Towards a Conceptual Framework for Resilience Engineering

Azad M. Madni, Fellow, IEEE, and Scott Jackson

Abstract—As systems continue to grow in size and complexity, they pose increasingly greater safety and risk management challenges. Today when complex systems fail and mishaps occur, there is an initial tendency to attribute the failure to human error. Yet research has repeatedly shown that more often than not it is not human error but organizational factors that set up adverse conditions that increase the likelihood of system failure. Resilience engineering is concerned with building systems that are able to circumvent accidents through anticipation, survive disruptions through recovery, and grow through adaptation. This paper defines resilience from different perspectives, provides a conceptual framework for understanding and analyzing disruptions, and presents principles and heuristics based on lessons learned that can be employed to build resilient systems.

Index Terms—adaptive capacity, disruptions, resilience engineering, risk management.

I. INTRODUCTION

TRAGIC accidents and catastrophic failures have unfortunately become a fact of life when it comes to complex systems and enterprises such as transportation, aviation, telecommunications, power generation, and healthcare [1], [2], [3], [4], [5]. It has also been the case that more often than not human error has been identified as the cause of such mishaps [1], [6]. However, today there is a growing recognition that such accidents and failures can be traced to organizational factors that create conditions that invite disaster. All one has to do is look back to the Columbia space shuttle accident of 2003. The relentless pursuit of “better, cheaper, faster” led management into making decisions that eroded safety margins without management realizing that the risks had dramatically increased [7]. A retrospective look at the major mishaps and accidents reveals that these incidents have several characteristics in common (Table 1).

<table>
<thead>
<tr>
<th>COMMON CHARACTERISTICS OF MAJOR ACCIDENTS [6], [7]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Severe production pressure/tight schedule</td>
</tr>
<tr>
<td>• Pressing need for safety, but eroding safety margins (obscured by pressure to produce)</td>
</tr>
<tr>
<td>• Over-confidence (based on past success) replacing “due diligence”</td>
</tr>
<tr>
<td>• Failure to revisit it and revise initial assessments with new evidence</td>
</tr>
<tr>
<td>• Breakdown in communications at organizational boundaries</td>
</tr>
<tr>
<td>• Unchecked risk buildup because of schedule pressure</td>
</tr>
<tr>
<td>• Failure to re-interpret previous facts in light of new evidence</td>
</tr>
</tbody>
</table>

In the aftermath of such accidents, it has become quite evident that complex systems development invariably demands both high productivity and ultra-high safety levels. It is this recognition that has stimulated the noticeable rise in interest in resilience engineering.

Unlike conventional risk management approaches that employ hindsight and calculations of failure probabilities [7], [8] resilience engineering is a proactive approach that looks for ways to enhance the ability of organizations to explicitly monitor risks, and to make appropriate tradeoffs between required safety levels and production and economic pressures [6], [9], [10]. In resilience engineering, failures do not imply a breakdown or malfunction of a normal system. Rather, they represent an inability of the system to adequately adapt to perturbations and changes in the real world given finite resources and time [1], [2], [11], [12]. As such, success is defined by the ability of the system to monitor the changing risk profile and take timely action to prevent the likelihood of damage. Failure, in this context, is simply the absence of this ability, when needed.

Resilience engineering is still a relatively new concept. Not surprisingly, there are some unanswered questions on how well it can deliver on its promise. In Hollnagel, Woods, and Leveson [1], an early treatise on this subject, a central idea is that failure is not necessarily a consequence of malfunction or poor design. Rather, it is a result of the “web of ongoing interactions and adaptations” that characterizes complex systems behavior in the real world. What this means is that individuals and organizations must continually adapt their behavior to the circumstances at hand to stay within safety margins and still make schedule [12]. Of course, in the face of time pressures, and finite cognitive and physiological resources, such adaptations cannot be expected to be optimal leaving room for accidents to occur. It is also worth noting that the concept of resilience can be extended to ecological systems. Here resilience means cultural adaptability in the face of external disruptions such as regulatory reform or climate change. In light of the foregoing, this paper discusses resilience from different perspectives and provides a conceptual framework for understanding and analyzing disruptions, and building resilient systems.

II. THE MANY FACES OF DISRUPTION

Disruptions are conditions or events that interrupt or impede normal operations by creating discontinuity, confusion, disorder or displacement [2]. Disruptions can take

Special Issue on Resilience Engineering
a variety of forms. Major disruptions include operational contingencies [13], [14], [15], [16], [17], natural disasters [16], [18], terrorism and political instability events [19], and financial meltdowns (Table 2).

### Table 2: The Many Faces of Disruptions

<table>
<thead>
<tr>
<th>Type A – External Disruptions</th>
<th>Type B – Systemic Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Contingencies</td>
<td>Financial Meltdowns</td>
</tr>
<tr>
<td>• equipment malfunctions and systemic failures (e.g., Aug. 14, 2003 grid blackout in northeast U.S.)</td>
<td>• subprime rate and mortgage leader meltdown</td>
</tr>
<tr>
<td>• abrupt discontinuity of supply (e.g., supplier goes out of business, bankruptcy)</td>
<td>• 1929 and 1987 stock market collapse</td>
</tr>
<tr>
<td>• human-centered disruptions (e.g., strikes, fraud)</td>
<td></td>
</tr>
<tr>
<td>Natural Disasters</td>
<td></td>
</tr>
<tr>
<td>• earthquake, hurricanes, storms (e.g., 1992 Hurricane Andrew, 2006 Hurricane Katrina, 1995 Kobe earthquake in Japan)</td>
<td></td>
</tr>
<tr>
<td>Terrorism and Political Instability</td>
<td>9/11/2001 World Trade Center attack</td>
</tr>
<tr>
<td>• 9/11/2001 World Trade Center attack</td>
<td>• sabotage, political instabilities in third world countries</td>
</tr>
<tr>
<td>• Financial Meltdowns</td>
<td></td>
</tr>
<tr>
<td>• subprime rate and mortgage leader meltdown</td>
<td></td>
</tr>
<tr>
<td>• 1929 and 1987 stock market collapse</td>
<td></td>
</tr>
</tbody>
</table>

With respect to coping with disruptions, it is important to distinguish between two types of resilience: reaction and adaptation. Reaction implies immediate or short-term action while adaptation implies long-term learning. In the following paragraph, we describe the different types of disruptions, the key implications of each type, and how resilience can be created for each type.

