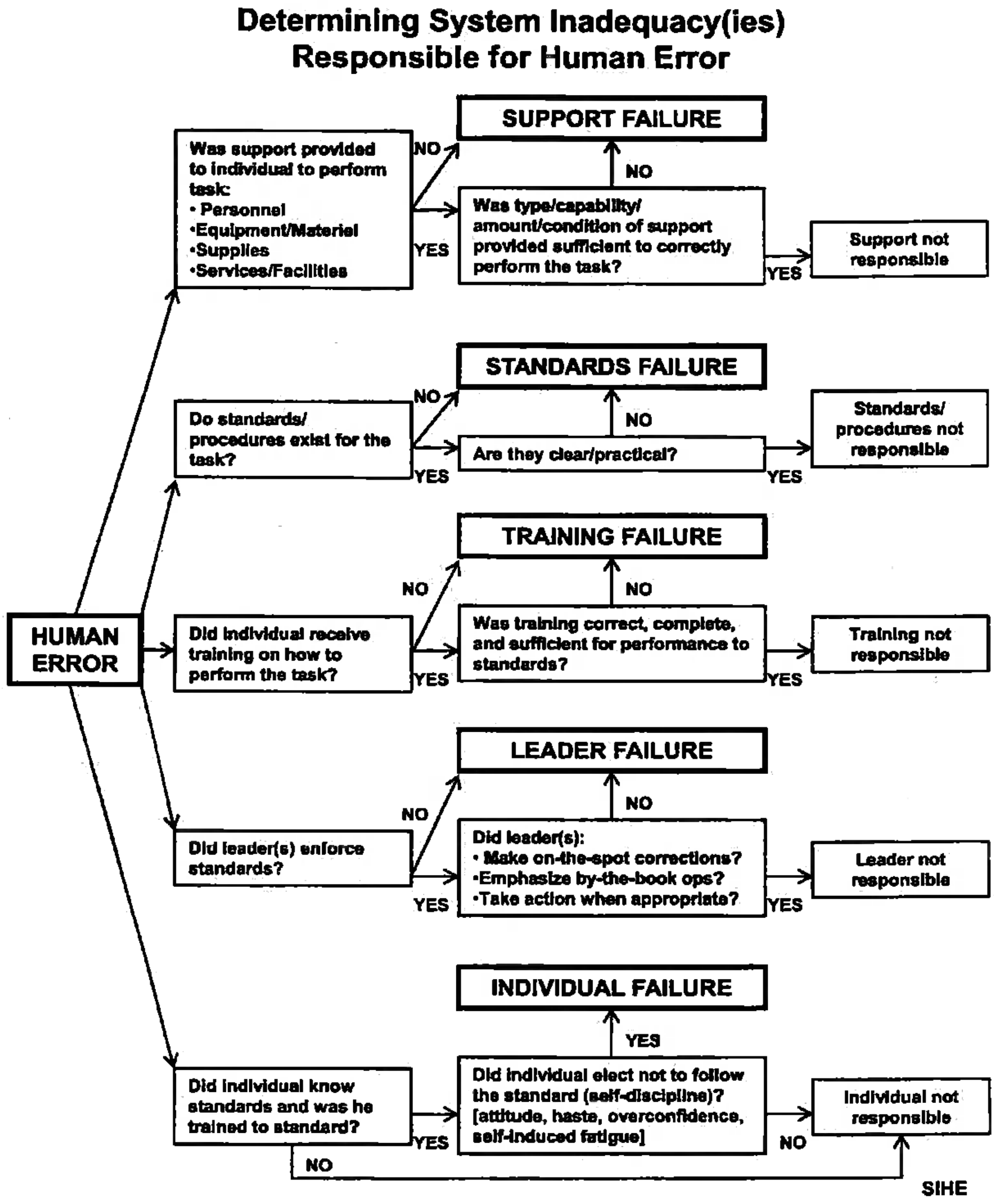

Determining System Inadequacy(ies)
Responsible for Human Error
HUMAN ERROR
Was support provided to individual to perform task:
• Personnel
•Equipment/Materiel
•Supplies
•Services/Facilities
NO
YES
SUPPORT FAILURE
NO
Was type/capability/ amount/condition of support provided sufficient to correctly perform the task?
YES
Support not responsible
Do standards/ procedures exist for the task?
NO
YES
STANDARDS FAILURE
NO
Are they clear/practical?
YES
Standards/ procedures not responsible
Did individual receive training on how to perform the task?
NO
YES
TRAINING FAILURE
NO
Was training correct, complete, and sufficient for performance to standards?
YES
Training not responsible
Did leader(s) enforce standards?
NO
YES
LEADER FAILURE
NO
Did leader(s):
• Make on-the-spot corrections?
•Emphasize by-the-book ops?
•Take action when appropriate?
YES
Leader not responsible
Did individual know standards and was he trained to standard?
YES
NO
INDIVIDUAL FAILURE
YES
Did individual elect not to follow the standard (self-discipline)? [attitude, haste, overconfidence, self-induced fatigue]
NO
Individual not responsible
SIHE

Figure 9: Determining System Inadequacy(ies) Responsible for Human Error (United States Army, 2009)

This flow chart was used during this thesis research for the purpose of evaluating Army accident reports. The questions posed have cross program connotations and are not system unique but do provide insight into how the accidents were reviewed by Army personnel. Accidents are thoroughly evaluated by Army personnel, contract employees, and safety personnel for root cause and corrective action. This data is used to make safety of flight decisions for the fleets.

As a result of these investigations, one of the most speculated complacency issues for military aviation has been complacency due to pilot overconfidence. Even among high-time pilots, overconfidence in abilities can result in accidents. In fact, overconfidence is frequently cited as a contributing factor or cause of a failure or accident in the U.S. Army Combat Readiness Center's Risk Management Information System (RMIS) (Stewart II, 2006). Pilot overconfidence involves 4 of the 6 identified complacency factors and all can occur simultaneously during a maneuver or task. A pilot, who shows overconfidence, can experience the following complacency factors:

- Discounting Risk
- Assuming risk decreases over time
- Over reliance on automation
- Ignoring warning signs

A lapse in judgment or poor risk decision making during a maneuver or situation can create a hazardous situation; combine that with "hot dogging" or overconfidence and the result can be catastrophic. Referring to the DoD human factors categorizations, this overconfidence is one of the main factors in pre-conditioned unsafe actions. Overconfidence in ones abilities can lead a pilot to discount what their instruments are telling them and instead rely on their experience. Conversely, an inexperienced pilot might become too focused on their instruments rather than using all data available. Overconfidence can also lead pilots to ignore cautions and warnings or attempt procedures that are not sanctioned by the U.S. Army.

Working to eliminate complacency in the cockpit can be a double edged sword. While the U.S. Army has identified overconfidence as an issue, where does that overconfidence come from? Generally it is thought to be a human factor induced in some by life experiences such as training and a high amount of flying hours. Training and experience should seem like a good thing but when paired with someone who has the type of mentality that breads complacency it can create the illusion of preparedness. At the other side of the preparedness spectrum, there are those who have very little training and experience. The training and flight time are obviously needed to improve pilot ability but can too much training occur? Ultimately, one cannot blame the training received or flight hours accumulated. Therefore, It is critically important to identify the inherent traits that forms a pilot's risk tolerance and can lead to complacent or overconfident behavior.

In order to help in identify desirable traits for a military pilot, the U.S. Army Research Institute, in 2006, proposed the development of an Army Aviator Selection Instrument. This computer based, webadministered selection tool would be used to correct identified deficiencies in the Army's current aviator selection instrument (Katz, 2006). Scales were developed to establish a pilot's ability in the following categories: adaption, attention to detail, decisiveness, multi-tasking, internal locus of control, reasonable risk taking, risk tolerance, and stress tolerance. The evaluation of risk tolerance is particularly important in identifying those pilots who might exhibit complacent behavior.

Risk tolerance is defined as the amount of risk that an individual is willing to accept in pursuit of some goal (Hunter, 2002). When a pilot exhibits a high risk tolerance they may be more likely to select a course of action that can expose them to more hazards and increase the likelihood of an accident. The Army recognizes that someone with a high risk tolerance can exhibit traits associated with overconfidence and will be willing to accept more risk, and thus more likely to experience an accident. Recognizing the need to avoid complacent behavior is the first step in developing a successful engineering or flight program. While the U.S. Army's proposed selection criteria is geared to identifying complacent behavior in pilots, this concept is one of the methods the author of this thesis is proposing for engineering and pilot behaviors. Once complacent evidence is identified, a way in which that behavior can be readily identified, such as through a series of questions like the U.S. Army is proposing for pilot selection, can be established for a particular group or project. That data can then be used to develop programs to combat complacency.

