

# Chapter 1. Introduction

On January 28, 1986, the space shuttle *Challenger* exploded, forever altering the course of America's space policy. Prior to the final *Challenger* mission, labeled STS-51L by NASA<sup>3</sup>, the policy had mandated that the space shuttle would be America's "primary launch vehicle for both national security and civil government" and "available to authorized users—domestic and foreign, commercial and governmental."<sup>4</sup> This policy is controlled by an executive branch document, the National Space Policy, which outlines the strategic planning in this area for the U.S. government. Within months following the accident, the nation changed courses and the policy was rewritten to limit who and what could fly on future space shuttle missions.<sup>5</sup> No longer would the shuttle be permitted to fly commercial or foreign payloads.<sup>6</sup>

Just as significantly, the revised National Space Policy no longer called for the shuttle to be America's primary launch vehicle, but rather advocated a mixed-fleet concept that promoted expendable launch vehicles.<sup>7</sup> NASA long had been hailed as a shining example of all the good things in America and held up as the standard for those interested in understanding how best to manage large complex technical systems. Now NASA would not only see the scope of its mission significantly modified, but it would have to sit and watch as its image was battered and its competence questioned.

## 1.1 The Quandary

Today, the *Challenger* failure is perhaps the most chronicled system failure in history. It has been the subject of hundreds of scholarly reviews, professional papers, books, and academic journal articles as well as the focus of countless television, radio, newspaper and magazine commentaries. In addition, NASA maintains literally tons of procedures and other standard

---

<sup>3</sup> The space shuttle program originally was named the Space Transportation System (STS) and flights were numbered in sequence. It also was referred to as the National Space Transportation System (NSTS)

<sup>4</sup> United States Space Policy, The White House Fact Sheets, 4 July 1982, p. 98, col. 2.

<sup>5</sup> Presidential Directive on National Space Policy, 11 February 1988.

<sup>6</sup> An exception was provided for those commercial or foreign payloads that required the Shuttle's "unique capabilities," human presence, or supported national security.

<sup>7</sup> Presidential Directive on National Space Policy, 11 February 1988, p. 192.

paperwork for each space shuttle launch. To illustrate the quantity of the source material, there are over one million separate steps involved in processing the shuttle for each mission and the library of primary sources for the internal NASA review of the *Challenger* failure filled over four thousand square feet of warehouse space. These data are in addition to the data recorded in the launch and operations computers that are retrieved or printed only in unusual cases.

Despite the volumes of data, surprisingly enough, over a decade after the accident, still there is no agreement on answers to the two most fundamental questions. First, what exactly was the “root cause” of the failure? Second, what were the ultimate consequences? While there is general agreement that the now infamous O-Rings were the triggering event leading directly to the explosion of *Challenger*, debates continue to rage over the “real” cause. Was it that senior NASA officials, lacking in integrity, succumbed to political pressures and agreed to a series of budget compromises that resulted in the design and construction of an inherently unsafe space shuttle? Was the NASA culture, blinded by its successes, collectively engaged in groupthink? Was it an ineffective NASA Safety organization coupled with a new willingness on the part of NASA managers to launch at risk to human life? Was it the arrogance of a single NASA manager at the Marshall Space Flight Center who overrode the advice of his engineers not to launch *Challenger*? Or was it that NASA succumbed to political pressure and agreed to launch *Challenger* in spite of the known risks on that fateful day in January 1986? The hypotheses about the root cause of the space shuttle *Challenger* failure are as varied as there are those interested in expressing opinions.

Just as there is no agreement on the root cause, there is no consensus on the ultimate consequences of the failure of the space shuttle *Challenger*. All agree the death of seven people and the destruction of a two billion-dollar national asset were tragic, but who suffered most in the long run depends upon one’s perspective. Was it the set back to space science? Was it the loss of America’s competitive advantage in the launch market? Was it a commercial satellite market, which lost millions of dollars in revenue and had to expend even more to find new transportation into space? Was it a weakened national defense that could not get its spy satellites into space? Was it a tarnished NASA image that would never recover? Or something else?

