35

Patterns for Achieving Resilience in Engineered and Organizational Systems

Scott Jackson, Victoria Hailey, Keith D. Willett, Timothy Ferris, and Eric A. Specking

Introduction

This chapter introduces the concept of system resilience and provides a foundation from which to identify recurring patterns of resilience in resilient system design applicable to engineered and organizational systems. Specifically, we are concerned with how resilience in different domains is affected by the system type commonly found in those domains and the adversities encountered. This chapter focuses on how resilience is achieved in two different types of systems (engineered and organizational) and the patterns involved in achieving that resilience.

Traditionally fields like psychology, ecology, and materials science define resilience as "the capacity to recover quickly from difficulties; toughness" ("Resilience," 2018, para. 1). An assumption is the definition applies to regaining the state or functionality affected by the adversity or recovery from some functional degradation caused by the adversity. More recently researchers (e.g., Hollnagel, Woods, & Leveson, 2006) have adopted a broader definition to include anticipating, withstanding, adapting, anticipation, and avoidance. This is the definition adopted by the systems engineering community.

For engineered systems the definition of resilience is "the ability to provide required capability in the face of adversity" (BKCASE Editorial Board, 2016, para. 4). BKCASE is the Body of Knowledge and Curriculum to Advance Systems Engineering Project, which is the compendium of knowledge about systems engineering overseen by the International Council on Systems Engineering (INCOSE). Four characteristics of resilient systems (identified by

Scott Jackson, Victoria Hailey, Keith D. Willett, Timothy Ferris, and Eric A. Specking, *Patterns for Achieving Resilience in Engineered and Organizational Systems* In: *Multisystemic Resilience.* Edited by: Michael Ungar, Oxford University Press (2021). © Oxford University Press.
DOI: 10.1093/oso/9780190095888.003.0036

Madni & Jackson, 2009) are the ability to anticipate, absorb, reconfigure, and restore capability in the face of a threat. These characteristics apply to both engineering and organizational systems). Jackson and Ferris (2013) identify a set of design principles, which can also be called techniques for a system to achieve these characteristics associated with resilience.

Domain Characteristics and Resilience

For our purposes, a domain is a specified boundary of knowledge or activity. Following are the five characteristics of domains that influence the ability of a system to be resilient.

System Resilience

According to BKCASE Editorial Board (2016), system resilience is the ability to provide required capability in the face of adversity. By this definition, an adversity must have an effect for recovery from that effect to occur. Therefore, the concept of resilience is a response to an adverse effect. Resistance is the ability to withstand the initial impact of the adversity. Following the initial impact, the system may adapt to the adversity or it may degrade to an acceptable level of capability. If the degradation is gradual, this is called tolerance. Finally, the system may recover to an acceptable level of capability. This recovery does not necessarily imply full recovery but rather recovery to a level acceptable to system stakeholders.

To understand a system's resilience, the type of system being examined must be accounted for. According to INCOSE (2015) a system is "an integrated set of elements, subsystems and assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements" (p. 5). For this chapter, the systems of interest are the broadest range of systems defined by Sillitto and collegues (2017) in which the essential characteristics of a system are any entity consisting of (a) many parts, (b) a relationship between parts, and (c) emergent properties not exhibited by the individual parts. These systems can be real or abstract.

One system type is a system of systems (SoS). This type of system is comprised of multiple component systems independently developed but acting together for a common goal. Sometimes in the SoS context the interaction between component systems makes it harder to achieve resilience. Other times the interaction enhances resilience. Jamshidi (2009) provides a comprehensive study of SoS.

Adversity

The quality of system resilience depends on how well the system responds to an adversity or adverse effect. There are many types of potential adversities. Some domains are inherently hostile, such as nature. Adversities can be human-made or natural and may originate within the system (endogenous adversity) or from without the system (exogenous adversity). Endogenous adversities include inclement weather, natural disasters, and adversaries with intelligence and intent.

In any domain, particularly in the civil domain, adversities can be either natural or human-made. In human-made domains adversities can be internal, that is, the result of internal latent faults.

Responding to an adversity may not mean fully regaining what was lost nor full recovery. If the system is human-made, the acceptable degree of recovery will depend on the expectations of stakeholders.

Capability

Central to resilience is the concept of capability. According to the INCOSE (2015) handbook, capability is the "ability to achieve a specific objective under stated conditions" (p. 262). Capability is one expression for system efficacy, that is, the system's ability to bring about a desired result. To recover is to compensate for the temporary or permanent loss. The system of interest (SoI), that is the system being addressed, may not get back what it lost even as it continues to produce desired results via compensation from other functions. In other words, part of system resilience is it *regains* what it lost or *recovers* from a loss through compensation for that loss.

Capability also includes the ability to anticipate or avoid an adversity, to withstand an adversity, to degrade gracefully following an encounter with an adversity, to recover to an acceptable level, and to remain an integral system before, during, and after an encounter with an aversity.

Central to the SoI's consistent and comprehensive ability to sustain desired capability are *patterns* that help retain efficacy, prevent the loss of ability to perform a function, regain what it lost, or recover from that loss. Patterns of robustness help the system withstand the adversity. Patterns of adaptability help the system recover or regain (e.g., return to a prior state). Patterns of tolerance allow a system to degrade gracefully to a lower but acceptable level of capability. Patterns of integrity allow a system to remain whole before, during, and after an encounter with adversity.

Timeframe

In all domains, damage by an adversity and recovery will occur over a period of time. Intervals of interest include times to prepare for the adversity, time to anticipate and detect the adversity, time to react to the adversity, and the time to recover. The capability required of a system may be constant through all the times referred to in the previous sentence, where the need is for a system, which under a very wide spanning envelope of conditions would be required to produce constant available capability. Other systems may perform roles where the necessity for available capability changes in response to *time* or some other factor.

