UNDERSTANDING THE *CHALLENGER* DISASTER: ORGANIZATIONAL STRUCTURE AND THE DESIGN OF RELIABLE SYSTEMS

C. F. LARRY HEIMANN *Michigan State University*

The destruction of the space shuttle Challenger *was a tremendous blow to American space policy. To what extent was this loss the result of organizational factors at the National Aeronautics and Space Administration? To discuss this question analytically, we need a theory of organizational reliability and agency behavior. Martin Landau's work on redundancy and administrative performance provides a good starting point for such an effort. Expanding on Landau's work, I formulate a more comprehensive theory of organizational reliability that incorporates both type I and type II errors. These principles are then applied in a study of NASA and its administrative behavior before and after the* Challenger *accident.*

On 28 January 1986, the entire nation focused on a single event. Seventy-three seconds after lift-off, the space shuttle *Challenger* was destroyed in a powerful explosion fifty thousand feet above the Kennedy Space Center. The losses resulting from this catastrophe were quite high. Seven astronauts, including Teacher-in-Space Christa McAuliffe, were killed as the shuttle broke apart and fell into the sea. The shuttle itself had to be replaced at a cost of over two billion dollars. The launch of many important commercial and military satellites had to be delayed as American space policy ground to a complete halt. The accident had a profound impact on the National Aeronautics and Space Administration (NASA), as well. The agency's credibility and its reputation for flawless execution of complex technological tasks were lost, along with the *Challenger*. To this day, the legacy of the *Challenger* haunts the decisions of both the agency and its political superiors in Congress and the White House.

An examination of the shuttle remnants and other launch data revealed the technical cause of the accident. The shuttle was destroyed when an O-ring seal on the right solid rocket motor failed, allowing the escaping hot gases to burn through and ignite the main fuel tank of liquid hydrogen and liquid oxygen. Although identifying the technical cause of this disaster is important, it represents only one aspect of the problem. Perrow (1984) has argued that organizational and technological failures have become so intimately linked that to fully understand the cause of most major accidents, we must analyze both the administrative and technical aspects of the situation. While there have been some administrative critiques of NASA in the wake of this disaster, almost all have centered on issues of bureaucratic culture, such as the agency's propensity to ignore key evidence and its myopic view of its mission. Surprisingly little has been done on a systematic analysis of the NASA organization structure and how it may or may not have contributed to the loss of the *Challenger*.

One reason for this void is that the analytical tool necessary—a comprehensive theory of organizational reliability—is still lacking. Those involved in the debate over structural design have adopted two opposing stances. The traditional public administration focus on organizational design has involved the pursuit of efficiency in the sense of minimizing costs for a given level of output. Implicit in this traditional analysis is that the reliable performance of the organization was constant. The critical question, therefore, has usually been how one might achieve same level of services at a lower cost. As a result, the policy recommendations from this traditional line of thinking have been to streamline administrative systems and reduce organizational redundancy as much as possible.

The work of Martin Landau (1969) on redundancy in organizations was a particularly important contribution to this debate, inasmuch as he recognized that administrative reliability is dependent on structural factors. In breaking with conventional wisdom, Landau's landmark 1969 essay, "Redundancy, Rationality, and the Problem of Duplication and Overlap," asserted that the critical question was not how to cut the costs of administrative performance but, rather, how to ensure the organization's effectiveness. Landau began by noting that, "no matter how much a part is perfected, there is always the chance that it will fail" (p. 350). As he observed, a streamlined system requires only one part to fail for the entire system to fail. Drawing on concepts from engineering reliability theory, Landau argued that redundancy built into the system can make an organization more reliable than any of its parts. Therefore, Landau concluded, administrative redundancy and duplication can be an important part of effective government.

Some work has been done to extend Landau's initial insights regarding organizational redundancy and administrative reliability, primarily by students and colleagues of Landau. Jon Bendor's (1985) *Parallel Systems*, originally written as a dissertation under Landau, was the most comprehensive effort to follow up on these ideas. Bendor formalized many of Landau's concepts and was the first to conduct empirical testing of these propositions, focusing on transportation planning and operations in three American metropolitan areas. Donald Chisholm's (1989) *Coordination without Hierarchy,* also written originally as a dissertation under Landau, discussed the notion of reliability and redundancy as it existed in informal organizational structures. Others have extended some of Landau's concepts of reliability to the operations of air traffic controllers and aircraft carrier battle groups (LaPorte and Consolini 1991; Rochlin, LaPorte, and Roberts 1987).

The policy prescriptions that follow from these two positions are thus quite different. The traditionalist argument tells us to reduce redundancy and streamline administrative systems whenever possible, whereas Landau advocates increasing redundancy by adding parallel units to the system. Most interesting, however, is the fact that an analysis of the organizational changes at NASA reveals that neither the traditionalists nor Landau are fully correct. Certain parts of the space agency followed a traditionalist policy of streamlining, while other segments of NASA adopted the Landau perspective by generating new parallel linkages. Yet (as I shall show), both these decisions were wrong and contributed to the untimely destruction of the *Challenger*.

How can this be? The reason is a fundamental limitation in the current framework for discussing organizational reliability. Most work in this area has implicitly assumed that there was only one kind of institutional failure and thus only two possible states for organizational performance: the agency either adopted the proper policy or not. But it should be recognized that the latter possibility conceals two different problems: the agency can simply fail to act, or it can adopt an *improper* policy. Considering the impact of both forms of error is important, because it leads us to a different set of policy prescriptions. An organizational structure that is effective at preventing one type of error may not be equally effective at preventing the other type of error.

To date, Bendor alone has formally recognized this distinction; but his analysis was limited (1985, 49–52). I shall extend our understanding of organizational reliability by exploring how each kind of failure is affected by different kinds of administrative structures. I shall lay a foundation for an analysis of multiple forms of administrative failure by describing the principles from engineering reliability theory, then show how different kinds of structures leave the agency vulnerable to different kinds of errors. Applying these arguments to the structure and decision-making process of NASA in the pre- and post-*Challenger* eras, I shall argue that the disaster had its roots in the structural changes adopted by the space agency in the 1970s and 1980s.

Although occasionally cited by students of public administration, Landau's work on institutional performance and reliability has received little attention from political scientists. One possible reason for this stems from the engineering roots of reliability theory. Political scientists may have considered the issue of organizational redundancy and reliability simply to be a technocratic problem that could be solved by reference to engineering formulas that dictate the appropriate structural form and do not raise political issues. Indeed, if we limit the scope of the problem to two-state devices, this apolitical view of structural design has some merit. But in a system with multiple types of errors, trade-offs between the errors must be made; and this moves us into the realm of politics. Which goals will be embraced? How will resources be allocated to combat each kind of error? Answers to these questions are ultimately political issues.

TWO TYPES OF ADMINISTRATIVE ERRORS

Before proceeding further, it is important to discuss more thoroughly what is meant by the term *policy failure*. As just noted, administrative problems often have a richer structure than the simple two-state (operating/failed) model can incorporate. In particular, bureaucracies are often in the position to commit two types of errors; (1) implemention of the wrong policy, an error of commission; and (2) failure to act when action is warranted, an error of omission. If we consider the agency's decision to take action to be comparable to the acceptance of a hypothesis, we can relate these two kinds of failures to the more familiar type I and type II errors often studied in statistics.

To establish this link, we must first define the null and alternative hypothesis in terms of potential bureaucratic action. Since presumption often favors the status quo, let us consider the null hypothesis to be that the agency should not take any new action and the alternative hypothesis to be that the bureau should take such action. Therefore, if the agency chooses to act when it is improper to do so (rejects the null hypothesis when it is true), a type I error has been committed. Likewise, if the bureau fails to act in a situation where it should (accepts the null hypothesis when it is false), then a type II error has been committed.