### A. Type A – External Disruptions

The most obvious examples of external disruptions are natural disasters, such as hurricanes, tsunamis, tornados, earthquakes, floods, fires and droughts. Westrum [17], for example, discusses the failures of government agencies to deal with Hurricane Katrina in 2005. A far worse disaster, though, was the Galveston hurricane of 1900, described by Larson [19], in which over 6000 people perished. Woods’ principle of cross-scale interaction [1] is the predominant resilience strategy for dealing with this type of disruption. Simply put, cross-scale interaction is achieving communication and collaboration among all the elements of the civil infrastructure system charged with responding to natural disasters. These elements include power, water, law enforcement, medical and transportation.

It is important to recognize that external disruptions are caused by factors (e.g., random phenomena, input transients) outside the system [2]. As such, systems need to be able to detect these and perform appropriate corrective action [12]. For example, an aircraft flying close to another can affect the latter with its aerodynamic wake [3]. If the wake is sufficiently strong, it can affect the structural integrity of the second aircraft. In particular, the random direction and nature of the wake could affect software processing in the second aircraft causing it to misinterpret the angles of attack and yaw [3]. An equally important implication is that systems need to be tolerant to external disruptions, (e.g., not be susceptible to failure, or fail gradually rather than abruptly). The Concorde supersonic aircraft disaster in the year 2000 described in the BEA report [20] is an example of the latter. In this case, a small strip of metal on the runway caused the aircraft to fail suddenly and catastrophically. Since there was no detection, there was no possibility of corrective action, or gradual degradation.

Ensuring resilience is a challenge, when the magnitude of a potential disturbance cannot be predicted. Is it possible to make a system resilient to a disturbance of unknown magnitude? The answer to this question is not that straightforward. One can collect data on the history of certain phenomena (e.g., tides, winds and temperatures) and use that knowledge to build resilience. But what if a system encounters a disruption of greater magnitude than that encountered in any historical incident? Or what, if a disruption is completely unexpected (e.g., the “twin towers” attack)? Then the concept of disruption magnitude becomes moot.

The primary implication of external disruptions is that systems need to be built with adequate safety margins to account for uncertainty. For example, this margin is typically 50% for the various elements of a commercial aircraft [21], [22].

### B. Type B – Systemic Disruption

A systemic disruption is a disruption of function, capability or capacity [2], [3]. It manifests itself in technological systems when, for example, a component fails, (e.g. Challenger space shuttle disaster). Similarly, a software error that results in an erroneous signal being sent to other system modules, is an example of a loss of function disruption. One of the best examples of functional disruption, related by Eyles [23] is the guidance software failure on Apollo 11 that nearly resulted in a landing failure on the moon. Fortunately, humans as “backups” managed to save the day proving that the manned system was resilient.

According to Aviation Week and Space Technology [24] an interesting, but benign, case of systemic disruptions occurred on February 19, 2007 when a squadron of F-22 Raptors experienced a loss of their navigational computers because the software had not been programmed, or tested, to account for crossing the International Date Line. Fortunately, the pilots were able to fly the aircraft manually and return to home base. Even so, this is an illustration of a small, but avoidable mistake that could have had tragic consequences.

Another example of a systemic disruption is the Nagoya accident described by Zarboutis and Wright [25]. In this accident, the pilot inadvertently provided an incorrect command to the flight control software causing the human element to be in conflict with the software. Tragically, all passengers died. In retrospect, it is neither useful nor factually accurate to simply blame the pilot. What is important is that the entire system, pilot and aircraft, were not capable of adapting even though there are many ways to increase the adaptability of the pilot-aircraft system (e.g., notify pilot of miscompare with flight control system, give the pilot more options, and let FCS adjust to the situation).

While these types of failures, which typically result from inadequate reliability or safety measures, can be effectively addressed by traditional analytical methods, such failures are
becoming increasingly less frequent, in recent years. More recent literature, (e.g., Vaughn [26]) has pointed to inattention to risk as the root cause of mishaps and accidents.

The systemic sources of disruptions encompass humans, automated systems, and various combinations of the two. For the sake of convenience, we refer to these sources as “agents.” In the most general sense, an agent is an element of a system. Each agent, by virtue of its inherent capabilities, can potentially be both a source of disruption as well as the means to contain and recover from disruptions. In the following paragraphs, we discuss these aspects.

**Human Agent Disruption.** When it comes to disruptions, human agents are a double-edged sword. On the one hand, they can act unpredictably (e.g., the human pilot in the Nagoya accident was central to the events leading up to the accident). On the other hand, their ingenuity is what makes them most adaptable and capable of responding to disruptions. The Apollo 13 mission, for example, was saved by the quick and ingenious actions of its crew. In this case, described by Leveson [27], a Type B disruption - - power loss in the main module was the culprit. The crew was able to exploit a resilience principle (i.e., flexibility) by moving to the smaller landing module that was available.

Many large-scale systems tend to be human-intensive. For example, the infrastructure setup for responding to natural disasters, such as Hurricane Katrina, is invariably human-intensive. Such systems potentially bring the greatest capability but are also the most vulnerable given their complexity. From a system point of view, it is reasonable to conclude that the reason that the air traffic control system is not totally automated is that humans are viewed as more capable of detecting and handling unpredicted situations than machines. Regardless, the human agent is viewed as a net asset despite human shortcomings.

**Automated Agent Disruption.** Since, most complex systems tend to be software-intensive, it is not surprising, that software deficiencies often contribute to disruptions. In fact, software deficiency was one of the contributing factors in both the Nagoya and Mars Polar Lander accidents. Given today’s state-of-the practice, software performance is highly dependent on the ability of software designers to envision the possible circumstances in which the software is expected to operate --- a tall, mostly impossible, order. As such, if an unanticipated situation arises that the software is not sensitive to, then the software can become a source of potentially serious disruptions.