Reviewing an operational timeline for resilience can help distinguish the nuances of the different phases. Figure 35.1 shows a general timeline for resilience that includes *before an event*, *during an event*, and *after an event*. Upon threat initiation, the SoI may be resistant to its effects. For example, a common system is a coastal community threatened by a hurricane. In the earliest phase of the timeframe a hurricane may be detected far out at sea. It is not known whether this particular hurricane will strike the community or not. However, even during this phase the coastal communities may have taken some preliminary steps such as

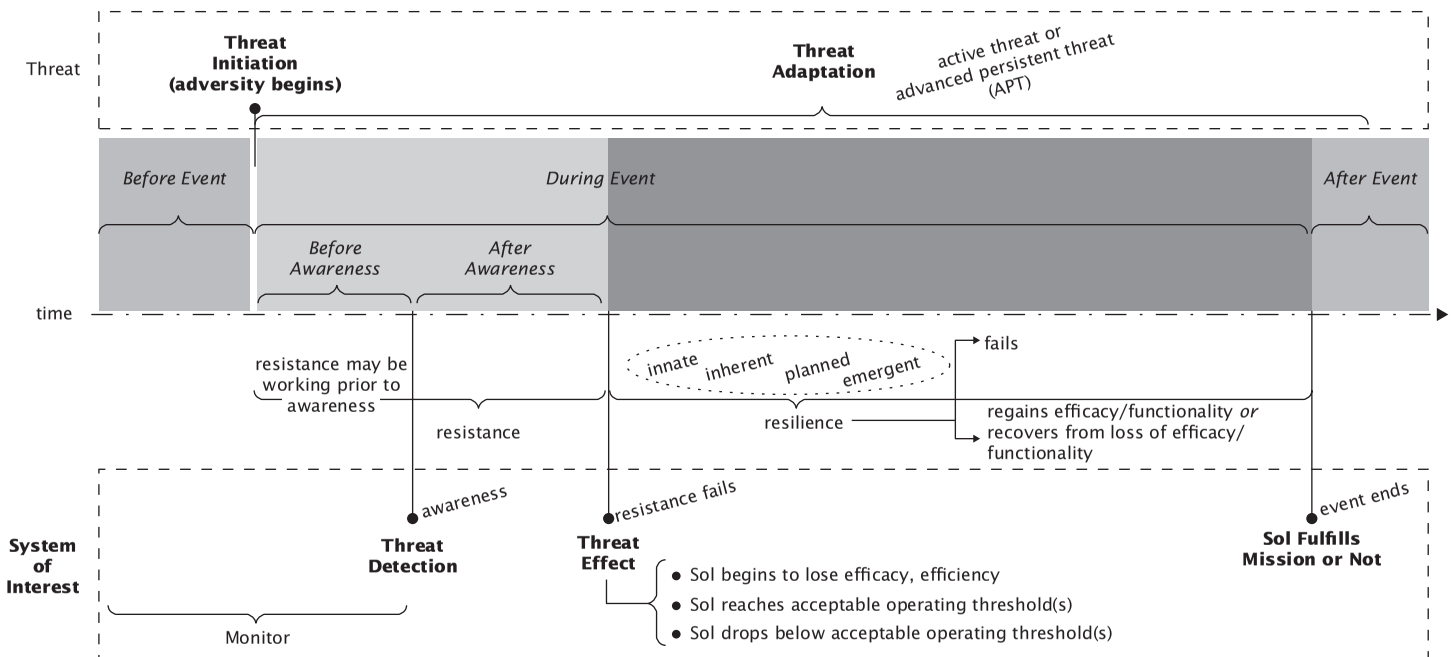

FIGURE 35.1 Resilience timeline (operational view).

providing distributed power systems (e.g., generators) to residents. Anticipating a series of such storms, many such communities require houses to be built on stilts to allow for water surges. During this predisaster phase, the progress of the hurricane is tracked using satellites and aircraft, all aspects of resilient infrastructure. When the hurricane strikes land, the system (the community) enters the protection phase in which residents are protected with materials such as plywood, which can be used to cover windows and protect homes from water damage. Following the impact of the storm, water is diverted away from the community through channels. If the community is resilient and has the right resources in place before, during, and after the hurricane, it will return to normal.

Three phases for resilience emerge from this timeline: *detection* of an adversity's effect, *response* to an adversity's effect, and *recovery* from an adversity's effect. We may then define functions within these phases to monitor, detect, triage, notify, respond (e.g., withstand or resist), change (e.g., reconfigure, reconstitute, restart), fail over (e.g., invoke redundancy), fail gracefully (e.g., tolerance), failsafe, and recover (e.g., adapt, restore). These phases provide a framework within which to identify recurring themes of resilience such that we can design guidelines to produce resilient systems (i.e., identify and codify *resilient system patterns*).

Techniques

During the development phase of a human-made system, the designer will incorporate in the design one or more features using design techniques. For engineered systems these techniques are based on principles identified by Jackson and Ferris (2013), such as absorption, physical redundancy, and functional redundancy. Each will be discussed further later in this chapter. These principles are guides to the design of the system, which may indicate the physical or behavioral characteristics of the system. For organizational systems, the techniques are for the most part human activity techniques (ISO 22301, 2012). The design features incorporated in both cases will reflect the actual adversities for which the system is able to respond.

Patterns

A *pattern* is a depiction of a regular form (Alexander et al., 1977), which provides us with architectural patterns. Software engineering provided us with design patterns to capture and reuse development knowledge. Decision patterns capture and reuse business and mission knowledge (e.g., cybersecurity decision patterns; Willett, 2016). All actual patterns are not arbitrary design ideas, but rather emerge from observation; that is, actual patterns are mined from real experiences. All patterns start with a notional idea, a concept for a particular pattern.

Resilience design patterns provide a repository of regular forms that represent real-world resilience occurrences that meet the requisite criteria for invariance. A resilience design pattern language provides the lexicon, syntax, and grammar to help articulate the abstractions of recurring resilient themes. The design patterns and the pattern language help systems engineers design solutions that provide resilience and systems that have the ability to be resilient. For engineered systems, there will be patterns of design techniques that

enhance resilience. For organizational systems, there will be patterns of human activity that do the same.

The Engineered System Domain

The engineered system domain consists primarily of systems that are human-made and physical, as opposed to organizational. This section describes these types of systems, their adversities, their expected capabilities, the timelines over which they encounter adversities, and the techniques they use to achieve resilience. This section also provides case studies that illustrate the application of these principles and the consequences of the failure to apply them. Some of the systems may have human operators. In those cases, these systems are called sociotechnical systems.

