

# Chapter 1

---

## On Resilience

---

The world suffered vicariously as firefighters entered the towers and never returned. We imagined ourselves as passengers on United 93 as it plunged toward a field in Pennsylvania. We felt the temperatures rise as the Space Shuttle Columbia's tiles peeled away. In New Orleans, we saw waters break through the levees and flood our houses while we waited in vain for help to come.

And yet, the persistent question remains: could all these calamities have been prevented; or worse, would it have been possible to survive and recover from them and continue functioning? And furthermore, whose fault was it? Was it bad design, or a cultural problem, or management, or politics, or something else? The answer is “yes” to all these questions. And the approach to disaster avoidance, survival, and recovery from such disruptions requires that expertise from a multitude of disciplines be executed to an unprecedented degree. Hence, these three elements, accident avoidance, survival, and recovery constitute what has come to be called resilience. These three elements will be discussed more in Chapter 2, System Resilience and Related Concepts.

The opposite of resilience is called brittleness. One challenge of research is to determine ways to find out when a system is “drifting” toward brittleness. What can be measured? What can be observed? And, most importantly, what can be done to stop the drift toward brittleness?

The purpose of this book is to answer these questions within an integrated framework. To create this integrated framework, many factors are brought together: management and technical functions should be considered a single interconnected discipline. Other disciplines, such as organizational psychology, are brought into the mix. The distinctions among human, software, and

hardware systems are erased. Chapter 7, Infrastructure, defines an infrastructure system that encompasses all relevant organizations. Finally, to create systems that are resilient to and survive major disruptions requires considerations far beyond current practices that might be considered just good engineering. This framework extends beyond the breadth currently envisioned in most academic, government, and industrial institutions. However, the expectation is that these practices will be incorporated into all aspects of system development wherever they may be needed.

## 1.1 THE MULTIDISCIPLINARY CHALLENGE

We live in a world of specialists. Even the family doctor has a limited understanding of what the cardiologist does. There are very few Renaissance men like Leonardo. But even more to the point, the gulf among artists, psychologists, managers, and scientists is enormous. Resilience demands Renaissance men and women who are at once practitioners of multidisciplinary and transdisciplinarity. The multidisciplinary nature of system resilience makes it clear that system resilience is not another specialty but rather a collaborative effort among many specialties, both technical and nontechnical.

Nicolescu (2007, Part 1: The war of disciplines) describes multidisciplinary as using several disciplines to enhance the topic in question. The bringing together of management and technical capabilities satisfies this definition. Transdisciplinarity, however, according to Nicolescu, “concerns that which is at once between the disciplines, across the different disciplines, and beyond all disciplines.” Performing the risk management process and addressing the psychological paradigm of risk denial seem to fall in this category. Jackson (2007) focuses on the multidisciplinary aspects of system resilience.

Researchers all over the world, such as the Resilience Engineering Network, are studying system resilience. Hollnagel et al. (2006) and Hollnagel and Rigaud (2006) are two examples of the products of the Resilience Engineering Network. They are a unique group, which consists of engineers, psychologists, sociologists, physicians, and other specialists. They all have one thing in common: an interest in solving the mysteries of resilience and a new discipline of resilience engineering. Could Chernobyl have been prevented? If not, how could anyone survive such an event? These experts all agree on one point: that the answer to this question does not lie solely in engineering expertise but rather in a broad range of interconnected disciplines, both technical and human. In addition, the study of resilience has attracted the attention of the legal profession. The George Mason School of Law has instituted the Critical Infrastructure Protection (CIP) Program. The CIP report (2007) provides an in-depth study of the benefits of a resilience approach *versus* the traditional protection approach.

These researchers come with many ideas, and there is not yet a consensus among them on many points. This book will summarize many of those ideas.

The one principle that the researchers all agree on is that resilience to disaster and survival of disruptions are not purely technical subjects. In the early days of space flight, many failures could be traced to technical causes. That is, a system would fail because of unreliable components. Today, such failures are largely under control. However, systems continue to fail because of causes beyond the technical. The Caltech physicist Richard Feynman (1988) had asked National Aeronautics and Space Administration (NASA) management what they thought the probability of failure was for a space shuttle. They replied, relying on reliability analysis, that it was about 1 in 100,000. Working engineers put the number at about 1 in 100. Range safety experts estimated the number to be 1 in 25. History has shown that the latter numbers were closer to the truth. In short, the disparity in these estimates demonstrates that Feynman seemed to understand that the causes of catastrophe were far beyond technical considerations, at least as currently understood in the engineering community.