In a review of fratricide incidents which occurred during the Global War on Terror, a study period from September 11, 2001 through March 31, 2008, the U.S. Army again identified that complacency and overconfidence can have deadly outcomes (U.S. Army Aeromedical Research Laboratory, 2010). Fratricide is defined by the U.S. Army as the "employment of friendly weapons and munitions with the intent to kill the enemy or destroy his equipment or facilities, which results in unforeseen and unintentional death or injury to friendly personnel (Department of the Army, 1992)." An example of this might be a pilot opening fire and mistargeting on friendly ground personnel based on the pilot's poor situational awareness.

The U.S. Army Combat Readiness/Safety Center used information gathered from witness statements, radio logs, weather reports, reenactments, and accident investigation results to come to the conclusion that human factors was a causal factor in approximately 80% of mishaps (Webb & Hewett, 2010). Under that percentage they talk about how the emotional states of complacency and overconfidence contributed to those mishaps. The Army then recommended that based on their results human error factors such as complacency and overconfidence must be considered in the design and development of fratricide countermeasures; however, they stop short and do not offer any resolution or thoughts on how to incorporate those countermeasures into design and development. The development of the Army's pilot selection process as discussed prior may aide in eliminating some of the human error factors associated with fratricide, however it will be important that the proper questions are identified to gauge an aviator's likelihood to succumb to overconfidence and complacency.

4.2.2 U.S. AIR FORCE

The U.S. Air Force operates a large majority of the United States Department of Defense fixed-wing and rotorcraft aircraft. The active fixed-wing aircraft include the C-17 Globemaster III cargo transport, the B-52H Stratofortress bomber, and the F-22 Raptor Fighter (United States Air Force, 2010b). With a strong emphasis on aircraft, complacency, as defined by the DoD, can be present in everyday operations.

4.2.2.1 Case Study 1: B-52H Accident Fairchild AFB, Washington

The B-52, Stratofortress, is a long-range, heavy bomber that the U.S. Air Force uses to perform a variety of missions. It is approximately 159 feet in length and has a wingspan of 185 feet, with a maximum takeoff weight of 488,000 pounds. Eight Pratt & Whitney engines, each producing up to 17,000 pounds of thrust, power the B-52. It travels at a cruise speed of 650 miles per hour and at a range of 8,800 miles (United States Air Force, 2010c). Figure 10 on the following page shows a B-52 aircraft (United States Air Force, 2010c).

Figure 10: B-52 Stratofortress

While the B-52 was originally designed for a crew of six, a typical crew now consists of five persons. The pilot, co-pilot, and electronic warfare officer (EWO) are seated on the upper flight deck, and on the lower deck are the navigator and radar navigator (Global Security, 2011). Figure 11 on the following page shows the crew configuration (Global Security, 2011).

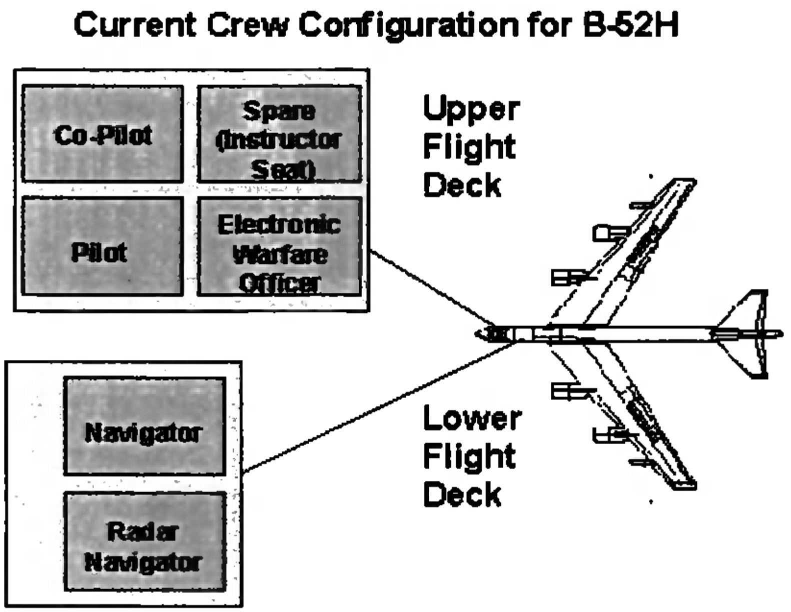


Figure 11: B-52H Crew Configuration

On June 24, 1994 a B-52H assigned to Fairchild Air Force Base, Washington, was practicing for an upcoming airshow on the 26th. The crew knowingly briefed, through the Wing Commander level, and flew a flight profile that exceeded authorized flight maneuvers and FAA regulations. At the end of the practice profile, the aircraft experienced a missed approach, because another aircraft was executing a touch-and-go landing, and was forced to execute a go-around maneuver. At mid-field the B-52H began a tight 360-degree left turn around the base's control tower at only 250 feet above ground level (AGL), with 60-degrees of bank, replicating one of the airshow profile turns. This tight turn was done because the pilot did not want to enter into restricted airspace, a nuclear weapons storage facility, located directly behind the control tower. Approximately three-quarters of the way through the turn, the B-52H banked past 90-degrees, stalled, lost altitude, and then impacted the ground. Although the pilot had previously executed this tight and steeply banked turn, the aircraft altitude was extremely low making stall recovery impossible (U.S. Air Force Accident Investigation Board, 1994). Figure 12 on the following page shows the B-52H as it made impact with the ground at Fairchild AFB, WA (U.S. Air Force Accident Investigation Board, 1994).

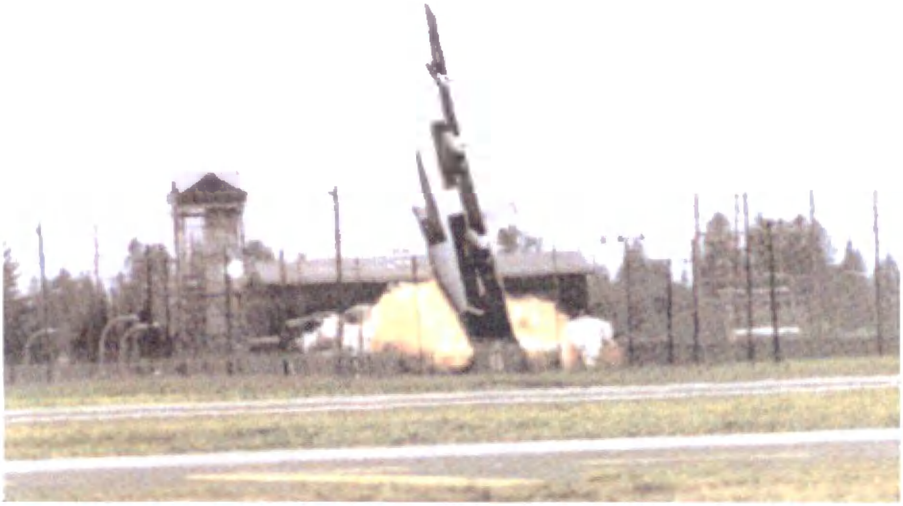


Figure 12: B-52H as it makes impact with the ground at Fairchild AFB, WA

The pilot of the B-52H aircraft was Lieutenant Colonel Bud Holland. He was responsible for the knowledge and enforcement of academic and in-flight standards for all flying operations at the 92nd Bombardment Wing. He had accumulated more than 5,200 hours of flying time and had been regarded by many as an outstanding pilot. However, he had also established a reputation as an aggressive pilot who often broke flight safety rules. Violations included flying below minimum clearance altitudes and exceeding bank angle limitation and climb rates (Kern, 1995). In fact due to his aggressive nature, many airmen refused to fly with him and his co-pilot during the Fairchild airshow mishap, Lieutenant Colonel Mark McGeehan, had unsuccessfully attempted to have upper leadership restrict Holland from future flying (U.S. Air Force Accident Investigation Board, 1994).

The accident investigation board determined that pilot error was the primary cause of the accident. While that may be the cause on the surface, upon further investigation, it is apparent that the overarching cause was complacency on the part of the pilot and of the leadership to enforce procedures and regulations. Discounting risk because of overconfidence on the pilot's part and ignoring warning signs on the part of Fairchild AFB leadership were the factors noted upon review of the accident investigation report.

4.2.2.1.1 Factor 1: Discounting Risk

Lieutenant Colonel Bud Holland was praised by those around him as a gifted pilot. However, within the same breath they would comment that he was over-aggressive and some refused to fly with him because of his risk-tolerant flight behaviors. Through eyewitness testimony and the examination of footage from previous flights piloted by Holland, it is evident he was overconfident in his abilities and complacent with altering or disregarding flight safety regulations. The risk associated with operating an aircraft at its maximum limits was discounted greatly.

On the day of the crash, Holland operated the B-52H in excess of bank angles, speed, and altitude restrictions established for the aircraft; ultimately pushing the aircraft past its design limits and into a catastrophic low altitude stall scenario. The maneuvers he planned were not approved by the U.S. Air Force and was a violation of flight safety regulations. This type of over-aggressive flying was not a first for Holland and, unfortunately, this time his risky behavior cost him and his crew their lives. He had established rhetoric of unabated risky behavior that allowed him to become complacent in his ability to perform these maneuvers.