Systems for the Engineered System Domain

A Department of Homeland Security report (2018) identifies 16 infrastructure sectors that are critical. These sectors include chemical processing; commercial facilities, such as offices; communications, such as telephones; manufacturing, such as automobiles; dams; emergency services, such as ambulances; energy, such as electrical power generation; financial services, such as banks; food and agriculture, such as farms and food processing; government facilities, such as state and federal office buildings or military bases; the healthcare sector, such as hospitals; the information technology sector, such as databases; water and waste systems, such as water mains and sewers; nuclear reactors; and transportation systems, such as railways and airports. The systems discussed in this section are primarily civil rather than military in mission. Many of these systems are systems of systems. For example, the electrical power system, in whatever form, provides power to almost all other systems.

Techniques for the Engineered Systems Domain

Each system within the engineered systems domain has its own set of techniques that can be identified and implemented in the development phase. All of the techniques described next are abstractions; that is, they do not identify a specific solution. They only suggest an approximate form for the final solution to take. The following paragraphs describe some of the more notable techniques followed by a case study of its application.

The Absorption Technique

This technique protects the system from forces or stresses to a predicted design level (it absorbs the stress to maintain functioning). This level is accompanied by an acceptable margin of strength and an acceptable level of degradation. Almost every domain has an absorption level to which the system is designed. For example, in the aviation domain, all commercially certified aircraft have to meet the bird strike requirement. This is the requirement that the engines of an aircraft should be able to *absorb* the impact of a bird of a certain weight without loss of power. According to the Federal Aviation Administration (2015), this weight is about four pounds. This does not mean that the requirement will not be exceeded. If they are, as

was the case with US Airways Flight 1549 that was forced to land on the Hudson River in New York after striking a flock of Canada geese (Pariès, 2011), the aircraft will have to rely on other techniques such as *functional redundancy* described in the following text to maintain capability.

The Physical Redundancy Technique

This is one of the most widely recognized techniques in engineering. It simply states that the system should be designed with two or more identical and independent branches. If one of the branches fails, the other branch will be able to sustain the predicted load despite adversity. Following the failure of the U.S.–Canada power grid in 2003, the U.S.–Canada Task Force (2004) issued a report that called for "backup capabilities of all critical functions" (p. 9). This is tantamount to *physical redundancy*.

The Functional Redundancy Technique

Functional redundancy is similar to physical redundancy except that the two branches are physically and functionally different. This technique has been found to be useful in many cases. The idea is that there is one branch that the system depends on for normal operation. There is a second branch with less capability but sufficient to maintain an adequate level of capability. In the case of US Airways Flight 1549 the primary branch was the engines designed with the *absorption* technique in mind. When that system failed (shut down), the secondary branch consisted of internal power provided by a ram air turbine and control by the pilot, the latter constituting the *human in the loop* technique described next. These two techniques provided the secondary capability for the aircraft to land in the river and save the lives of the 155 passenger and crew, thus achieving functional redundancy.

The Human in the Loop Technique

This technique states that the system should be designed to allow for human cognition where needed. One of the most well-known examples of the use of this technique is the Apollo 11 mission. According to Eyles (2009) computer problems on this mission forced the operator Neil Armstrong to land the module on the moon manually. It can be said that the *human in the loop* technique was critical to the success of the mission.

The Distributed Capacity Technique

This technique states that the system should be designed so that its nodes are independent such that if one or more nodes are damaged or destroyed, the remaining nodes will continue to operate. For example, following a hurricane, the electrical power system employs this technique by installing portable generators in critical structures, such as hospitals. An example of the use of this technique was the deployment of generators during the engagement timeframe as described by Mendoça and Wallace (2006) to restore power in New York after the 9/11 attacks. Distributed systems are usually expected to be enduring, perhaps with replacement of assets which form parts of the system. In the case of 9/11, the distributed systems were stored for emergency use and then deployed as needed. Distributed systems allow the entire system to degrade more gradually when it encounters an adversity.

Organizational Systems Domain

Organizations are systems, satisfying the various definitions of resilience through their form and function: they have interrelated elements—people, processes, technology, information, data, and feedback loops—that are interdependent and produce more than the sum of their parts. By nature, organizational systems are comprised of multiple systems or SoS. Each individual employed in an organization is, by nature, both a system as well as a system element. A division of a corporation may be a self-sustaining system within a larger organizational system. The relationships formed by the SoS structures are virtually infinite in their range, making control over such systems challenging.

Organizations rarely follow an engineering process during their early formation and development. People form relationships, more or less formally, that develop into new organizations, which are usually allowed to evolve organically toward a shared goal. For example, as most people know, Apple was the result of a working partnership between college buddies Steve Jobs and Steve Wozniak that coalesced around an idea to popularize personal computing.

Organizational processes, as qualities of systems, function similarly in bee or ant colonies: each is a superorganism whose shared goals, means, and opportunities translate into shared objectives, tasks, and processes. Likewise, the United Nations, as an international organization, shares the same characteristics as the local neighborhood recycling collective: both share the same general behavioral patterns that people (and some insects) follow when collectively organizing to accomplish a specific purpose or goal.

It takes time and effort for organizational teams to form, storm, norm, and then perform. Once formed, the system's components—people and other resources—are constantly changing, even as their processes stabilize. This dynamic aspect of organizational behavior is apparent in any commercial corporation: its people, structures, processes, products, services, suppliers, and customers are always changing and intentionally evolving to a level of performance capability that can provide a return for corporate investors.

Individual elements, as well as their composition, can and must be replaceable for the organization to meet its customer needs consistently, as a measure of its quality performance. When viewed in this way, the organization can be seen to be continually undergoing change, with that undercurrent of constant activity challenging the limits of its control and efficacy in perpetuity.

When viewed through a resilience lens, one of the critical prerequisites for achieving organizational capability to recover is having the required level of *process* capability already well established in the event of a disruption. For example, organizations often believe they are resilience-capable because they have documented policies, processes, procedures, and job descriptions, but are surprised to learn they also need adequate resources to execute production processes. To recover from a potentially catastrophic event, the organization needs to be able to reproduce its own set of derived or designed processes when the need arises, together with the resources, whether material or human, to execute a recovery plan. When the twin towers were attacked on 9/11, the stark reality was that those organizations housed in only one location, and without distributed resources, perished. Those with distributed plans, resources, policies, procedures, and the resources to use them, were able to recover.

Whether sales, finance, operations, management, or governance, each set of processes has its own key resources that become essential elements for recovery that, while unique, can be replicated, if and when needed. However, not all organizational processes should be prioritized as essential to begin recovery. For example, to prioritize sales over operations as the first recovery target in the midst of a disaster could be viewed by existing customers as disloyal, or worse, profiteering, when it appears that a corporation is ignoring its operational responsibilities to its customers.

