Research Paper

Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges

Payuna Uday and Karen Marais*

School of Aeronautics and Astronautics, Purdue University, West Lafayette, IN 47907

Received 20 October 2014; Revised 15 July 2015; Accepted 7 October 2015, after one or more revisions
Published online 23 November 2015 in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/sys.21325

ABSTRACT

Resilience is the ability of a system to react to and recover from disturbances with minimal effect on its dynamic stability. While resilience has been the focus of research in several fields, in the case of systems-of-systems (SoSs), addressing resilience is particularly interesting and challenging. As infrastructure SoSs, such as power, transportation, and communication networks, grow in complexity and interconnectivity, measuring and improving the resilience of these critical SoSs is vital in terms of safety and providing uninterrupted services. While the resilience of SoSs depends on the reliability of their constituent systems, traditional reliability and risk assessment approaches cannot adequately quantify their resilience. In this paper, we provide an evaluation of the various methods available and challenges associated with designing resilient SoSs by (1) indicating important differences between resilience and various related system attributes, (2) providing a critical assessment of the current reliability and risk techniques in addressing SoS resilience, and (3) discussing the application of recent multidisciplinary research that can guide the design of resilient SoS. Finally, we highlight key challenges in this design process and propose a series of research themes that can shape future research in this field. © 2015 Wiley Periodicals, Inc. Syst Eng 18: 491–510, 2015

Key words: reliability; resilience; risk; safety; design; review; system-of-systems

1. INTRODUCTION

Resilience is the ability of a system, process or organization to react to, survive, and recover from disruptions. But, due to the often expensive nature of resilience, maintaining or improving performance is frequently given priority, resulting in systems that are (partly) resilient to only a small set of disruptions. In addition, long-lasting systems, such as infrastructure networks (e.g., energy, transportation, communications), may be resilient to certain disruptions, but as time passes after the system is fielded, changes in the operating environment may make the networks less resilient to both old and new types of threats.

In particular, there is a pressing need to develop methods to model, assess, and manage resilience in *systems-of-systems* (SoSs). Examples of SoSs include the U.S. Air Transportation System (ATS) and tactical SoSs used by the military. Figure 1 shows an example of naval warfare operations. The mission comprises aircraft carriers, littoral combat ships (LCSs), unmanned surface vehicles (USVs), unmanned aerial vehicles (UAVs), and helicopters (MH-60). These systems work together to detect and neutralize enemy agents, such as ships, submarines, and mines. Each system

*Author to whom all correspondence should be addressed (e-mail: kmarais@purdue.edu).

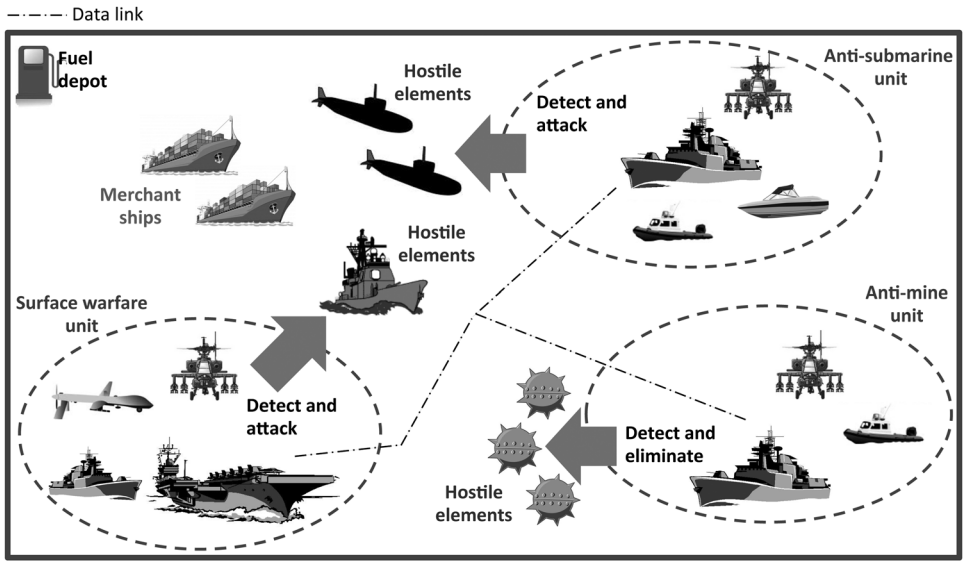

Figure 1. Illustrative naval warfare SoS.

performs one or more functions; collaborations between systems enable higher level capabilities.

As systems continue to grow in scale and complexity, several research efforts have focused on developing methods for engineering resilient systems. For example, *Engineered Resilient Systems* was identified as a strategic investment priority by the U.S. Department of Defense as part of its program objectives for 2013–2017 [DoD, 2011]. Also, the International Council on Systems Engineering (INCOSE) has a dedicated working group for Resilient Systems that shapes research on the use of systems engineering practices to achieve resilience [INCOSE, 2000]. The Resilience Alliance [2001] is another research organization that facilitates research in the scientific community with the specific aim of improving resilience in socioecological systems. The interest in resilience has led to significant developments in studies and models, but our review of the literature reveals that the research on SoS resilience is still in its nascent stages in terms of defining, measuring, and identifying methodologies to achieve resilience. In particular, we were unable to find any published papers that provide a focused review of designing and operating resilient SoSs.

From a design perspective, the questions that need to be answered to construct and operate resilient SoSs can be grouped into three key questions (see Fig. 2): (1) when is resilience needed or appropriate? (2) how can resilience be designed? and (3) how can resilience be maintained?

While the resilience of SoSs depends in part on the reliability of their constituent systems, traditional reliability and risk approaches do not provide adequate guidance on how to achieve or manage resilience. Given the diversity and often wide geographic distribution of SoS constituent systems, inclusion of backup redundant systems for an SoS is usually impractical and costly. In addition, high levels of interdependency between the systems imply increased risks of failures cascading throughout the SoS. At the same time, the features (such as heterogeneity) giving rise to these hurdles also offer the opportunity to improve the resilience of the overarching system through unconventional means.

To illustrate the above observations, consider, for example, a critical infrastructure SoS, such as the national transportation network. At present, research, development, and operation for each sector of the U.S. National Transportation System (NTS) is generally conducted independently, with little consideration of multimodal impacts, societal and cultural influences, and network interactions [DeLaurentis et al., 2007]. Typically, resilience is addressed at a modal level: the robustness of a particular transportation network is addressed independently of other modes of transportation. Designers assume that the remaining transportation network is available when one part of one mode fails. For example, when a subway line is suddenly unavailable due to some failure or threat, the unmet demand spills onto the road network [comprising buses and automobiles). Individual organizations that cover several modes, such as, for example, the Massachusetts Bay Transportation Authority (MBTA), do plan for such disruptions, but there is less coordination between organizations. Thus, for example, if Logan Airport closes due to weather, AMTRAK rail service cannot meet all the spillover demand in a reasonable time. There may also be interdependencies between modes. For example, in the aftermath of Hurricane Sandy in 2012, while the airports in New York were able to resume operations relatively quickly, road and rail services took longer to provide adequate services. As a result, airline employees were unable to get to work at the airports and airlines had to fly in technology specialists and customer service agents from Atlanta to maintain their specific airport operations [Brown and Drew, 2012]. In contrast, in the weeks after an earthquake in southern California [1994], although Los Angeles road networks were critically impacted, rail services were resumed relatively quickly. In particular, the existence of a separate freight rail system in the city allowed officials to augment the commuter rail services by using the cargo line during this period [Giuliano and Golob, 1998].

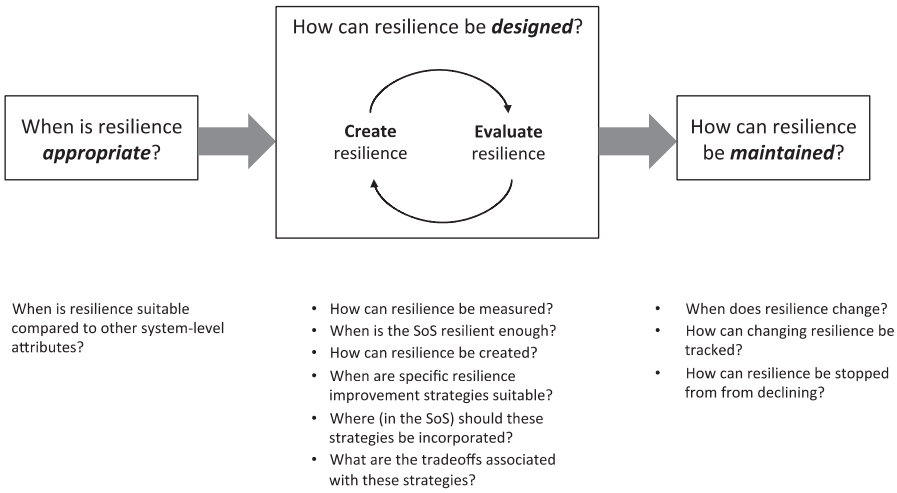

Figure 2. Simplified process of designing and maintaining SoS resilience.

The answers to the questions in Figure 2 lie in a wide range of fields—reflecting the diverse nature of SoSs. Here, we review and integrate the progress on answering the first two questions. Section 2 provides a brief overview of SoSs. Section 3 addresses the first question through a discussion of resilience and related system attributes, such as reliability, robustness, and flexibility, in system design. Section 4 addresses the second question through a review of tools and existing research that can be applied to designing resilience in SoSs. Section 5 highlights key challenges in designing SoS resilience and presents a series of research needs that can provide direction to further work. Finally, Section 6 concludes the paper.

2. DEFINITION OF SoSs

In this section, we provide a brief overview of SoSs in the context of resilience. The interested reader is referred to Crossley [2004], Abbott [2006], Dahmann and Baldwin [2008], DoD [2008], Jamshidi [2008], Gorod and Sauser [2008], Luzeaux [2011], Barot et al. [2013], and TTCP [2014] for a broader discussion of SoSs.

The term system-of-systems is used to denote networks that are formed from the integration of independently operating complex systems that interact with one another to provide an overall capability, which cannot be achieved by the individual systems alone [White, 2006; DeLaurentis, Crossley, and Mane, 2011]. These metasystems are characterized by the operational and managerial independence of the constituent systems, the evolutionary nature and emergent behavior of the larger SoS, and the geographic distribution of the subsystems [Maier, 1998].