Many airmen were leery of Holland's complacency and discounting of risk. It was apparent through accident investigation transcripts that Holland treated his colleagues' perception of his abilities as a joke. After the accident, Captain Mike Meyers was interviewed and testified: "Holland made a joke out of it when I said I would not fly with him. He came to me repeatedly after that and said 'Hey, we're going flying Mikie, you want to come with us.' And every time I would just smile and say, 'No. I'm not going to fly with you (U.S. Air Force Accident Investigation Board, 1994)." Another incident of laughing off risk occurred during a training mission in March 1994. Holland commanded a mission to the Yakima Bombing Range to provide an authorized photography crew to document the aircraft as it dropped munitions. The minimum aircraft altitude permitted was 500 feet AGL, but Holland pushed the envelope and flew so low that he only cleared a ridgeline at just 3 feet AGL. Fearing for their lives, the copilot grabbed the controls to prevent Holland from flying the aircraft into the ridge. Captain Jones recounts his experience in the accident investigation report:

> *We came around and (Lt) Col Holland took us down to 50 feet. I told him that this was well below the clearance plane and that we needed to climb. He ignored me. I told him (again) as we approached the ridge line. I told him in three quick bursts '**climb-climb-climb.**'...I didn't see any clearance that we were going to clear the top of that mountain ... It appeared to me that he had target fixation. I said '**climb-climb-climb.**' again, he did not do it. I grabbed ahold of the yoke and I pulled it back pretty abruptly ... I'd estimate we had a cross over around 15 feet . . . The radar navigator and the navigator were verbally yelling or screaming, reprimanding (Lt) Col Holland and saying that there was no need to fly that low ... his reaction to that input was he was laughing--I mean a good belly laugh* (U.S. Air Force Accident Investigation Board, 1994).

After the mission, the crew refused to fly with Holland ever again and reported the incident to leadership. Holland did not take the fact that airmen were refusing to fly with him as a sign that his behavior was risky. He was complacent with his standings as one of the most senior B-52 pilots and instructor at Fairchild AFB.

Was it the large number of flight hours or the fact that he had previously survived risky behavior that made Holland discount the risk associated with his behaviors? While it cannot be determined exactly what human factor made Holland so overconfident, it can be established that the majority of those around him accepted his behavior rather than counteracting.

4.2.2.1.2 Factor 2: Ignoring Warning Signs

Fairchild AFB was in trouble. From 1991 to 1994, they experienced high turnover in leadership and as a result had become lenient on procedures. They also failed to keep lines of communication about past events open and due to this ignored many warning signs. This lack of communication created a hole in which complacency could brew. Although Holland had established a history of rogue flying and had been reported by fellow airmen, senior leadership ignored the warning signs that a catastrophic event was on the horizon.

The accident investigation board reviewed prior airshow flights where Holland had flown aggressively or committed a regulatory infraction. A total of nine prior flights over a three year period were identified in which Holland's behavior jeopardized crew and/or spectator life and in addition violated flight safety regulations. Of the nine that occurred, the most notable is that of the training mission to the Yakima Bombing Range on March 10, 1994 (missing a ridge by three feet). After the co-pilot took command and the aircraft landed safely, the crew decided that they would no longer fly with Holland and reported the incident to the bomb squadron leadership. The squadron commander, Lieutenant Colonel Mark McGeehan, then reported the incident to the Deputy Commander of Operations (DO) Colonel Pellerin and recommended that Holland be removed from flight status. Pellerin met with Holland and without review of flight video, discussions with crew, or deliberations with prior DOs decided to only give him a verbal reprimand. The DO did not document the incident or notify his superiors of the violations.

Pellerin effectively ignored the fact that Holland was putting those around him at risk. He made no attempts to cease Holland from unapproved flight maneuvers or to correlate the stories of other crew members. In the author's opinion, more was not done to stop Holland's behavior because they were complacent with his senior ranking position. Holland was the most senior and experienced B-52 pilot at Fairchild and because of that the credibility associated with the title could have masked his actual behaviors. Even so, warning signs were ignored by senior leadership.

4.2.2.1.3 Results

The accident at Fairchild AFB in 1994 is often used as an example in military and civilian training as a prime example of the importance of enforcing safety regulations. Although violations of safety regulations, poor leadership management, and overconfidence on the part of Holland were identified as factors in the accident, the U.S. Air Force failed to correct the underlying complacency factors associated with the event. This would lead to a C-17 accident in Alaska, nearly identical to that at Fairchild AFB. Table 7 on the following page details the complacency factors and events for the 1994 B-52H Fairchild AFB accident.

Table 7: 1994 B-52H Fairchild AFB Complacency Factors and Events

1994 B-52H FAIRCHILD AFB COMPLACENCY FACTORS AND EVENTS		
Factors:	**Events:**	**Outcome:**
Discounting Risk	• Rhetoric of risky behavior over nine consecutive airshow flights. • Although other airmen refused to fly with Holland due to his aggressive maneuvers, he continued to operate the aircraft at or above its design limits. • Risk associated with his flying habits was discounted as a joke.	• Aircraft entered into an unrecoverable stall scenario during a non-regulation profile, resulting in loss of aircraft and crew.
Ignoring Warning Signs	• Frequent leadership changes from 1991 to 1994 left hole of ignorance in Holland's long term behavior. • Supervisors did not question pilot's risky behavior or disregard for procedures even though other airmen had requested Holland be grounded.	• Aircraft entered into an unrecoverable stall scenario resulting in loss of aircraft and crew.

4.2.2.2 Case Study 2: C-17A Accident Richardson, Alaska

The C-17A is one of the U.S. Air Force cargo aircraft. It is used to deliver troops and cargo to operating bases or deployment areas. The aircraft is also capable of performing tactical airlift and airdrop missions. It is approximately 174 feet in length and has a wingspan of 169 feet, 10 inches, with a maximum takeoff weight of 585,000 pounds. Four fully reversible Pratt & Whitney engines, each producing 40,440 pounds of thrust, power the C-17A. The aircrafts cruise speed is 450 knots and its range is global with in-flight refueling capabilities. A typical crew for a C-17A will consist of a pilot, co-pilot, and loadmaster (U.S. Air Force, 2010d). Figure 13 below shows a C-17A Globemaster III cargo transport (U.S. Air Force, 2010d):

Figure 13: C-17A Globemaster III Cargo Transport

On July 28, 2010 a C-17A, Tail Number 00-0173 and with a crew of four (pilot, co-pilot, loadmaster, and safety officer), was practicing maneuvers for an upcoming airshow at Joint Base Elmendorf-Richardson in Alaska. The airshow consisted of four different practice demonstrations, designated as "profiles" by the U.S. Air Force, and on this day the crew was practicing for Profile 3 which was 12-minutes in length. The components of the profile were for the C-17A to conduct a maximum performance climb to 1,500 feet AGL, 80/260-degree reversal turn, and finish with a 500-foot AGL high-speed pass (U.S. Air Force Accident Investigation Board, 2010).

The maximum performance climb requires for the pilot to pitch the aircraft nose upward achieving maximum climbout speed. This speed demonstrates the aircrafts capability to climb and clear an obstacle with only three of the four engines operating. After this climbout, the aircraft performs an 80/260-degree reversal turn to transition the aircraft from its original outbound direction to align with the runway to perform the final high-speed pass. To perform the high-speed pass, the aircraft descends from 1,500 feet AGL to 500 feet AGL during the 80/260-degree reversal turn. Once the C-17 reaches 500 feet, the aircraft accelerates to 250 knots (U.S. Air Force Accident Investigation Board, 2010). Figure 14 illustrates the flight path taken by the C-17A for profile 3 maneuvers (U.S. Air Force Accident Investigation Board, 2010):

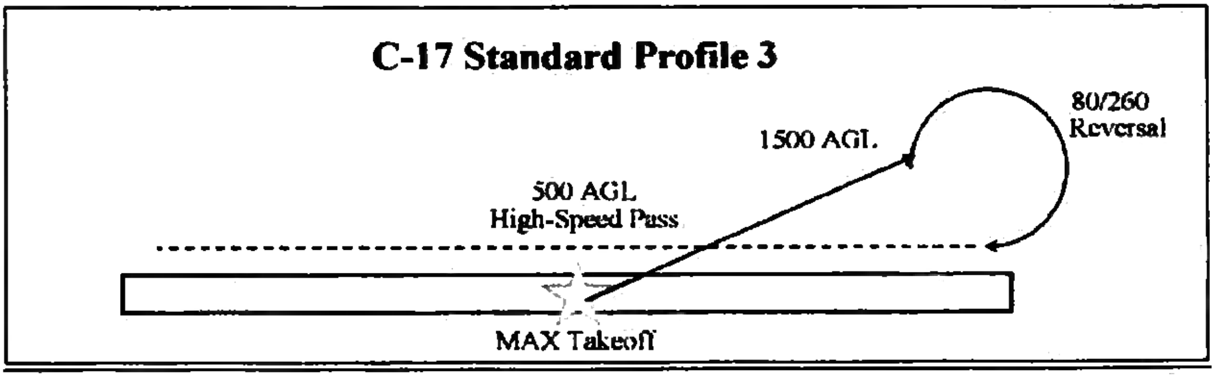


Figure 14: C-17 Standard Profile 3

As the mishap aircraft completed its initial climb and left turn after takeoff, the pilot, Major Michael Freyholtz, executed an aggressive right turn. During this aggressive banking maneuver, the stall warning system activated. The C-17A stall warning system is designed to alert the crew of an impending stall. The aircraft computer analyzes inputs from the engines and various aircraft sensors to determine the current and correlating stall speed. If that stall speed is being encroached upon, the pilot and co-pilot sticks shake and an audible indication sounds (U.S. Air Force Accident Investigation Board, 2010).