What can we learn by examining the underlying assumptions used by those who have studied this failure? What insights can be gained by those engaged in trying to better understand system failure? What do the assumptions the analysts make teach us about the causes of these failures? What guidance do they offer in attempts to avoid or mitigate the ensuing consequences?

Answers to these questions cannot be found by a closer examination of the evidence surrounding the *Challenger* failure. Given the exhaustive analysis of the failure to date, my contribution to its understanding comes not from yet another review from the same vantage point. Instead, it comes from an analysis of the foundations upon which past examinations of system failure are grounded and how they relate to the *Challenger* failure.

## 1.2 The Argument

The expanding global economy is fueling greater competition, driving the development of more and more complex systems in the never-ending effort to accomplish more with less. Remaining trade barriers are disappearing through such agreements as the North American Free Trade Agreement and the common monetary system in Europe represented by the Euro. Industries within a country, which formerly had been protected, now must compete on an international level. “American” cars are made in Mexico and Mercedes Benz (now Chrysler-Benz) sport utility vehicles are made in Alabama. In this larger market, the competition is less tolerant of failure. Managing risk becomes a fundamental requirement for any successful organization.

This cycle appears only to be quickening as we enter the next century. Fueled by the explosion in communications, business is conducted 24 hours a day around the world. No longer do we look only at the Dow Jones, but at the London FTSE, Toyko Nikkei, and Frankfurt DAX averages on the world market. With pressure to be the first to market, design cycles are shortening, testing is accelerated, and not-quite-ready products are being sold. This situation is not new to our generation. Throughout history, the pace has quickened with each generation. The difference is that the rate at which change occurs continues to accelerate to the point where no single person can be cognizant of all the aspects surrounding a particular system.

The widespread use of these complex systems introduces risks to those individuals who depend on them for their livelihood or services they provide as well as those who may be exposed to them. When one of these complex systems fails, the result most often is a significant loss of capital; substantial equipment or facility damage, injury or loss of life, and of course, in many cases the loss of public confidence. As aircraft are being designed to carry more people and industrial systems become more automated, many of these systems are employed in arenas where their failure results in the loss of human life. For example, highway construction deaths continue to skyrocket, climbing from 489 in 1982 to 780 in 1988.<sup>8</sup> Stephen Fehr, writing in the *Washington Post* noted that “the number of people killed in accidents at highway construction sites is increasing so fast in Maryland, Virginia, and other states that the National Transportation Safety Board called yesterday on federal, state, and industry officials to develop a safety program.”<sup>9</sup> Acting Board Chairwomen at the time, Susan M. Coughlin, warned “if you combine the upward trend in accidents with the increased construction activity, it’s spelling a foregone conclusion.”<sup>10</sup>

Another casualty of a system failure is the ensuing loss of public confidence that translates into losses in funding, profitability, and jobs. The grounding of Value Jet airlines in the aftermath of the May 11, 1996 crash of Flight 592 into the Florida Everglades provides evidence of the penalties associated with failure. In addition to the loss of a multimillion-dollar airplane and the tragic deaths of 110 people, the airline would suffer a significant loss of public support and its bottom line would take a beating. Once the pride of discount airline carriers, Value Jet saw its fleet increase from two planes and eight routes to 51 planes and 320 routes and watched revenues soar to \$368 million in just three short years.<sup>11</sup> With the crash Value Jet overnight became the target of a barrage of investigations into its operations and its stock plummeted 37 percent from the \$17.88 price on May 10, one day before the crash.<sup>12</sup>

---

<sup>8</sup> Stephen C. Fehr, “Highway Construction Deaths Skyrocket, Safety Panel Says,” *Washington Post*, 13 May 1992, Sec. A, p. 2, col. 2. According to Fehr and the National Transportation Safety Board this was the latest year national figures cumulatively compiled

<sup>9</sup> Fehr, Sec. A, p. 2, col. 2.