Typically, the systems in an SoS are individually acquired and integrated into the larger structure. Also, the design and development of these systems are generally independent of each other. For instance, although almost every military system is operated as part of an SoSs, most of these systems are optimized sequentially (i.e., the new system must fit well in the existing context), rather than holistically (i.e., how should new, existing, and possible future systems be combined to maximize desired SoS attributes [e.g., Mane, Crossley, and Nusawardhana, 2007]). In unfortunate cases, this insular systems development practice can lead to failures and undesired emergent behavior of the overall SoS, as shown in the earlier Hurricane Sandy example.

Interfaces are critical areas of concern for SoS development. Apart from impacting the seamless integration of different systems, a direct consequence of interfaces is the creation of interdependencies between the constituent systems. Furthermore, as SoSs themselves evolve into even more complex networks, the links between SoSs (e.g., between communications and energy networks) are gaining increased attention [Thissen and Herder, 2009; Zio and Ferrario, 2013].

From an organizational standpoint, the wide range of owners, managers, and stakeholders of the systems constituting the SoS increases uncertainty and complexity. For example, the global ATS architecture is driven by the goals of regional and global economies. It comprises multiple stakeholders such as regulatory authorities, aircraft manufacturers, air traffic control, airlines, airports, and the flying public. Each one is concerned with maximizing its own objectives. Air traffic control is concerned with flight safety and maximizing throughput, the airlines are concerned with maximizing profits, airports are concerned with conserving costs while providing acceptable service, and the passengers are interested in getting the best value (low fares, minimum delay, and good customer service) from the ATS.

Finally, SoSs are typically never fully formed or complete [Abbott, 2006]. Their development is evolutionary and adaptive as components, functions, and goals, are added, removed, and modified over time. For example, while NextGen aims at transforming (through upgrades and new technology) the airspace to achieve better operational and environmental efficiency, several critical legacy systems will still be part of the overall system. This implies that key SoS characteristics, such as performance and resilience, must be constantly reviewed as the systems and their operating environments change with time.

Based on the type of central control and organizational hierarchy of the constituent systems, SoSs can be classified as directed, virtual, collaborative, or acknowledged [Maier, 1998; Dahmann and Baldwin, 2008]. Directed SoSs (e.g., Integrated Air Defense) are centrally managed to fulfill specific purposes. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose. On the other hand, virtual SoSs (e.g., the World Wide Web) lack a central management authority and a centrally agreed-upon purpose for the SoS. Large-scale behavior emerges, and may be desirable, but this type of SoS must rely on relatively invisible mechanisms to maintain it. In collaborative SoSs (e.g., the Internet), the component systems interact more or less voluntarily to fulfill agreed upon central purposes. Finally, acknowledged SoSs (e.g., Ballistic Missile Defense System) have recognized objectives, a designated manager, and resources. However, the constituent systems retain their independent ownership, objectives, funding, development, and sustainment approaches. This difference in central control architecture impacts the interfaces between the constituent systems as well as the interactions experienced at the system boundaries, resulting in implications for the design and optimization of key attributes such as resilience [Barot et al., 2013].

3. WHAT IS RESILIENCE AND WHEN IS IT APPROPRIATE?

Resilience is one member of an expanding family of system-level attributes. This section reviews the attributes that are closely related to resilience: robustness, survivability, reliability, flexibility, pliability, agility, and safety. We present the fundamental idea behind each system attribute and compare it with resilience. We give illustrative examples to show that making these distinctions has value in that it adds to the richness of overall SoS design and development.

There are many different ways to distinguish between these system-level attributes, or "ilities." For example, Chalupnik, Wynn, and Clarkson [2013] define these attributes based on the design changes required (or not) for a product or process to respond to off-nominal conditions. Here, we take a system requirements perspective and apply it to different levels in the SoS. This approach allows us to focus on the implications of each attribute for engineering decision-making. All the characteristics discussed here deal with the idea of a system having to cope with or adjust to some kind of change, after it has been fielded. This change can be either: *external*, for instance, disruptions due to operating environment threats, changing policies, and global economics, or *internal*, for instance, component and link failures. In some cases, the differences between the definitions are explicit, while in others the differences are subtler. We classify the attributes on the basis of the impact the change has on the system requirements, as shown in Figure 3. In some situations, systems are expected to meet their original requirements in the face of a disruption. Qualities that attempt to satisfy these *constant* system requirements during the disturbance include resilience, robustness, reliability, and survivability. In other cases, the system goals and requirements themselves vary in order to maintain

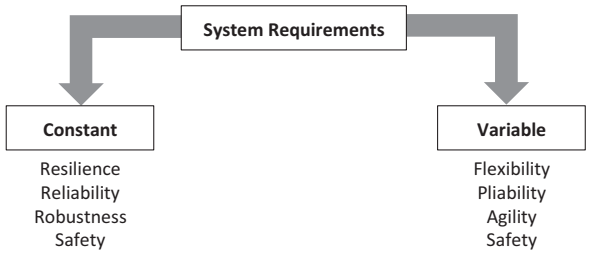

Figure 3. Classification of attributes based on system requirements.

functionality during and after perturbations. Attributes that allow a system to satisfy new or variable requirements include flexibility, agility, and pliability. We do not consider these attributes further here, the interested reader is referred to Saleh, Mark, and Jordan [2009] and Ryan, Jacques, and Colombi [2013] for reviews of flexibility; Mekdeci et al. [2012] discuss pliability; and Dove [2001] and Albert and Hayes [2003] discuss agility.

3.1. Defining Resilience

In the engineering domain, several definitions have been put forward to describe resilience. For instance, in Hollnagel, Woods, and Leveson [2006], an early collection of work on resilience, resilience is defined as the "ability of a system or organization to react to and recover from disturbances at an early stage with minimal effect on its dynamic stability." See also [INCOSE, 2000], Laprie [2008], Jackson [2010], and Ruault, Vanderhaegen, and Luzeaux [2012] for similar definitions.

Resilience is usually represented as a combination of survivability and recoverability, as shown in Figure 4.[1] This notional representation is widely used in the literature to depict the fundamental ideas behind resilience (e.g., Tierney and Bruneau [2007], Castet and Saleh [2012], and Ayyub [2014]). Resilience, in other words, is not only concerned with reducing the likelihood of failure. It also stresses the need to recover from unexpected disturbances in the operating environment. Essentially, resilience implies the ability of a system to "bounce back" and hence, is a function of several system properties, including component reliability, reconfigurability of the architecture, and diversity of subsystems and components. Resilience can be divided into two categories [Rose, 2007; Whitson and Ramirez-Marquez, 2009]: (1) "static resilience" is related to the "ability of an entity or a system to maintain function," or to survive, when disrupted; while (2)

[1]Several definitions for resilience have been proposed in the literature. Some authors view resilience as a superset of two attributes: surviving the disruption and then recovering from it. Others consider survivability to be the overarching attribute. For example, according to Richards et al. [2009], survivability (a property that has emerged from the development of military systems and describes the ability of systems to minimize the impact of finite-duration disturbances on value delivery) consists of three aspects: Type I survivability deals with reducing the likelihood or magnitude of a disturbance; Type II minimizes performance (value) loss in the immediate aftermath of a disturbance; and finally Type III survivability enables the recovery of value delivery in a defined period of time.

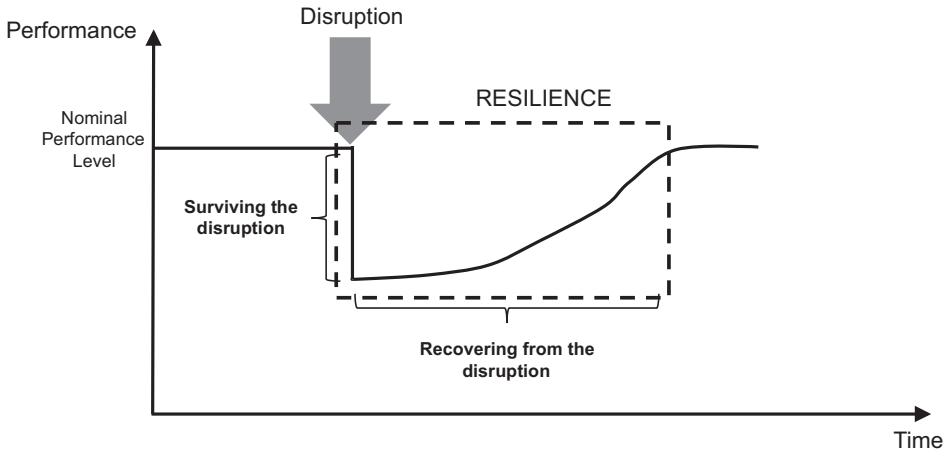

Figure 4. Notional depiction of resilience following a disruption ("resilience curve").

"dynamic resilience" deals with recovery of the system after a shock. We agree with this perspective wherein resilience is viewed as a combination of survivability and recoverability, with an emphasis on the ability of systems to rebound after a disruption.

Resilience is highly context dependent—it depends on the structure (architecture) of the system (which could be an SoS, an organization, a network, etc.), its operational environment, and the disruptive event. For example:

- Different systems are resilient to different disruptions. For instance, O'Hare International Airport (ORD) is reasonably well equipped to handle snowstorms, but 3 inches of snow in southern United States caused Atlanta Hartsfield International Airport (ATL) to shut down in early 2014 [CBS, 2014].
- A system could be resilient to one type of disruption but not to another type. For example, an airport may be resilient to thunderstorms but vulnerable to cyberattacks on its security systems.

Figure 5 highlights a couple of extreme cases of variation in possible resilience curves. In the aftermath of a disruption, the performance drop does not necessarily happen steeply and suddenly. During the time between a disruptive event and the full impact, performance usually starts to deteriorate and a more *gradual decline* may be observed. For example, when access to critical automotive components was blocked during the 2002 West Coast port lockout, instead of halting production immediately, logistical constraints meant that it took New United Motor Manufacturing Inc. (NUMMI) four days to stop all assembly activities [Sheffi and Rice, 2005]. Similarly, there are several different ways an SoS can recover from disruptions. Recovery measures can include an *increase in performance* for some time after a recovery to make up for lost capability. For instance, NUMMI used airfreight to get parts to the plants during the port lockout and then made up for closures by running at higher-than-normal utilization to make up for lost production. Conversely, in other cases, despite adequate recovery, disruptions can have *long-term impacts* on SoSs. For example, the network of small-scale shoe factories in Kobe, Japan, lost 90% of its business in the wake of the 1995 earthquake as buyers shifted to other Asian factories, and most buyers never came back [Sheffi and Rice, 2005]. Another example of long-term impact is the increased costs of computer hard drives, through 2013, after the 2011 floods in Thailand (second largest computer hard drive supplier in the world) [WEC, 2014].