One would think that automated agents that are predominantly hardware would be relatively immune to disruptions. Not so. The vibrating struts in the Mars Polar Lander are an example of hardware-driven disruption. The Tacoma Narrows bridge disaster described by Ketchum [28] is an example of mostly “hardware” impacted by unpredicted aerodynamic forces. Unlike software, hardware is constrained by the laws of physics and, to that extent, predictable. However, the forces that act on the hardware are often difficult to predict; hence, the element of unpredictability in “hardware.”

**Multiagent Disruption.** Disruptions can often occur when two or more agents find themselves in conflict. Clearly, any number of agents can be at odds in a multiagent network causing the entire network to go down. Multiagent disruptions can take different forms. For example, interacting agents could be a hardware-software combination, as in the case of the Mars Polar Lander, or a human-software combination, as in the case of Nagoya. Another highly publicized example of two-agent weak disruptions was the Mars Climate Orbiter described by NASA [29]. In this case, the flight control computer sent a signal to the thrusters in English units rather than metric units—a totally avoidable problem.

**Predictable vs. Unpredictable Disruptions.** Traditional system safety analysis, as documented in MIL-STD-882 [30] depends, for the most part, on designing systems to survive previously encountered disruptions. Even so, the expectation exists that a system designed for resilience will avoid, survive and recover from unpredicted disruptions also. Fortunately, many disturbances are predictable, at least on a probabilistic basis. Hurricanes on the Gulf Coast, earthquakes in California, and tornadoes in Kansas happen often enough that their frequency of occurrence and magnitude are well known.

Unpredictable disturbances can occur, either because a phenomenon was unknown to modern science, or because it was unanticipated/unknown to the systems designers. The disruptions of the turbulent boundary layer effect in the Tacoma Narrows bridge collapse of 1940 is an example of unpredicted disturbance. The disruption caused by the Van Allen Radiation Belts, described by the Encyclopedia Britannica, whose existence was not even known, is another example of an unprecedented disturbance.

The source of unpredictable disruptions is often, but not always, humans. Despite extensive training, humans can still act in completely unpredictable fashion. Invariably, these acts are not a result of lack of competence or mal-intent. Rather, they tend to be completely innocent mistakes. Woods [31] notes that “it is fundamental in the universe that you can’t anticipate everything.” This means that strong disruptions do not depend on the quality of the engineering because its causes are completely random. Of course, the quality of engineering does come into play in determining whether or not the system is able to survive the disruptive event. This is also where resilience engineering comes into play.

### III. CLARIFYING DEFINITIONS

There are several terms, originating in different fields, that describe concepts that are similar to resilience. These include: safety, reliability, and survivability. While these terms cannot be fully deconflicted because of some overlap, their specific emphasis tends to be different.

Safety is a system property, that encompasses the behavior of and interactions among subsystems, software, organizations, and humans. Major mishaps and case studies over the last decade point to the need for organizations to retool their engineering processes and capabilities to address human and organizational risk factors [21], [32]. This is where resilience engineering can play a crucial role in that it is
concerned with exploiting insights on failures in complex systems, organizational contributors to risk, and human performance drivers to develop proactive engineering practices. These include understanding and measurement of the sources of resilience, decision support for performing production/safety tradeoffs, and dynamic assessment and update of risk models that enhance an organization’s ability to effectively prioritize safety investments.

At the outset, it is helpful to clarify the differences between reliability and resilience. Reliability in the engineering domain deals with the ability of the system and its components to perform required functions under stated conditions for a specified period of time. This reductionist view underlies modeling techniques such as the traditional form of probabilistic risk (or safety) assessment (PRA or PSA). These methods tend to be satisfactory for day-to-day operations of certain kinds of engineered systems (e.g., nuclear and chemical plants) in which system components and their behaviors are treated largely as mutually independent. While this assumption may be valid on a day-to-day basis, ignoring longer-term influences (e.g., poor maintenance, staff reductions) that often produce coupling between components can quickly invalidate this assumption.

In light of the foregoing, resilience offers a vastly different approach. Research has shown that high reliability organizations (HROs) create safety by anticipating and planning for the unexpected. These organizations do not accept past success (or the absence of manifest failures) as a reason for confidence. Rather, they invest in techniques for anticipating the changing potential for failure because of the deeply held belief that their cumulative knowledge is fragile in the face of the hazards and looming changes in their work environment. From this perspective, safety becomes a dynamic capability that requires reinforcement and investment on an ongoing basis. It goes without saying that learning is at the heart of resilience engineering in that the changing likelihood of failure can potentially guide proactive changes in making safety-risk tradeoffs without waiting for a mishap to occur.

It is also important to recognize that safety is a dynamic characteristic of a system that, once introduced, does not persist unless reinforced during systems operation on an ongoing basis [2]. This view is in keeping with Hollnagel and Woods [1] who argue that safety is something (that results from what) a system or an organization does, rather than something a system or an organization has. Interestingly, the existence of safety can only be conveyed by the absence of mishaps (i.e., accidents, failures). Furthermore, if an untoward event does occur, it does not mean that safety provisions in place have failed, because “safety-proofing” a system is neither complete, nor absolute. In other words, resilience engineering does not assure safe system operation; rather, it does biases the odds in that direction. It is for this reason that resilience engineering foregoes the pursuit of safety as a property (defined in terms of adherence to standards, policies, and error typology) in favor of viewing resilience as a quality exhibited during system operation. Traditionally, safety is assessed using reliability metrics (e.g., probability of failure is below a certain value). Such trailing indicators have been found to be inadequate [2]. The concept of resilience attempts to define leading indicators [2]. A resilient system is expected to have the ability to survive and recover from unexpected perturbations, disruptions, and operational environment degradations. What this means is that resilience cannot be engineered merely by adding procedures, safeguards, and barriers. Rather, it requires continuous monitoring of system performance and, performance margins to assure a high degree of safe system operation with managed risk. As such, resilience is a means of coping with system complexity [1], and maintaining control in the face of ongoing disruptions.

Westrum [11] argues that resilience consists of at least two of the following: avoidance, survival, and recovery. Each concept is described next.

**Avoidance** – This term describes the preventive aspects of system resilience relative to a disruption. Avoidance goes beyond traditional system safety considerations in that it encompasses the *anticipation* of a mishap based on the ability to detect “drift” towards system brittleness, a harbinger of potential accidents.