Although the stall warning was initiated, Freyholtz continued into their right turn, ignoring the stall warning and at first did not implement the necessary stall recovery procedures. Ultimately the aircraft entered into a stall from which recovery was not possible. The aircraft impacted wooded terrain and was destroyed on impact. Although the crew did eventually attempt to recover from the stall, sufficient altitude was not available and incorrect stall procedures were applied. Figure 15 on the following page shows the devastation of the C-17A after impact with wooded terrain (Trimble, 2010).

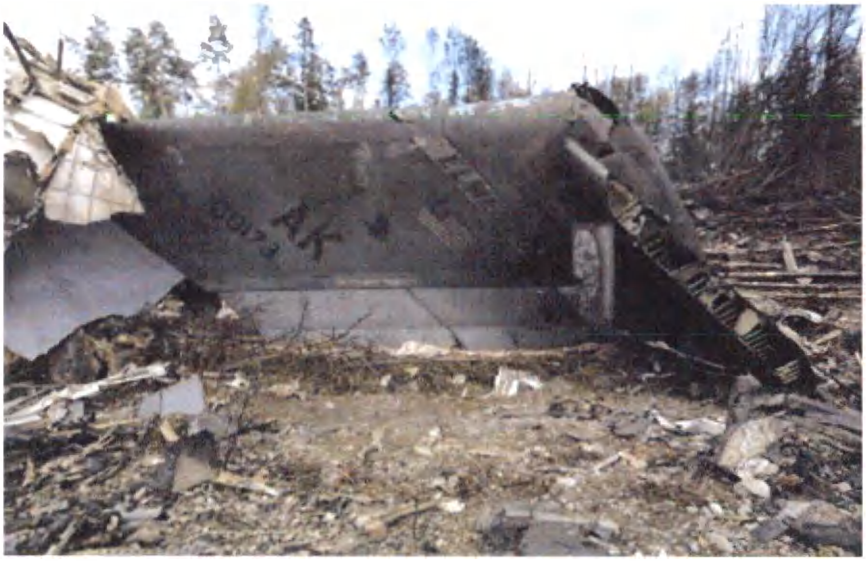


Figure 15: Devastation of C-17A after Impact with Wooded Terrain

Analysis of leadership issues noted in this accident have often been compared and contrasted to those that occurred in the 1994 B-52H accident at Fairchild AFB. Complacency on the part of leadership to allow for lax procedural enforcement will be discussed.

4.2.2.2.1 Factor 1: Ignoring Warning Signs

The most obvious complacency factor for this particular C-17A accident is that the crew ignored warning signs that the aircraft was entering into a stall scenario. Shortly after takeoff, approximately 5-seconds into the 260-degree reversal turn, an audible stall warning was annunciated. The pilot then was heard on the voice recorder saying, "Acknowledged crew…Temperature, altitude lookin' good (U.S. Air Force Accident Investigation Board, 2010)." Although operating procedures state that stall procedures must be executed upon warning indication, the crew continued to operate the aircraft in the unsafe condition and did not attempt to make any flight control adjustments until the aircraft had stalled.

The important question to ask in a scenario such as this is why the crew would ignore an audible warning that the aircraft was entering an unsafe condition? The answer to this has to be complacency. The pilot had performed this particular maneuver several times in anticipation for an air show without event and the crew had come to expect to perform a certain list of tasks without talk or argument. The pilot's mindset was that of overconfidence in his abilities and he had become complacent with his ability to continue through the turn without initiating stall procedures. The crew, on the other hand, had become complacent with their position or place in aircraft operations. The pilot established his command the way in which he expected and the crew blindly followed without challenging his directive.

4.2.2.2.2 Factor 2: Discounting Risk

When an aircraft enters into a stall scenario, the angle-of-attack at which the aircraft is traveling increases to a point where the lift generated by the wings is decreased such that the aircraft can no longer stay aloft (Federal Aviation Administration, 1965). If a stall occurs shortly after takeoff, such as with the C-17A accident, the aircraft may not have a sufficient amount of altitude to either recover from the stall or land safely if stall procedures are not put into effect upon indication. Because the pilot was able to recover previously from impending stall scenarios without the need to begin stall recovery procedures, he discounted the risk associated with doing so.

An underlying factor in the accident is that the crew did not properly execute "challenge and reply" procedures; a blatant discount of risk. Challenge and reply is a communication procedure used to show supportive feedback or acknowledgement to ensure personnel correctly understood announcements or directives. Freyholtz was the lead C-17 aerial demonstration pilot for that particular base. With that, he was in charge of training and it was noted that he routinely instructed and planned to ignore stall warnings during aerial demonstrations. It was noted through eyewitness testimony that the pilot trained simulator students that stall indication warnings were an "anomaly." He considered these warnings to be transitory due to the aggressive nature of the aerial demonstration maneuvers (U.S. Air Force Accident Investigation Board, 2010).

Another violation, Freyholtz also routinely instructed demonstration co-pilots to retract flaps and slats "on speed" automatically without a challenge or reply (U.S. Air Force Accident Investigation Board, 2010). It was noted in the accident investigation report that the co-pilot, Captain Jeffery Hill, had retracted flaps prior to the 260-degree turn which reduced the wings surface area which was vital for low speed conditions such as this (Trimble, 2010). It is not known whether Freyholtz was aware that the flaps had been retracted because challenge and reply procedures were not implemented. This factor and the failure of the crew to challenge and reply the stall warning implies that the pilot had become complacent in his C-17 aerial demonstration cockpit capabilities and that he also inculcated that same complacency onto his crew.

Similar to both Space Shuttle accidents discussed in the previous section, discounting the risk associated with a particular maneuver or phenomena can prove catastrophic. Freyholtz had accomplished or survived it before, why wouldn't he this time? The pilot's blatant violations and teachings of military procedures should have come as a warning to those around him. However, the accident investigation showed that Freyholtz was considered an experienced pilot and "because he was an accomplished aviator, leadership allowed him to operate independently with little or no oversight (U.S. Air Force Accident Investigation Board, 2010)." The pilot had been labeled as having overconfidence; however, because of his ability to operate the aircraft in that manner successfully to date, he was allowed to continue with his risky behavior. Supervisors assumed that Freyholtz was "within regulatory compliance" and "did not inquire or review [his] techniques or performances (U.S. Air Force Accident Investigation Board, 2010)." There were no checks and balances established and without them, the safety culture at the Elmendorf-Richardson base had become complacent and began to accept more risk based on a flawed perception of an individual's capabilities.

4.2.2.2.3 Results

While Freyholtz is ultimately blamed for the C-17A crash, the safety culture of the 3rd Airlift Wing at Elmendorf-Richardson is also to blame. Lax procedural enforcement and a complacent safety program allowed for inappropriate flying techniques and behavior to continue.

The pilot and crew ignored obvious warning signs of an impending stall and also discounted the risk of ignoring the stall indication procedures. Lax procedural compliance on the part of the crew led to an ill-informed cockpit environment and ultimately the death of all on board. Table 8 reiterates the complacency factors and events for the 2010 C-17A accident at Elmendorf-Richardson AFB:

Table 8: 2010 C-17A Elmendorf-Richardson AFB Complacency Factors and Events

2010 C-17A ELMENDORF-RICHARDSON COMPLACENCY FACTORS AND EVENTS		
Factors:	**Events:**	**Outcome:**
Ignoring Warning Signs	• Audible stall warning occurred but crew proceeded with current operations. • Stall procedures were not initiated.	• Aircraft entered into an unrecoverable stall scenario resulting in loss of aircraft and crew.
Discounting Risk	• Pilot trained crew to treat stall warnings as an "anomaly." • Stall procedures were not initiated because the risk of stall was deemed an anomaly. • Challenge and reply procedures were violated. Crew initiated maneuvers and ignored warnings based on previous discussions with the pilot. • Supervisors did not question pilot's risky behavior or disregard for procedures.	• Lax procedural enforcement on the part of supervisors leads to acceptance of greater risk. • Aircraft entered into an unrecoverable stall scenario resulting in loss of aircraft and crew.