<sup>10</sup> Fehr, Sec. A, p. 2, col. 2.

<sup>11</sup> Mary Schiavo, “Flying Blind, Flying Save,” Excerpts in *Time*, 31 March 1997, p. 55.

<sup>12</sup> Cable News Network, Inc. 21 May 1996 <http://cnfn.com/archivenews/9605/21/valujet/index.htm>

Those seeking to understand system failure do so in an attempt either to prevent future occurrences or to assign blame for past failures. The first objective is to understand what led to the failure so that it will not be repeated. In those cases where the failure cannot be effectively prevented, the system operators seek then to minimize the effects that would result from an additional failure. In addition to these operational steps, stakeholders inside and outside the organization seek to locate the people “accountable” for the failure. Legal representatives, insurance companies, and the general public demand answers, which include the identification of responsible parties. Inside the organization, managers are replaced, offices shuffled, and processes changed. As Malcolm Gladwell recently wrote in a commentary in The New Yorker:

In the technological age, there is a ritual to disaster. When planes crash or chemical plants explode, each piece of physical evidence - of twisted metal or fractured concrete - becomes a kind of fetish object, painstakingly located, mapped, tagged, and analyzed, with findings submitted to boards of inquiry that then probe and interview and soberly draw conclusions. It is a ritual of reassurance, based on the principle that what we learn from one accident can help us prevent another.<sup>13</sup>

Gladwell continues on to note that “In real accidents, people rant and rave and hunt down the culprit.”<sup>14</sup>

Those analyzing system failures bring with them knowledge, training, and prejudices that create conceptual lenses which frame their analysis. These conceptual lenses influence how the analyst looks at the system failure. These conceptual lenses further guide what the analyst looks for and what is deemed important. The analyst’s background determines what questions he or she asks about a system failure. In turn these questions and their answers determine what the analyst sees in the failure and its aftermath. Finally, these observations influence the analyst in recommending how the organization should act before, during, and after a system fails.

Most who study system failures utilize the classical paradigm. The basic premise of the classical paradigm is that with enough research one can accurately discern all the facts surrounding a system failure. The classical paradigm is built upon the principles of classical mechanics, specifically reductionism, cause and effect, and determinism. Using these concepts, analysts believe that they can accurately determine and predict the cause and consequence of any

---

<sup>13</sup> Malcolm Gladwell, “Blowup,” The New Yorker, 22 January 1996, p. 36.

<sup>14</sup> Gladwell, p. 36.

system failure. Analysts, however, do not always agree on how best to employ the classical paradigm, and thus frequently develop conflicting findings. Although they may not all agree on the answer, or for that matter even the questions, they all implicitly accept the validity of the classical approach.

While the classical paradigm has served us fairly well to date, on its own it appears to be inadequate in explaining causes and consequences of a system failure. First, the general lack of agreement about the root cause of most failures illustrates that the paradigm does not clearly resolve the issues surrounding the failure. Second, the model levies a preferred framework on the examination process, forcing the failure into one of a number of predefined categories. Third, analysts using this paradigm ignore factors which, though they could have a bearing on the failure, do not fit into their frame of reference.

Modern physics provides an alternative paradigm, which I have chosen to call the contemporary paradigm, to improve our analysis of system failure. This paradigm does not discard the Newtonian world which palpably we can see and feel, but rather provides us with tools for increasing our ability to understand the events which lie behind the actual system failures. The theories embodied in the paradigm, grounded in the concepts of modern physics and nonlinear mathematics, hold that the 'real' world is far more complex and uncertain than previously believed. This complexity limits our ability to measure and predict either the causes or consequences of a system failure.