**Survival** – This term pertains to the ability of the system to resist destruction or incapacitation in the face of a disruption.

**Recovery** – This term pertains to the ability of the system to survive a major disturbance albeit with reduced performance occasionally. This capability is a central focus of system resilience.

In light of the foregoing, one might argue that if avoidance is achieved, then the need for survival and recovery are naturally circumvented. This, however, is not the case because some systems tend to be sufficiently complex and unpredictable, that avoidance may not be fully achievable. In such circumstances, the only realistic recourse is survival and recovery. It is also important to realize that system resilience can only be achieved within a resilient enterprise. A resilient enterprise is one with adequate resources and “buffers” to withstand dramatic changes in resource demands imposed by the external environment [2]. Resilience is also essential in achieving agility (e.g., meet surge demands, exploit fast-moving, business opportunities, and successfully counter disruptions created by competitors).

The opposite of resilience is referred to as “brittleness.” A brittle system is one that is unable to adapt to unanticipated disturbances or disruptions and, consequently, breaks down. Most resilience researchers tend to focus on the preventive aspects of resilience. For example, Hollnagel [1] states that “resilience is the ability to maintain effective barriers that can withstand the impact of harmful agents and the erosion that is a result of latent conditions.” These characteristics speak to the capabilities that have to be in place, the culture that has to exist, and the responsiveness of the infrastructure within which the system is developed, deployed, operated, and maintained. Weick and Sutcliffe [4] refer to this type of organization as a high reliability organization (HRO).
Another key concept that shares much in common with resilience is that of “survivability.” Survivability has its roots in the military domain and is specifically addressed in the context of weapon platforms. Richards et al. [33] defines survivability as “the ability of a system to minimize the impact of a finite disturbance on value delivery, achieved through either the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance or the reduction of the likelihood or magnitude of a disturbance.” Survivability includes both passive and active techniques which show up in the physical, operational, and organizational design of systems. Physical disturbances today can be traced to terrorism in addition to traditional threats from state aggression and natural disasters. Electronic disturbances arise from information warfare and cyber attacks. And, of course, rapidly changing contexts can detract from the value proposition of long-lived complex systems. Today’s systems engineering tools, based on reductionist techniques, are capable of addressing the survivability of a component or subsystem. These tools typically employ traditional risk analysis and bottom-up verification. However, these tools offer precious little to address survivability at higher levels in the system architecture [11]. For example, there are no survivability analysis tools that can address tradeoffs between costs, utility and survivability of complex systems and enterprises. What is known, however, is that survivability arises from a combination of robustness and changeability or adaptability [11]. When considered above the component level, survivability becomes an emergent property of system architecture that has meaning primarily within the overall operational context of the system. Understandably, survivability requirements are extremely difficult to specify for system operation and maintenance, and when procuring systems [34].

So, what are the similarities and differences between survivability and resilience? Survivability is the ability to withstand attack or countermeasures. This definition does not illuminate how it achieves that. It also does not imply that withstanding attack means preservation or restoration of original form, position, or configuration. In other words, it does not imply “elasticity” as a system property [2]. Resilience, on the other hand, is the elasticity that allows a system to return to its original form, position, or configuration after being bent, compressed or stretched [2]. In other words, there is a learning and adaptation aspect to resilience. Thus, survivability implies the ability to withstand without buckling, whereas resilience implies the ability to “bounce back” after undergoing deformation of some sort [2].

IV. RESILIENCE ENGINEERING CHALLENGES

In resilience engineering, failure is seen as the inability to perform necessary adaptations to cope with real-world complexity, rather than as breakdown or malfunction. In the resilience engineering mindset, the performance of individuals and organizations needs to continually adjust to the prevailing conditions. Clearly, because of finite time and resources, such adjustments are necessarily approximate. Thus, failure represents breakdowns in adaptations directed at coping with complexity. Success relates to the ability of organizations, groups and individuals to recognize and adapt to unexpected change and surprising developments. The measure of success for groups and organization is the ability to “create foresight” and anticipate the changing shape of risk, before failures occur and cause harm. Conversely, failure is seen as the temporary or permanent absence, of this ability. Groups and individuals, skillful at recognizing the side effects of change, are able to adapt their model of risk and their profile of countermeasures, accordingly. Investigation boards of various large-scale recent accidents have found that improving safety requires new tools to perform safety/production tradeoffs and enhance resilience in the face of variability.

The engineering of organizational resilience pertains to concretely helping organizations maintain and manage an acceptable level of risk in both the short-term and the long-term. This requires explicit guidance on how to strike a balance between variables that act in tradeoff fashion such as production pressures and safety. Such guidance needs to be directed at people and teams in relevant managerial and other consequential organizational positions. When operating under rapid and efficient production pressures, the relaxation of safety practices may go unnoticed or, worse yet, be misunderstood or discounted. Under severe production pressures, it may become necessary to perform tradeoffs that would otherwise be considered unacceptable, and to accept increased risk with attendant adverse consequences that are often overlooked in the heat of the moment. In other words, when disruptive conditions persist, harmful consequences of changing safety practices may go unnoticed or, worse yet, be misunderstood or discounted. Under severe production pressures, it may become necessary to perform tradeoffs that would otherwise be considered unacceptable, and to accept increased risk with attendant adverse consequences that are often overlooked in the heat of the moment. In other words, when disruptive conditions persist, harmful consequences of changing safety practices may go unnoticed or, worse yet, be misunderstood or discounted. Under severe production pressures, it may become necessary to perform tradeoffs that would otherwise be considered unacceptable, and to accept increased risk with attendant adverse consequences that are often overlooked in the heat of the moment. In other words, when disruptive conditions persist, harmful consequences of changing safety practices may go unnoticed or, worse yet, be misunderstood or discounted.