4.3 NTSB: COMMERCIAL AND PRIVATE AVIATION

Like the U.S. Army, the NTSB has a code in their accident investigation manual dedicated to complacency, code 31140. When performing an accident investigation, the NTSB investigates the psychological condition of the pilot or crew as one of the possible causes. Often pilot error due to complacency or overconfidence is an underlying factor in commercial and private aviation accidents. A pilot's complacency in their abilities, failure to follow guidelines, or inattention to surroundings can lead to catastrophic events.

A major influence on private and commercial aviation is automation-induced complacency. Automation is a process of substituting some device or machine for a human activity (Parsons, 1985). In the cockpit this can be seen with the inclusion of avionics and navigational systems. The addition of aviation automation technology has resulted in a significant decrease in the number of aviation incidents and accidents. However, this has also led to an increase in the number of failures labeled as pilot error due to pilot-automation interaction (Prinzel, 2001). As automation continues to become more sophisticated, the role of the pilot is shifting to a supervision role. Instead of actively controlling many of the direct processes, pilots are increasingly tasked to evaluate a computed solution and are often times flying on automated control. This paradigm shift from the traditional idea of a "stick and rudder" pilot is important because it has created a breeding ground for complacency within the cockpit.

Singh, Molloy, and Parasuraman noted in studies that complacent behavior often coexists with other conditions such as operator experience with equipment, high workload, or fatigue (Singh, Molloy, & Parasuraman, 1993). They go on to say that "...combination of the crew's attitude toward automation (e.g. overconfidence) and a particular situation (e.g. high workload) may lead to complacent behavior." The combination of these conditions can lend to pilot inattention to instruments or over-reliance that the instrument output is correct.

4.3.1.1 Case Study 1: DC-9-82 Northwest Airlines Flight 255 Accident Romulus, Michigan

The DC-9-82 is manufactured by McDonnell Douglas and is powered by two Pratt & Whitney turbofan engines capable of producing 40,000 lbs of thrust. It is approximately 147 feet in length with a wingspan of 107 feet. It travels at a speed of 574 miles per hour and has a range of 1,800 statute miles. Figure 16 shows a McDonnell Douglas DC-9-82 (Pries, 2002).

Figure 16: McDonnell Douglas DC-9-82

On August 16, 1987 a Northwest Airlines DC-9-82 out of Detroit Metro airport crashed shortly after take-off. The DC-9-82 began rotation at 1,200 feet from the end of the runway and eyewitnesses stated that the aircraft's wings rolled to the left and then to the right. The aircraft's left wing collided with a light pole 2, 760 feet beyond the end of the runway and continued to collide with obstacles as it slid along the ground, breaking up as it went.

A total of 145 people passed away as a result of the accident. The NTSB determined that the aircraft was not properly configured for takeoff. The flaps and slats on the wings should have been fully extended but the crew failed to observe this because of a failure to perform the taxi checklist procedures and a failure of the takeoff warning system (NTSB, 1987).

4.3.1.1.1 Factor 1: Over reliance on automation

Accident investigation findings determined that the crew neither called nor completed the taxi checklist procedures. The first item on the taxi checklist for this particular aircraft is for both pilot and co-pilot to check and verify orally that the flaps and slats are positioned correctly. This particular checklist is completed within 1 to 2 minutes of the aircraft beginning to taxi on the runway. Completing this checklist while the aircraft is moving is within FAA regulations; however, if these items are completed at this time, it is very likely that the flight crew is busy with other tasks in addition to the list. These tasks can include checking radios by making contact with Air Traffic Control (ATC) and receiving ground control instructions. This is a prime example of the automation-induced complacency with workload factors that Singh, Molloy, and Parasuraman noted in their research.

Other Northwest pilot's testified to the Accident Investigation Board that this taxi checklist was almost always done during taxi and never before (NTSB, 1987). The crew was conditioned to having completed these steps within the first several minutes and it is possible that they had become complacent with their procedures, believing the taxi checklist had been completed. It was noted through black box cockpit recordings that the crew did not appropriately follow the challenge and reply rules associated with checklists and this could have further added to the checklist confusion. The pilot never called up the checklist and it is possible that he assumed that it was being completed by other crewmembers.

It was also noted by pilot interviews post accident that it was commonly known that crews would rely on the automatic takeoff warning system to check their configuration while taxiing out for takeoff (NTSB, 1987). To do this, a pilot would advance one or more throttles to see it the takeoff warning annunciated. If there was no warning, then the assumption was that the airplane was in proper configuration. While this was against Northwest procedures, some airmen became complacent and relied on this annunciation to circumvent particular checklist steps. While this does seem like an intelligent way in which check takeoff configuration, a failure of the takeoff warning system would place the aircraft at a higher risk for a catastrophic accident. This was the case for the Northwest Airlines flight.

A complacent reliance on the automated takeoff warning system placed the aircraft in a catastrophic scenario. As the aircraft lifted off the crew was under the assumption that they were properly configured and with no annunciation to indicate to the crew otherwise, they continued until the aircraft entered a stall. Had the airmen known that they were in an improper configuration, they could have quickly adjusted the flaps and slats to allow more surface area on the wings. Believing that the aircraft was configured correctly, the pilot and copilot were ill informed and attempted to fly the airplane as if they had encountered wind shear. Again, they received no takeoff warning to indicate to them that the aircraft was anything other than configured appropriately for takeoff.

4.3.1.1.2 Results

As pilot's become more of a supervisorial role in the cockpit, the threat of automation-induced complacency is a threat. As seen in the DC-9-82 accident, the crew was unaware that they were flying the aircraft in a dangerous configuration. The takeoff warning annunciation failed and the crew was unaware of the aircrafts configuration. It can be surmised that if the takeoff warning had not malfunctioned that the pilot and copilot would have reacted differently to the stall indication. The crew had become victim to automation-induced complacency. Table 9on the following page provides a summary of the complacency factor and events.

Table 9: 1987 DC-9-82 Northwest Airline Flight 255 Romulus, Michigan Complacency Factor and Events

1987 DC-9-82 NORTHWEST AIRLINES FLIGHT 255 ROMULUS, MICHIGAN COMPLACENCY FACTOR AND EVENTS		
Factors:	**Events:**	**Outcome:**
Over reliance on automation	• Crew failed to perform taxi checklist procedures. • Automated takeoff warning system failed and did not annunciate to crew that aircraft was improperly configured. • Crew attempted to recover from stall with inappropriate procedures because they believed that the flaps and slats were in correct position for takeoff.	• Aircraft began to roll from left to right, ultimately contacting a light pole and then the ground.

4.3.1.2 Case Study 2: Bombardier Q-400 Colgan Air Flight 3407 Accident Buffalo, NY

Colgan Air operates the Bombardier Q-400 on behalf of Continental Airlines. This aircraft is a twin-engine turboprop with a maximum cruise speed of 350 knots and a range of 1,260 nautical miles. The Q-400 has a length of approximately 107 feet and a wingspan of 93 feet (Transport Canada, 2001). Figure 17 on the following page shows a Bombardier Q-400 (Pries, 2002).

Figure 17: Bombardier Q-400

On February 12, 2009, a Colgan Air Bombardier Q-400 operating as Continental Connection flight 3407 was operating on an instrument approach when it crashed into a residence just 5 miles northeast of the airport. The aircraft was destroyed on impact and all persons aboard and one on the ground were killed. The events leading up to the catastrophic accident point to a cockpit that was succumbing to complacency. The co-pilot admittedly was flying while ill and the crew conversed in non-essential discussions throughout critical portions of the flight where the FAA requires a silent cockpit.

The weather on the night of the mishap was considered normal for winter conditions in the Buffalo area. This meant that icing was a concern and that crewmembers should be on alert for icing build up. The Flight Data Recorder (FDR) recorded activation of the airframe and propeller deice equipment while the Q-400 was climbing to its assigned cruise altitude. Upon activation of the deice equipment, the pilot would have turned the ref speed switch to the increase position. On the Q-400, the ref speeds switch was to be set to the increase position before an airplane entered icing conditions and was to be set to the off position when airplane was free of ice (NTSB, 2009). When the pilot on the mishap flight turned the ref speeds switch to the increase position, it lowered the aircraft angle of attack reference for the stall warning activation and raised the position of the low-speed cue by about 15 knots. A red bar on the primary flight display indicates the low-speed cue. Figure 18 on the following page shows the primary flight display for the Q-400 (NTSB, 2009).