To illustrate the concept of type I and type II errors in organizational systems, let us consider the example of NASA and its decision to launch the space shuttle. The space agency traditionally approaches the launch decision with the assumption that a mission is not safe to fly. Subordinates are then required to prove that such is not the case before the launch is permitted. The null hypothesis, therefore, is that the mission should be aborted. If NASA were to reject the null hypothesis by launching a mission that is actually unsafe, it would be committing a type I error. On the other hand, if NASA decided not to launch a mission that was technologically sound, then it would have committed a type II error. The agency's choices and consequences are summarized in Figure 1.

Each form of failure is associated with a different set of costs. By committing a type II error, NASA loses the opportunity to achieve its objectives and wastes time, effort, and materials that could have

FIGURE 1

Summary of NASA Responses and Possible Errors Regarding Launch Decisions

NASA decides to:	The proper course of action: Launch	Abort
Launch	Correct Decision Mission successful	Type I Error Accident occurs; Possible loss of life and/or equipment
Abort	Type II Error Missed opportunity; wasted resources	Correct Decision Accident avoided

null hypothesis: the mission should be aborted.

been usefully employed elsewhere. For example, the shuttle's propellants in the external tank, liquid hydrogen and liquid oxygen, are lost if the mission is scrubbed and have alone been valued at approximately five hundred thousand dollars. Furthermore, the agency may forfeit the opportunity to carry out rare scientific research, as was the case when NASA missed the launch date for its ASTRO mission to study Halley's Comet. The *Challenger* accident clearly demonstrated, however, that a type I failure may be far more costly. The destroyed shuttle was replaced by the *Endeavour* at an expense over two billion dollars, and the death of the seven astronauts represents an incalculable loss. Certainly, in the case of NASA, type I errors are associated with greater costs than type II failures. The exact cost trade-off between these types of failure would vary, of course, for different agencies and according to the individual circumstances prevailing at the time of each decision. For this reason, it is important to develop a general approach to the study of organizational reliability that recognizes both types of errors and identifies the consequences associated with them.

By recognizing both forms of potential failure, we are better able to understand the nature of the trade-offs demanded. As with hypothesis testing, gains in type I reliability often come at the expense of type II reliability. However, just as it is conceivable to reduce both α and β in hypothesis testing by increasing the sample size, it is possible to increase both type I and type II reliability by raising an agency's resource levels. But because of resource limitations in the real world, it is inevitable that bureaucrats and their political superiors will have to strike a balance between each type of reliability. On the whole, three-state devices allow us to consider both forms of error and thus provide a richer framework for studying the issue of organizational reliability.[1]

BASIC CONCEPTS OF STRUCTURE AND RELIABILITY

General Assumptions

Throughout this discussion I will be contrasting *component* and *system* reliability. It is important to clarify, in advance, what is meant by these terms. A system is a collection of subunits, known as components, which are linked together in a particular structure. In administrative theory, identifying components is dependent on the system level in question. If one were concentrating on the behavior of an agency, then the agency as a whole is the system, and the offices within it are the components. Alternatively, if one were looking at the executive branch as a whole, that would be the system and each agency a component within the system. In an organizational context, determining what the components are depends largely on the system with which you are concerned. In this case study of NASA, the system of concern is the agency, and each component represents an office or division inside NASA.

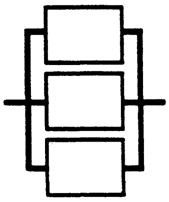
Three other assumptions of this work must also be specified. First, I start by assuming that the probability of failure for each component in the system has already been determined either by testing or past history,[2] then, later, relax this assumption, demonstrating that the theoretical framework is valuable even when the exact probabilities of component failure are not known. Making this assumption at the onset, however, is useful for developing the theory; since the components are assumed to be known quantities, the remaining question is how to assemble these components into a reliable network. Second, I assume that organizational reliability is static, not dynamic. In the engineering literature, reliability is often treated as time-dependent so as to simulate the breakdown of mechanical components; the probability of such failure naturally increases with age. For administrative systems, however, it is not clear how component reliability would change over time. One might argue that agents become more reliable over time because they have greater experience and expertise with the issues and are thus better able to address them. On the other hand, it could be said that agents are less reliable over time because they are more secure in their positions and lose their incentive to perform well. Additionally, interest-group capture of some public agency may affect the reliability of its performance. While these ideas raise interesting questions, static models of administrative reliability will provide sufficient insight for our needs here. Finally, I assume that the states of all components are statistically independent. In other words, the failure of one component or subsystem does not affect the probability of failure of other components. Those who study public administration may question the

FIGURE 2

Redundant System in Parallel

(a) serial configuration

(b) parallel configuration



validity of this assumption. Bendor, however, proves a theorem demonstrating that some degree of component interaction does not negate the general results of reliability theory (1985, 44–49). Therefore, the assumption of component independence is a useful simplifying assumption that does not undercut the generalizability of the results. With these assumptions in hand, we can now focus our attention on the structural configurations commonly found in organizations.

Types of Organizational Structures

There are several basic organizational forms employed in the development of administrative systems. The first is a serial structure, a form often found in organizations. In a traditional serial structure, pictured in Figure 2, the first component must correctly process a policy initiative before sending it on to the next component. To be effective, policy must successfully pass through each of these components. The result is that in order for the system as a whole to fail, it is only necessary for one of the components in series to fail. If any one component were to fail to pass the policy to the next unit, then all the components that followed it would be unable to act, and the policy could not get through the system.

Another possible organizational form is the establishment of parallel linkages between components. In a parallel structure, such as the one illustrated in Figure 2, a policy may pass through any one of the components in order to get to the implementation stage. It is different from the serial structure inasmuch as even if one or more units fail to pass the policy along, it may still be able to make it through the system. The end result is that for a policy to fail to get through this type of system, all components must fail.

One variation of this structural form is the k-out-of-m unit network. In certain cases, we require that a certain number, k, of the m units in an active parallel redundant system must work for the system to be successful. One example of this type of system might be the requirement that at least two of the space shuttle's four major computers be on-line for launch. An organizational application of this system would be an agency director's decision rule not to implement any policy that a majority of the staff cannot agree upon ($k = \frac{m}{2} + 1$).

There are two special cases of the k-out-of-m unit network which merit attention. The first instance is where $k = 1$, in which case we are back to a simple parallel system. The second case is where $k = m$, which effectively reduces the structure to a serial system. (See Appendix for proof.) In the latter case, although the network is configured as an active parallel system, in terms of reliability it is behaving as a serial structure. To differentiate between this type of system and a traditional serial network, we will classify this type of structure as a *serially independent* system. This name signifies that while the system is essentially a serial one, its components operate completely independently from each other.

In an organizational context, an important distinction between a serially independent system and the traditional serial structure is the difference in processing time. In a traditional serial system, the first component must process the information, then pass it on to the next component for processing. This continues until all the components have processed the information. The total processing time of the system is the sum of processing times for each component plus some factor to account for transmission delay between units. In contrast, the serially independent system allows all components to operate simultaneously. The time needed for the serially independent system to complete its task is simply the time it takes the slowest component to finish its operations. So while both structures yield the same level of reliability, serially independent systems require less processing time.

Larger organizations often utilize combinations of serial and parallel structural forms. Two examples of this can be seen in Figure 3. In a series–parallel system there are several parallel subsystems linked together in a serial fashion. A parallel–series configuration is the result of several serial substructures combined into a larger parallel network. As these two examples illustrate, most large and complex structures can be decomposed into smaller units for easier analysis.