As a result, organizations may, for very different reasons, behave in ways that are more risky than they realize or want [1]. The only time this is discovered is when an accident or breakdown occurs. The difficulty in effectively performing these tradeoffs has long been recognized as the major contributor to the slow, but sure erosion of safety margins, and subsequent drift towards failure. Tools that enable calculation of leading indicators make it possible to assess the consequences of risky decisions. In this regard, the specific questions that such tools need to help answer are:

1) How can safety concerns be balanced against severe, program pressures for superior throughput and efficiency?
2) How can the resilience of organizations be measured? How capable is the organization in coping with unexpected, disruptive events?
3) How can resilience be engineered in organizations? How can critical leverage points for the various stakeholders
be identified and addressed?

Answers to such questions are key to developing a proactive approach that would enable stakeholders to revisit and modify their priorities and preferences based on risk-benefit tradeoffs.

It is worth noting that safety is an emergent system property which arises from the behavior of and complex interactions among subsystems, software, organizations, and humans [2], [36]. The investigation of major mishaps over the past three decades and subsequent case studies have shown that organizations need to continually revisit and revise their assumptions about their capabilities by concurrently addressing technical, human and organizational risk factors on an ongoing basis. Analysis of past accidents [13], [15], [16], [37], [38] and case studies point to the need to explicitly manage risk continuously and throughout the system lifecycle and, in particular, to find ways to achieve and maintain a balance between safety requirements and production and efficiency pressures.

Traditional approaches, such as probabilistic risk analysis (PRA) and probabilistic safety assessment (PSA), are inadequate in this regard because of their use of oversimplified models of accidents as cause-effect chains [1], [2], [8]. Insights gleaned from the study of failures in complex systems, organizational contributors to risk, and human performance all point to the fact that safety is an emergent property of a system. This means that safety cannot be predicted from the attributes of the constituent parts of the system. Said another way, safety is a consequence of how a system behaves, rather than a static property of the system. This requires an understanding of how a system can proactively ensure that things stay under control. It is for this reason that systems should be made resilient, rather than merely reliable. This is not the argument that the failure probability is acceptably low is simply not enough. The system needs to be able to recover from unexpected perturbations, disruptions, and degradations of the operational environment.

One of the first international symposiums, held in October 2004 [39] invited thought leaders from various disciplines (software safety, engineering, psychology, sociology) as well as practitioners from diverse fields (e.g., aviation, nuclear power, healthcare, petrochemical industry) to address the principles for organizational resilience and identify factors that determine human and organizational performance. The results of this symposium provided a basis for how to incorporate human and organizational risks in lifecycle systems engineering and how to build knowledge management tools that proactively capture how human and organizational factors affect risk. Even so, there are serious holes in our knowledge base. In particular, we still need ways to address the following:

1. Help organizational decision makers in making tradeoffs between severe production pressures, required safety levels and acceptable risk. Getting a better grip on how these decisions are made and how they could be supported in resource-constrained, intense-competition environments is of particular importance, when an organization resorts to downsizing and outsourcing to lower costs.

2. Measure organizational resilience. This requires us to think beyond traditional trailing indicators of mishaps (e.g., errors, error rates) and identify new “leading indicators” that accurately reflect critical aspects of an organization’s resilience [2]. The key to achieving this end is to capture the organization’s understanding of its own risks. Today, models of risk can be found in safety management systems, responses to incidents, and countermeasures taken. However, such models can become easily miscalibrated relative to environmental uncertainty and change.

3. Identify ways to engineer the resilience of organizations. According to Weick and Sutcliffe [4], safety is a dynamic property of an organization and, as such, amenable to (“a dynamic non-event”) intervention. This means that potential breakdowns and failures can be recognized at an early stage, possibly even before they have had visible effects, and countermeasures can be initiated in timely fashion.

In light of the foregoing, it is worth discussing the techniques available for introducing resilience in systems. These techniques can be broadly divided into: analytical methods; and integrative methods. Each is discussed next.

Analytical Methods. Analytical methods tend to be based on traditional probabilistic techniques. Such methods can be brought to bear on those disruptive situations that can be predicted. The unique requirement of analytical methods is that traditional processes, such as requirements definition, and verification need to be specified at a greater level of detail than is done today. For example, with respect to the Mars Polar Lander, the requirements for strut vibration and software logic could have indeed been developed to a greater level of detail and analyzed through simulation to reduce the likelihood of the failure that eventually occurred. The time and cost of developing such simulations would have been well-justified given the potential severity of the failure.

Another key characteristic of analytical methods, (that has the potential for dealing with weak disruptions), is that of breadth. Analytical methods, as practiced, are often limited to a single product/system (e.g., a commercial aircraft) and one organization (e.g., the developer). Of course, developers today do attempt to extend these principles to their suppliers who provide components and subsystems. However, the extension of analytical principles to maintenance and production systems is rare, especially when the maintenance organization, for example, is separated from the developer by multiple organizational boundaries. Such was the case in the ValuJet accident, described by Chiles [40], in which the maintenance organization was separated from the developer by two layers of organizational boundaries. In such cases, rigorous extension of requirements and verification across these boundaries are essential to achieve resilience.
**Integrative Methods.** The term, integrative, is used to describe those methods that are comprehensive in the sense that they cover heuristics, risk management, and cultural factors. In general, heuristics can be applied to almost every type of disruption. For example, the heuristic of tolerance is particularly important for external disruptions while Billing's heuristics of human-machine interfaces are important for systemic disruptions such as loss of function, capability or capacity. An example of an overarching heuristic is that of, the human always being in control. For environmental disruptions, the heuristics of margin and cross-scale interactions are especially significant [1], [2].

V. A VISION OF RESILIENCE

Resilience is a semantically overloaded term [2] in the sense that it means somewhat different things in different fields. Generally speaking, it means the ability to “bounce back” from a shock or disturbance [2]. When it comes to systems, the term resilience takes on different meanings (Table 3) depending on the system under consideration (e.g., ecology, economics and business, industrial and organizational safety, networks).