In the contemporary paradigm, the elements of a system failure cannot be reduced to a single cause or consequence, or a comprehensive set of contributing elements with their relationships clearly defined. Instead, the paradigm recognizes that each system failure has multiple causes and consequences which cannot always be accurately identified or precisely measured to determine their relative importance in the occurrence of the failure. Similarly, the contemporary paradigm does not embrace the classical concept of cause and effect. Replacing the classical concept of determinism that the effect of change can be predicted and measured in advance, the contemporary paradigm holds that many situations are too complex to accurately predict the complete range of consequences which result.

These characteristics of this contemporary paradigm provide an alternative structure for understanding and managing complex systems. The paradigm does not assume there is a single answer to the questions raised by the classical analysts. Rather than attempt to settle on a single root cause of a failure, contemporary analysts examine how the various factors contribute to a failure. Also, with no preconceived notion of the framework into which the failure should fit, the contemporary analyst looks to the failure itself to help define the best method for examining the cause-consequence equation.

Without a preferred frame of reference, the contemporary analyst does not bring a bias from which to examine the failure. As a result, the questions asked are not tailored to elicit any particular set of data for use in a constrained paradigm. With this wider data set, the analyst has the opportunity to view the failure through a broader lens, incorporating pieces of data that could reveal a more coherent picture of the failure. In turn, this larger picture can influence the way in which the organization acts to prevent future failures or its response in the aftermath of a given failure.

### 1.3 The Approach

The failure of the space shuttle *Challenger* provides an ideal mechanism for demonstrating the differences between the classical and contemporary paradigms as well as for exploring the relative utility of each paradigm. It represents an undeniably complex system and has many implications for national policy development and decision making. Because it is a real life example I was able to use actual data as opposed to hypothetical data, discuss the preceding and subsequent events with participants, take advantage of the vast amount of literature surrounding the event, and employ multiple data collection methods. In addition to the written records maintained by NASA and the other public and private organizations, I reviewed observations from outside observers and conducted interviews with many people who actively participated in the *Challenger* mishap investigations. The availability of multiple sources

allowed me to combine data collection methods on a single topic and to cross correlate data from different sources.<sup>15</sup>

In addition to being perhaps the most extensively documented system failure in history, the *Challenger* failure also has the unique advantage of being recent enough in time that many of the individuals involved were available to be questioned. I was able to interview actual participants about the events prior to and following the failure. Many of these individuals still work in the field and have kept abreast both of the particulars of the failure and of the industry. Many have read extensively the post-mortem analyses of the failure and are familiar with the competing theories surrounding the failure. At the same time, enough time has passed for academicians and practitioners alike to step back and consider the accident objectively.

I have chosen to adopt the approach used so successfully by Graham Allison in Essence of Decision: Explaining the Cuban Missile Crisis. In this seminal work, Allison begins by examining the assumptions and methods used by an analyst to examine decision-making. Then, he uses these data to build a paradigm that provides a structured summary of the analyst's approach. This paradigm is used to explain actions taken by the decision-makers in a particular situation, in this case the Cuban Missile Crisis. Allison follows by defining alternative paradigms and illustrates how they provide different insights into the crisis and its surrounding events.

I have adapted this approach to the study of system failure. First, I review the current system failure literature to understand the findings of each author, the concepts on which these findings are built, and the underlying assumptions, which formed the foundation for these concepts. A review of the literature revealed a number of common patterns. The majority of the literature focuses on determining the root cause of the failure. At no time is the discovery of this root cause considered beyond the reach of the analyst. The remaining analysts look to the consequences that resulted from the failure. Their findings are considered the inevitable result of actions taken by participants in the failure situation. In turn, the analyst develops concepts that script these actions as closely as dance steps in a complex choreography.

---

<sup>15</sup> This is highly desirable when articulating the need for a new theory and supporting one's argument using the case study approach. See Kathleen M. Eisenhardt, "Building theories from Case Study Research," Academy of Management Review, 1989, Vol. 14, No. 4, pp. 532-550.