THE ADVANTAGE OF PARALLEL SYSTEMS IN A TWO-STATE WORLD

Components aligned in a series configuration are perhaps the easiest systems to analyze, as well as the most commonly encountered. As I noted earlier, in order for the system as a whole to fail, only one of the components in series has to fail. Defining the probability of failure for component i as f_i, a mathematical statement of the reliability of a serial system with m components would be

$$R_{sys} = \prod_{i=1}^{m} (1\text{-}f_i). \qquad (1)$$

FIGURE 3

Combinations of Structures with m Units in Series and n Units in Parallel

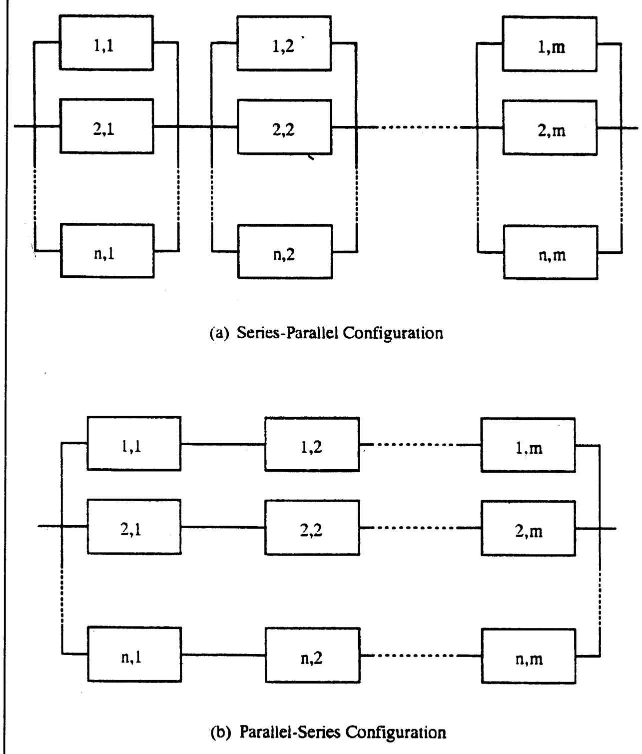
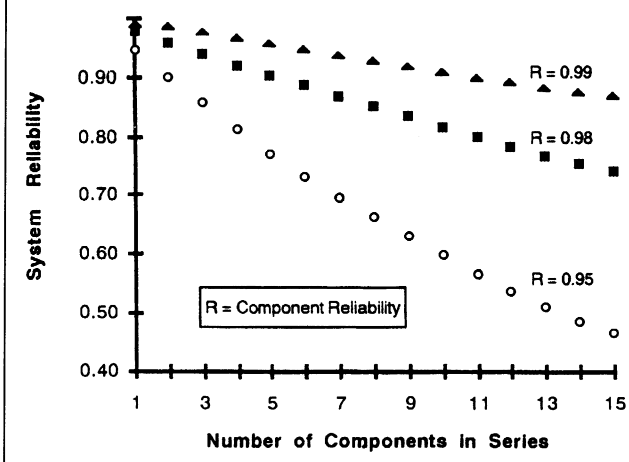


FIGURE 4

Declining Reliability of Serial Systems



We can see that two factors determine the reliability of a series system: component reliability and the number of components in the system. In order to increase the reliability of this type of system, one must either increase the reliability of the components or decrease the total number of components employed. As illustrated in Figure 4, marginal gains in system reliability from increasing component performance decrease as component reliability increases. Because the costs of increasing component reliability often rise exponentially, it is more effective in many cases to reduce the total number of components in series to reach reliability goals.

Perhaps the most common means of increasing reliability in a two-state world is to add parallel components to a system. It is assumed that all branches are active and that a signal needs to pass through only one branch to be successfully transmitted. Since it is assumed that all branches must fail in order for the system to fail, the reliability function for a parallel system with n components is simply

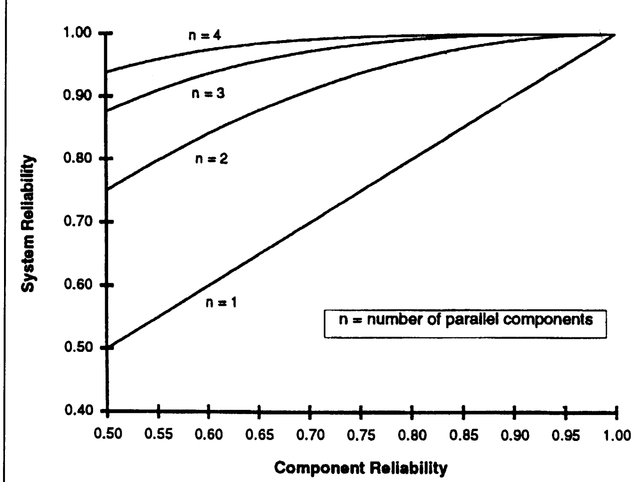
$$R_{sys} = 1 - \prod_{i=1}^{n} f_i .$$

Figure 7 illustrates the relationship between component reliability, the number of parallel elements, and overall system reliability. In this case, we see that the marginal gains from adding parallel channels decrease as the number of parallel components increases.

In comparing Figures 4 and 5, the attractiveness of parallel systems in a two-state world is clear. Holding component reliability constant, the addition of redundancy in a parallel fashion will raise the reliability of the overall system, while creating serial redundancies decreases total system reliability. It is not surprising, therefore, that many scholars in this area have spurned serial systems and focused, instead, on parallel linkages when discussing this issue. Pressman and Wildavsky (1973) have criticized the existence of "multiple clearance points" (a serial system) for an implementive decision because it reduces the likelihood that any policy can ever be executed. Landau (1969) directs the same logic against "streamlined" serial structures, claiming that such systems are more susceptible to failure than those with paral-

FIGURE 5

Increasing Reliability with Parallel Systems



lel redundancies. As a result, the major policy prescription of the work of Landau (1969, 1973, 1991) and others (Bendor 1985; Lerner 1986) has been to emphasize the use of parallel linkages in order to create more reliable organizations.

However, if it is true that serial systems are generally less reliable, why are such structures ever adopted by organizations? To answer this question fully, we must go beyond the two-state world to allow for multiple forms of error.

TYPE I AND TYPE II ERRORS IN AN ADMINISTRATIVE SETTING

The Advantages of Serial Systems in a Three-State World

As we have seen in the two-state world, serial structures are less reliable than others of comparable size. Nonetheless, it is clear that this structural form has been employed repeatedly in the development of bureaucracies. The reason this type of organizational structure has survived, I will suggest, is that it is valuable when we must design systems to accommodate multiple types of error. I previously assumed that there existed only two states for every component: good (operating) and failed (not operating). I shall now elaborate a theory of organizational reliability that allows for the existence of both type I and type II errors.

In general, a series structure is better suited to stop type I errors from occurring. Since the null hypothesis is that the agency should not take any action, if any component chooses to pass the proposed policy through its part of the system, then it is rejecting the null hypothesis. For any policy to pass through a serial system successfully, all units must agree to pass it along. If rejecting the null hypothesis was actually the incorrect decision (a type I error), then all units must commit such an error for the serial system as a whole to fail. Mathematically, we can identify both the probability of a type I failure occurring in the system (F_α) and the reliability of the system against this error (R_α) as

$$F_\alpha = \prod_{i=1}^{m} \alpha_i$$

$$R_\alpha = 1 - \prod_{i=1}^{m} \alpha_i,$$

where α_i is the probability of a type I error occurring in the i^{th} component and m is the number of components linked in series.

For an example, consider NASA's launch decision process. We would find that a serial structure is more effective in preventing unsafe launches. In order to approve an unsafe launch in a serial system, every unit must err. The more hurdles are established (via increasing numbers of serial components), the harder it is for an unsafe launch proposal to pass through the system unopposed.

With regard to type II errors, however, series structures are less effective. Consider the fact that if one unit accepts the null hypothesis of no new action, then the policy cannot be passed through the rest of the serial system. If accepting the null hypothesis was actually incorrect (a type II error), then the whole system would have failed. Thus, in order for a type II error to occur at the system level, only one component in series must fail in this manner for the system to fail. The more components added in series, the greater the probability that a component will commit a type II error, causing the system to fail (F_β). The reliability of a series structure with regards to type II errors (R_β) can be represented as

$$F_\beta = 1 - \prod_{i=1}^{m} (1 - \beta_i)$$

$$R_\beta = \prod_{i=1}^{m} (1 - \beta_i),$$

where β_i is the probability of a type II error occurring in the i^{th} component and m is the number of components linked in series.