Next, we contrast the related system-level attributes with resilience, and discuss when each attribute is appropriate (perhaps as part of a set of attributes).

3.2. Reliability

Formally, *reliability* in the engineering domain is the ability of a system and its components to perform required functions under stated conditions for a specified period of time (e.g., Modarres, Kaminsky, and Krivtsov [1999]; Rausand and Høyland [2004]; Madni and Jackson [2009]). Reliability is now a mature topic in the literature and a variety of methods exist that enable the design of reliable components and systems. However, as systems become more complex and interdependent, understanding reliability in the context of the resulting SoSs is not necessarily straightforward or trivial. To illustrate the nuances of reliability and resilience implications from an SoS perspective, we compare these attributes at different levels of the ATS, as shown in Table I. The SoS builds upward from lower level components (e.g., fuel selector valves on aircraft), to systems (e.g., aircraft), and finally to the highest level SoS (the ATS).

At the component level, measures such as mean time to failure (MTTF, for nonrepairable components) and mean time between failure (MTBF, for repairable components), describe in part the reliability of elements. At this level, reliability is an important attribute that drives component design and selection. Components can be designed to minimize the likelihood of a failure, for example by selecting better quality parts, but once a failure occurs, by definition they do not have the inherent ability to survive and recover from the failure. A component can be reliable, but on its own, it cannot be resilient (since it cannot recover on its own), and no additional design guidance can be gained by considering resilience.

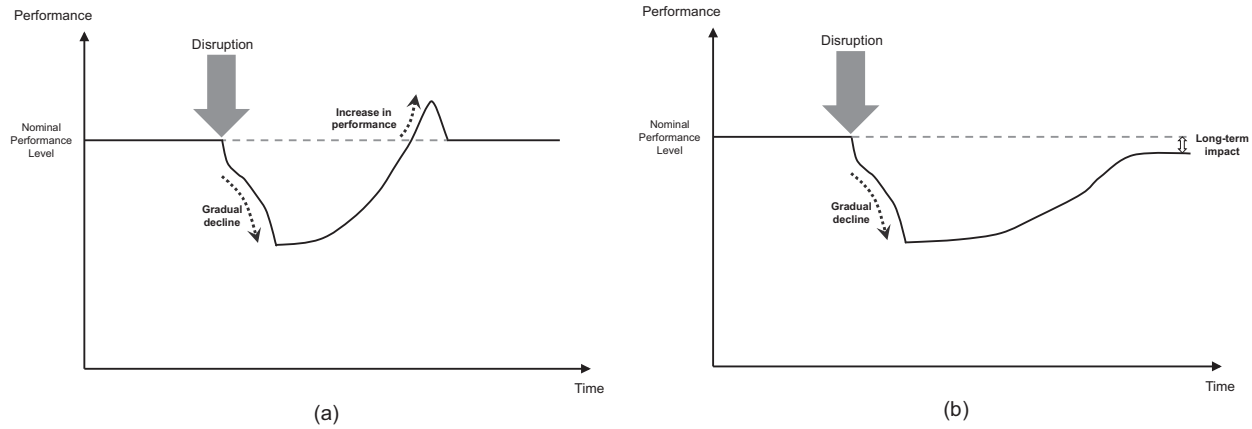

Figure 5. Variability in possible resilience curves: (a) recovery measures can include a temporary increase in performance and (b) disruptions can result in long-term impacts on performance.

Table I. Reliability and Resilience Considerations at Different Levels of SoS Hierarchy

SoS Element	Example	Comparison between Reliability and Resilience Implications
Component	Fuel selector valve	Reliability and resilience are functionally equivalent. Classic reliability techniques are applicable and useful.
System (simple)	Fuel pump	
System (complex)	Aircraft	The distinction between reliability and resilience is one of degree. Designers must determine when reliability or resilience is more appropriate. Classic reliability techniques are applicable in specific cases of reliability management; such as the use of FMECA in developing suitable aircraft maintenance plans.
SoS	Air Transportation System or ATS	Reliability and resilience are distinctly different. The definition of SoS reliability is highly context-dependent. Classic reliability techniques based on component reliability must be augmented by additional tools (e.g., robust scheduling of airlines) when managing reliability.

The same interpretation can often be applied to simple systems. A fuel pump is reliable if it pumps fuel at the specified rate when required to, and, if it does not pump fuel when not required to. We can for example define an MTBFs for the pump—though this measure must be defined in the context of some set of possible failure levels (e.g., the pump only provides 95% of the required pressure, vs. the pump fails completely). The fuel pump's reliability is a function of its components' reliability, as well as its overall design (e.g., use of redundancy). A fuel pump with backup components is designed to be reliable despite failures of its components. As with a component, considering resilience does not provide additional design guidance.

As we consider more complex systems, the context aspect of reliability becomes more important, and the statistical measures become harder to define and interpret. For example, MTBF depends on what level of failure is deemed significant at the aircraft level. So, in the case of an aircraft, we might say it is 80% reliable if it is able to conduct a successful flight 80% of the times it is called upon to do so, given nominal operating conditions. An aircraft that must frequently cut missions short or operate at a reduced level due to failures in nominal operating conditions is not reliable. Reliability engineering techniques can be used to identify the sources of this unreliability.

While aircraft engines are designed to be highly reliable, aircraft are also designed to be *resilient* to an engine failure: when an engine fails, the remaining engine(s) compensate for the loss. The engine reliability springs from design, component selection, and a tightly controlled maintenance program that work together to minimize the likelihood of component failure. The aircraft's resilience to engine failure springs from redundant design (the remaining engines provide sufficient thrust to compensate for the loss), protection (the engine cowling is designed to contain any failures, and the engine mountings are designed to fail and release the engine if it presents an unbalanced load), and training (the pilot is trained to shut down a malfunctioning engine and use the aircraft control surfaces to compensate for asymmetric thrust).

Finally, at the SoS level, reliability and resilience are distinct and highly context-dependent. At this level, reliability is typically some function of the performance of the overall SoS. For instance, we would say that the air transportation network is reliable if some majority of flights arrive and depart as scheduled under some defined set of nominal weather conditions. This reliability is primarily driven by reliable systems (aircraft) and by robust scheduling. On the other hand, the system is *resilient* if it can continue to deliver passengers to their destination despite rare or unexpected disruptions. The ATS is not highly resilient—a large blizzard in one region can

disrupt flights around the country for several days. In contrast, some public transportation systems are resilient: when a subway line is unavailable, passengers are transported using buses.

3.3. Robustness

The terms resilience and *robustness* are often used interchangeably; however, there is an important difference between these concepts. Robustness can be thought of as the property of a system that allows it to satisfy a fixed set of requirements, despite changes in the environment or within the system [Saleh et al., 2009]. While the definition of resilience involves a similar idea, the distinction between the two attributes is that while no performance loss is allowed in the case of robustness, a resilient system may permit a (sometimes temporary) performance loss in "bouncing back" from the adverse event [Haimes, 2009]. Robust systems are expected to satisfy the original performance requirements during a disruption, which may be difficult or costly. Therefore, robust responses are appropriate for a small range of disturbances—those that occur frequently or that can be handled robustly in a cost-efficient manner. Less frequent disturbances, or those that are expensive to respond to without a performance loss, are better responded to in a resilient manner. For example, passenger aircraft are expected to encounter rain and thunderstorms quite frequently. They are therefore designed to be robust to rain, and to fly with enough fuel to be routed around (un)expected thunderstorms encountered en route. In contrast, severe crosswinds occur less often, and constructing and operating passenger aircraft capable of landing in severe crosswinds is costly. A resilient response is therefore more appropriate. When severe crosswinds occur, aircraft are diverted to the nearest suitable airport for landing. The passengers and crew are safe, but not at their intended destination, thus in this case the response is resilient, not robust.

3.4. Safety

The difference between resilience and safety is quite distinct. Safety refers to the objective of ensuring accident prevention through actions on multiple safety levers, such as technical, organizational, or regulatory [Leveson, 1995, 2012; Saleh, Marais, and Favoró, 2014]. This attribute values human life (or property loss) over other performance traits. Specifically, with respect to resilience, safety can be thought of as the aspect of survivability that is related to minimizing loss of life (or property). In some cases, both these attributes go hand-in-hand. For instance, in the event of a disruption to a transportation system (e.g., a hostile attack on an airport) designers need to plan for both safe (ensuring safety of travelers and employees) and resilient (reduce subsequent delays that occur due to airport closure and redirection of flights to other airports) operations of the SoS. In other cases, such as financial markets and global economies, the emphasis is on performance recovery (e.g.: minimizing fall in stock prices due to shocks to the system). In this case, loss of human life (safety) is not a major concern, rather, the concern is safeguarding profits. The above transportation example highlights the role of safety when the system needs to satisfy the same requirements it was designed for (provide transportation services with minimum delay). Safety must also be maintained when other requirements change (though the level of acceptable safety may change). For example, if an aircraft is retrofitted for use as a crop duster, the design must ensure that the pilot is not exposed to the crop dusting chemicals. Thus the retrofitted aircraft must maintain the safe air environment for the pilot.

Safety-critical systems are systems whose "failure might endanger human life, lead to substantial economic loss, or cause extensive environmental damage" [Knight, 2002]. For instance, the flight management system (FMS) on aircraft is a safety-critical system as it provides the crew with centralized control for the aircraft navigation sensors, computer-based flight planning, fuel management, radio navigation management, and geographical situation information. Many SoS include safety-critical systems at various levels. For example, in addition to the FMS on board an aircraft, the air traffic control system is another safety-critical system. Because these systems' failure can have such negative impacts, there is an entire field of research and practice devoted to ensuring their safety (see, e.g., Bowen and Stavridou [1993] and Storey [1996]).

To summarize, reliability is appropriate when high frequency–low impact disruptions (e.g., rain showers) occur and the SoS (e.g., ATS) is expected to maintain functionality without any loss in performance. Robustness is suitable when high (or medium) frequency–moderate impact events (e.g., thunderstorms) occur and the SoS is expected to maintain functionality without any loss in performance (e.g., route aircraft around the thunderstorm). Finally, resilience is appropriate when low frequency–high impact disruptions (e.g., blizzards) occur and the SoS is expected to survive and recover from the adverse event (e.g., divert aircraft to other airports). Note that any real system will usually require a combination of all three attributes (in addition to other system-level attributes like cost and performance), and that the appropriateness of each attribute is to a large extent dependent on stakeholder preferences (e.g., how often is too often for a particular type of failure?). Also, a given disruption may be treated with a combination of responses, similar to the idea of defense-in-depth in safety.