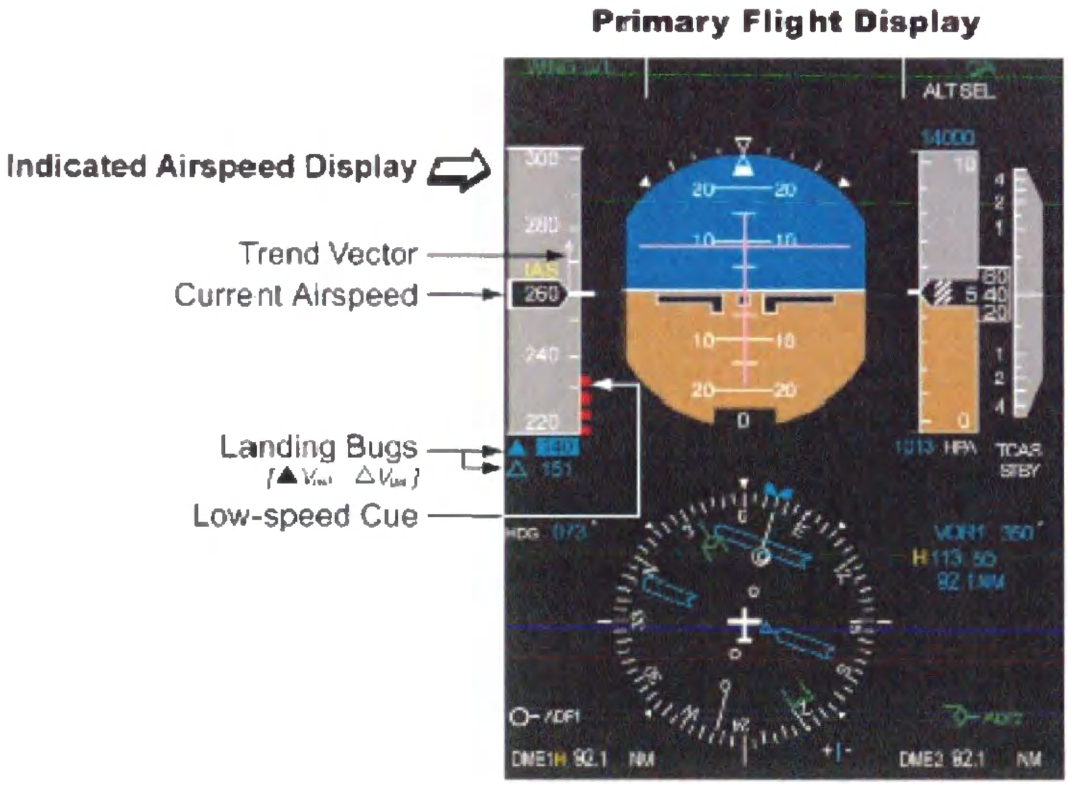


Figure 18: Bombardier Q-400 Primary Flight Displays

The low-speed cue and deicer equipment correlation are important to know because of the need for the pilot to be more vigilant of his indicated speed display. For an unknown reason, the pilot on the mishap aircraft did not monitor his Indicated Airspeed Display (IAD) and failure to monitor put the aircraft in a position to stall that was annunciated by the stall warning system.

The aircraft entered into an impending stall and the pilot inappropriately responded to the warning by failing to advance the power levers to maximum and inappropriately raising the flaps. The pilot's inappropriate responses lead to aerodynamic stall and a left-wing-down roll, which was unrecoverable. The NTSB determined that the cause of the accident was the pilot's inappropriate response to a warning of an impending stall. Contributing to the pilot's inappropriate response was the crew's failure to monitor airspeed and their inattention in the cockpit due to non-flight related conversation.

4.3.1.2.1 Factor 1: Ignoring Warning Signs

The FDR found that the crew was engaged in non-essential discussion throughout critical portions of the flight where FAA regulations require a silent cockpit. Because of their personal conversations, the flight crew was inattentive in operational tasks, monitoring, maintaining situational awareness, managing possible threats, and preventing potential errors (NTSB, 2009). The crew's willingness to violate FAA regulations and to have personal conversations was a sign that they were complacent with their current flight responsibilities. To them, there was no indication that they were in impending danger. However, had the pilot not been complacent he would have better managed his cockpit and determined that the aircraft was quickly approaching a low-speed stall. In addition to missing the warning sign that the aircraft was approaching stall speeds, the pilot and co-pilot discuss ice as a possible threat to the aircraft but neither took appropriate measures to mitigate the threat.

The crew was not the only ones to miss warning signs. Colgan Air failed to manage their crew appropriately. The pilot had failed many instrument flying checks in his early career and he continued to show weakness in basic aircraft control and instrument flying (NTSB, 2009). Although he had showed inefficiencies within the cockpit, Colgan Air did not identify the trend and failed to adequately address his weaknesses. Not only was the pilot lacking in his instrument capabilities, the copilot was newly hired three months prior. The combining of an inexperienced copilot and a mediocre instrument capable pilot was a poor managerial decision and another missed warning sign on the part of Colgan Air. It is these deficiencies and inexperience that could have led to his inappropriate corrections to the stall.

4.3.1.2.2 Factor 2: Discounting Risk

The fact that the crew was engaged in conversations during critical portions of the flight also indicates that they were complacent and discounted the risk associated with their flying conditions. As was noted with the military case studies, when a pilot discounts the risk associated with their mission or flight they become overconfident or comfortable with their surroundings. It is this complacency that creates an opening for a catastrophic failure to occur. In the case of the Colgan Air flight, the pilot and copilot had become comfortable with operating the Q-400 and discounted the risk associated with the winter weather.

4.3.1.2.3 Results

Remaining alert and on constant vigilance within the cockpit is essential to avoiding complacency. The Colgan Air pilot and copilot had become complacent with their atmosphere and conversed in non-essential discussion throughout the flight, ignoring warning signs that the aircraft was entering into a stall scenario. They had discounted the risk associated with their flight and ultimately lost their lives and the lives of all on board. Colgan Air contributed to the complacency by ignoring important trends in poor pilot performance and pairing crewmembers that were both would benefit from a more experienced counterpart. Table 10 on the following page shows the complacency factors and events for the Q-400 Colgan Air Flight 3407.

Table 10: 2009 Q-400 Colgan Air Flight 3407 Buffalo, New York Complacency Factors and Events

2009 Q-400 COLGAN AIR FLIGHT 3407 BUFFALO, NEW YORK COMPLACENCY FACTORS AND EVENTS		
Factors:	**Events:**	**Outcome:**
Ignoring Warning Signs	• Pilot and copilot conversed in non-essential discussions during critical flight portions against FAA silent cockpit regulations. • Pilot failed to monitor aircraft low-speed indications and entered into a stall scenario. • Pilot incorrectly attempted to recover from impending stall. • Colgan Air failed to recognize a trend in failed check-rides on the behalf of the pilot for instrument procedures. • Colgan Air paired an inexperienced copilot with a mediocre instrument experienced pilot.	• Aircraft entered into an unrecoverable stall scenario resulting in loss of aircraft and all aboard.
Discounting Risk	• Pilot and copilot conversed in non-essential discussions during critical flight portions against FAA silent cockpit regulations.	• Pilot was distracted and failed to properly monitor indicated air speed displays. • Aircraft entered into a stall scenario and the pilot inappropriately corrected resulting in loss of aircraft.

5.0 DISCUSSION

It is important to note that the analysis completed on these case studies occurred with hindsight into the outcomes, meaning that it was known in advance the human error was occurring and that there could be some form of complacency associated with that failure. This hindsight made it possible to identify those complacency factors more readily. In a real world scenario it is much more difficult to realize when complacency is occurring, especially if it occurs within a matter of moments.

While it seems there is consensus amongst the military, private aviation and NASA community that complacency is a serious problem, there is little or no consensus as to how to combat it (as is evident by reoccurring accidents) or a broadly accepted method for measuring complacency. It is believed that through review of the above case studies that an emphasis should be placed on proper problem reporting, frequent trending of failures, pilot character screening, pilot qualifications, and a push to open up the lines of and continually improve communication.

5.1 DISCUSSION OF RESULTS

While no scenario was the same, each of the researched organizations experienced complacency. Whether only one of the six or all of the complacency factors were seen, the organizations' reaction to those complacency factors is what made for the catastrophic situation. Among those complacency factors were items that boosted the effects of complacency on a situation or individual. Those items were communication throughout the organization, ineffective problem reporting methods, overconfidence, over reliance on automation or redundancy, and regarding a mission as routine. To gauge which complacency factors were most prominent across all of the case studies, a scoring method was developed. For this, all six of the complacency factors were assessed for each case study; if a factor occurred a score of 1 was assigned, if a factor did not occur a score of 0 was assigned. Table 11 on the following page shows the scorecard for the seven case studies discussed.