## 1.2 THE CONCEPT OF THE SYSTEM

Whenever two or more things act together to achieve a common purpose, you have a system. A mousetrap is a system; the government is a system; a troop of Girl Scouts is a system; and a chemical power plant is a system. If all the parts of the system do not work properly, the whole system may fail. The concept of the system is discussed in Chapter 2, System Resilience and Related Concepts.

### 1.2.1 The Paradox of Humans in the System

To understand and design for resilience, the role of the human needs to be understood. Humans are not simply operators of the system, like pilots. Nor are they simply maintainers of the system, like aircraft mechanics. They are not only producers of the system, like factory workers. They are not simply designers of the system, like engineers. All the above examples are parts of the system. Sometimes humans constitute the entire system itself, such as a troop of soldiers. These are called human systems. Some human systems, such as hospitals, have hardware and software components, such as X-ray machines and other test equipment. However, the predominant elements are human, such as doctors, nurses, and other staff members. For these types of systems, the term “human-intensive systems” applies.

Many researchers, such as Bennis (1999), have studied humans within an organizational context. However, the design rules of human systems can best be determined by the attributes, laws, and heuristics discussed in Chapter 8, Resilience Architecting. Heuristics are the design rules of systems architecting, as described by Reichtin (1991), rather than verifiable requirements as in the traditional systems approach. There is no way to test the humans in all possible scenarios to determine whether they perform correctly. There are ways to reduce human error, such as training. Nevertheless, human actions may be

highly unpredictable leading to unpredictable outcomes. These outcomes are a result of Type B disruptions—that is, disruptions caused by degradation of function, capability, or capacity, which will be discussed later in Chapter 3, Disruptions. The saving grace of humans is that they are adaptable and can sometimes create solutions not even imagined by the designers. An example is the restoration of electrical power in New York after the attack on the twin towers as described in Chapter 4, Case Histories.

In any discussion of humans, the question of *human error* always arises. This is a subject about which there is abundant misunderstanding. This issue is particularly important in the health care domain as described by Rooney et al. (2002). The authors point out that “the majority, 80 to 85%, of human errors result from the design of the work situation, such as the tasks, equipment and the environment.” These data exclude malevolent acts. In other words, human errors are *systemic* in nature and cannot wholly be blamed on individuals. Reason (1990, p. 173) makes the following statement with regard to human error:

Rather than being the main instigators of an accident, operators tend to be the inheritors of system defects created by poor design, incorrect installation, faulty maintenance, and bad management decisions. Their part is usually that of adding the final garnish to a lethal brew whose ingredients have already been long in the cooking.

Chapter 3, Disruptions, describes human error as a source of disruptions, that is, events that can lead to disaster. Hence, the inevitable conclusion is that the pilot of the aircraft in the Nagoya incident described in Chapter 4, Case Histories, might not have made the fatal mistake if the appropriate features had been designed into his aircraft. Chapter 8, Resilience Architecting, describes these features as adaptable and agile. Nevertheless, Rooney et al. (2002) conclude that significant reductions in human error can be achieved with good training, good work situation design, good procedures, and a good corrective action system. Rooney et al. (2002, p. 35), discussing human error in the health care domain, also recognize the adaptability of the human by insisting that a prerequisite for reducing human error is the “freedom to act.”

In short, whereas humans may be a major source of accidents, designers of most modern systems, such as commercial aircraft, recognize that the adaptability of humans makes them essential components for resilience.

### 1.2.2 The Infrastructure as a System

An infrastructure is the collection of people and equipment that design, operate, produce, and maintain a product system, such as an aircraft or spacecraft. An infrastructure also consists of the relationships between these elements. Or the infrastructure itself, such as a civil infrastructure, may be the system. Thinking of this collection as a system is not a traditional way to characterize a system. Yet it is central to resilience. One has to think of what the

pilot does, what the maintainer does, and so on. It is this system that should operate flawlessly so that the aircraft or spacecraft can also operate flawlessly. This concept becomes tractable when the boundary of the system is defined. Chapter 2, System Resilience and Related Concepts, describes the systems approach in which boundary definition is essential. Because all these human elements contribute to the objective of the system, it is only logical to conclude that they are components of the system.