We may also be interested in the overall reliability of the system—the likelihood that an agency would commit either a type I or type II error. To find this, we assume that for a given event at a given time, it is not possible for an administrative system to commit both a type I and a type II error simultaneously. This assumption is not unreasonable. A type I error requires that the agency act, while a type II error demands that the agency postpone any action. An organization cannot both act and not act at the same time. Consider NASA's decision to launch the shuttle. The space agency can either decide to launch the shuttle now (possibly resulting in a type I error) or abort the launch until another time (possibly resulting in a type II error). It cannot decide to both launch and abort at the same time.

Given this argument, we can conclude that type I and type II errors are, at any point in time, mutually exclusive events. Therefore, the probability of either a type I or type II error in a serial system can be found as

$$P(F_\alpha \cup F_\beta) = P(F_\alpha) + P(F_\beta) = \prod_{i=1}^{m} \alpha_i + \left(1 - \prod_{i=1}^{m} (1 - \beta_i)\right).$$

The overall reliability of the serial system is then found to be

$$R_{sys} = 1 - P(F_\alpha \cup F_\beta) = 1 - \left(\prod_{i=1}^{m} \alpha_i + 1 - \prod_{i=1}^{m} (1 - \beta_i)\right)$$

$$R_{sys} = \prod_{i=1}^{m} (1 - \beta_i) - \prod_{i=1}^{m} \alpha_i.$$

A brief numerical example will demonstrate these properties of serial systems. Assume that the NASA launch decision structure has two components that operate in series, each having the probability of committing a type I error $\alpha = .10$ and the probability of committing a type II error $\beta = .20$. The probability that the overall system approves the unsafe launch (type I) is $F_\alpha = .01$, which is much less than either of the two components. However, the probability that NASA will abort a safe launch (type II) is $F_\beta = .36$. The system as a whole is more likely to commit the type II error than either of its elements. The overall reliability of the system is found to be $R_{sys} = .63$.

If we concern ourselves only with the system's overall performance, we can find the number of elements in series that, for a given level of component reliability, will result in the optimal level of reliability. The system reliability of a series network consisting of m identical and independent components is $R_{sys} = (1 - \beta)^m - \alpha^m$. Differentiating this equation with respect to m and setting the result equal to zero will give us the optimal number of components to be linked in series in order to maximize the system's reliability. This result (derived in the Appendix) is

$$m^* = \frac{ln\left(\dfrac{ln\ \alpha}{ln(1-\beta)}\right)}{\left(ln\ \dfrac{(1-\beta)}{\alpha}\right)}.$$

The Disadvantage of Parallel Systems in a Three-State World

As the reader will have realized by now, there is a inverse relationship between the reliabilities of series and parallel systems. For instance, although series structures are ineffective against type II errors, parallel systems are able to reduce the probability of such errors occurring. This is because it is necessary for all components to fail in this manner for the overall system to commit a type II error. Likewise, type I errors are increased in such a framework, because it is only necessary for the incorrect action to pass through one channel in order to be implemented by the system. Therefore, the more independent parallel branches are attached to a structure, the more likely a type I error will occur but the less likely a type II error will be committed by the system.

The mathematical formulation of the reliability of a parallel system is

$$F_\alpha = 1 - \prod_{i=1}^{n} (1 - \alpha_i)$$

$$R_\alpha = \prod_{i=1}^{n} (1 - \alpha_i)$$

$$F_\beta = \prod_{i=1}^{n} \beta_i$$

$$R_\beta = 1 - \prod_{i=1}^{n} \beta_i$$

$$R_{sys} = \prod_{i=1}^{n} (1 - \alpha_i) - \prod_{i=1}^{n} \beta_i.$$

Modifying the example used earlier, let us assume that instead of connecting the two units in series, NASA links its components together in a parallel network. In this case, launch will occur if either unit recommends it. Now, the probability of launching an unsafe mission is greater, $F_\alpha = .19$; but the probability of aborting a good mission is only $F_\beta = .04$. The overall reliability of this system in preventing either type of error is much greater than before: $R_{sys} = .77$ in parallel, while $R_{sys} = .63$ in series.

Just as we were able to do earlier for the series structure, we can calculate the optimal number of identical and independent components linked in parallel. The system reliability of a parallel network consisting of n identical and independent components is $R_{sys} = (1 - \alpha)^n - \beta^n$. Differentiating this equation with respect to n, and setting the result equal to zero will give us the optimal number of components to be linked in parallel in order to maximize the system's reliability. This result (derived in the Appendix) is as follows:

$$n^* = \frac{ln\left(\dfrac{ln\ \beta}{ln(1-\alpha)}\right)}{\left(ln\ \dfrac{(1-\alpha)}{\beta}\right)}.$$

Combinations of Serial and Parallel Systems

In hypothesis testing, the probability of type I and type II errors can be simultaneously reduced by increasing the sample size. Similarly, we can lower the probability of both types of error occurring in reliability theory by adding additional components to the system both in series and in parallel.

With regard to multiple errors, we may employ the expressions derived earlier to analyze the reliability of networks that contain both parallel and series subsystems. To do this, we must first reduce the overall structure into a set of serial and/or parallel subsystems. The various subsystems are evaluated to find the probability of type I and type II failure at this level. Each subsystem is then treated as a single component in a larger model of the overall structure.

Using this system reduction method, we are able to find the reliability of more complex administrative networks.

Finding the optimal number of components in a mixed structure is more difficult than it was for simple series or parallel systems. Consider a combined system having m components in series and n components in parallel. We can raise the overall reliability level of the system to a point arbitrarily close to 1 by simply increasing the number of components in both series and parallel without bound (Barlow and Proschan 1965, 187). However, given a fixed number of components in either series or parallel, we can find the optimal number of components needed in the other dimension. I shall discuss this for both series–parallel and parallel–series systems.

First, let us consider a series–parallel system having m components in series and n components in parallel (as in Figure 4). All components are assumed to be identical and independent. Regarding the system only as a series, we find that its overall reliability is

$$R_{sys\text{-}sp} = (1 - F_\beta)^m - F_\alpha^m.$$

Next, we must find the probability of type I and type II errors in each parallel subsystem.

$$F_\alpha = 1 - (1 - \alpha)^n$$

$$F_\beta = \beta^n.$$

Combining these equations, we find that the overall system reliability of the n × m series–parallel network is

$$R_{sys-sp} = (1 - \beta^n)^m - (1 - (1 - \alpha)^n)^m.$$

Once we have the equation for the overall reliability of the system and have decided whether to fix the level of m or n, we can find the optimal number of components in the other dimension by differentiating $R_{sys\text{-}sp}$ with respect to the variable we seek to optimize and setting the result equal to zero. There are a number of computer routines available that are also capable of solving this type of problem.

This approach also works for parallel–series systems. Figure 5 shows a parallel–series network of n × m independent and identical components. Using the same method as before, we find the overall system reliability of a parallel–series system to be

$$R_{sys-ps} = (1 - \alpha^m)^n - (1 - (1 - \beta)^m)^n.$$

Again, once we have the equation for the overall reliability of the system and have decided whether to fix the level of m or n, we can find the optimal number of components in the other dimension by differentiating $R_{sys\text{-}ps}$ with respect to the variable we seek to optimize and setting the result equal to zero.

ALTERING RELIABILITY THROUGH SYSTEM LINKAGES AT NASA

This theoretical approach to structural design can now be used to examine the institutional failures at NASA that ultimately led to the destruction of the *Challenger*. I will show that during the 1970s and 1980s, NASA altered its organizational structure in order to achieve different reliability goals. I examine changes within two specific areas of the NASA's structure that the Rogers Commission mentioned in its report on the *Challenger* accident in 1986. The first area of concern involves the organization of NASA's reliability-and-quality-assurance (R&QA) functions. The second area involves changes that took place in the agency's launch decision structure.

Changes Within NASA's Reliability-and-Quality-Assurance Function

Prior to 1961, NASA had no explicit reliability-and-quality-assurance function within the agency.[3] In trying to match the Soviet space achievements, NASA devoted little of its effort toward preventing bad launches (type I error) and used almost all its resources trying to launch as often as possible (avoiding type II error). As a result, the agency's mission success rate from 1958 to 1961 was dismal (Weiss 1971).