Table 11: Complacency Factor Scorecard

COMPLACENCY FACTOR SCORECARD						
	Discounting Risk	Unrealistic Risk Assessments	Assuming Risk Decreases Over Time	Over-Reliance on Redundancy or Automation	Ignoring high-consequence, Low probability Events	Ignoring Warning Signs
Challenger Shuttle Accident	0	1	1	0	1	1
Columbia Shuttle Accident	0	1	0	0	1	1
Mars Polar Lander	0	0	1	0	0	1
B-52H Accident, Fairchild AFB	1	0	0	0	0	1
C-17A Accident, Elmendorf-Richardson AFB	1	0	0	0	0	1
DC-9-82 Accident, Northwest Airlines Flight 255	0	0	0	1	0	0
Q-400 Accident, Colgan Air Flight 3407	1	0	0	0	0	1
TOTALS:	3	2	2	1	2	6

From this scorecard we can see that there was a prevalence of the complacency factor "ignoring warning signs". This can come from aviators or engineers viewing a situation as routine or simple. This type of thinking leads to a discounting of the risk associated with that scenario. Just because a pilot or hardware has survived a particular maneuver before does not mean the risk associated with completing that procedure is null. This is seen in both Shuttle accidents as well as in each airshow case study. Discounting the risk of a situation can also be tied to overconfidence in abilities or hardware success.

It can also be noted from the scorecard that the "discounting risk" complacency factor had more prevalence in the case studies where pilot overconfidence or pilot error were the main catalyst for complacency. While discounting risk is one of the results of overconfidence, overconfidence can lead to experiencing all 6 of the identified complacency factors and appears the hardest to circumvent. Overconfidence is a human factor that spawns from personal experiences. The more successful a mission or the more times a person survives risky behavior, the more confident that person becomes in their ability to perform the task again. It takes a catastrophic accident for that overconfidence to be put into check and for a reevaluation of the scenario to occur. NASA, the U.S Air Force, and the NTSB all take steps to evaluate past actions once an accident has occurred. The lines of communication are open once the complacency becomes apparent.

Occurrences of the "unrealistic risk assessment" complacency factor appear to be centered around long running, mission-oriented systems where risk assessments are conducted on previous flight failures prior to continuance. This type of complacency factor can be due to poor problem reporting or lack of communication of system capability. While unrealistic risk assessments were noted in those programs with reoccurring system failure and poor failure reporting methods, all of the researched organizations exhibited issues with communication as it pertains to the complacency factors. Communication gaps can lead generate misunderstandings in mission success, crew responsibility or managerial decisions. As was seen with the Challenger disaster and the B-52H airshow accident, the most senior management was not made aware of unwanted behavior on the part of the pilot or O-ring hardware. Communication of issues to those that make decisions is an important aspect in fighting complacency. Management needs to be able to make informed risk-based decisions; whether that is a decision to launch or to remove a pilot from duties.

A form of strengthening the lines of communication can be accomplished through effective problem reporting and evaluation of those problems. Effective problem reporting can provide better risk-based decisions and open the lines of communication to management. Both Shuttle accidents were victims of ineffective problem reporting evaluation. Time and again, both Challenger and Columbia experienced reoccurring failures of the O-ring and external tank foam respectively. Problem reporting, while completed, was not used to its full potential. Trending analysis was not completed for either failure mode, nor were proper problem closure procedures implanted. Both Shuttle missions had previous similar failures and both were bought off as a lower risk because it had occurred before without incident. It was, essentially, a ticking time bomb. This type of problem reporting without stringent trending or appropriate closure before next mission opens the gate to complacency.

In aerospace, reliance on automation or redundancy can lead to unrealistic risk assessments and possesses an extensive threat to successful operation. Redundancy is, in theory, a good thing to have built in to a system. However, over-reliance on redundancy or incorrectly identified redundancy such as in the

Challenger case, can lead to inappropriate managerial decisions. In the cockpit automation can be a double-edged sword. While the pilot workload is being decreased, aviators are being reduced to a supervisorial role. It is this supervisorial role where complacency can breed. It is important for aviators and engineers to maintain vigilance with redundancy and automation within their systems to avoid missed data points for risk analysis or inappropriate risk-based decisions.

Review of accident investigations revealed that complacency is a potential threat across all aerospace entities. A reoccurring theme found in each entity and through each case study was that trending of failures was imperative to identifying that a complacency issue existed. Analysis of problem reports, failures, and airmen behaviors can open up the lines of communication to senior management. Senior management are the persons responsible for making risk-based decisions for missions and recognition of complacency can be difficult without all the necessary information for identification. Trending would provide additional data points on reoccurrence of failure modes for management to make better informed risk-based decisions.

5.2 IMPLICATIONS OF RESULTS

5.2.1 Contributions to practice

The recognition of complacency and suitable corrective action can save lives and extensive hardware damage. Millions of dollars due to catastrophic loss or life or hardware, process escapements, or failures due to complacency can be saved with proper mitigation techniques.

5.2.2 Implications for future research

With proper access to accident investigation data and failure reports, it is the author's opinion that significant research can be compiled on complacency factors through trending analysis. Localized trending analysis can be extremely beneficial to an organization. Trending of failures on a particular part or process may reveal complacency in manufacturing, qualification or process operation. If access to one of the above case study organizations can be obtained, further investigation into a single failure can be conducted to examine complacency on a much more narrow scale.

5.3 LIMITATIONS OF STUDY

5.3.1 Biases

Working as an engineer within the aerospace industry has generated a bias towards focusing research and accident investigations primarily in the aerospace field. However, through extensive research on the root causes of complacency, it is evident that complacency can be a problem within any engineering or repetitive task oriented functions. While this is widespread issue, again, working within the aerospace community compelled the investigation in this area.

5.3.2 Lack of data

Limitations within the study came with the issue of confidentiality of data from the military programs, specifically the U.S. Army. As a contract employee for a military entity, there is a wealth of accident data available. However, only publicly available data can be discussed within this investigation.

6.0 SUMMARY

This investigation into engineering complacency and its root cause occurring in aerospace and aviation safety was completed with analysis of historical accident investigation data and the circumstances involved. Case studies were obtained from the aerospace and aviation industry that involve both engineering and operator error. Catastrophic accidents within military aircraft, NASA systems, and commercial aviation were explored. Accident case studies were drawn from the U.S Air Force, the U.S Army, NASA and the NTSB. These organizations were selected because they represent a large sampling of government aviation and aerospace programs as well as the commercial and private aviation sector. Analysis was conducted to look at the system safety programs, risk management, and corrective action procedures for each organization.

Examination of the different case studies showed that complacency exists across all forms of aerospace. During case study review the following question was asked to aide in developing a clear definition of complacency: Are safety philosophies and processes that are established to evade catastrophic events being given a low priority in the systems engineering process? From this question there are several subcategories that were identified that can be reviewed to further determine if complacency is an issue within a program. These include:

- Failure or Problem Reporting Methods: Were they not recording detailed information for escapements or failures and or incorrectly evaluating that data?
- Sedimentary Mind-set: Was the company in a "why change" mind-set? Being satisfied with the status quo or being too lazy to seek out and recognize improper operating conditions.
- Monotony: Was there a lack of interest – Not feeling challenged by a long running or seemingly easy program? Having a mindset that we don't need to learn much else. Ignoring small operational problems.

Asking this overall arching question during the investigation helped to determine reoccurring factors that categorize complacency. Six complacency factors were identified as reoccurring themes within the case studies. These factors are as follows:

- Ignoring Warning Signs
- Discounting Risk
- Unrealistic Risk Assessments
- Assuming Risk Decreases Over Time
- Ignoring high-consequence, low-probability events
- Over-reliance on redundancy or Automation

It was noted that in each case study the warning signs of complacency were seen in reoccurring hardware failures or repeated risky behaviors. It is this repetition that has led the author to conclude that effective problem reporting, trending of failures, and implementation of appropriate corrective actions prior to additional missions would facilitate to eliminate some complacency centered accidents. Analysis of failures through trending would allow for management to make better informed risk-based decision and allocation of resources.

7.0 CONCLUSION

7.1 RESEARCHER'S PERCEPTION OF THE STUDY

Complacency is a substantial risk throughout any human oriented task or engineering centric organization, not just aerospace. Complacency can be evaluated in the oil industry, nuclear industry, manufacturing and everyday tasks such as operating an automobile. This study was conducted across a broad aerospace scale but, while this was acceptable for identifying the complacency factors, it would be better explored on a smaller scale. Focusing on a particular failure mode in a single organization would allow for concentrated analysis and corporate culture specific trending.

7.2 RECOMMENDATIONS FOR FUTURE RESEARCH

Implementation of trending analysis to evaluate failure modes within all of the aforementioned organizations is imperative to identifying areas where complacent factors can occur. Trending analysis can be completed on pilot history (i.e. numerous check-ride failures), a specific type of failure mode for a subsystem, or a process failure.

REFERENCES

Aeronautica Civil of the Republic of Columbia. (1995). *Controlled Flight Into Terrain, American Airlines Flight 965, N651AA, Near Cali, Columbia, December 20, 1995.* Sante Fe de Bogota: Aeronautica Civil of the Republic of Columbia.