The scope of the infrastructure system becomes even more foreboding when the number of people and organizations involved are considered. The communications among these organizations become points of brittleness. The people themselves and the decisions they make are critical to the system success. For example, a patient waits for a donated heart. Is the blood type correct? An error in this situation is a matter of life or death. This is an example of a fragile infrastructure system consisting of a hospital, doctors, a blood donation organization, and other elements. The concept of the infrastructure system is discussed more fully in Chapter 2, System Resilience and Related Concepts, and in Chapter 7, Infrastructure.

### 1.2.3 The Architecture of a System

So what is it that makes a system resilient? For the most part, it is its architecture. The architecture of a system is how the parts of the system are arranged and how they interact with each other. Rechlin (1991) coined the term “architecting” to describe the process of creating an architecture. For example, if a fire protection system has multiple ways of putting out fires, then those methods would be part of the fire protection system’s architecture. This example appears in Appendix A, Domain-Specific Example for Architecting a Fire Protection Infrastructure System.

Zachman (2007) writes on the subject of architecture, especially enterprise architecture. Zachman (2007, p. 6) says:

“Architecture” is the set of descriptive representations relevant for describing a complex object (actually any object) such that an instance of the object can be created and such that the descriptive representations serve as the baseline for changing an object’s instance (assuming that the descriptive representations are maintained consistent with an instantiation).

Zachman notes that many people confuse the *implementation* of an architecture, for example a building, with the architecture itself, which Zachman describes as a representation. Zachman’s definition is valid for any type of system, for example, infrastructure systems or technological systems.

In Zachman’s definition, descriptive representations are models that enable the analyst to view the object or system from a desired perspective. It can be said that an architecture is an abstract view of a system and not a physical view

as observed in a photograph. One of the most common architectural views is the hierarchical representation, but there are many other views.

So how does one “architect?” Rehtin suggests a set of heuristics, or guidelines derived from experience for creating the architecture of a system. Chapter 8, *Resilience Architecting*, provides heuristics focused on creating a resilient system.

### 1.3 DISRUPTIONS

When Hurricane Katrina slammed into New Orleans, the effect was a *disruption* of the normal activities of the city. When the power went out on Apollo 13, the loss of power was a disruption of the mission of that space vehicle.

The analysis of disruptions is essential to the study of resilience. The question is as follows: When the function of a system is disrupted, will it cause a catastrophic failure? Can the systems survive the disruption? Can the system recover and continue to function at any level? To what extent is the resilience of the system dependent on the type of disruption?

When the Tacoma Narrows bridge collapsed in 1940, the failure can be categorized as a Type A, or *disruption of input*, as defined in Chapter 3, Disruptions. That is to say, the bridge experienced a phenomenon not known to the designers, namely the effects of the turbulent aerodynamic boundary layer on the bridge.

When the Challenger spacecraft failed, it experienced a degradation of function, capability, or capacity, which is the second type of disruption. These disruptions are called systemic disruptions. The O-rings, which are an internal component of the system, failed, resulting in the catastrophe. When a human is part of the system and makes an error, as in the Nagoya aircraft failure, this error is an error of function.

Hurricane Katrina is an example of a disruption caused by a change in the environment, which is also a disruption of input. However, the failure of the levees can also be categorized as an internal, or systemic, disruption. The winds of Hurricane Katrina constituted a disruption of immense magnitude. Hurricane Katrina is also an example of a network disruption in which the failure of one element of the system, for example, the levees, resulted in the failure of other elements, for example, the transportation system. All these examples are discussed in Chapter 4, Case Histories. These examples also show that the presence of humans and software in systems introduce unprecedented degrees of disruption.

Sometimes disruptions of function can result from the interaction of two elements of the system. This kind of disruption can occur even when the individual components operate as designed. Such was the case for the Mars Polar Lander, in which the interaction between the landing struts and the software resulted in the premature shutdown of the engines. Although such

disruptions can be attributed to poor integration, predicting them may require analysis to a greater level of detail than is common.

## 1.4 ADAPTABILITY

Adaptability can be said to be an *emergent* characteristic of a system that enables it to avoid, survive, or recover from a disruption. Many existing and past systems had a large degree of natural, or built-in, adaptability, discussed in Chapter 8, Resilience Architecting. Apollo 13 was a good example as discussed in Chapter 4, Case Histories. When the main power failed, the crew saved power by moving to a smaller module. In this way, they were restructuring the system, which is a key attribute of adaptability. Adaptability is, in this case, emergent because it illustrates the relationship between the modules and is not a characteristic of each module when treated singly.