At that point, the Soviet Union seemed to be winning the space race, inasmuch as they were able to draw attention to their many successes, while the United States had experienced a number of visible failures.[4] It became clear that the only hope of beating the Soviets was for the United States to play down the numbers of launches and emphasize mission quality. This fact underscored the need for an agencywide effort to increase type I reliability. Consequently, NASA administrator James Webb established the first R&QA function within the space agency in 1961.

The R&QA function was initially formed on three levels: within headquarters, at the field centers, and in the contractors' plants. As such, it represents a classic example of serial redundancy. For a mistake to be made by NASA, the error would have to pass all through three checkpoints undetected. As I have noted, system reliability with regard to type I error increases with each additional serial component. Constructing such an organizational structure is wholly consistent with the agency's increased concern over type I reliability at this time.

Following the success of the Apollo program in the 1970s, NASA faced less demand for type I reliability and more for type II reliability. In the Apollo era, NASA's primary concern was for successful achievement. The agency had a specific mandate that it knew had to be fulfilled at any cost. Having secured victory in the race to the moon, NASA faced increasingly tighter budget constraints. At the same time, the demand from politicians for services continued unabated. This meant that NASA now had to do more with fewer resources available. As a result of the changing political and economic landscape, the agency focus in the Shuttle era had shifted to the efficiency and cost-effectiveness of its policies (Heimann 1991).

By demanding that NASA develop more cost-effective policies, politicians put the agency under greater pressure to pursue type II reliability. As noted earlier, type II failure costs are generally associated with wasted resources and inefficient behavior. From a short-term perspective, then, a concern for type II reliability appeared to be more sensible than type I reliability.[5] The greater pressure for efficient space policy, therefore, led NASA to allocate more of its resources to type II reliability.

The results of this shift are visible in the changes in the R&QA structure since 1970. At the headquarters level, there was a consolidation of the R&QA Office with the Safety Office to take advantage of economies of scale.[6] Later in 1973, this office was combined with other staff and placed under the associate administrator for organization and management.[7] Some of the R&QA work was integrated with the Office of Procurement at this time. Further consolidations occurred in 1977, and all safety- and reliability-oriented functions were transferred to the Office of the Chief Engineer.

Placement of the R&QA function within the Office of the Chief Engineer did not promote type I reliability. Documentation from NASA makes it clear that while safety and reliability were considered important, they were a secondary function of the chief engineer's office (National Aeronautics and Space Administration 1983). The efforts of R&QA were also hampered by the continual loss of personnel. From 1970 to 1985, NASA experienced a 31% decline in total personnel; but within the total R&QA function, this decline was over 62%. As a result, the NASA staff allocated to R&QA was just over 5.1% in 1970; in 1985, it was less than 2.8%.[8]

By the end of 1985, the R&QA staff at NASA headquarters totalled only 17 people. As Chief Engineer Silveira stated in an interview, "We were trying to use the field center organizations rather than having that function here:"[9] NASA had all but eliminated one of the serial components in its safety and reliability-and-quality-assurance function. This action reduced the probability of NASA's committing a type II error but increased the chances of experiencing a type I failure.

The R&QA function was not immune to changes at the field centers. This level experienced reductions in manpower, as well.[10] From 1970 to 1985, the three major centers for manned space flight (i.e., the Johnson Space Center, Kennedy Space Center, and Marshall Space Flight Center) cut R&QA personnel by 38, 54, and 84%, respectively. The heavy cuts at Marshall, in particular, were understandable, given the pressure the center was under to be cost-effective. Again, cutting R&QA personnel can be seen as reducing the serial linkages at this level that can serve to prevent Type I errors.

In addition to the personnel reduction, the field centers' ability to supervise the activities of contractors was limited in this period. Normally, NASA seeks to "penetrate" its contractors to provide an adequate check on their work. Aerospace contractors, however, generally conduct business with the Department of Defense, as well as NASA. The Defense Department in the 1970s became concerned that too many NASA inspectors at the contractors' plants could jeopardize national security and wanted to place a cap on the number and scope of their inspection activities (Smith 1989, 230–31). Inasmuch as the agency was dependent on the Defense Department for political support for the shuttle program, NASA had little choice but to accept these limitations on the plant inspection efforts.

After the *Challenger*, NASA's R&QA function changed dramatically. The Rogers Commission castigated the space agency for its "silent safety program" and recommended that it revitalize its R&QA function. In response, NASA created the Office of Safety, Reliability, Maintainability, and Quality Assurance (later renamed the Office of Safety and Mission Quality). Established as a level 1 organization, this office is headed by an associate administrator who reports directly to the NASA administrator. Staffing for the new headquarters office was immediately doubled and has since experienced more than 350% growth over its 1985 level. While NASA personnel levels have grown by 10% over the past five years, the R&QA function as a whole has increased by 123% during that time. As a result, R&QA as a percent of total NASA staff is back at 5.6%, similar to its position at the time of Apollo 11 in 1969; NASA has made a strong and visible effort to restore the serial component at this level.

Within this office, there exist several divisions, such as the Safety Division and the Space Station Safety and Product Assurance Division, which formulate office policy in their respective areas and provide some monitoring to ensure compliance. The real "teeth" of the office, however, are found in the Systems Assessment Division and the Programs Assurance Division. In Systems Assessment, top-level senior engineers from a wide range of disciplines perform independent evaluation of technical problem areas and testing of systems readiness. The Programs Assurance Division also employs senior engineers to identify critical technical problems and to ensure that the office's concerns are properly addressed by the program organizations and field centers. Inasmuch as either of these two units have the ability to stop a launch perceived to be unsafe, these two divisions work as serially independent linkages within the headquarters office. Creating two serial components within the larger serial component at headquarters increases the organization's reliability with regard to type I errors.

The R&QA function at the field center level has also been resuscitated in the wake of the *Challenger* failure. Marshall, which had initiated the largest cuts in this area, has since increased its R&QA personnel by 178% over 1985 levels. R&QA staffing levels at the Kennedy Space Center and the Johnson Space Center have also increased over 1985 levels by 175% and 56%, respectively.

The agency has further augmented its R&QA function through the development of the NASA Safety Reporting System (NSRS). Run by a contractor with no other NASA business, the NSRS provides employees with a confidential means of reporting problems that they believe have not been properly addressed. The system acts as an additional serially independent component in the NASA R&QA structure. Officials at the Office of Safety and Mission Quality state that there have been "no showstoppers" among the reports received by the NSRS. Furthermore, the problems coming through the NSRS have almost always been identified by the office first, evidence that their administrative structure is doing its job properly.

It is important to consider these organizational changes in the context of three-state reliability theory. In Table 1 (Set A), I analyze the various R&QA structures first under the assumption that each component has a 15% chance of making type I and type II errors. The original Apollo structure had three serial units, reducing the change of a type I error to a remote .3%. The advantage of the Apollo structure can be clearly seen. Even if the individual components are not that reliable with regard to type I error, the structure as a whole would guard against such a failure. As we noted earlier, the NASA structure in the Shuttle era prior to *Challenger* was effectively reduced to a single unit. This shift resulted in a dramatic reduction of type II errors and lowered the probability of either form of system failure from 38.9% to 30.0%. The disadvantage is that a type I error, such as the *Challenger* accident, would be far more likely, rising in this case from .3% to 15.0%. Since then, NASA has made a concerted effort to restore the serial structure in R&QA and has even added an additional unit through the Office of Safety and Mission Quality. Adding the fourth component to the serial unit in this case lowers the probability of a type I error to a paltry .1%.

Some could argue that a change to a more streamlined structure would be acceptable if accompanied by an increase in component reliability. This is not necessarily the case. In Set B, I allow each component to lower its probability of error by a factor of three, from 15% to 5%. Under these circumstances, the pre-*Challenger* structure has a 5% chance of committing a type I error. The Apollo structure, even with less reliable components, had less than a 1% chance of committing such an error. This comparison makes it clear that these structural changes at NASA were consequential. As this analysis has shown, streamlining the R&QA function increased the probability that a type I failure such as the *Challenger* accident would eventually occur.