4. DESIGN APPROACHES

Key questions related to designing SoS resilience are shown in Figure 2. We now review existing approaches in the literature that can help answer the above questions. First, we discuss whether and how existing reliability and risk assessment techniques can be leveraged to address SoS resilience. Next we consider "newer," more multidisciplinary approaches that can be applied to achieving SoS resilience. We provide several tables to summarize the applicability of the tools in addressing the questions in Figure 2. While this section describes a broad range of methods and tools that can be used to address design considerations, Section 5 takes an explicit top–down approach in discussing design challenges and directions for future research.

4.1. Risk-Informed Design

Reliability engineering and risk assessment both ask versions of the following four questions [cf., Kaplan and Garrick, 1981]: (1) what can go wrong? (2) how likely is it? (3) what are the consequences? and (4) what can be done about it? Reliability engineering typically focuses on the ability to continue providing some predefined functionality despite performance failures, and on quantifying reliability at various levels in the system. Risk assessment considers a slightly different problem, that of operating without causing loss of life or property. Thus, in risk assessment, the analysis typically begins by attempting to identify all the ways that the system could fail. For example, in air transportation, risks include midair collision, or engine failure. Once these risks have been identified, various approaches can be used to characterize the risks. Here we briefly review some of the techniques used in reliability engineering and risk assessment, and then focus on their application to designing SoS resilience. For more depth on the techniques, the reader is referred to the many excellent texts on reliability engineering and risk assessment (e.g., Rausand and Høyland [2004]).

Hazard identification is one of the hardest parts of risk analysis, because it is not a purely analytical process. Instead it requires a combination of imagination and technical skill. Many approaches to hazard identification have been proposed; most are essentially versions of checklists, which provide the analyst with ideas on what might go wrong [Vaidhyanathan and Venkatasubramianian, 1995; Dunjo et al., 2010]. Hazard identification is difficult in complex systems because the hazards may be largely unknown. There have been attempts to expand the range of hazards to include unknowns (e.g., Paltrinieri et al. [2011]) and several tools have been developed for robust risk analysis to deal with uncertainties [e.g., Ben-Haim [2012] and Cox [2012]). While SoS specific hazard analysis tools have not been developed to date, current techniques can be applied. For example, Robinson [1995] provides an overview of applying HAZOP analysis to electrical power grids and transport systems; Mahnken [2001] describes the use of case studies to identify latent design deficiencies—for instance, best practices from the hazard identification process in the chemical industry can be used to discover flaws in electrical power grids.

Failure modes, effects, (and criticality) analysis (FMEA/FMECA) traditionally considers the impact of component failures on system-level risk. An FMECA analysis begins by identifying the various failure modes of a component (e.g., valve fails open, valve fails shut), and then determines its effects (e.g., coolant not provided), and how critical the failure is to the system (e.g., runaway reaction). FMECAs can be similarly used to identify potential failure modes and to investigate their impact on the overall SoS functionality. Here, each failure is considered individually and independently from other failures, and hence, these techniques will be most helpful for isolated failures in an SoS. For instance, in the air transportation network, FMECA can be used to assess the impact of individual airport failure modes (e.g., airport closed due to terror alert, or airport closed due to weather) on the overall SoS's capabilities, which in turn could be used to investigate and institute better equipment and procedures at critical airports.

A *fault tree* is a logic diagram that indicates how a system-level failure can be generated by component failures. This analysis begins with an undesirable end state (failure) and then works backward (deductively) to find which combinations of component failures can result in the end state. An *event tree*, on the other hand, is a logic diagram that allows designers to systematically study the propagation of a basic initiating event to its potential consequences. Event trees are almost the reverse of fault trees in that they work forward (inductively) from an initiating event and develop a time-sequence of events to determine which, if any, undesirable end states can be reached from the initiating event [Rasmussen, 1975]. Although their application to (and, in particular, quantification) complex systems is challenging (see Siu [1994]), fault and event trees can be used in SoS resilience analysis to document how system failures can combine to decrease SoS performance (e.g., Fleming et al. [2013]).

Because SoSs are particularly susceptible to common cause failures and partial failures, we believe that fault and event trees do not serve well to assess probabilities of failures. Similarly, other tools for quantifying failure probabilities, such as Bayesian-based statistics [Clemen and Winkler, 1999], whether based on system or component-level data, are also harder to apply to complex systems and SoS involving a combination of hardware, software, and people [Aven, 2013a]. Here, as in hazard identification, new or complex systems are especially challenging. For example, over its lifetime, assessments of Space Shuttle reliability ranged from 1 in 100 to 1 in 100,000 [Feynman, 1986]. When systems must operate in a wide range of, or poorly understood, environments, risk quantification becomes even more difficult. For example, because the risk of earthquakes in the U.S. Northeast was underestimated in the 1970s, nuclear power plants in the region actually have the highest risk of seismic damage [Dedman, 2011].

State-based techniques such as Markov chains and Petri nets consider risk by defining sets of safe and unsafe states. Then safety is maintained by ensuring that the system (or SoS) never reaches the unsafe states. They can also be used to show the progression of a system from one state to another. Markov chains are constructed by defining states and the transitions, which may be stochastic or deterministic, between them. Mane, DeLaurentis, and Frazho [2011] show how development interdependencies and delay propagation in SoSs can be modeled using Markov chains—a similar approach can be applied to assess propagation of failure and recovery in operational SoS. While Markov chains are quite intuitive, and there is a well-established body of theory on them, they are susceptible to state explosion, making them harder to apply to SoS.

Petri nets are also relatively simple and provide a graphical illustration of how a process occurs [Leveson and Stolzy, 1987]. They are constructed by combining three elements: places (the system states), transitions, and directed arcs, which relate places and transitions. The current state of the system is indicated by a token. They are widely used in computer and automatic control research, but can also be applied

to systems and SoS involving a variety of electronic, mechanical, and human aspects [Basnyat et al., 2007; Landegren, Johansson, and Samuelsson, 2014]. Like Markov chains, Petri nets tend to grow rapidly and become difficult to understand as the scale of the system increases.

Recent research efforts have attempted to adapt some "traditional" reliability engineering methods, such as *Bayesian belief networks (BBN)* and component importance measures, to networks of complex systems. BBNs are directed acyclic graphs used to illustrate the relationships between system failures and their causes or contributing factors. BBNs are considered to perform better than fault trees at reliability analyses since they are not limited to binary events and can handle partial failures. For example, Weber and Jouffe [2006] formalize a method using Dynamic Bayesian Networks to model the reliability of manufacturing processes. Their focus on the flows between systems highlights key dependencies and common failure modes. This Bayesian approach can potentially be applied to the design of interdependencies in SoSs.

Component-failure-based reliability and risk techniques typically suggest using higher reliability components or redundancy to improve system-level reliability. While some SoS systems can be made more reliable (e.g., more reliable aircraft), the extent of possible improvement is often limited (e.g., we can provide snow-clearing at an airport, but during a blizzard the airport will have to shut down for safety reasons). Also, given the heterogeneity and, often wide geographic distribution, of the constituent systems, redundant systems in an SoS are impractical and costly. Using redundancy alone runs the risk of overlooking other, more optimal, resilience improvement measures. Section 4.2 highlights some alternative techniques to creating resilience in SoSs.

Some recent research has acknowledged the limitations of the direct application of existing reliability techniques and offered ways to expand these methods for the useful analysis of SoS resilience [Johansson, Hassel, and Zio, 2013; Zio and Ferrario, 2013]. For example, Zio and Ferrario [2013] apply an extension of existing reliability analysis using Monte-Carlo simulations to assess the seismic risk for a nuclear power plant embedded in the power, water, and transportation networks that support its operation.

In summary, reliability and risk-based approaches to resilience in SoS do have application, but their use can also lead to incorrect assessments of resilience (see Table II). Most reliability and risk assessment techniques assume that a system design exists and that weaknesses must be identified, or that safety must be proven. These techniques therefore can lead to a reactive design philosophy, where deficiencies are "fixed." For example, if an FMEA identifies a failure-critical component, it is replaced with a more reliable component, rather than a new design that does not need the component at all. Park et al. [2013] suggest that the lack of progress on resilience engineering in SoS may be "partly because quantitative design approaches consistent with principles of resilience remain elusive, and partly because analytic approaches to resilience in engineering have become conflated with existing approaches to analysis of risk." Given the limitations of traditional reliability and risk techniques in addressing resilience, Section 4.2 describes recent efforts that have focused on new ways to tackle this issue.

4.2. SoS Design Approaches

Other than suggesting reduction of failure rates (e.g., through better components, or more frequent maintenance), reliability and risk analysis methods do not provide guidance on other types of mitigation strategies. As a result, in many cases, resilience is achieved through a trial-and-error process rather than through detailed SoS-level analysis. Such ad hoc approaches could result in achieving too much (unused) resilience in one part of the network, and too little resilience in another. Also, such approaches could make an SoS highly resilient to certain kinds of disruptions but less resilient to other threats. To design and test for resilience across a broad range of conditions requires understanding at a much finer grained level how the systems will be used, the environments in which they will be used, and the threats they can expect to encounter. This view echoes that of researchers who raise the need for a different perspective of resilience in the context of SoSs [Sheard and Mostashari, 2008; Madni and Jackson, 2009; Neches and Madni, 2012; Goerger, Madni, and Eslinger, 2014].

This section draws on a variety of "newer" research efforts to provide a sense of how SoS resilience can be evaluated and created. We broadly categorize these studies into a set of three design approaches: principles, tools and models, and metrics (see Table III), and highlight how useful they are in providing specific design guidance.

4.2.1. Design Principles

A design principle, or heuristic, is an abstraction of experience that can be used to effectively guide engineering design [cf. Maier and Rechtin, 2000]. For example, in systems engineering, one design principle is to minimize coupling, which can, for example, be accomplished by increasing the modularity of the design. Here, we present a set of nine design principles to guide the design of SoS-level resilience. Although this list is not intended to be exhaustive, we believe many resilience improvement strategies derive from these principles. While several of the principles outlined below are rooted in systems engineering (see Jackson and Ferris [2013] for a recent compilation), the relevant heuristics have been adopted here for SoS design guidance.[2] The list is organized by theme as follows: the first four principles represent system-level design features; the next two represent network-level design features; the following three are based on human involvement (observation, decision-making, communication); and the last principle suggests a combination of the previous nine (see also Table IV).