The unpredictability and complexity of organizational systems take root in the dynamic nature of one of its main system elements: people who, by nature, tend to resist change, are unpredictable and perpetually fail to understand their own biases and limitations, including learning from history (Kahneman, 2011). These aspects of human nature make it more difficult to predict with any certainty that outcomes can be achieved without specific plans, accountabilities, and responsibilities in place to orchestrate events.

Sometimes, organizational systems are not designed or engineered with a purpose in mind, instead evolving into their operational forms. Organizations that spontaneously materialize, such as grassroots citizen movements that evolve into formalized activist groups, demonstrate that direction, purpose, and goals are not always defined or even understood. The emerging entity forms around a shared belief or vision. Greenpeace emerged from an ad hoc citizen's group called the "Don't Make a Wave Committee" whose members protested underground nuclear testing. Over time, its members formalized the Canadian nonprofit, nonviolent environmental protest group, with its name representing the unity of the peace and ecology movements (Greenpeace, 2019).

Organizations seeking resilience as an inherent system characteristic need to be cognizant that the pursuit of this attribute often implies a return or recovery to a former operational state prior to the adversity. To build resilience requires having a target capability defined. Without defined, organized, and structured organizational systems in place, the recovery target can remain undefined, and recovery cannot be assured. The various components of the organization must be identified to do so. Given that each organization is different and that the recovery context will be derived from the organizational context, all the elements that are comprised by the "organization," whether permanent or variable, must be identified if they are to be targeted to be a vital system element needing to be recovered.

In addition to such elements as people, systems, processes, policies, procedures, and relationships, there is an endless array of system elements that contextualize each system's recovery efforts, such as buildings, locations, market capitalization, materials, reputation, and intellectual property. The value and priorities for recovery for each of these, as elements of that organizational system, must be determined if resilience is to be achievable when needed.

But what about situations in which resilience is achievable, but a return to a former state is neither possible nor desirable? For example, all organizations, including governments, corporations, businesses, and cooperatives, large and small, urban and rural, are facing the uncertainties of climate change. It may not be possible for recovery to a former state, for example, when hurricanes and monsoons leave a wake of geophysical changes in coastlines, landscapes, and waterways. Instead, recovery may mean adaptation to a new and different state where continuity is once again possible.

Consider, then, those organizations expecting to achieve climate resilience when faced with weather-related disasters. They must understand their operational processes in their current state—their inputs, activities, and outputs—and, in doing so, bring into focus considerations of such issues as whether to source from local or national or global suppliers in the face of disruptive climate events. Interactions between systems and process interdependencies must also be understood if plans for a successful recovery strategy are to be successful, especially when supply chain reliability affects critical infrastructure.

Identifying existing vulnerabilities and threats to recovery is key to understanding, and eliminating, the potential failure points when recovery plans are triggered into action. A full understanding of the current physical and operational states before, during, and after impact requires a precautionary approach when identifying weaknesses, so that realistic recovery plans can be developed to achieve a specified future recovery target. When this step is omitted, results can be catastrophic, and the planned recovered state can be unachievable. For example, regulators' assumptions about Fukushima's vital cooling systems capabilities were wrong when faced with an earthquake-induced 50-foot tsunami. By failing to recognize, and plan for, the nuclear facility's actual, as opposed to perceived, vulnerabilities: "Three of the six reactors melted down, with their uranium fuel rods liquefied like candle wax, dripping to the bottom of the reactor vessels in a molten mass hot enough to burn through the steel walls and even penetrate the concrete floors below (Fackler, 2017, para. 7). It took officials six and a half years to move from "disaster" to "clean-up," with full recovery never being achieved, and the facility undergoing decommissioning instead.

Priorities help with decisions concerning the deployment of scarce and urgent resources. Decisions, made by appropriate authorities, should determine the necessary course of action at the moment of impact: who should do what, when, where, and how, with the *why* having become the trigger to act. Stimulus–response type decisions, similar to automated systems inputs/outputs, progressing through if–then–else decision logic, must also be "programmed" into organizational decision-making processes. Decisions have to be made well in advance, not at the time of impact, when the emotional human response is limited to fight, flight, or freeze.

Responsible authorities, both public and private, are the appropriate accountable parties for determining whether recovery is even possible, such as with Fukushima or with a devastating corporate loss of reputation resulting from a corruption indictment. In some contexts, perseverance is the ideal continuity strategy, whereas in other circumstances, without knowing what the desired operational state is or what it takes to achieve it, achieving expected outcomes in the face of adverse conditions becomes an impossible task.

When planning for organizational resilience, preparing to mitigate the effects of such far-reaching and all-encompassing catalysts for change, such as global warming and biodiversity loss, organizations are often criticized for being too risk-averse. However, as unwelcome as the task is, preparation for disaster is also the critical first step in determining which possible actions will best determine successful organizational outcomes—in this case, resilience in the face of disruptions.

Organizational System Adversity

Adversity in organizational systems translates to threats arising from internal and external sources. External threats to organizations are virtually infinite, from distributing malware to

industrial espionage, making context and probability two key components in determining what threats to resilience need to be managed. In some cases, when external threats cannot be avoided easily, such as the location of a facility on a fault line in an active earthquake zone, other strategic safeguards are required to ensure risks are appropriately mitigated to make resilience achievable.

An organization's need to understand, for example, the multifaceted nature of climate change—an external threat—will force a different analysis of risk than a competitive analysis. The specific threats, vulnerabilities, and required safeguards each present a varied set of resilience targets to be managed, with different impacts being mitigated to achieve recovery. Each organization must be able to identify its risk sources according to its own unique context. To do so, it must evaluate the probability and severity of its critical threats and their impacts, providing an accurate assessment of existing vulnerabilities.

By way of illustration, organizations that provide critical infrastructure services, such as telecommunications and hospitals, are expected to have a recovery plan at the ready that offers seamless 24/7 service capability, even in the event of a Category 5 storm. Despite such dangers, critical infrastructure is expected to withstand unpredictable, chain reactions of hazardous events such as lightning strikes, floods, power outages, downed communications, and failures in transportation.