TABLE 1

Probabilities of Failure for NASA R&QA Structures (all results expressed as a percentage)

COMPONENTS & STRUCTURES	SET A	SET B
Component Failure		
Type I error	15.0	5.0
Type II error	15.0	5.0
Apollo Structure		
Type I error	0.3	<0.1
Type II error	38.6	14.3
Overall error	38.9	14.3
Shuttle Structure		
Before Challenger		
Type I error	15.0	5.0
Type II error	15.0	5.0
Overall error	30.0	10.0
After Challenger		
Type I error	0.1	<0.1
Type II error	47.8	18.5
Overall error	47.8	18.5

Note: A Type I error for NASA would be a decision to launch an unsafe mission. A Type II error would be a decision to abort a technically sound mission.
The figures for component reliability, as well as the calculations which follow, are not empirically derived estimates but rather they are assumptions made for the purpose of illustration.

Changes in the Launch Decision Structure

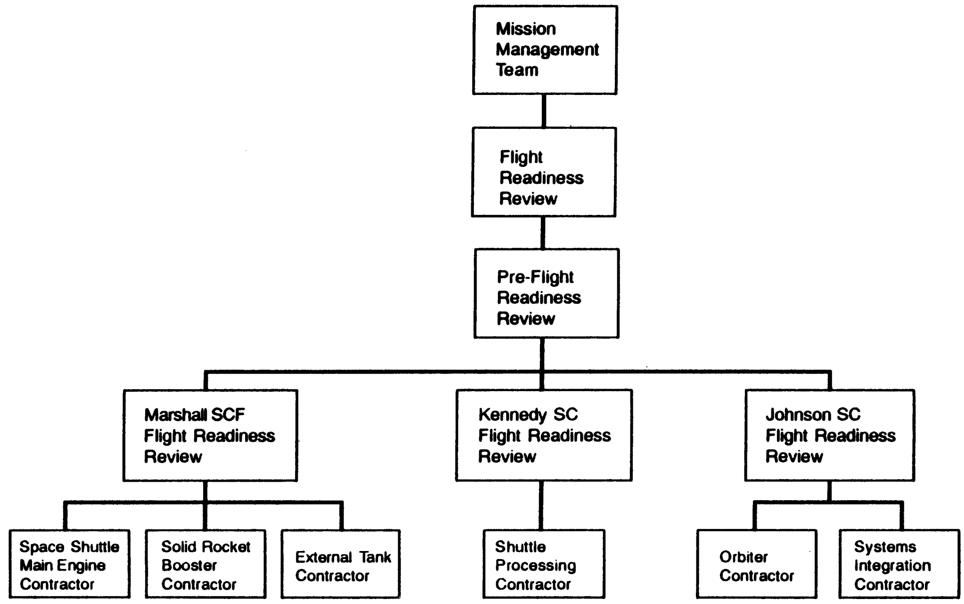
At the same time that the R&QA function at NASA was undergoing significant modifications, important changes in the launch decision process also occurred that exacerbated the problem of type I reliability at NASA. I shall examine both the development and the impact of structural changes in the launch decision process prior to the *Challenger*.

Figure 6 illustrates NASA's official launch decision structure. Designed originally in the Apollo era to limit type I errors, the system has a large number of serial components. Although the field centers are configured as parallel units in the diagram, this level of the structure actually operates as a serially independent system. The reason for this is that the operating rule at the preflight review is that if any center reports it is unready to fly, the mission is aborted. This is an example of a k-out-of-m network, where k = m. While most of this structure remained intact throughout the shuttle program, critical changes occurred at the Marshall Space Flight Center.

Marshall has responsibility for three aspects of the shuttle program; the main engines, the external tank, and the solid rocket boosters. At the center, there is a project manager and staff assigned to each section of the program. Before a launch, contractors for each element in the shuttle must certify in writing that their components have been examined and are ready to fly the specified mission. After this step, the Marshall staff responsible for that segment of the program must also verify that it is safe to fly under

FIGURE 6

NASA Official Launch Structure, 1981–1986



'these conditions. This process is illustrated in Figure 7.

This structure works well at preventing type I failures, but it is not as effective with regard to type II errors. Assume for a moment that the probability of each component in this system committing a type I error is 5% and the chance of a type II error is 15%.[11] In such a case, each subsystem (solid rocket boosters, main engine, and external tank) has only a .25% chance of committing a type I failure; but a 27.75% chance of allowing a type II error. The probability that the center as a whole would be responsible for any type II launch failure is 62%.

This is certainly not good news for Marshall, which was under a great deal of pressure to operate cost-effectively. The center had been slated for shutdown following the completion of Apollo. As former NASA administrator James Fletcher told his successor, "Closing Marshall has been on the Office of Management and Budget's agenda ever since I came to NASA in 1971" (Smith 1989, 84). To prevent this from occurring, NASA headquarters sent several high-visibility projects, such as the Space Telescope and the shuttle's solid rocket motors, to Marshall. Despite these efforts, Marshall was still threatened with large reductions in personnel and other resources following Apollo.[12]

This pressure became even more intense as the shuttle neared operational status. In 1978, the OMB had expressed to NASA that it wished to impose major cuts at Marshall. Although NASA suggested "new roles" for the center, OMB officials made it clear they were not interested.[13] While NASA as an institution faced strong pressure to run its operations cost-effectively, Marshall felt this demand more intensely. Consequently, managers at the center sought to increase their type II reliability, so as not have a launch stopped on account of a Marshall part (McConnell 1987, 109, 112).

To achieve this objective, Marshall Center director William Lucas unofficially changed the organizational structure from a serial system to a parallel one (Figure 8). If either the contractor or the Marshall staff stated that a launch was justifiable, Lucas would insist that

FIGURE 7

Official Structure of Flight Readiness Review at the Marshall Space Flight Center

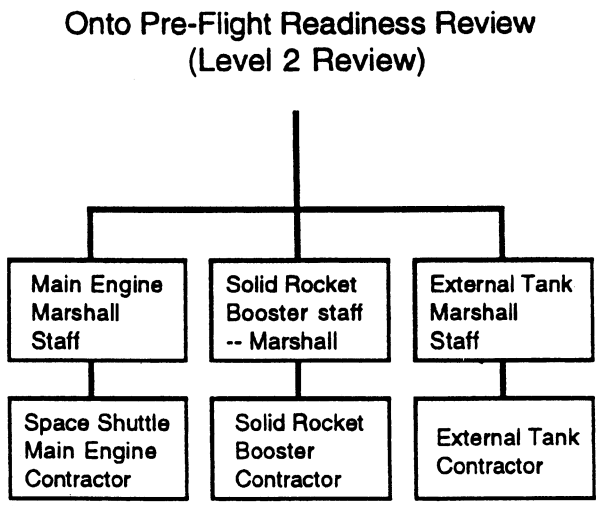
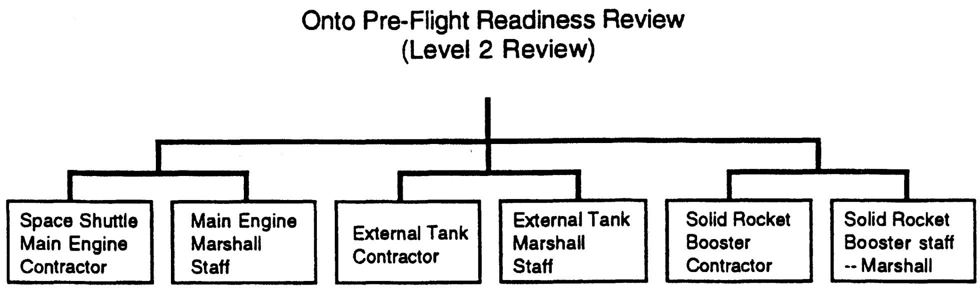


FIGURE 8

An Unofficial Change in the Structure of the Flight Readiness Review at the Marshall Space Flight Center



all parties agree to forward the necessary paperwork. Through his personal supervision of the launch decision process and his domineering style of management, Lucas was able to ensure that this unofficial structure prevailed.