<table>
<thead>
<tr>
<th>TABLE 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THE MANY FORMS OF RESILIENCE</strong></td>
</tr>
<tr>
<td>- Ecological Resilience [41]</td>
</tr>
<tr>
<td>- definition 1: rate at which a system returns to a single steady or cyclic state following a perturbation or transient;</td>
</tr>
<tr>
<td>- definition 2: a measure of the amount of change or disruption that is required to transition a system from being maintained by one set of mutually reinforcing processes and structures to a different set of processes and structures (for reorganizing systems only)</td>
</tr>
<tr>
<td>- Economics and Business Resilience [42], [43]</td>
</tr>
<tr>
<td>- ability of a local economy to retain function, employment and prosperity in the face of perturbation caused by shock of losing a particular type of local industry, or employer</td>
</tr>
<tr>
<td>- Industrial and Organizational Resilience [44]</td>
</tr>
<tr>
<td>- ability of an industry/organization to strengthen creation of robust, flexible processes in a proactive fashion</td>
</tr>
<tr>
<td>- Network Resilience [45]</td>
</tr>
<tr>
<td>- ability of a network to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations;</td>
</tr>
<tr>
<td>- the acceptable level of service pertains to being able to access information when needed, maintain end-to-end communications, and assure smooth operation of distributed processing and networked storage</td>
</tr>
<tr>
<td>- Psychological Resilience [46]</td>
</tr>
<tr>
<td>- the capacity of people to cope with stress and catastrophe</td>
</tr>
<tr>
<td>- psychological resilience is often contrasted with “risk factors”</td>
</tr>
<tr>
<td>- Socio-ecological Resilience [51]</td>
</tr>
<tr>
<td>- resilience controlled by slowly changing variables</td>
</tr>
<tr>
<td>- a function of investments in natural, human, social, and physical capitals</td>
</tr>
</tbody>
</table>

Resilience engineering, in part, emerged as a new discipline within systems [47], and safety engineering [48], to specifically address these various concerns. In particular, resilience engineering is concerned with monitoring organizational decision making with explicit identification and of monitoring of risks. Resilience Engineering views “failure” as an inability of the system to adapt to perturbations and surprising events in the real world, rather than a breakdown or malfunction. As such, Resilience Engineering calls for individuals and organizations to continually adjust their behavior/responses to changes in the real world conditions [49] in a safe, and risk-managed fashion.

In our view, resilience is a multi-faceted capability [2] of a complex system that encompasses avoiding, absorbing, adapting to, and recovering from disruptions (Fig. 1).

![Fig. 1. The Many Faces of Resilience](image-url)

Avoiding disruptions requires anticipation, which is enabled by predictive or lookahead capabilities. As such, a system that exhibits avoidance requires the ability to preview outcomes and take proactive action to circumvent either the occurrence or consequences of disruption. Withstanding disruptions requires the system to be robust. Robustness is achieved by having “shock absorbers” in the form of, for example, resource buffers that enable the system to withstand a disruption without having to reconfigure itself to respond to the disruption [50]. Adapting to unexpected change requires the ability to reconfigure form (i.e., structure) or available capacity. Finally, recovering from disruptions implies the ability to restore the system’s pre-disruption state as closely as possible. The latter may entail some performance degradation because the restoration may not be perfect.

It is interesting to note that Diamond [51] in his book on how societies collapse and go under, identifies three ‘stops on the road to failure.’ These are: 1) the failure to anticipate a problem before it has arrived; 2) the failing to perceive a problem that has actually arrived; and 3) the failure to attempt to solve a problem once it has been perceived (rational bad behavior). Arguably, a society that collapses can be viewed as an extreme case of lack of resilience. In fact, one can argue that the same criterion applies to individuals, organizations, and systems. Thus, a resilient system must have the ability to anticipate, learn and adapt. Resilience engineering, therefore, must address the principles and methods by which these capabilities can be created. In what follows, we elaborate on these proactive properties of resilient systems.

**Anticipation** involves the ability to “look down the line” to determine how the environment is expected to change with a view to making decisions and taking actions in the present that promote desirable outcomes and circumvent disruptions in the future. **Learning** encompasses continuously monitoring the external environment and system operation for contextually-relevant changes and reflecting them in the system’s models.
and knowledge bases. Context here is characterized by the mission, the state of competitive forces, available human and equipment resources, terrain and weather conditions, and time available for decision making. Adaptation involves the ability to adjust to new circumstances through reconfiguration and dynamic reoptimization of available capacity and resources. Anticipation, learning and adaptation are endemic to the resilience process.

Disruptions. Disruptions can be indexed and catalogued as cases in a case repository. A disruption would be indexed as natural or man-made, external or systemic, single agent or multiagent, and short-lived (i.e., transient) or enduring.

System Attributes. These are the properties or characteristics of the system including organizational infrastructure, system functionality, system complexity, system performance and system breakdown structure. A disruption can impact one or more of these characteristics. As such, depending on the type of disruption, resilience may need to be introduced into one or more of the impacted system attributes.

Methods. Methods encompass traditional probabilistic risk (and safety) assessments, safety-schedule-utility-cost tradeoffs, integrative/holistic methods, expert and history-derived heuristics, and proactive risk management on an ongoing basis. To achieve resilience, organizations need assistance in making effective production/safety tradeoffs. When performing such tradeoffs, production efficiency goals may need to be temporarily sacrificed, or production schedule relaxed, to stay within the safe performance envelope.

To make risks a part of proactive management decision-making requires knowing when to relax the pressure on throughput and efficiency goals, and how to help organizations decide when and to what degree to relax production pressures to reduce risk. In this regard, research is needed to understand the role of human judgment in organizational processes. Past research on judgment and decision making has shown that the decision to give greater weight to production than safety is implicit and unrecognized. These decisions can only be sound when set against local judgment criteria, given the time and budget constraints and short-term incentives that shape behavior. In fact, it is in normal, day-to-day operations that one can find clues of both organizational failures and successes. Not surprisingly, it is these processes that demand dramatic advances in safety. Today, individuals and organizations tend to take greater risks than they would ever want to, in retrospect. The effectiveness of tradeoffs that have been made is especially difficult to gauge because in hindsight it may appear that the relaxation of a particular constraint or making a particular compromise may have been unnecessary because “nothing bad happened.” Clearly, in such circumstances it is important to assess how peers and superiors would have reacted to such decisions.