Using these concepts and assumptions, I then construct the paradigms that serve as the basis for each analysis. As Robert Merton notes in Social Theory and Social Structure, paradigms provide a “codified guide” for documenting the basic tenets of each method of study and their organizing concepts.<sup>16</sup> He writes, “They thus reduce the inadvertent tendency to hide the hard core of analysis behind a veil of random, though possibly illuminating, comments and thoughts.”<sup>17</sup> These elements are described in more detail through a series of general propositions supported by specific propositions that describe the underpinnings of the paradigms. The paradigms represent the minimum amount of structure required to illustrate the differences in approaching a system failure, and to provide a basis for comparing these approaches.

Merton cites several advantages of using paradigms in this type of analysis:

1. Paradigms have a notational function. They provide a compact arrangement of the central concepts and their interrelations that are utilized for description and analysis...
2. Paradigms lessen the likelihood of inadvertently introducing hidden assumptions and concepts, for each new concept must be either logically derived from previous components of the paradigm or explicitly introduced into it...
3. Paradigms advance the cumulation of theoretical interpretation...
4. Paradigms, by their very arrangement, suggest the systematic cross-tabulation of significant concepts and can thus sensitize the analyst to empirical and theoretical problems which he might otherwise overlook...
5. Paradigms make for the codification of qualitative analysis in a way that approximates the logical if not the empirical rigor of quantitative analysis.<sup>18</sup>

Second, using these two paradigms, which provide a structured framework for examining a system failure, I examine the failure of the space shuttle *Challenger* from each vantage point. By using one failure, the space shuttle *Challenger*, the variable represented by the system failure itself becomes a constant and provides a level playing field against which to explore the relative utility of both paradigms. The similarities and differences between the paradigms come into focus when both are applied to a single case study.

---

<sup>16</sup> Merton, p. 109.

<sup>17</sup> Merton, p. 69.

<sup>18</sup> Robert K. Merton, Social Theory and Social Structure, 3<sup>rd</sup> ed. (New York, NY: The Free Press 1968), pp. 70-72.

I chose the embedded single case study design to test and refine the conceptual lenses provided by the classical and contemporary paradigms, because my objective was not to present a “statistically significant survey of events,” but rather to determine how we might better understand and manage system failure in the future.<sup>19</sup> I did not use statistical sampling techniques because they are more suited to research in which a random sample of a population is surveyed, with the goal to determine the distribution of results across the population as a factor of the variables involved.<sup>20</sup> As Yin notes in Case Study Research - Design and Methods, “survey research relies on statistical generalization, whereas case studies rely on analytical generalization.”<sup>21</sup> “In analytical generalization, the investigator is striving to generalize a particular set of results to some broader theory.”<sup>22</sup> Hence, my decision to utilize case study methodology is particularly appropriate because I am not proposing a refinement of existing practices but instead departing from the theories presented in current system failure literature. As Yin notes, this is the preferred design when a “critical case” can be defined and more than one unit of analysis within the same case will be examined.<sup>23</sup> Limiting the study to a single case enabled me to conduct a more comprehensive study of managing the risk of complex system failure.

Necessary to any discussion of this case study is a basic understanding of the shuttle system and its components. As shown in Figure 1-1, the shuttle is composed of the aircraft-like orbiter, an external tank which provides the fuel for the orbiter’s engines, and two solid rocket boosters which give the shuttle initial thrust on launch. Much of the discussion on the *Challenger* accident focuses on the performance of the solid rocket boosters. These boosters ultimately became the focus of a public investigation into the *Challenger* failure.