Following the investigation of the *Challenger* accident, it was widely publicized that Marshall solid rocket booster managers had coerced engineers at Morton Thiokol into agreeing to a launch they opposed. Such pressure, however, has worked in both directions. In January 1985, solid rocket booster manager Larry Mulloy sent an urgent memo to Thiokol concerning O-ring erosion. A week later, in the review for shuttle mission 51-D, Thiokol's launch decision was to "accept risk" (Presidential Commission on the Space Shuttle *Challenger* Accident 1986, vol. 1). Once this opinion was expressed, the ability of the Marshall staff to stop the launch was extremely limited. In sum, the launch decision structure at Marshall had been transformed from a serial system, which would require both parties to authorize the flight readiness of the equipment, into a parallel structure needing only one component to approve the launch.

This structural shift had a profound impact on the reliability of the launch decision process at Marshall. Table 2 (Set C) contrasts the organizational reliability of each system, assuming once again, that each component commits type I and type II errors with a probability of .05 and .15, respectively. The new parallel structure reduces the probability that any subsystem will commit a type II error from 27.75% to 2.25%. Curtailing this form of error was completely consistent with Marshall's requirements at the time. The converse is that the probability of a type I failure in each subsystem increases from .25% to 9.75%. The probability that at least one subsystem at the Marshall center would commit a type I error rose from .75% to 26.49% under the new process.

As noted, NASA had changed its emphasis from type I to type II reliability. To consider the impact of this transformation, Table 2 (Set D) compares the two structures with the component probabilities of type I and type II errors reversed. Even when biased toward type II reliability, the serial decision structure is able to keep type I error rates at a low 2.25% in each subsystem. In contrast, the new parallel organization increases this failure rate to 27.75%. The prescribed serial structure clearly limits the possibility that such organizational changes would lead to fatal type I mistakes, a feature that is lost in the unofficial launch process. In light of this analysis, perhaps the most surprising aspect of the *Challenger* accident was that it did not happen earlier.

Since then, the launch decision process at Marshall has been restored to its previous status. In addition, the Office of Safety and Mission Quality has been given a direct voice in the launch decision at the flight readiness review. This office now has the authority to stop any launch that it believes is unsafe, linking it to the system in a serially independent manner. This authority has been exercised on previous launch attempts when the office was concerned with hydrogen leaks on the shuttle, defective door lug-bolts, and other technical problems. On the whole, the launch decision system is now structured to be more protective against type I failures and prevent another mishap like the *Challenger*.

TABLE 2

Probabilities of Failure for Marshall Launch Decision Structures (all results expressed as a percentage)

	SET C		SET D	
COMPONENTS & STRUCTURES	TYPE I	TYPE II	TYPE I	TYPE II
Component Failure	5.0	15.0	15.0	5.0
Serial Structure				
Subsystem Failure	0.25	27.75	2.25	9.75
Center Failure	0.75	62.29	6.60	26.49
Parallel Structure				
Subsystem Failure	9.75	2.25	27.75	0.25
Center Failure	26.49	6.60	62.29	0.75

Note: A Type I error for NASA would be a decision to launch an unsafe mission. A Type II error would be a decision to abort a technically sound mission.
The figure for component reliability, as well as the calculations which follow, are not empirically derived estimates but rather they are assumptions made for the purpose of illustration.

CONCLUSION

Several conclusions can be drawn at this point. First, organizational structure can have an important impact on administrative reliability. I have demonstrated, both in theory and for the case of NASA, that changes in the number and alignment of administrative components alters the probability that an agency would commit either a type I or type II error. Perhaps most interesting is the fact that NASA changed its institutional configuration to appease both the traditional and the Landau schools of thought in public administration, yet both decisions contributed to the biggest failure in NASA history. With regard to its reliability-and-quality-assurance function, NASA followed the traditional public administration prescription by eliminating redundancies and streamlining its organizational system. At the same time, the space agency also heeded the advice of Landau by creating parallel linkages in the launch decision structure. As I have shown, however, both those decisions were incorrect and contributed to the destruction of the *Challenger*.

While recognizing its limitations, we should not be overly critical of the work in this field by Landau and his colleagues. It is clear that Landau's major objective at the time was to respond those in the discipline who emphasized efficiency over the pursuit of reliability. As such, his work was path-breaking; and his focus on two-state (operating/failed) devices was understandable. As I have shown here, however, the three-state world gives us a theoretically richer and more empirically useful framework for evaluating organizational reliability. Expanding this subject to allow for multiple types of error is an important step toward a more general theory of organizational reliability and agency behavior.

Using this theoretical framework, it is also clear that the agency's choice of structure can provide insights on its priorities. The NASA case is particularly illustrative of this point. In the Apollo era, the agency pursued type I reliability more than type II. To do this, they developed a large serial structures in both the reliability-and-quality-assurance function and in the launch decision process. Over time, there was greater demand for type II reliability, which was met through a series of structural changes in the agency. The intense criticism following the *Challenger* led NASA to radically shift its structure to a system that was even more effective against type I errors. That structural changes mirrored the shifting demands for each form of reliability does not surprise us. As Alfred Chandler, the eminent management historian, once put it, structure follows strategy (Chandler 1962). By looking at the structural modifications within an agency and understanding how these changes influence organizational reliability, we can gain some insight into the agency's true preferences and priorities with regard to different types of reliability.

It is possible to perform such an analysis even if we do not know the exact values of component reliability for both types of error. In the theoretical section, I assumed that the reliability of each component was known. When analyzing NASA, however, I was still able to apply these principles by making some reasonable assumptions about the reliability of the components. More generally, when circumstances dictate greater effort toward one form of reliability, we can use these principles to develop a set of structures that are relatively better at minimizing the error of concern. The theory can also be used to recognize potential weak points in more complex organizations and allow us to reinforce them with regard to the particular error of concern.

Explicitly incorporating multiple forms of error in our analysis will open up new avenues in the public administration research agenda. For example, more work could be done on the study of agency incentives to pursue different forms of reliability. This work helps us to understand *how* agencies may adjust their structural design to meet the demands for different forms of reliability. The question of *why* agencies make the choices they do is one that would be of great interest to political scientists. As Moe (1990) notes, structural choice is, at heart, a political issue. This is particularly true when we recognize that agencies, endowed with limited resources, must make trade-offs between each form of reliability. These choices have political consequences and are influenced by political factors.

Further research could also be done comparing component and systems reliability. Till now, the focus has been on the system as a whole, not the individual components. Concentrating on component issues raises a whole new set of questions. What factors affect component reliability? To what extent is component reliability influenced by the strategic behavior of agents? To what extent can and should agencies pursue reliability objectives through increased component reliability, rather than through structural changes? Answering these questions will also contribute to the development of a more general theory of organizational reliability and agency behavior.

In the end, we must recognize that a theory of organizational reliability is not sufficient to eliminate risks altogether. Space exploration is still a risky business—it always has been and always will be. The men and women who have gone into space understood these risks. Even with the technological advances resulting from Project Apollo and the organizational changes after the *Challenger*, there remains a large element of danger in manned space flight. According to a report by the Office of Technology Assessment in April 1990, there is a 50% chance of losing another orbiter over the next 34 missions. Understanding organizational reliability cannot eliminate these risks altogether, but it can help to ensure that NASA's next technical problem is not compounded by managerial mistakes.

APPENDIX

Proof That a k-out-of-m Unit Network Reduces to Serial System Where k = m

Since the success/failure of each of the m units can be modeled as a Bernouilli process, we can use the binomial distribution to describe the system reliability for a k-out-of-m unit network. Letting f represent the probability of failure for each independent unit, the overall reliability of a k-out-of-m unit network may be represented mathematically as

$$R_{k/m} = \sum_{i=k}^{m} \binom{m}{i}(1-f)^i f^{k-i}.$$

When k = m, this expression reduces to

$$R_{k/m} = \binom{m}{m}(1-f)^m f^{m-m},$$

which further reduces to $R = (1 - f_i)^m$. Note that this expression is equivalent to equation 1, which represents the reliability of a serial system in a two-state world.