Each recovery context, however, needs to maintain its own unique and predetermined plans of organizational capability. Operations and communications with customers and suppliers depend on critical infrastructure to move goods and services, and even have employees report for work. An online, for-profit games developer, on the other hand, itself dependent on critical infrastructure to function, is unlikely to be expected to remain operational during such hazards.

External threats are also context specific. Generally, an organization's purpose and mode of operation are readily identifiable through commonly obtained, industry-specific threat lists that characterize those threats most likely to be experienced within a specific sector. For example, there is little value in a hospital reviewing the threats lists of a construction company. However, building resilience requires also identifying the unique risk sources. Common organizational threats, such as bad actors and natural disasters, are more obvious, while others may be unique to their own purpose, such as the inability to procure suppliers in a new industry space.

Assessment of risk is a knowledge area required by most organizations if they plan to achieve resilience. Insurance is an industry that manages resilience risk using actuarial science. Ironically, insurance customers, as the industry's primary revenue source, are also one of its biggest threats and liabilities, when too many legitimate claims require immediate payouts.

Internal threats are sometimes considered easier to identify, since they are attributable to the activities and behaviors occurring within the organization's boundaries. However, internal threats warrant equal, and in some domains even more, attention than publicly known external threats, since by nature internal threats to resilience are easier to mask outside the glare of public scrutiny. Confidentiality and nondisclosure agreements often compound the secrecy surrounding internal threats and their co-existing vulnerabilities, making them even

more insidious, and potentially delaying recovery, and in doing so, increasing their negative impact.

On the other hand, some of the most challenging adversities are those that arise from within, such as fraud or intellectual property theft because they are often hidden. When internal threats materialize and go unmitigated or unnoticed, they can weaken and destroy an organization's overall capabilities to recover, especially if vulnerabilities are continually exploited and capabilities are eroded without scrutiny. For example, employees working in a toxic organizational culture are less likely to contribute productively when working for repressive, bullying bosses (Van Rooj & Fine, 2018). Internally unstable, the organization's recovery becomes increasingly uncertain as the integrity of the system itself erodes under the impact of internal threats.

Contrast this result with organizations promoting positive psychological benefits, where employees benefit and feel motivated to perform at higher levels as a consequence of feeling emotionally stronger in a positive and thriving work environment (Cameron, Dutton, & Quinn, 2003; Hargrove, Nelson, & Cooper, 2007; Luthans, 2002; Wright, 2003). In such cases, when faced with the threat of change, transformation, and uncertainty, the positive psychological benefits that enable employees to be resilient are reflected in their performance (Luthans, Avolio, Avey, & Norman, 2007). Similarly, resilience in leaders has been shown to positively affect both employees' and an organization's performance (Youssef-Morgan, 2004).

The prerequisite for recovery, then, is a clearly defined pathway forward after adversity. The organization needs to ask, and sufficiently answer, the following questions if it is to assure itself of continuity:

- What processes need to be enacted once an adversity triggers action?
- How do the system elements need to re-identify, regroup, and reprioritize to meet the recovery plan?
- Who is responsible and who is accountable for the recovery?
- When must recovery actions be triggered and complete, and what time constraints must be considered in the recovery planning?
- Where does recovery materialize and manifest?
- Why is recovery and continuity being assured?

Resilience manifests in an organization when a threat that acts on a vulnerability within the system materializes, resulting in a loss of some kind. Typically, the loss affects the organization's ability to continue to operate in some way, such as when a data center is flooded in a storm, triggering a switch to its backup systems.

Even when due diligence is practiced, and processes are consistent, the inherent stability of the organization is at risk of being compromised any time a threat is realized. Consequently, when organizational processes operate at a low maturity level, epitomized by hero employees and managers diligently putting out fires when faced with go/no-go decisions, the costs are typically born elsewhere and often in unintended consequences.

Predictability of a process to achieve its planned and intended purpose—the ability of inputs to be translated into their intended outputs—diminishes as process discipline

diminishes. Lack of process capability always translates into increased process risk and, in turn, organization risk (ISO/IEC NP/TR 33015, 2014). This point illustrates why start-ups, due to their trial and error nature, lack resilience.

Predictability of process performance also becomes critical in the evaluation of the system's behavior, relative to its purpose. Organizational systems often devise their own constraints to prevent specific activities and behaviors from continuing, such as through the choice of markets, sectors, or technologies. These constraints operate as parameters for what the organizational systems *shall not* do, bound by good governance principles and policies. For example, within the bounds of civilized society, organizational systems cannot break the law, harm humans, or ignore their safety responsibilities to their employees, without being held accountable.

Resilience requirements, or *shall not* constraints, often serve to protect the integrity of the system itself by establishing priorities. They provide insight into managing resource capability, as well as the specification of acceptable and unacceptable recovery activities. This specification narrows the recovery requirements such that system boundaries are visible or can be established in a way that enables recovery to occur: what is in the system and prioritized as needing resilience capability and what is out of the system and of little value or interest?

Organizations that decide what not to do become better at what they are capable of doing because they avoid resource conflicts by providing clarity of focus. Organizations that fail to do so bring truth to the ancient adage, "Jack of all trades, master of none."

When resources operate in a consistent state of reactive behavior and fail to adhere to the rigors of process discipline—communication, documentation, records, monitoring, traceability, accountability—decisions are made without all the data and evidence necessary for consideration, and mistakes are commonplace. Such errors tend to be proportionate to the degree of complexity of the project underway, such as a company's decision to go live with a facial or emotion recognition technology system whose artificial intelligence hasn't learned how to identify and mitigate racial and gender biases, causing more harm than benefit when false readings occur (Rhue, 2019).

Organizational Processes

The complexity of organizational systems is exacerbated by their inherent nature. As a systems of systems structure, the ability to reliably predict system outcomes is no longer a matter of design, but of risk management of the less reliable system elements—humans—which require constant scrutiny through vigilant monitoring and oversight.

Organizational resilience requires a high degree of organizational maturity to be effective. The inherent process capability of each of the processes used to achieve resilience becomes a measure of risk in determining whether or not resilience can be achieved (ISO/IEC NP/TR 33015, 2014). As a general principle, when confidence in expected outcomes is high, risk is perceived to be low. When confidence is low, risk is perceived to be high and potentially unacceptable. Credit ratings reflect this type of zero-sum thinking, when organizations operate at low maturity levels, making credit harder to achieve when it is needed most. This is one of the reasons that start-ups typically have to rely on investors rather than creditors.