Another attribute is interelement collaboration or communication and cooperation between elements. Hurricane Katrina is an example in which virtually no communication or cooperation occurred among government agencies. This system failed the adaptability test with catastrophic results. The rapid restoration of power in New York after the attack on the twin towers is an example of adaptability. This case is discussed in Chapter 4, Case Histories. Adaptability can be designed into a system using the holistic methods that are part of the systems approach as described in Chapter 8, Resilience Architecting. As explained in Chapter 2, System Resilience and Related Concepts, holistic methods take into account the relationship among system elements, whereas analytic methods focus on individual components.

## 1.5 CULTURE

The Columbia Accident Investigation Board (2003) found that cultural factors were at least as important a contributor to the Columbia disaster as technical factors. The NASA culture of accepting risk in the pre-Challenger days was described by Vaughn (1996, p. 415) as the “normalization of deviance.” She uses this phrase to describe a cultural environment in which risks were accepted to be an established norm.

The term *culture*, as discussed in Chapter 5, Culture, may refer to the individual, organizational, or national beliefs that govern our actions. Although the cultural influences on resilience are well documented, for example, in Vaughn (1996) and in the Columbia Accident Investigation Board report (2003), this aspect has received little attention in industry or government.

Basically, two ways are available for an enterprise to address culture. First, designers of the enterprise can make their processes so rigorous that these processes would be virtually impervious to culture. Alternatively, they could attempt to change the culture. Neither of these techniques is easy. Chapter 5 outlines some potential methods for changing culture.

## 1.6 MEASURING RESILIENCE

A major topic among resilience researchers is whether resilience or, better put, lack of resilience, called *brittleness*, can be predicted or measured. One school of thought is that accidents are so random that any type of prediction is out of the question. However, others point to defects and near-misses that almost always precede major accidents. This idea is called the iceberg theory, as discussed in Chapter 10, Measuring Resilience. Can it be said, for example, that an aircraft that requires more maintenance is more likely to have an accident? The answer to this question is not known, but it is possible. Some statistical evidence exists for example, from the Scottish Railways study, which collected and analyzed data on defects and major accidents in the railway domain. This study indicated a statistical correlation between minor events and major accidents, as described by Wright and Van der Schaaf (2004).

If developed, such evidence would have an enormous benefit. This information could be used to create better designs, better operational procedures, or better maintenance procedures. In short, although the iceberg theory does not directly measure resilience, it could be a step in the process of designing more resilient systems.

Otherwise, the following conclusions can be drawn. First, traditional reliability and safety analyses can be used to arrive at quantitative results. However, these results are based almost entirely on historical data and may reflect, to a certain extent, the ability of the system to survive predicted disruptions. Second, data exist for human error in some domains—for example, in commercial aircraft. Hence, to the extent that such data do exist, they can be used to supplement reliability and safety analyses to arrive at quantitative results. Finally, there is the issue of unpredicted threats, as discussed in Chapter 3, Disruptions. It can be concluded that the measure of the resilience to unpredicted threats is only possible to the extent that a given resilience method has proven useful against *other* unpredicted threats.

## 1.7 THE CHALLENGES

If there is a more difficult problem to solve than resilience, it is hard to say what it is. Can multiple disciplines as widely diverse as engineering and psychology, for example, be corralled to analyze resilience in its entirety? Can multiple organizations, including, for example, aircraft developers, customers, government agencies, operators, and maintainers, be integrated to solve communications and decision-making problems? Can disruptive events, such as conflicts between operators and software, be predicted and eliminated? Can adaptive systems be created to survive and recover from major disruptions, such as terrorist attacks and hurricanes? Can cultural change actually be achieved that will result in risk-conscious organizations that will anticipate and address threats to resilience? Finally, are there indicators of potential weaknesses in

systems that can be exploited to make more resilient systems? All of these examples are potential steps toward designing resilient systems.

## **1.8 FURTHER EXPLORATION**

Given what you know so far about system resilience, write a short essay on all its aspects. These aspects should include resilience itself, the importance of multiple disciplines, the concept of a system and its broader meanings, the concept of an infrastructure system and its importance, adaptability, and resilience measurement. Take advantage of outside sources for this essay.