Series Systems Optimization

The system reliability of a series network consisting of m identical and independent components is $R_s = (1 - \beta)^m - \alpha^m$. Differentiating this equation with respect to m and setting the result equal to zero will give us the optimal number of components to be linked in series in order to maximize the system's reliability:

$$\frac{\partial R}{\partial m} = [(1-\beta)^m \ln(1-\beta)] - [\alpha^m \ln\alpha] = 0$$

$$(1-\beta)^m \ln(1-\beta) = \alpha^m \ln\alpha$$

Taking the natural log of each side and grouping like terms,

$$m\left(\ln\frac{(1-\beta)}{\alpha}\right) = \ln\left(\frac{\ln\alpha}{\ln(1-\beta)}\right)$$

$$m^* = \frac{\ln\left(\frac{\ln\alpha}{\ln(1-\beta)}\right)}{\left(\ln\frac{(1-\beta)}{a}\right)}$$

Parallel System Optimization

The system reliability of a parallel network consisting of n identical and independent components is $R_s = (1 - \alpha)^n - \beta^n$. Differentiating this equation with respect to n and setting the result equal to zero will give us the optimal number of components to be linked in parallel in order to maximize the system's reliability:

$$\frac{\partial R}{\partial n} = [(1-\alpha)^n \ln(1-\alpha)] - [\beta^n \ln\beta] = 0$$

$$(1-\alpha)^n \ln(1-\alpha) = \beta^n \ln\beta.$$

Taking the natural log of each side and grouping like terms,

$$n\left(\ln\frac{(1-\alpha)}{\beta}\right) = \ln\left(\frac{\ln\beta}{\ln(1-\alpha)}\right)$$

$$n^* = \frac{\ln\left(\frac{\ln\beta}{\ln(1-\alpha)}\right)}{\left(\ln\frac{(1-\alpha)}{\beta}\right)}$$

Notes

A previous version of this paper was presented at the 1992 Midwest Political Science Association Meeting. I am indebted, for their helpful comments, to Don Chisholm, John Gilmour, Jim Granato, Tom Hammond, Paula Kearns, Jack Knight, Jack Knott, and Bill Lowry.

1. A three-state device is a unit that can be described as either operating correctly, committing a type I error, or committing a type II error. One might argue that what we have here are four-state devices, inasmuch as there are two types of correct decisions, as well. While this is true, the focus of reliability theory has historically been on the analysis and impact of failure. As a result, it is the norm to refer to multiple error units as three-state devices.

2. While it is later relaxed, making this assumption is not unreasonable. Measuring personnel productivity is a subject that has been discussed in industrial engineering and other areas of management science. Research from these areas make it possible to generate statistically sound estimates of component performance and reliability.

3. The reliability-and-quality-assurance function at NASA refers to those offices and individuals specifically charged with agency oversight on matters of reliability and safety. This function is not limited to a single office and has undergone a number of changes over time.

4. The Soviets' control over the media allowed them to limit their coverage to the successful flights. In contrast, the United States' first attempt to launch a satellite was a highly publicized failure. The United States learned from this embarrassing experience and tried to minimize press coverage in later launch activities. Such news can rarely be kept a complete secret in our society, however; and the continued contrast between Soviet success and American failure had a political impact at home and abroad.

5. It may well be that considering the policy over a longer time horizon would demonstrate the cost-effectiveness of type I reliability. However, the American political system is notorious for its myopic approach to many public policy issues. After the *Challenger*, many experts were critical of the space agency's shortsightedness and claimed that such behavior was irrational. If the political environment of the agency is factored in, the policy outcomes may seem undesirable; but they are not irrational from the agency's perspective (Heimann 1990, 1991).

6. While these two offices had overlapping responsibility, the Reliability and Quality Assurance Office was primarily concerned with hardware and technological issues, while the

Safety Office focused on human factors and included responsibility for worker safety procedures.

7. Special Announcement, February 6, 1973, "Establishment of Office of Safety and Reliability and Quality Assurance," NASA History Office Library.

8. Figures on reliability-and-quality-assurance manpower were calculated from numbers provided to Congress by the chief engineer and by the Office of Safety and Mission Quality and the Office of Human Resources at NASA.

9. Mark Tapscott, "Cuts Hurt NASA's Safety," *Washington Times*, 5 March 1986.

10. Directors at each center have traditionally been given flexibility to set R&QA staffing and funding for projects under their control. Before the *Challenger*, R&QA officials at headquarters could make recommendations about center staffing, but had no direct control over this process so as to reinforce the independent nature of the field center unit.

11. This assumption would be consistent with the belief that NASA is generally risk-averse with regard to type I error. As noted earlier, however, increasing type I reliability often raises the likelihood that a type II error could occur.

12. News Release, 5 March 1974, no. 74-31, NASA History Office Library.

13. Memorandum, assistant associate administrator for management operations to associate administrator for management operations, September 7, 1978, "Institutional Assessment Presentation to OMB," NASA History Office Library.

References

Barlow, Richard E. and Frank Proschan. 1965. *Mathematical Theory of Reliability*. New York, NY: John Wiley & Sons, Inc.

Bendor, Jonathan B. 1985. *Parallel Systems: Redundancy in Government*. Berkeley, CA: University of California Press.

Chandler, Alfred. 1962. *Strategy and Structure: Chapters in the History of Industrial Enterprise*. Cambridge, MA: MIT Press.

Chisholm, Donald W. 1989. *Coordination Without Hierarchy: Informal Structures in Multiorganizational Systems*. Berkeley, CA: University of California Press.

Heimann, C. F. Larry. 1990. "Reliability Versus Efficiency: Striking a Balance in the Political Arena." Presented at the Annual Meeting of the Southern Political Science Association. Atlanta, November 8-10.

Heimann, C. F. Larry. 1991. *Acceptable Risks: A Theory of Organizational Reliability and Agency Behavior*. Ph.D. Dissertation, Washington University, St. Louis.

Landau, Martin. 1969. "Redundancy, Rationality and the Problem of Duplication and Overlap." *Public Administration Review* 29(4) (July-August):346–358.

Landau, Martin. 1973. "Federalism, Redundancy, and System Reliability." *Publius* 3(2) (Fall):173–196.

Landau, Martin. 1991. "On Multiorganizational Systems in Public Administration." *Journal of Public Administration Research and Theory*. 1(1) (January):5–18.

LaPorte, Todd R. and Paula M. Consolini. 1991. "Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations." *Journal of Public Administration Research and Theory*. 1(1) (January):19–47.

Lerner, Allan W. 1986. "There is More Than One Way to be Redundant." *Administration and Society*. 18(3) (November): 334–59.

McConnell, Malcolm. 1987. *Challenger: A Major Malfunction*. Garden City, NY: Doubleday & Company, Inc.

Moe, Terry M. 1990. "The Politics of Structural Choice: Towards a Theory of Public Bureaucracy." In *Organization Theory*, ed. Oliver E. Williamson. New York: Oxford University Press.

National Aeronautics and Space Administration. 1983. *The NASA Organization*. Internal report: NASA.

Perrow, Charles. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York, NY: Basic Books.

Pressman, Jeffrey L. and Aaron Wildavsky. 1973. *Implementation*. Berkeley, CA: University of California Press.

Rochlin, Gene I., Todd R. LaPorte, and Karla H. Roberts. 1987. "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea." *Naval War College Review*. (Autumn): 76–90.

Smith, Robert W. 1989. *The Space Telescope*. Cambridge, England: Cambridge University Press.

U.S. Presidential Commission on the Space Shuttle Challenger Accident. 1986. *Report to the President*. Washington: The Commission.

Weiss, Howard M. 1971. "NASA's Quality Program—Achievements and Forecast." Presented at 25th ASQC Technical Conference, Chicago.

C. F. Larry Heimann is Assistant Professor of Political Science, Michigan State University, East Lansing, MI 48824-1032.