Credit tends to be abundant when it is needed least, reflecting confidence in maturity and responsibility, both of which contribute to resilience capability.

For any organization to become resilient, it needs to first decide which processes are essential and are actually required by customers or regulators. This effort, in itself, often requires significant analysis and reanalysis to get it right. Most organizations, when they are first conceived, rarely invest the time, effort, and what are often scarce resources to formally evolve their purpose, goals, outcomes, costs, and processes. With change so rampant in the early days of an organization's evolution, processes are rarely documented until some level of reproducibility, and therefore an aspect of resilience, is required. The impetus to demonstrate a capability for resilience is often triggered by customers requiring their suppliers to provide evidence-based confidence in the supplier's capacity to continue.

The capability of the organizational system to design for, and achieve, resilience is a direct measure of the maturity of its processes. Beneficial outcomes associated with maturity include self- and other-awareness (of other organizations, stakeholders, competitors, etc.) consistency, reliability, discipline, evidence-based decision-making, plans, resources, and leadership—all necessary components for building the capability to survive adversity (Ungar, 2018). Whether natural disasters, fluctuating market conditions, or such opaque threats as internal mistakes and fallible human judgment, mature organizations possess the functional capability to understand how to replicate their priority operations and enable them to recover.

These patterns are similar for engineered systems. When computer or physical systems are built to be resilient, the specification of required target recovery levels must be precise enough to flow through the subsequent inputs and activities as outputs, since any errors will flow through the process—thus, the euphemism, "Garbage in, garbage out." These errors affect the next downstream process and often impact upstream processes as well, such as customer service, when a complaint is reported.

Processes also need to be relatively consistent and predictable if they are to become reproducible (imagine trying to build an assembly line based on a prototype that is always changing). In many cases, it does not make sense for organizations to try to engineer for resilience while they are still evolving, especially entrepreneurial organizations whose limited resources are completely devoted to initial commercialization. Investing time, money, effort, and procedures to support recovery for a business that is still launching would make even the most conservative entrepreneur regret such critical resource mismanagement.

For these reasons, specified degrees of formalization are required, depending on the context, and only then does resilience become possible. Similar to any other system, resilience can be designed and engineered into the organization's performance characteristics.

Organizational System Capability

Organizations, as purpose-based systems, are driven to achieve their intended outcomes through a sharing of purpose, goals, strategies, and objectives. Whether processes are ad hoc or formal and documented, together as a system, they serve to satisfy organizational goals.

Organizational systems, being people-based, are rarely engineered as precisely as other systems. People-based systems face far more challenges to retaining cohesion and control than systems whose components can be engineered to a level of predictable precision.

Humans, as a dynamic and unpredictable element of systems behaviors, together with general resistance to being controlled, introduce management system engineering challenges that are constantly changing and evolving, especially given how little agency organizations have over their actors.

Organizations with externally imposed recovery targets, including those prescribed for critical infrastructure or bureaucracies, such as power companies, are accountable for service levels to regulators and customers. Resilience in these cases is an externally imposed requirement on utilities to ensure that formal recovery policies, processes, procedures, records, and identified resources are capable of providing a predictable level of stability and consistency, both in planning and execution.

Recovery goals are inherent within the organization's target resilience capability level. They provide the degree of reliability and integrity precision necessary to rely on not only the processes required to orchestrate the recovery effort, but also on any plans that were developed. In turn, those plans require the assurance that planning processes were followed with sufficient discipline and formality.

A dilemma eventually presents itself for organizations when considering the cost of loss versus the investment costs necessary to exercise prepared and planned recovery options. Where safety is concerned, risk-averse options always dominate. However, investments into full recovery option scenarios may not always be possible, especially if costs of recovery are less than the costs of starting over and absorbing all losses. If a business is worth US$2 million, but its ideal recovery plan costs $4 million, the decision becomes clear.

Organizational capabilities, when not entrenched in process knowledge and consistency, are harder to recover. Founders' knowledge, experienced-based team competencies, and relationships with customers are all areas of capability that contribute to organizational maturity but are virtually impossible to capture and measure. Similar to the concept of "good will," intangible social assets, such as high-performance teams, should also comprise aspects of organizational resilience that, depending on its criticality, should be replicable.

The risk of loss of long-term employees who have years of experience and broad knowledge of the organization must be measured against the organization's dependency on, and subsequent cost of the loss of, those critical resources. Losing a founder can be ruinous if no one shares their knowledge, but with a well-informed, well-trained, and well-performing team, the loss of a founder may be beneficial, if change is the objective.

To be effective, organizational resilience requires basic communication elements: policies, processes, procedures, records, and skilled resources, prioritized and assessed, are the simple building blocks of an effective recovery plan. Any deviation in process or behavioral dynamics that fails to undergo the rigor of change management risks becoming ad hoc and disruptive. Any such deviation becomes a precursor to uncontrolled change, where a significant degree of uncertainty and negative risk usually enter the resilience equation.

People are, therefore, constituent elements of organizational systems. However, by virtue of being human, people have an elevated status or worth when compared to other organizational resources. This understanding of basic human rights forces organizations to adopt a different perspective and approach to understanding their resilience resource requirements.

Skilled personnel, while replaceable and reproducible, are not expendable or disposable. A unique, one-of-a-kind prototype, such as a manufactured product, can be commissioned, created, replicated, dismantled, and thrown away. An individual person, by virtue of having intrinsic value in and of himself or herself may become part of, but still remain separate and distinct from, the organizational system of which the individual is a part. This fact constrains how resilience is achieved and requires a significant degree of flexibility and interoperability for recovery procedures to be effective.

Parallels may be drawn in the adoption of certain resource management principles, such as recycling, which can be applied to materials or to skills. However, beyond such similarities, people have special resource status. The cost of a human life is incalculable, placing even greater responsibility on the system to protect and preserve itself and its human elements. Humans as components of an organizational system present more constraints than perhaps other systems in the pursuit of available resilience options.

Despite these constraints, designing for organizational resilience should follow the same process as designing any other system requirement to fulfill its intended outcome. The development of an organization's resilience capabilities should follow the same systems engineering processes used to reliably enable any system capability. Once the organization's unique constraints are considered, it must engineer its systems to meet its own unique resilience requirements for its resilience-building recovery efforts to be successful in the face of adversity. This means designing resilience into all significant organizational processes and enabling them to deliver predictable outcomes. Engineering for resilience is similar to engineering systems for safety and reliability in the design of a jet engine, a medical device, or a software application: each step in the design follows a rigorous, tested process.