1. **Physical redundancy.** Employ redundant hardware (backups) to provide functionality when primary systems in the SoS fail [Jackson and Ferris, 2013]. For example, in the case of a public transportation network, one way to create physical redundancy is by maintaining extra buses at city depots. In the event of a disruption (e.g., traffic jam or an accident) these spare buses could be used on the original routes in place of the failed

[2] We do not explicitly consider cyber resilience here. Though cyber resilience is increasingly becoming an integral concern for these SoSs, principles that achieve this resilience require a different, more software-centric approach

Table II. SoS Resilience Design Guidance Provided by Traditional Reliability and Risk Assessment Techniques

Reliability and Risk Assessment Method	Design Questions Addressed by Method (Wholly or Partially)	Limitations with respect to SoS Design
FMEA/FMECA	• When are specific resilience improvement strategies suitable?	• Focus is on single component failures and hence cannot capture cascading failures due to interdependencies prevalent in SoSs • Typically deal with hardware component failures and cannot capture crucial software and organizational interdependencies inherent in SoSs
Fault and event trees	• How can resilience be created? • When are specific resilience improvement strategies suitable?	• Deal with binary failures—cannot handle partial failures as are often times seen in SoSs • Can result in large and complicated documentation—making them less likely to be useful for design guidance. • Requires near-complete identification of hazards (disruptions). • Does not provide specific insight on design improvement.
Bayesian belief networks	• Where (in the SoS) should resilience improvement strategies be incorporated?	• Consider binary failures—cannot handle partial failures.
Component importance measures	• Where (in the SoS) should resilience improvement strategies be incorporated?	Consider binary failures—cannot handle partial failures. • Assume system architecture is fixed—not applicable in case of SoSs where network is constantly evolving.

Table III. Design Guidance Provided by SoS-Focused Design Approaches

Design Approaches		Design Questions Addressed by Method (Wholly or Partially)
Create Resilience	Design principles	• How can resilience be created? • When are specific resilience improvement strategies suitable? • What are the trade-offs associated with these strategies?
Evaluate Resilience	Simulation tools and models	• How can resilience be created? • When are specific resilience improvement strategies suitable? • Where (in the SoS) should these strategies be incorporated?
	Metrics and frameworks	• How can resilience be measured? • When is the SoS resilient enough?

primary buses, or depending on the situation, they could even be used to augment service by running different routes.

2. **Stand-in/Functional redundancy.** Leverage heterogeneity in the SoS to provide redundancy without adding additional systems [Zhang and Lin, 2010; Jackson and Ferris, 2013; Uday and Marais, 2013]. For example, loss of the LCS (see Fig. 1) can be compensated for by using better equipped helicopters (carrying more weapons and larger fuel tanks) and improved USVs (sophisticated surface imaging and radar capabilities). The enhanced features on the helicopters and surface vehicles allow these systems to be re-tasked to perform new functions in the event of an LCS incapacitation.
3. **System-level Properties.** Improve system-level properties, such as flexibility, robustness, and adaptability, of the constituent systems to achieve SoS-level resilience. For example, flood protection (***robust design***) at entrances to subway stations in large cities can prevent flooding during extreme disruptions such as hurricanes, thereby preventing catastrophic repercussions to the rest of the transportation infrastructure [Higgins, 2012]. Another way to improve resilience at the regional transportation level is by enabling ***flexibility*** at the lowest service level (e.g., through the use of larger buses).
4. **Repairability.** Decrease total time to recovery, that is, ensure availability of adequate resources and personnel to limit disruption impact on the primary failed system [Jackson and Ferris, 2013]. For example, if a blizzard occurs at an airport, while closure of the facility is inevitable, having appropriate snow removal equipment, trained personnel, and instrumentation capabilities, can provide expedited recovery as the storm's impact weakens. The repairability principle can also be applied at the system level in order to have SoS-level benefits. For instance, if the primary radar at an airport fails, timely repair of this system will ensure speedy return to full service of both terminal and en-route operations.
5. **Internode Interaction.** Every node in the SoS should be capable of communicating, collaborating, and coordinating with every other node [Jackson and Ferris, 2013]. For example, in the event of a hostile attack that results in the loss of an LCS (see Fig. 1), other systems

Table IV. Resilience Improvement Implications of Design Principles

		Resilience Improvement			
Category	**Design Principles**	**Reduce Disruption Impact**	**Improve Survivability in Immediate Aftermath of Disruption**	**Improve Time to Recovery in Immediate Aftermath of Disruption**	**Improve Total Time Taken for Complete Recovery**
System level	1. Physical redundancy		√		
	2. Functional redundancy		√		
	3. System-level Properties		√	√	
	4. Repairability				√
Network level	5. Internode interaction		√	√	
	6. Localized capacity		√		
Human aspects	7. Human-in-the-loop		√	√	
	8. Drift correction	√			
	9. Improved communication		√	√	
All levels	10. Layered defense	√	√	√	√

in the SoS, especially those that draw from or provide information to the ship, must be immediately aware of its incapacitation. This can be achieved by improving the communication capabilities between the systems in the SoS.

6. **Localized Capacity.** If a single node in the SoS is damaged or destroyed, the remaining nodes should continue to function [Jackson and Ferris, 2013], that is, cascading failures should be prevented or minimized. For example, if an airport closes, having alternative airports with adequate capacity nearby will allow flights to be diverted, while minimizing the domino effect through the rest of the airspace.
7. **Human-in-the-loop.** Humans should be in the loop when there is a need for "rapid cognition" and creative option generation [Madni and Jackson, 2009]. For example, the blackout across the Northeast in 2003 happened in part due to cascading automatic failures: preset relays were programmed to protect individual equipment, and as each one acted, isolating a power line or a transformer, the cascading disturbance caused a massive blackout impacting hospitals, airports, and subways [Wald, 2013].
8. **Drift correction.** Preemptively initiate resilience measures before the disruption so that mitigation steps may be initiated before the onset of the actual adverse event [Jackson and Ferris, 2013]. For instance, in the aftermath of the Icelandic volcano in 2010 that had widespread impact on global aviation services, sensors are being developed to provide warning of volcanic ash and to provide pilots with real-time information to alter their flight paths [BBC, 2010].
9. **Improved communication at organizational level.** Facilitate real-time information sharing and command and control activities between stakeholders and operators [Chang et al., 2013]. Improved communication at the organizational level can minimize confusion and mismanagement in the aftermath of a disruption. For example, in the event of a terror attack at an airport, timely and effective sharing of information regarding recovery procedures between regulatory authorities, airports, and airlines, can help minimize performance impacts on the larger network: passengers can be evacuated safely and redirected to other modes of transport efficiently.
10. **Layered defense**: Use a combination of the above design principles to balance protection (disruption prevention) and resilience (surviving and recovering from a disruption) in SoSs [Haimes, Crowther, and Horowitz, 2008].

Table IV highlights which region of the resilience curve (survivability and recoverability) each design principle addresses.

4.2.2. Simulation Tools and Models

Improved computational capabilities in recent decades have led to the development of high-fidelity simulations and models. These tools can aid the design process in several ways; for example, simulations can help study failure propagation, evaluate different recovery strategies, and identify critical nodes and links. While we can leverage existing network theory-based models to analyze links and nodes in SoSs, many of these methods assume homogenous nodes, leading to difficulties in capturing key SoS characteristics such as diversity and interdependencies. Given the inherent complexity of SoSs, efforts are needed to build on these network-based models by harnessing multiple fields such as control theory, statistical analysis, and operations research. Researchers have in recent years begun to address these issues and here we review efforts on relevant and useful simulation tools. In the next section, we highlight specific needs of scientific development with respect to model and tools.

Failure Propagation. Understanding how disruptive impacts propagate is an important element of any resilience analysis, especially in the case of SoSs where the coupling between independent systems is not always evident. Failure

propagation models are useful to identify critical links and to assess recovery options. Such models can be used, for example to the ATS to identify critical airports and to assess recovery options (road, rail, and air) if services at these airports fail.

Most resilience-related research uses some aspect of network theory to study effects of disruptions [Crucitti, Latora, and Marchioori, 2004; Ash and Newth, 2007; Kurant and Thiran, 2007; Ulieru, 2007; Reed, Kapur, and Christie, 2009; Buldyrev et al., 2010; Sterbenz et al., 2011]. With many SoSs, the assumption of homogenous nodes is not justified and the resulting approaches are not applicable to the analysis of networks with heterogeneous nodes, that is, nodes performing different functions. A few studies have considered nodes with the same function but different capacities [Motter and Lai, 2002; Crucitti et al., 2004].

Instead, multilayer networks resilience is gaining increasing attention as a better way to represent heterogeneous networks. Networks can be modeled as multilayers in two different ways. First, the network may consist of different physical layers. For example, the transportation system can be modeled as a road layer, a rail layer, and so forth. Or a network may require support from different layers. For example, the rail network depends on the electricity network. Research in this field has led to the introduction of interdependent network analyses to characterize the properties of such networks [Rinaldi, 2004; Newman et al., 2005; Kurant and Thiran, 2007; Xu et al., 2011; Ouyang, Dueñas-Osorio, and Min, 2012; Trucco, Cagno, and Ambroggi, 2012; Filippini and Silva, 2013]. Applying these studies to SoSs, designers can study how a failure in one network can have repercussions in the other and how interdependent networks can fail catastrophically after the removal of a small fraction of nodes. These results in turn can guide resource allocation at critical nodes. For example, in a multimodal transportation network, impacts of disruptive events can be avoided by colocating certain subway and bus stations thereby providing redundancy for the two transportation modes.

Apart from network-theoretic approaches, recent research has attempted to leverage control theory to deal with resilience of interconnected and interdependent systems (e.g., Barabási and Albert [1999], Liu, Slotine, and Barabasi [2011], and Alessandri and Filippini [2013]). For instance, with the ultimate goal of developing resilient controllers, Alessandri and Filippini [2013] present an initial framework that uses switching linear dynamics to cope with nominal and off-nominal (failure) behavior of interconnected systems.