Association, I. E. (2010). *International Ergonomics Association.* Retrieved July 8, 2010, from What is Ergonomics?: http://www.iea.cc/01_what/What%20is%20Ergonomics.html

Bryson, M. C. (1984). Predicting low-probablity/hihg-consequence events. In R. Walker, & V. T. Covello, *Low Probability High Consequence Risk Analysis: Issues, Methods, and Case Studies* (pp. 188-189). New York: Plenum Press.

Department of Defense. (2005, January 11). *Department of Defense Human Factors Analysis and Classification System.* Retrieved April 2010, from United States Coast Guard: http://www.uscg.mil/safety/docs/ergo_hfacs/hfacs.pdf

Dupont, G. (1997). The dirty dozen errors in maintenance. *Eleventh Federal Aviation Administration Meeting on Human Factors Issues in Aircraft Maintenance and Inspection* (pp. 45-49). Wasington D.C.: Federal Aviation Administration/Office of Aviation Medicine.

Ericson II, C. A. (2005). *Hazard Analysis Techniques for System Safety.* Hoboken: John Wiley & Sons, Inc.

Federal Aviation Administration. (1965). *Aerodynamics for Naval Aviators.* Renton, Washington: Aviation Supplies & Academics, Inc.

Gehman, H. (2003). *Columbia Accident Investigation Report.* Washington D.C.: National Aeronautics and Space Administration.

Global Security. (2011). *B-52 Strtofortress.* Retrieved September 2011, from Global Security: http://www.globalsecurity.org/wmd/systems/b-52-describe.htm

Hunter, D. R. (2002). *Risk Perception and Risk Tolerance in Aircraft Pilots.* Washington D.C.: Federal Aviation Administration.

III, L. P. (2002). *The Relationship of Self-Efficacy and Complacency in Pilot-Autmation Interaction.* Hampton, Virgina: National Aeronautics and Space Administration, Langley Reserach Center.

Katz, L. C. (2006). *Finding the 'Right Stuff': Development of an Army Aviator Selection Instrument.* Fort Rucker: U.S. Army Research Institute for the Behavioral and Social Sciences.

Kern, T. (1995). *Darker Shades of Blue: A Case Study of Failed Leadership.* Washington, D.C. : U.S. Air Force.

Kraft, C. (1995). *Report of the Space Shuttle Management Independent Review Team.* Houston: National Aeronautics and Space Administration, Johnson Space Center.

Leveson, N. G. (2004). *Massachusetts Institute of Technology.* Retrieved January 13, 2010, from What System Safety Engineering Can Learn from the Columbia Accident: http://sunnyday.mit.edu/papers/issc04-final.pdf

Leveson, N. G. (2005). *Modeling, Analyzing, and Engineering NASA's Safety Culture.* Retrieved February 6, 2010, from Massachusetts Institute of Technology, Aeronautics and Astronautics Department: http://sunnyday.mit.edu/Phase1-Final-Report.pdf

Leveson, N. G. (2002). *System Safety Engineering: Back to the Future.* Cambridge: Massachusetts Institute of Technology.

Leveson, N. G. (2001). *Systematic Factors in Software-related Spacecraft Accident. AIAA Space Conference and Exposition. Paper AIAA 2001-4763.* Reston, VA: AIAA.

Machol, R. (1975). The Titanic Coincidence. *Interfaces* , 53-54.

NASA JPL. (2000, March 22). Retrieved May 23, 2010, from Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions: http://sunnyday.mit.edu/accidents/mpl_report_1.pdf

NASA KSC. (2006). *NASA Facts: Orbiter Thermal Protection System.* Retrieved March 2, 2010, from National Aeronautics Space Administration, Kennedy Space Center: http://www-pao.ksc.nasa.gov/kscpao/nasafact/pdf/TPS-06rev.pdf

NASA. (1985). *National Aeronautics and Space Act of 1958, As Amended.* Washnigton D.C.: National Aeronautics and Space Administration.

NASA. (1986). *Report of the Presidential Commision on the Space Shuttle Challenger Accident.* Washington D.C.: National Aeronautics and Space Administration.

NTSB. (1987). *Aircraft Accident Report Northwest Airlines McDonnel Douglas DC-9-82, N312RC Detroit Metropolitan Wayne County Airport Romulus, Michigan August 16, 1987.* Washington D.C.: National Transportation Safety Board.

NTSB. (2009). *Loss of Control on Approach Colgain Air, Inc Operating as Continental Connection Flight 3407 Bombardier DHC-8-400, N200WQ Clarence Center, New York February 12, 2009.* Wshington D.C.: National Transportation Safety Board.

NTSB. (2006, December 21). *National Transportation Safety Board Statute.* Retrieved September 18, 2010, from National Transportation Safety Board: http://www.ntsb.gov/alj/NTSB_statute.htm#1111

O'Connor, B. (2009, Summer). *National Aeronautics and Space Administration.* Retrieved July 25, 2010, from NASA Ask Magazine: http://askmagazine.nasa.gov/issues/35/35i_safety_lessons_learned.html

Organization, I. C. (1984). *Accident Prevention Manual.* ICAO.

Parsons, H. M. (1985). Automation and the Individual: Comprehensive and Comparative Views. *Human Factors* , 99-111.

Petroski, H. (1992). *To Engineer is Human: The Role of Failure in Success Design.* New York: Vantage Books.

Pries, J. (2002 йил 11-January). *Airliners.net.* Retrieved 2011 йил August from Airliners.net: http://www.airliners.net/photo/Northwest-Airlines/McDonnell-Douglas-MD-82/0212595/

Readdy, W. F. (2001, Septemeber 6). Testimony of William F. Readdy to the Subcommittee on Science, Technology and Space. (U. S. Senate, Interviewer)

Reserach Integration. (2007). *ASRS Incident Report Analysis Flight Deck Automation Issues.* Retrieved November 12, 2010, from Research Integration: <www.flightdeck-automation.com/incidentstudy/indicentanalysis.aspx>

Singh, I. L., Molloy, R., & Parasuraman, R. (1993). Individual differences in mointoring failures of automation. *Journal of General Psychology* , 357-373.

Stewart II, J. E. (2006). *Technical Report 1182: Locus of Control, Attribution Theory, and the "Five Dealy Sins" of Aviation.* Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.

Transport Canada, Safety and Security Commercial & Business Aviation, Operational Standards. (2001, April 15). *BOMBARDIER DHC8-400.* Retrieved September 15, 2011, from Transport Canada: http://www.tc.gc.ca/eng/civilaviation/standards/commerce-3776.htm

Trimble, S. (2010 йил 17-Decmeber). *C-17 crash report exposes cracks in USAF safety culture.* Retrieved 2011 йил 19-August from Flight Global: http://www.flightglobal.com/news/articles/c-17-crash-report-exposes-cracks-in-usaf-safety-culture-351032/

U.S. Air Force Accident Investigation Board. (1994). *Accident Investigation Report B-52H, SN 61-0026 Fairchild AFB, Washington.* Davis-Monthan AFB: United States Air Force.

U.S. Air Force Accident Investigation Board. (2010). *C-17A, T/N 00-0173 3rd Wing Joint Base Elmendorf-Richardson, Alaska.* Langley Air Force Base, Virginia: U.S. Air Force.

U.S. Air Force. (2010d). *U.S. Air Force Information Factsheet: C-17.* Retrieved September 2011, from United States Air Force: http://www.af.mil/information/factsheets/factsheet.asp?id=86

United States Air Force. (2010b, June 9). *U.S. Air Force Information Fact Sheet.* Retrieved September 18, 2010, from United States Air Force: http://www.af.mil/information/factsheets/factsheet.asp?id=2

United States Air Force. (2010c). *U.S. Air Force Information Fact Sheets: B-52.* Retrieved August 2011, from Official Site of the U.S. Air Force: http://www.af.mil/information/factsheets/factsheet.asp?id=83

United States Air Force. (2010a, February 9). *U.S. Air Force Posture Statement.* Retrieved Septemeber 18, 2010, from United States Air Force: http://www.posturestatement.af.mil/shared/media/document/AFD-100223-010.pdf

United States Army. (2009). *Safety: Army Accident Investigations and Reporting.* Washington D.C.: Department of the Army.

United States Army. (2006, February 6). *United States Army.* Retrieved September 18, 2010, from United States Army Posture Statement: http://www.army.mil/aps/05/index.html

United States Army. (2010, Septemeber). *United States Army.* Retrieved September 18, 2010, from U.S. Army Center of Military History: http://www.history.army.mil/

Webb, C. M., & Hewett, K. J. (2010). *An Analysis of U.S. Army Fratricide Incidents during the Global War on Terror (11 September 2001 to 31 March 2008).* Fort Belvoir, Virgina: United States Army Aeromedical Research Laboratory.