Furthermore, real-life decisions rarely meet the norms of rational decision making. Although decision theory and psychology tend to depict decisions as explicit and unique acts, decisions more often than not tend to be implicit [52]. Decisions also reflect bounded rationality, i.e., humans settle for good enough decisions (i.e., satisficing), rather pursue optimal choices [53]. Finally, humans in retrospect tend to revise their decision criteria to justify their decision choice (post-decision consolidation [54]). As a result, certain consequences of decisions may end up getting suppressed or neglected.

A study of the “information environment” in which actual decisions are made and shaped, in which local rationality is constructed, is key to understanding organizational decision making. By studying individual and group behavior in these situations through actual encounters, in conjunction with case studies, retrospective analyses, and interviews with decision makers, one can increase problem awareness and

**Fig. 2. Resilient System Vision [2]**

**Fig. 3. Conceptual Framework for Resilience Engineering [2]**

**Disruptions.** Disruptions can be indexed and catalogued as cases in a case repository. A disruption would be indexed as natural or man-made, external or systemic, single agent or multiagent, and short-lived (i.e., transient) or enduring.

**System Attributes.** These are the properties or characteristics of the system including organizational infrastructure, system functionality, system complexity, system performance and system breakdown structure.

**Methods.** Methods encompass traditional probabilistic risk (and safety) assessments, safety-schedule-utility-cost tradeoffs, integrative/holistic methods, expert and history-derived heuristics, and proactive risk management on an ongoing basis. To achieve resilience, organizations need assistance in making effective production/safety tradeoffs. When performing such tradeoffs, production efficiency goals may need to be temporarily sacrificed, or production schedule relaxed, to stay within the safe performance envelope.

To make risks a part of proactive management decision-making requires knowing when to relax the pressure on throughput and efficiency goals, and how to help organizations decide when and to what degree to relax production pressures to reduce risk. In this regard, research is needed to understand the role of human judgment in organizational processes. Past research on judgment and decision making has shown that the decision to give greater weight to production than safety is implicit and unrecognized. These decisions can only be sound when set against local judgment criteria, given the time and budget constraints and short-term incentives that shape behavior. In fact, it is in normal, day-to-day operations that one can find clues of both organizational failures and successes. Not surprisingly, it is these processes that demand dramatic advances in safety. Today, individuals and organizations tend to take greater risks than they would ever want to, in retrospect. The effectiveness of tradeoffs that have been made is especially difficult to gauge because in hindsight it may appear that the relaxation of a particular constraint or making a particular compromise may have been unnecessary because “nothing bad happened.” Clearly, in such circumstances it is important to assess how peers and superiors would have reacted to such decisions.

Furthermore, real-life decisions rarely meet the norms of rational decision making. Although decision theory and psychology tend to depict decisions as explicit and unique acts, decisions more often than not tend to be implicit [52]. Decisions also reflect bounded rationality, i.e., humans settle for good enough decisions (i.e., satisficing), rather pursue optimal choices [53]. Finally, humans in retrospect tend to revise their decision criteria to justify their decision choice (post-decision consolidation [54]). As a result, certain consequences of decisions may end up getting suppressed or neglected.

A study of the “information environment” in which actual decisions are made and shaped, in which local rationality is constructed, is key to understanding organizational decision making. By studying individual and group behavior in these situations through actual encounters, in conjunction with case studies, retrospective analyses, and interviews with decision makers, one can increase problem awareness and
Special Issue on Resilience Engineering

understanding. Specifically, one can begin to: 1) understand how to get individuals and organizations to recognize and acknowledge the implicit tradeoffs that they make; and 2) determine ways to help individuals and organizations know when and how to continually balance investments in safety goals in the face of production schedule and efficiency pressures. Understanding tradeoff decisions is key to developing new forms of feedback on the side effects of changes and organizational decisions on program and system risks.

Metrics. A key aspect of resilience engineering is developing metrics and indicators of resilience. These are intended to alert management about potential conflicts between production pressures and safety needs. Making decision makers aware of risks arising from potential changes to daily practices is a necessary prerequisite to pursue corrective action. In this regard, resilience engineering views system safety (and risk) from a systemic perspective rather than as a causal model. The system model could then “explain” how mishaps and accidents can be an emergent phenomenon, rather than merely a consequence of cause-effect chains. Systemic accident models such as FRAM [9] and STAMP [6] have already begun to show what one should monitor (e.g., the possibility of undesired resonance, loosening of system constraints, or erosion of control among hierarchical organizational layers).

Such metrics can potentially provide insights into the tradeoffs space and enable testing of new leading indicators of an organization’s resilience? Organizational success depends on ability to perform safety/production tradeoffs in timely fashion. This requires management commitment, reporting practice, learning culture, preparedness/anticipation, and a degree of agility. Performance monitoring, is especially important when making tradeoffs made to accommodate sustained resource and schedule pressures. In such cases, the possible negative consequences may either be missed due to limited foresight or explained away because current needs usually have a disproportionate influence on decisions. These previous findings (and the leading indicator sets for each) could, for example, be transformed into a series of tradeoffs among the various sources of organizational resilience. These can serve as the initial basis for performing key tradeoffs. The validity and usefulness of each attribute can be tested through retrospective event analyses, case studies, and interviews. Such analysis can reveal how general organizational attributes come into play in decision processes that affect day-to-day operations and management of projects. This type of analysis and testing can illuminate how organization level resource scarcity and competition translate into local managerial or operational constraints that result in one decision option being favored over another—thereby potentially amplifying an organization’s exposure to risk? This understanding is crucial to understanding how an organization gradually can erode safety [55].

Engineering of resilience. While leading indicators of organizational resilience are a way forward in proactively addressing safety, additional insights are needed into the dynamic aspects of resilience. Resilience, like agility, comes at a cost [50]. Therefore, it is imperative to place resilience only where needed to contain costs [50]. Engineering resilience implies knowledge of the resilience tradeoff space and some degree of control over the relevant system parameters. In this regard, one aim is to identify critical leverage points for incorporating resilience into organizational processes. Such leverage points are typically associated with operational, managerial and political perspectives. As such, it is important to be able to identify, study, refine and extend the different instruments that stakeholders in various industries can employ to steer the organization, program and system away from potential disruptions.