Recovery Strategies. Simulation tools can (1) allow designers to study a range of resilience improvement options, (2) facilitate in-depth studies by allowing a large number of parameters to be varied, and (3) usually provide some visual representation of design implications that is vital to stakeholder communication. Most of these tools have been developed for infrastructure networks, and can be applied to other SoSs relatively easily [Bruneau and Reinhorn, 2004; Shinozuka et al., 2004; Miles and Chang, 2006; Zobel, 2011; Barker, Ramirez-Marquez, and Rocco, 2013; Barker and Baroud, 2014]. For example, Shinozuka et al. [2004] developed several restoration curves to study the return of electric power and water supply to customers after major catastrophic events, such as earthquakes. Similarly, Miles and Chang [2006] developed a simulation tool that generates recovery paths for communities in the aftermath of a disaster.

Critical Nodes and Links. Mathematical models and simulations can help designers identify resilience-based regions of concern (critical nodes and links) within SoSs [Garvey and Pinto, 2009; Guarniello and DeLaurentis, 2013]. Guarniello and DeLaurentis [2013] use the Functional Dependency Network Analysis model (originally proposed by Garvey and Pinto [2009]) to identify critical systems in SoSs and critical dependencies between constituent systems. For instance, in the naval warfare SoS, disruption of the LCS could lead to incapacitation of the weapons-equipped helicopter since the LCS is now unable to transmit crucial target information to the airborne system.

4.2.3. Metrics and Multicriteria Assessment Frameworks

Measuring resilience is a key component of designing resilience (see Fig. 2): quantitative assessment techniques are needed to evaluate the effectiveness of and to compare various resilience improvement designs. While metrics and frameworks add significant value to the SoS analyst's toolkit, developing generalizable measurements that can be applied broadly across a wide range of different SoSs is challenging. In addition, given the diversity of stakeholders associated with SoSs, difficulties arise with capturing all aspects of interest such as cost, performance, and safety, in a resilience metric. In this section, we review various metrics and frameworks.

Metrics. Ayyub [2014] proposes a resilience metric that is a function of the failure profile, recovery profile, as well as the various times involved with resilience, such as time of disruption, time during of failure, and time duration of recovery. Henry and Ramirez-Marquez [2012] define resilience as a ratio of system recovery to the loss after a disruption, where recovery and loss are measured as changes with respect to SoS performance. Francis and Bekera [2014] develop a resilience factor that is a function of speed of recovery and the various performance levels before and after the disruption and recovery actions. These metrics can be used to estimate the overall resilience of different SoS designs. For example, military operators can adopt these metrics to perform analysis of alternatives—for example, should target identification for a mission be provided using satellites or UAVs? Which SoS architecture would be most resilient to known and unknown threats?

Although there are advantages to using a single calculated value to define resilience, it is also important to recognize the potential issues associated with doing so [Haimes, 2009]. In particular, an overall metric provides little, if any, information regarding specific areas within the SoS that need attention. Also, in the context of SoSs, the uncertainties associated with network operations, evolution, and management are quite large and hence one metric may not be able to capture all the unknowns. To address these concerns, some studies focus on capturing or disentangling the various dimensions of resilience. These research efforts allow the resilience

measure to indicate the relative value of different situations to a particular decision-maker, and thus help to capture the varying perceptions and interpretations of the actual resilience inherent in a given SoS. For example, Barker et al. [2013] developed two resilience-based component importance measures for networks. Their study quantifies the impact of a link disruption on overall resilience, as well as the impact when a link cannot be disrupted. Han, Marais, and DeLaurentis [2012] propose a conditional resilience metric using Bayesian networks to measure each constituent system's contribution, and subsequently to identify the most critical systems to the overall SoS resilience. Pant, Barker, and Zobel [2013] use an extension of the economic input–output model to investigate the resilience of interdependent infrastructures. They develop two metrics: *static economic resilience*, which focuses on the survivability aspect of the overall network, and *dynamic economic resilience*, which includes the recovery of the network after a disruption. The present authors have developed a family of system importance measures (SIMs) that rank the constituent systems based on their impact on the overall SoS performance [Uday and Marais, 2014]. Instead of focusing on an overall metric, the set of SIMs provides designers with specific information on where an SoS is lacking resilience (or has excess resilience) and hence on where improvements are needed (or where downgrades are possible). For example, in the naval warfare example, these metrics can facilitate optimal selection of systems (helicopters, unmanned vehicles, support systems) and allocation of individual resources (weapons, communication bandwidth)

Multicriteria Assessment Frameworks. Frameworks have been the dominant trend in urban infrastructure resilience research. For example, the Multidisciplinary Center for Earthquake Engineering Research (MCEER) at the State University of New York views resilience as a combination of four "R"s: robustness, redundancy, resourcefulness, and rapidity, and proposes a framework to measure each "R" [Bruneau et al., 2003; Shinozuka et al., 2004]. Other work that has emerged from MCEER suggests a resilience index between 0 and 1 for each infrastructure network and then proposes a technique to aggregate all the indexes for an overall resilience measure [Renschler et al., 2010]. Similar efforts at Carnegie-Mellon's Software Engineering Institute have resulted in a Resiliency Engineering Framework (REF), which posits a vector of 21 capability areas that can be used to score the resilience of cyber services [SEI, 2009]. While most of these frameworks do consider, to a certain degree, the stochastic (uncertain) nature of inputs, the data needed for resilience studies are in most cases limited and incomplete. To handle these issues, Attoh-Okine, Cooper, and Mensah [2009] present a method to construct resilience index for urban infrastructure using belief functions that are capable of handling imprecise and subjective information.

5. CHALLENGES AND OPPORTUNITIES IN DESIGNING RESILIENT SoS

The characteristics of SoS provide both challenges and opportunities for designers. Here, we use these characteristics to identify design questions and suggest potential research directions, as summarized in Table V.

5.1. SoSs are Typically Large-Scale Networks that Consist of a Variety of Heterogeneous Systems

The ability of SoSs to provide capabilities that single systems cannot stems from their inherent diversity, that is, the variety of their constituent systems (heterogeneous nature of SoSs) and, in many cases, the geographical distribution of these systems (large-scale feature of SoSs). While these characteristics are essential to achieving SoS goals, they present challenges that can stymie efforts to effectively analyze SoSs, particularly with respect to modeling SoS resilience. These issues include modeling the interactions within and between SoSs, and computational challenges associated with large models.

All complex systems pose a modeling challenge, which essentially comes down to determining what the minimum level of fidelity is that will still provide useful results (and whether this fidelity is computationally tractable). This problem is especially tough in the case of SoSs, where even low-fidelity models can rapidly become very large and hence computationally challenging and difficulty to verify and validate. Several researchers have been addressing this problem by modeling SoSs as networks, which enables them to leverage network theory. But this approach requires that nodes be identical, or that only a few types of nodes be considered. Other work has extended modeling and measurement efforts to include performance levels of heterogeneous nodes rather than just flows between nodes in a network. However, most of these studies tend to be infrastructure-specific, and hence have limited use. Given the above discussion (see also Section 4.2), it is fair to ask:

How can we develop sufficiently detailed models to analyze SoS resilience?

The first set of research questions relates to developing models of adequate fidelity to analyze SoS resilience. Specifically, (1) How can we develop sufficiently detailed models that do not oversimplify the problem? (2) How we can we efficiently capture cross-domain coupling? and (3) How do we deal with computational challenges associated with large models? Answers to these questions will provide useful contributions to the SoS engineering community. Some routes to solving these questions are:

- **Use pattern recognition to model evolution of SoS operations.** One promising approach is to leverage advances in "Big Data" tools and techniques to the analysis of resilience in SoSs. This method has been used effectively in weather prediction and modeling. Computer software is used to identify previous weather patterns that closely resemble the current conditions, and then the predicted outcome is based on some weighted combination of the previous, similar, outcomes. Similarly, exploring response patterns of existing SoSs to previous disruptions could be used to evaluate new architectures. For example, Kalawsky, Joannou, and Fayoumi [2013]

Table V. Key Questions in Designing Resilient SoSs

SoS Characteristic	Specific design questions
Large-scale with heterogeneous systems	• How can sufficiently detailed models be developed that do not oversimplify the problem? • How can models capture cross-domain coupling effectively? • How can the computational challenges associated with large models be dealt with efficiently?
Uncertainties in SoS evolution and operating environment	• How can internal and external uncertainties be modeled? • Where should resilience be added? • Will there be any unintended consequences of resilience improvement measures? • What is an acceptable or suitable level of resilience for a particular SoS?
Multiple stakeholders and/or partial control of SoS	• How can we develop strategies that incentivize and facilitate resilience improvement measures for the overall SoS in a climate of uneven distribution of costs and benefits, and uncertain realization of benefits?

use pattern recognition to model emergency response (SoS comprising police departments, fire brigades, and ambulance services) for a major incident in the United Kingdom.

- **Use cloud-based computing to facilitate the development of large SoS models.** Some advantages of using this approach include: (1) the ability to separately develop various aspects of the larger model (colocating simulations and resources is no longer a constraint), and (2) the ability to involve multiple, distributed contributors and expertise simultaneously (researchers need not "reinvent the wheel": existing models can be used and built upon remotely).
- **Use Metamodels that consider multiple models, multiple experts, and shared variables and parameters to represent and analyze SoSs.** For example, consider the case of a rise in sea level due to climate change and its impact on saltwater intrusion into coastal groundwater aquifer systems. Haimes [2012] describes three system models to analyze this phenomenon: hydrological (water modeling), agricultural–social (impacts on agriculture and domestic water supplies), and regional economic models (economic impacts). All three models draw inputs from the same database (here, external climatological models). In other work, Filippini and Silva [2015] present a modeling language (I®ML) to facilitate analysis of interdependencies with the aim to improve SoS (in particular, critical infrastructure) resilience. The authors also provide a discussion of other useful models, such as the functional resonance analysis model [Hollnagel, 2012] and an interdependency model based on failures and repairs [Johansson and Hassel, 2010]. Carley [2003] presents the concept of Dynamic Network Analysis to evaluate network evolution and change propagation in large-scale, dynamic networks; this approach provides fertile ground for the development of SoS-focused metamodels.
- **Leverage Human–System Integration (HSI) research to improve SoS design and accessibility for human operators.** As SoSs continue to grow in size and complexity, the integration of humans with software and systems becomes increasingly significant. Currently, human capabilities and limitations and their implications on the design, deployment, operation, and maintenance of SoSs are typically not explicitly addressed in SoS engineering and acquisition lifecycles [Madni, 2010]. This challenge can be addressed by incorporating HSI ideas such as cognitive compatibility, identification of HSI patterns, and human performance modeling. For example, one specific ongoing project [Rouse, 2012] explicitly models human behavior and performance as part of a larger effort to improve the application of systems engineering to SoSs.
- **Develop metrics for the price of uncertainty to provide guidance in establishing modeling requirements.** Apart from building SoS resilience models, a key challenge is evaluating the models themselves. Specifically, what level of model fidelity can provide the required quality of guidance to decision-makers? One way to answer this question is through the development of suitable metrics and methods that help assess this price of uncertainty.