Organizational resilience is a non-functional organizational system requirement that organizations must engineer into their management system components—their processes—to benefit from the essential behaviors, activities, relationships, and information flows at the time they are needed (even if they are never used). Internal and external systems and processes interface, cross, and co-mingle at various systems boundaries. These exchanges often become critical vulnerabilities when organizations, as a result of low maturity and/or ineffective communication, fail to identify and manage their risks.

Unique Techniques

As with any system type, assuring the capability to resist and recover from adversities requires establishing plans, well in advance, that are able to script and orchestrate the necessary sequence of activities that must occur for a resilient state to be realized. Risk assessments that project as much foreknowledge and experience as possible into test scenarios also need to track changing priorities against risk tolerances. Responsible teams, also subject to change, are required to remain vigilant and aware of the changing threat environment, including accounting for and monitoring evolving threat agents and triggers that could initiate a response. Hospitals are examples of proceduralized systems that require the establishment of a variety of standby plans, each of which can be invoked on demand.

If resilience is a response to a stressor, then organizational resilience must be a response that plans for recovery to be feasible. The process of engineering resilience into an

organization's systems and processes as a means of recovery assurance requires a systematic deployment of actions and decisions that contribute to recovery, as and when needed. Like an army at the ready, embedding resilience into organizational processes includes the assurance that activities, such as the following are performed consistently and competently:

- Analyzing the threat landscape according to the organization's unique context, from proximity to hazardous land features that precipitate natural disasters to unreliable data as input to critical decisions.
- Mapping out the organization's processes and systems that prioritize critical core processes and subsystems to differentiate them from supporting, noncritical systems.
- Determining where the organization's vulnerabilities are, such as targeted takeover bids.
- Estimating the probability of occurrence of the adverse event.
- Assessing and analyzing the impact to the organization and its customers or stakeholders.
- Determining and specifying the required target recovery capability.
- Planning for various recovery scenarios, based on the need for full or partial recovery.
- Providing assurance of the expected capability against required capability.
- Reporting on any expected changes in recovery potential.
- Maintaining readiness to achieve target levels of required capability including readiness to respond, training capabilities, job competencies, and materials and equipment availability.

Organizational Resilience through Management Systems Standards

On April 24, 2014, during the UN's deliberations on its own resilience capability, the High Level Committee on Management chair opened their meeting by "noting that the Organizational Resilience Management System (ORMS) was approved by the General Assembly as the emergency management framework for the organization." (UN, 2014, para. 1). They had determined the need for and the criticality of systematizing the process of becoming resilient so that, through testing, they can be resilient in the face of a calamitous event.

To become resilient, the organization's approach must be systematic, like the UN's. Achieving a required level of resilience that enables a successful recovery from an adverse event is dependent on fully comprehending the risks facing the organization. There's no point buying sandbags to ward off rising waters for a location in the desert.

Once risks are understood, they can be managed, and leadership can adopt a resilience framework, such as ISO 22301 or the UN's Organizational Resilience Management System. Frameworks, such as those provided by international consensus-based standards, provide a structured approach to achieving resilience that supports the discipline of assuring organizational ability, and subsequent capability, to survive adversity.

Systematic planning often leads to the recognition and adoption of resilience as an organizational priority, with that decision triggering the development of a business continuity plan. Engineering resilience into organizational systems is similar to the injection of any other nonfunctional requirement into a system's capability: the new capability—resilience—must

be conceived of, planned for, understood, resourced, designed, developed, documented, tested, and monitored. Confidence in its execution through verification and validation can assure the system's recovery. This systematic approach serves as a specification of the organization's required operation capability to recover.

The degree to which an unprepared organization, comprised of unprepared humans, will have the capability and capacity to react to stressors and adversity, and to ultimately recover, will depend on how much advanced preparation is invested into the task. Assessing this capacity is part of the process of making engineered systems and organizations resilient. Proactivity is a necessary step that organizational system must undertake to overcome humans' natural tendencies to resist, to procrastinate, and to negate the possibility that disasters can and do happen.

Conclusion

This chapter provides insights into the resilience of engineered and organizational systems. These domains contain both overlapping and unique resilient features. Each domain includes unique systems with necessary capabilities that face a variety of adversities at some point in time. These adversities can be due to internal, external, and/or environmental causes. Certain techniques are implementable to help improve system resilience. These techniques could be physical architectural, design principles, system attributes, fundamental objectives/means, or inherent system characteristics.

There are a few points to take away from this chapter that are reflected in Table 35.1. First, the main difference between engineered systems and organizational systems is that engineered systems are for the most part physical, while organizational systems are human intensive. This difference leads to several major differences in purpose and resilience:

TABLE 35.1 Comparisons of Domains With Respect to Resilience Aspects

Aspect	Engineered Systems	Organizational Systems
System type	Primarily physical systems: utilities, transportation, infrastructure, buildings.	Primarily human-intensive systems: enterprises, government. Generally more vulnerable than engineered systems.
Adversities	Natural: earthquakes, hurricanes. Human-made: terrorist attacks. Internal threats: reliability failures; software errors.	Bad actors; natural disasters.
Capability	Speed, range, power, etc.	Organizational goals, human resources, etc.
Time frame	Anticipation, withstanding, adaptation, gradual degradation, recovery.	Same as engineered systems.
Techniques	Physical and behavior architecture responses.	Human activity responses.
Patterns	Timeline patterns from anticipation to recovery; use of detection and adaptation techniques.	Vulnerability to physical adversities; same timelines as engineered systems; advantage of human cognition.

- Engineered systems will have intrinsically different goals. Engineered systems will have technical goals, while organizational systems will have organizational goals.
- While engineered systems will differ in their vulnerability, organizational systems will be physically more vulnerable than engineered systems.
- Organizational systems have one major advantage over engineered systems, namely, that organizational systems consist of human beings whose cognizance contributes to their resilience.
- If there is a common pattern to both engineered and organizational system resilience, it is the timeline pattern. All systems will have to transit through the same timeline from anticipation to recovery. Nevertheless, the physical differences between the two types of systems will lead to differing amounts of recovery time depending on the adversity.