VII. RESILIENCE HEURISTICS

System resilience typically results from a basic set of principles, laws and conditions that for the most part, have been accepted by the resilience community. From these, design heuristics can be developed. Simply, stated, heuristics are qualitative design methods grounded in experience. A notable proponent of the use of heuristics for architecting a system was Rechtin [36]. It is important to realize that resilience is still very much in the nascent stages in most domains. However, the one domain in which resilience is a relatively mature area is aircraft cockpit design where the Billings heuristics [56] have been exploited for several years.

It is important to realize that heuristics can complement each other in the sense that some heuristics become more effective if other heuristics are also implemented. Against the foregoing backdrop, we present resilience heuristics. These heuristics are directly traceable to the principles and laws presented in the literatures [1], [2], [3], [50], [56], [57], [58]. Table 4 presents a representation set of resilience heuristics. These heuristics augment Rechtin’s heuristics and operationalize Woods’ adaptability principles.
Table 4

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional redundancy</td>
<td>there should be alternative ways to perform a particular function that does not rely on the same physical systems</td>
</tr>
<tr>
<td>Physical redundancy</td>
<td>employ redundant hardware (e.g., processors) to protect against hardware failure when functional redundancy is not possible</td>
</tr>
<tr>
<td>Reorganization</td>
<td>system should be able to restructure itself in response to external change</td>
</tr>
<tr>
<td>Human backup</td>
<td>humans should be able to back up automation when there is a context change that automation is not sensitive to and there is sufficient time for human intervention</td>
</tr>
<tr>
<td>“Human-in-loop”</td>
<td>humans should be in the loop when there is a need for “rapid cognition” and creative option generation</td>
</tr>
<tr>
<td>Predictability</td>
<td>automated systems should behave in predictable ways to assure trust and not evoke frequent human over-ride</td>
</tr>
<tr>
<td>Complexity avoidance</td>
<td>systems should reflect system complexity and not complexity added by poor human design practices</td>
</tr>
<tr>
<td>Context spanning</td>
<td>system should be able to survive most likely and worst case scenarios, either natural or man-made</td>
</tr>
<tr>
<td>Graceful degradation</td>
<td>systems performance should degrade gradually when the unexpected occurs for which system is not prepared</td>
</tr>
<tr>
<td>Drift correction</td>
<td>system should be able to monitor and correct drift toward brittleness by making appropriate tradeoffs and taking timely preventive action</td>
</tr>
<tr>
<td>“Neutral” state</td>
<td>system should be able to prevent further damage from occurring when hit with an unknown perturbation until problem can be diagnosed</td>
</tr>
<tr>
<td>Inspectability</td>
<td>system should allow for human intervention needed without requiring humans to make unsubstantiated assumptions</td>
</tr>
<tr>
<td>Intent awareness</td>
<td>system and humans should maintain a shared intent model to back up each other when called upon</td>
</tr>
<tr>
<td>Learning/Adaptation</td>
<td>continually acquiring new knowledge from the environment to reconfigure, reoptimize, and grow</td>
</tr>
</tbody>
</table>

When it comes to heuristics and architected, it is worth noting that we are entering the realm of experience, judgment and intuition for which results can seldom be quantified or verified, in the traditional sense. So, if heuristics cannot be verified, what can we learn from them? First, certain design principles that go beyond verifiable requirements are often needed and, when employed, can enhance the system’s resilience to certain types of risks, cultural differences, and unknown threats. Of course, while the design can only be verified against known threats, there is always the expectation that the system will exhibit resilience in the face of unknown threats as well.

Heuristics are typically a function of the type of disruption, the type of system being architected, and the type of resilience needed (i.e., avoidance, survival, recovery). For example, some heuristics might apply to all systems ranging from government enterprises to infrastructure systems. Others may apply only to human-in-the-loop or socio-ecological systems.

As discussed earlier, there are two types of disruptions: degradation of input including unexpected changes in environment; and, degradation of function, capability or capacity. Of course, if the type of disturbance is unknown, the system may have to be designed for a variety of disruptions to increase coverage. However, it is safe to say that certain types of systems will typically be more likely to encounter certain types of disturbances. For example, physical systems, such as buildings, dykes and levees are more likely to encounter unexpected changes in environmental load. Of course, this does not mean that other types of disturbances can be ruled out.

VIII. CONCLUSION

In this paper, we have addressed resilience from a variety of perspectives and presented a framework and heuristics that jointly enable the design of resilient systems. We began by emphasizing that today when complex systems fail and mishaps occur, there is an initial tendency to often misattribute the failure to human error. We have characterized resilience engineering as the ability to build systems that are able to anticipate and circumvent accidents, survive disruptions through appropriate learning and adaptation, and recover from disruptions by restoring the pre-disruption state as closely as possible.

We have also clarified the differences between safety, reliability, survivability and resilience. Specifically, we have emphasized that resilience engineering does not view failure as a breakdown or malfunction of normal systems. Rather, failure is viewed as an inability of the system to either adequately absorb perturbations or adapt to changes in realworld conditions. In light of this definition, success is viewed as the ability to anticipate changing risk profiles that result from, for example, dynamic safety-schedule tradeoffs. With this definition, failure is viewed simply as the absence of this ability, when needed.

Importantly, we have presented a conceptual framework and heuristics for developing resilient systems. The framework comprises: disruptions, system attributes, methods and metrics. The rationale for these categories is to allow systems engineers to focus on what are the impacted system attributes, where resilience is needed, what methods are appropriate to achieve resilience in the relevant system attributes, and what resilience measures apply in a specific problem context. To this end, we have provided a set of heuristics that are intended to aid the system engineer in determining what type of resilience is needed, where it is needed, and how best to introduce it. It is important to realize that resilience comes at a cost. Thus, determining in which impacted system attributes to incorporate resilience is a matter of priorities, cost and coverage sought. In other words, determining how critical resilience is in a particular system attribute along with what it costs provides the basis for prioritizing where to incorporate resilience to get the “biggest bang for the buck.” Potential users of the framework and heuristics are systems architects and engineers working on the engineering of complex, socio-technical systems. The framework is intended to allow these professionals to continuously explore tradeoffs between resilience, utility,
cost, schedule, and performance throughout the system development and operation lifecycle.

REFERENCES