5.2. SoSs Operate in Environments of High Degrees of Uncertainty

Traditionally, system optimization has sought to identify the "best" point design given a fixed set of constraints for the entire lifetime of the system. However, in the case of long-lasting SoSs, such as infrastructure and transportation networks, this approach of deterministic optimization over a single period cannot be solved in a permanent sense. The key hurdle to identifying an optimal solution is the uncertain environment, both endogenous (internal) and exogenous (external), in which SoSs typically operate. Endogenous uncertainty includes SoS evolution in terms of phasing out of old systems, inclusion of new systems, upgrades to existing systems, and changes to the underlying communication (cyber). Exogenous uncertainty is driven by changes in the external environment, such as new types of threats, new requirements to interface with other SoSs, and changing stakeholder needs. Furthermore, this uncertainty ranges from the well-defined (e.g., we know that Boston will most likely experience several blizzards every winter), to the much

more difficult "unknown–unknowns." So, the second set of research challenges stem from the following question:

Given the uncertainties in hazards, technologies, and SoS structure, how can we make SoSs optimally resilient?

The uncertainties mentioned above have a significant impact on modeling and managing SoS resilience. Specific questions that decision-makers need to address include: (1) How can internal and external uncertainties be modeled? (2) Will there be any unintended consequences of resilience improvement measures? and (3) What is an acceptable or suitable level of resilience for a particular SoS? An SoS that is optimally resilient now to a certain class of threats may not be optimally resilient in the future as its constituent systems and the external threats change in time. There is also the question of what "optimally resilient" means. Other dimensions of risk, such as "dread" and "violation of equity" also play a role. For example, the threat of terrorism inspires dread in a different way than a natural disaster. As a result, societies will often prioritize responding to these types of risk over other, objectively "larger" risks. For example, in recent years airports have been made more resilient to terrorist attacks (through improved screening and emergency response procedures). However, as global warming–induced changes affect weather patterns, these airports may not be resilient to blizzards and rainstorms that may occur with higher frequency in the future. Also, specifically with respect to infrastructure SoSs, engineers and designers seldom have the opportunity to design an SoS "from scratch"—these SoSs typically evolve over many decades as systems are acquired, upgraded, and/or removed. And so a fourth question arises: is it possible to upgrade a formerly unresilient SoS into a resilient one?

Addressing unforeseen changes is a challenging task primarily because identifying "unknown–unknowns" by definition is impossible. However, while we do not always know why or how systems and processes might be disrupted, we can improve anticipation and recovery efforts through improved SoS modeling. For example, tools that facilitate the analysis of multisystem failures are valuable in directing resilience improvement resources. Similarly, as it is likely that different systems will come back online at different times (e.g., refer to previous example of impact of different rate of recovery of aviation and rail transportation in New York city in the aftermath of Hurricane Sandy), such tools would be useful to mitigate the harmful impact of asynchronous recoveries.

These situations highlight the need for discussions about the acceptable level of resilience an SoS needs to maintain and over what range of scenarios this resilience should be available. Another factor that has significant implications for managing resilience under uncertainty is the inherently multidimensional aspect of resilience: performance and time. As a result, in many cases decisions about resilience improvement must consider where the resilience should be placed, that is, following a disruption, should we improve the performance considerably albeit after a significant downtime or should we ensure a timely recovery with minimum performance recovery?

We believe that the above-mentioned challenges offer opportunities to "creatively" tackle the issue of SoS resilience, and here, suggest a few ways to approach this thorny challenge:

- **Identify "resilience pathways" that allow an SoS to remain resilient over long time periods.** As threats and the constituent systems of the SoS evolve stochastically over the lifetime of the SoS, the necessary optimization must put the SoS on a "path to resilience," that is, it must allow for incremental changes that can maintain resilience of the SoS over time.
- **Use the concept of multiple equilibria from ecology to design engineering resilience.** As the interdependencies between SoSs, and not just between their constituent systems, grow, the concept of multiple equilibria from ecology (ability of a system to move into a different equilibrium or stable state to maintain functionality in the face of a disruption [Holling, 1973]) could provide an interesting approach to developing resilient SoSs. For example, can we design transportation networks that allow demand to be shifted over and sustained on the bus networks in the event of a major railway disturbance, thereby shifting the "equilibrium" from rail to road? These studies would need to also take into account social behavior and preference patterns of the general public, further strengthening the idea that multiple disciplines as widely diverse as engineering and psychology, for example, would need to be corralled to analyze SoS resilience in its entirety [Jackson, 2007].

5.3. SoS Operations Involve Multiple Stakeholders and in Many Cases Partial Control over the SoS

The constituent systems in most civilian SoSs, such as infrastructure and transportation networks, are typically owned and operated by different entities and/or organizations. Similarly, in the military domain, although SoSs exhibit a defined structure with respect to their operations, a variety of stakeholders are involved in the development of the constituent systems. Hence, attempts to improve the resilience of SoSs may result in situations where some stakeholders are required to accept greater costs. The following question drives the third set of research challenges:

How can we develop strategies that incentivize and facilitate resilience improvement measures for the overall SoS in a climate of uneven distribution of costs and benefits, and uncertain realization of benefits?

Since the human element is a significant part of the development, operation, and maintenance of resilient SoSs addressing the above question can improve discussions about resilience improvement strategies. Some suggestions are provided below:

- **Develop tools to support decision-making and information exchange between stakeholders.** From a technological perspective, better decision-making tools that support stakeholder collaboration efforts are needed to improve the quality of resilience-related discussions. These tools can be developed by adopting recent advances in fields such as collaboration technology, information abstraction, visual analytics, and data sharing [Provan and Kenis, 2008; Neches and Madni, 2012]. In

addition, existing frameworks such as DoDAF [DoD, 2010] and the Open Group Architecture Framework (TOGAF) [Open Group, 2011] can be leveraged to facilitate SoS visualization and communication between analysts and stakeholders.

- **Improve stakeholder risk perception through the development of risk communication tools.** For the overall SoS to be made resilient, some fraction of the constituent systems must include features to mitigate effects of disruptions. This uneven spread of resilience requirements implies a disproportionate spread of stakeholder benefits and costs. Furthermore, the value of a particular resilience strategy is only realized when the disruptions or failures actually occur. As a result, improved risk communication tools need to be developed (as highlighted in Aven [2013b]) to improve risk perception and to help stakeholders make decisions.
- **Develop common standards to facilitate SoS development.** Just as common standards enable the concurrent but separate development of subsystems (e.g., testing standards ensure that all subsystems meet minimum electromagnetic compatibility requirements), common standards may enable multiple stakeholders to work together more effectively to develop SoSs. Obvious standards include selecting SI or English units—however, could more sophisticated standards be helpful? For example, would using the System Modeling Language (SML) contribute to faster or otherwise more effective development? Similarly, do the lessons and benefits of concurrent engineering transfer to SoS-level engineering?
- **Develop strategies to minimize cost-benefit imbalances to stakeholders.** Resilience improvement measures at the SoS level can result in an uneven distribution of costs and benefits across stakeholders, which may make some reluctant to participate. Given these potential imbalances, new approaches are needed to determine which strategies are most appropriate to persuading stakeholders to make the necessary changes or upgrades to their systems. For example, Marais and Weigel [2006] present a framework to encourage successful technology transition in civil aviation. Specifically, the authors use cost, benefit, and value distributions across stakeholders and over time to determine which strategies are most appropriate to persuading aircraft operators to adopt new equipage. Specific strategies could include phased implementation of resilience improvement measures, positive incentives such as monetary benefits or tax breaks to early participants, and mandates and punitive approaches.

6. CONCLUSION

SoSs are ubiquitous and here to stay. The services provided by SoSs are typically vital and time-sensitive. It is therefore essential that these networks be made resilient to adverse events. This survey paper provides a foundation that can shape research and policy in the field of designing resilience, specifically, in the domain of SoSs. In particular, our survey has shown that the current ad hoc, reactive, and mostly bottom–up approaches to the design and analysis of SoS resilience are not adequate.

We provided an overview of engineering resilience and decoupled its definition from related terms in the literature highlighting key benefits to overall SoS design that each attribute provides. We then offered a focused discussion of classical risk and reliability methods and metrics that can be applied to the analysis of SoS resilience. We believe that recent SoS-focused methods that leverage multiple disciplines promote a top–down decision-making approach [Hazelrigg, 1998] for SoS design rather than a set of more localized problem-solving processes (e.g., design of an aircraft that meets range, payload, and fuel efficiency criteria). As we continue demanding more from our SoSs, obtaining resilience that is optimal in some sense (e.g., cost-effective) will require considering the SoS as whole, and considering information obtained from a wide variety of sources. For example, an automated air traffic control system may be excellent at routing aircraft, but if air traffic controllers do not buy into it, it will most likely fail. Rather, given the complexities and stakeholders associated with SoSs, in many cases, minor changes need to be made in a phased manner to ensure overall resilience. Such design modifications lend themselves better to a decision-making approach rather than point solutions. Benefits of this approach include allowing human input and judgment as well as incorporating nontechnical disciplines.

Finally, we provided potential avenues and specific suggestions to shape future research in this area. While we have made several recommendations in Section 5, in our opinion, targeted research in two specific areas is vital for the development of SoS resilience. We highlight these topics as we believe they are ones where progress can be made in the near-term by building on recent research efforts.

- ***Use advanced data analysis techniques to model SoSs***: Leveraging large amounts of data and improved computing capabilities can enable improved SoS modeling, allowing analysts to study the effects of failures, disruptions, and recovery measures.
- ***Model and understand the human element within SoS operations***: Research on cognitive compatibility, identification of HSI patterns, and human performance modeling will shed light on human capabilities and limitations and their implications on the design, deployment, operation, and maintenance of SoSs.

ACKNOWLEDGMENT

This material is based on work supported in part by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004 RT#108. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

REFERENCES

R. Abbott, Open at the top; open at the bottom; and continually (but slowly) evolving, *IEEE International Conference on System of Systems Engineering*, Los Angeles, CA, 2006.

D.S. Albert and R.E. Hayes, Power to the edge, DOD Command and Control Research Program (CCRP), 2003, http://www.dodccrp.org/files/Alberts_Power.pdf, accessed March 1, 2014.