---

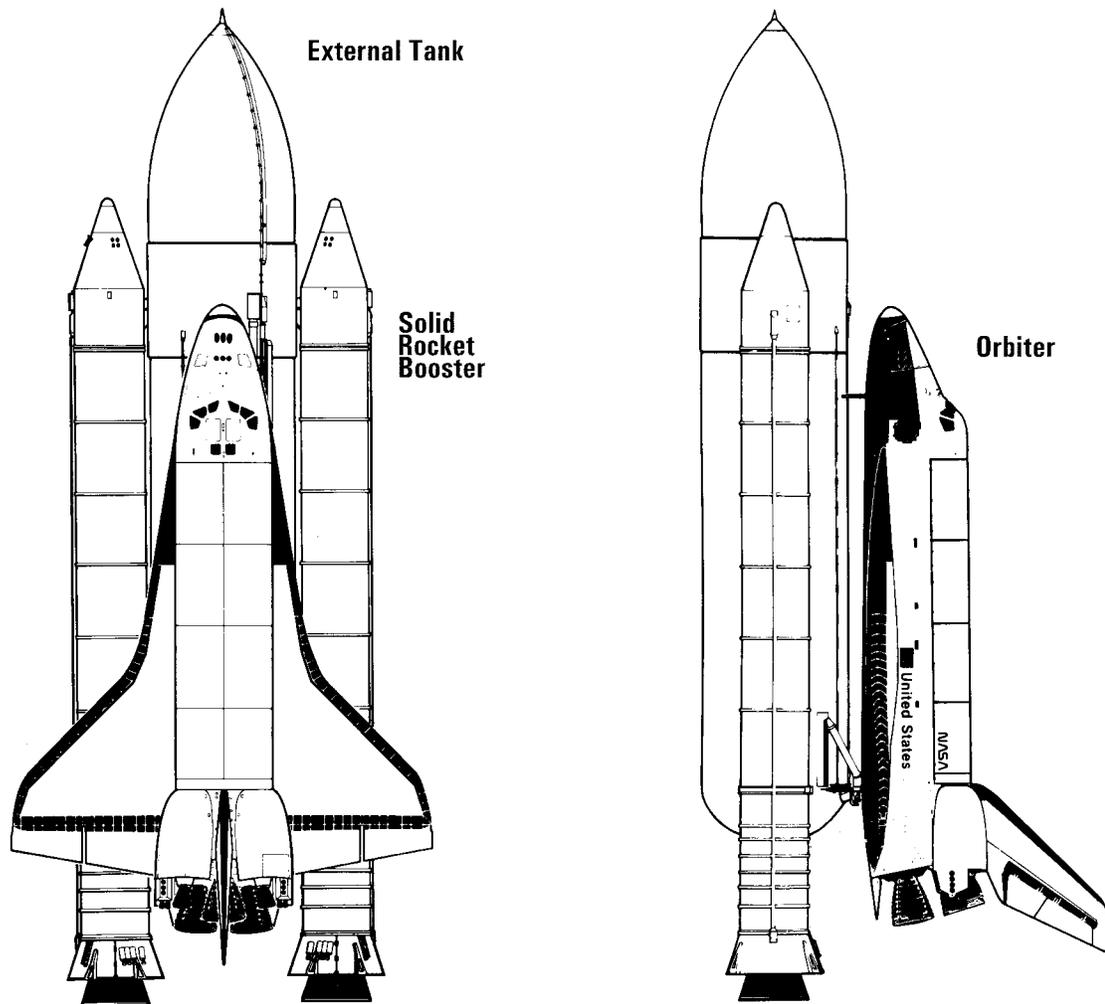
<sup>19</sup> See Robert K. Yin, Case Study Research: Design and Methods (Thousand Oaks, Cal: Sage Publications, Inc. 1994), p. 36-43 for more information about this design and the reasons for its selection as the preferred design.

<sup>20</sup> Eisnehardt, p. 534 and Yin, p. 36.

<sup>21</sup> Yin, p. 30-31.

<sup>22</sup> Yin, p. 36.

<sup>23</sup> Yin, p. 44.



Artist's drawing depicts Space Shuttle stacked for launch in view from dorsal side of Orbiter (left) and from the left side of stack.

Figure 1-1 - Space Shuttle System<sup>24</sup>

<sup>24</sup> Report of the Presidential Commission on the Space *Challenger* Accident, p. 3.