Regardless of the type of system, the key to achieving resilience is the capability of that system to resist, withstand, and recover from whatever stressors it faces, at the time that they are faced. That achievement depends on mature processes.

Key Messages

1. All domains examined revealed similar patterns in maintaining capability, recovery from an adversity, timeline of interaction with the adversity, and techniques to achieve resilience.
2. Engineering system resilience is dependent on system architecture and the adaptability of that architecture.
3. Organizational system resilience is dependent on the dynamics of human interaction.

References

Alexander, C., Ishikawa, S., Silverstein, M., Jacobson, M., Fiksdahl, I., & Angel, S. (1977). *A pattern language: Towns, buildings, construction*. New York, NY: Oxford University Press.

BKCASE Editorial Board. (2016). *Systems engineering body of knowledge (SEBoK)*. Retrieved from https://www.sebokwiki.org/wiki/System_Resilience

Cameron, K. S., Dutton, J. E., & Quinn, R. E. (2003). An introduction to positive organizational scholarship. In K. S. Cameron, J. E. Dutton, & R. E. Quinn (Eds.), *Positive organizational scholarship* (pp. 3–13). San Francisco, CA: Berrett-Koehler.

Department of Homeland Security. (2018, 18 August). *Critical infrastructure sectors*. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors

Eyles, D. (2009, July 18). 1202 computer error almost aborted lunar landing. *MIT News*. Retrieved from http://njnnetwork.com/2009/07/1202-computer-error-almost-aborted-lunar-landing/

Fackler, M. (2017, November 19). Six years after Fukushima, robots finally find reactors' melted Uranium fuel. *The New York Times*. Retrieved from https://www.nytimes.com/2017/11/19/science/japan-fukushima-nuclear-meltdown-fuel.html

Federal Aviation Administration. (2015). *Bird strike requirements for transport category airplanes*. Retrieved from https://www.federalregister.gov/articles/2015/07/20/2015-17404/bird-strike-requirements-for-transport-category-airplanes

Greenpeace. (2019). *About Greenpeace*. Retrieved from https://www.greenpeace.org/usa/

Hargrove, M. B., Nelson, D. L., & Cooper, C. L. (2007). *Generating eustress by challenging employees: Helping people savor their work* (Vol. 42). Washington, DC: American Psychological Association.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

International Council on Systems Engineering. (2015). *Systems engineering handbook: A guide for system life cycle processes and activities*. Seattle, CA: Wiley.

International Standards Organization. (2012). *Societal security: Business continuity management systems—Requirements*. *ISO 22301*:Retrieved from www.iso.org

International Standards Organization. (2014). *Information technology: Process assessment—Guide to process related risk determination*. ISO/IEC NP/TR 33015. Retrieved from www.iso.org

Jackson, S., & Ferris, T. (2013). Resilience principles for engineered systems. *Systems Engineering*, *16*(2), 152–164. doi:10.1002/sys.21228

Jamshidi, M. (Ed.). (2009). *System of systems engineering: Innovations for the 21st century*. Hoboken, NJ: John Wiley.

Kahneman, D. (2011). *Thinking fast and slow*. New York, NY: Farrar, Straus and Giroux.

Luthans, F. (2002). Positive organizational behavior: Developing and managing psychological strengths. *Academy of Management Perspectives*, *16*(1). doi:10.5465/ame.2002.6640181

Luthans, F., Avolio, B. J., Avey, J. B., & Norman, S. M. (2007). Positive psychological capital: Measurement and relationship with performance and satisfaction. *Personnel Psychology*, *60*(3), 541–572. doi:10.1111/j.1744-6570.2007.00083.x

Madni, M. A., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. *Institute of Electrical and Electronics Engineers (IEEE) Systems Journal*, *3*(2), 181–191. doi:10.1109/JSYST.2009.2017397

Mendoça, D., & Wallace, W. (2006). Adaptive capacity: Electric power restoration in New York City following the 11 September 2001 attacks. In E. Hollnagel & E. Regaud (Eds.), *Second Resilience Engineering Symposium* (pp. 209–219). Juan-les-Pins, France: Mines Paris.

Pariès, J. (2011). Lessons from the Hudson. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathhall (Eds.), *Resilience engineering in practice: A guidebook* (pp. 9–27). Farnham, UK: Ashgate.

Resilience. (2018). *Oxford Dictionaries*. Retrieved from https://en.oxforddictionaries.com/definition/resilience

Rhue, L. (2019, January 3). Emotion-reading tech fails the racial bias test. PHYS.ORG. Retrieved from https://phys.org/news/2019-01-emotion-reading-tech-racial-bias.html

Sillitto, H., Dori, D., Griego, R. M., Jackson, S., Krob, D., Godfrey, P., . . . McKinney, D. (2017). Defining "system": A comprehensive approach. *INCOSE International Symposium*, *27*(1), 170–186. doi:10.1002/j.2334-5837.2017.00352.x

Ungar, M. (2018). Systemic resilience: Principles and processes for a science of change in contexts of adversity. *Ecology and Society*, *23*(4), 34. doi:10.5751/ES-10385-230434

United Nations. (2014). *Action on the UN system Organizational Resilience Management System*. Retrieved from https://www.unsystem.org/content/organizational-resilience-management-system-orms

US-Canada Task Force. (2004). *Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations*. Washington, DC, Ottawa, ON.

Van Rooj, B., & Fine, A. (2018). Toxic corporate culture: Assessing organizational processes of deviancy. *Administrative Sciences*, *8*(3), 23. doi:10.3390/admsci8030023

Willett, K. D. (2016, November). *Cybersecurity decision patterns as adaptive knowledge encoding in cybersecurity operations*. Poster presented at the 4th Annual SERC Doctoral Students Forum and 8th Annual SERC Sponsor Research Review, Washinton, DC. Retrieved from http://docplayer.net/156473866-Cybersecurity-decision-patterns-as-adaptive-knowledge-encoding.html

Wright, T. A. (2003). Positive organizational behavior: An idea whose time has truly come. *Journal of Organizational Behavior*, *24*(4), 437–442. doi:10.1002/job.197

Youssef-Morgan, C. M. (2004). *Resiliency development of organizations, leaders and employees: Multi-level theory building and individual-level, path-analytical empirical testing* (Doctoral dissertation). Retrieved from https://digitalcommons.unl.edu/dissertations/AAI3131572/