A. Alessandri and R. Filippini, Evaluation of resilience of interconnected systems based on stability analysis, Lecture Notes in Computer Science, Vol. 7722, 2013, pp. 180–190.

J. Ash and D. Newth, Optimizing complex networks for resilience against cascading failures, Phys Rev A 380 (2007), 673–683.

N. Attoh-Okine, A.T. Cooper, and S.A. Mensah, Formulation of resilience index of urban infrastructure using belief functions, IEEE Syst J 3(2) (2009), 147–153.

T. Aven, On how to deal with deep uncertainties in a risk assessment and management context, Risk Anal 33(12) (2013a), 2082–2091.

T. Aven, Practical implications of the new risk perspectives, Reliab Eng Syst Saf 115 (2013b), 136–145.

B. Ayyub, Systems resilience for multihazard environments: definition, metrics, and valuation for decision-making, Risk Anal 34(2) (2014), 340–355.

A.-L. Barabási and R. Albert, Emergence of scaling in random networks, Science 286 (1999), 509–512.

K. Barker and H. Baroud, Proportional hazards model of infrastructure system recovery, Reliab Eng Syst Saf 124 (2014), 201–206.

K. Barker, J.E. Ramirez-Marquez, and C.M. Rocco, Resilience-based network component importance measures, Reliab Eng Syst Saf 117 (2013), 89–97.

V. Barot, M. Henshaw, C. Siemieniuch, M. Sinclair, S.L. Lim, S. Henson, M. Jamshidi, and D. DeLaurentis, SoA report, Trans-Atlantic Research and Education Agenda in Systems of Systems (T-AREA-SoS), 2013, https://www.tareasos.eu/docs/pb/SoA_V3.pdf, accessed January 28, 2015.

S. Basnyat, P. Palanque, B. Schupp, and P. Wright, Formal socio-technical barrier modelling for safety- critical interactive systems design, Saf Sci 45(5) (2007), 545–565.

BBC, Easyjet to trial volcanic ash detection system, BBC, 4 June, 2010, http://www.bbc.co.uk/news/10234553, accessed October 1, 2014.

Y. Ben-Haim, Why risk analysis is difficult, and some thoughts on how to proceed, Risk Anal 32(10) (2012), 1638–1646.

J. Bowen and V. Stavridou, Safety-critical systems, formal methods and standards, Softw Eng 8(4) (1993), 189-209.

R. Brown and C. Drew, Airlines begin a laborious comeback, New York Times, 31 October, 2012, http://www.nytimes.com/2012/11/01/business/after-hurricane-sandy-returning-to-the-air.html?pagewanted = all, accessed January 9, 2014.

M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, and D. von Winterfeldt, A framework to quantitatively assess and enhance the seismic resilience of communities, Earthq Spectra 19(4) (2003), 733–752.

M. Bruneau and A. Reinhorn, Seismic resilience of communities—Conceptualization and operationalization, *International Workshop on Performance-based Seismic Design*, Bled, Slovenia, 28 June–1 July, 2004.

S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, and S. Havlin , Catastrophic cascade of failures in interdependent networks, Nature 464 (2010), 1025–1028.

K.M. Carley, Dynamic network analysis, In: Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers (2003), Eds. Ronald Breiger, Kathleen Carley, and Philippa Pattison, Editors, Committee on Human Factors, National Research Council. (2003), 133–145. Available online at http://www.nap.edu/catalog/10735/dynamic-social-network-modeling-and-analysis-workshop-summary-and-papers.

J.-F. Castet and J.H. Saleh, On the concept of survivability, with application to spacecraft and space-based networks, Reliab Eng Syst Saf 99 (2012), 123–138.

CBS, Road to nowhere: Minor snowstorm brings Atlanta to standstill. CBS, 29 January, 2014, http://www.cbsnews.com/news/atlanta-other-parts-of-south-paralyzed-by-ice-snowstorm/, accessed October 1, 2014.

M.J. Chalupnik, D.D. Wynn, and J. Clarkson, Comparison of ilities for protection against uncertainty in system design, J Eng Des 24(12) (2013), 814–829.

S.E. Chang, E. McDaniels, J. Fox, R. Dhariwal, and H. Longstaff, Toward disaster-resilient cities: Characterizing resilience of infrastructure systems with expert judgments, Risk Anal 34(3) (2013), 416–434.

R.T. Clemen and R.L. Winkler, Combining probability distributions from experts in risk analysis, Risk Anal 19(2) (1999), 187–203.

L.A. Cox, Confronting deep uncertainties in risk analysis, Risk Anal 32(10) (2012), 1607–1629.

W.A. Crossley, *System of systems: An introduction of purdue university schools of engineering's signature area, Engineering Systems Symposium at MIT*, 29–31 March, Cambridge, MA, 2004.

P. Crucitti, V. Latora, and M. Marchioori, Model for cascading failures in complex networks, Phys Rev E 69(4) (2004), 045104-1–045104-4.

J. Dahmann and K. Baldwin, Understanding the current state of US defense systems of systems and the implications for systems engineering, *IEEE Systems Conference*, Montreal, Canada, 7–10 April, 2008.

B. Dedman, What are the odds? US nuke plants ranked by quake risk, NBC News, 17 March, 2011, http://www.nbcnews.com/id/42103936/ns/world_news-asia_pacific/t/what-are-odds-us-nuke-plants-ranked-quake-risk/#.UznaFq1dUvd, accessed March 4, 2014.

D. DeLaurentis, W. Crossley, and M. Mane, Taxonomy to guide systems-of-systems decision-making in air transportation problems, J Aircr 48(3) (2011), 760–770.

D. DeLaurentis, C. Dickerson, M. DiMario, P. Gartz, M.M. Jamshidi, S. Nahavandi, A.P. Sage, E.B. Sloane, and D.R. Walker, A case for an international consortium on system-of-systems engineering, IEEE Syst J 1 (2007), 68–73.

DoD, Systems engineering guide for systems of systems, Version 1.0, 2008, http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf, accessed January 18, 2015.

DoD, The DoDAF architecture framework Version 2.02, 2010, http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf, accessed January 21, 2015.

DoD, Department of Defense Science and Technology emphasis areas, 2011, http://www.acq.osd.mil/chieftechnologist/publications/docs/OSD%2002073-11.pdf, accessed January 22, 2015.

R. Dove, *Response ability—The language, structure, and culture of the agile enterprise*, Wiley, New York, 2001.

J. Dunjo, V. Fthenakis, J.A. Vilchez, and J. Arnaldos, Hazard and operability (HAZOP) analysis. A literature review, J Hazard Mater 19(32) (2010), 19–32.

R. Feynman, "Personal observations on reliability of shuttle," in *NASA Rogers Commission Report - Appendix F*, 1986,

http://history.nasa.gov/rogersrep/v2appf.htm, accessed March 3, 2014.

R. Filippini and A. Silva, A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies, Reliab Eng Syst Saf 125 (2013), 82–91.

R. Filippini and A. Silva, I®ML: An infrastructure resilience-oriented modeling language, IEEE Trans Syst Man Cybern Syst 45(1) (2015), 157–169.

C.H. Fleming, M. Spencer, J. Thomas, N. Leveson, and C. Wilkinson, Safety assurance in NextGen and complex transportation systems, Saf Sci 55 (2013), 173–187.

R. Francis and B. Bekera, A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliab Eng Syst Saf 121 (2014), 90–103.

P.R. Garvey and C.A. Pinto, Introduction to functional dependency network analysis, *International Symposium on Engineering Systems*, 15–17 June, Cambridge, MA, 2009.

G. Giuliano, and J. Golob, Impacts of the Northridge earthquake on transit and highway use, J Transp Stat 1(2) (1998), 1–20.

S. Goerger, A.M. Madni, and O.J. Eslinger, Engineered resilient systems: A DoD perspective, *Conference on Systems Engineering Research*, Redondo Beach, CA, 21–22 March, 2014.

A. Gorod and B. Sauser, System-of-systems engineering management: A review of modern history and a path forward, IEEE Syst J 2(4) (2008), 484–499.

G. Guarniello and D. DeLaurentis, Dependency analysis of system-of-systems operational and development networks, *Conference on Systems Engineering Research*, Atlanta, GA, 20–22 March, 2013.

Y.Y. Haimes, On the definition of resilience in systems, Risk Anal 29(4) (2009), 498–501.

Y.Y. Haimes, Modeling complex systems of systems with phantom system models, Syst Eng 15(3) (2012), 333–346.

Y.Y. Haimes, K. Crowther, and B.M. Horowitz, Homeland security preparedness: Balancing protection with resilience in emergent systems, Syst Eng 11(4) (2008), 287–308.

S.Y. Han, K. Marais, and D. DeLaurentis, Evaluating system of systems resilience using interdependency analysis, *IEEE International Conference on Systems, Man, and Cybernetics*, Seoul, Korea, 14–17 October, 2012.

G.A. Hazelrigg, A framework for decision-based engineering design, J Mech Des 120(4) (1998), 653–658.

D. Henry and H. Ramirez-Marquez, Generic metrics and quantitative approaches for system resilience as a function of time, Reliab Eng Syst Saf 99 (2012), 114–122.

A. Higgins, Lessons for the U.S. from a flood-prone land, New York Times, 14 November, 2012, http://www.nytimes.com/2012/11/15/world/europe/netherlands-sets-model-of-flood-prevention.html?pagewanted = all, accessed October 1, 2014.

C.S. Holling, Resilience and stability of ecological systems, Annu Rev Ecol Syst 4 (1973), 1–23.

E. Hollnagel, *FRAM, the functional resonance analysis method modelling complexsocio-technical systems*, Ashgate, Surrey, England, 2012.

E. Hollnagel, D.W. Woods, and N. Leveson, *Resilience engineering: Concepts and precepts*, Ashgate, Burlington, VT, 2006.

INCOSE, Resilient Systems Working Group, 2000, http://www.incose.org/practice/techactivities/wg/rswg/, accessed January 22, 2015.

S. Jackson, A multidisciplinary framework for resilience to disasters and disruptions, J Integr Des Process Sci 11(2) (2007), 91–108.

S. Jackson, *Accident avoidance and survival and recovery from disruptions*, Wiley, Hoboken, NJ, 2010.

S. Jackson and T.L.J. Ferris, Resilience principles for engineered systems, Syst Eng 16(2) (2013), 152–164.

M. Jamshidi, System of systems engineering—New challenges for the 21st century, IEEE Aerosp Electron Syst Mag 23(5) (2008), 4–19.

J. Johansson and H. Hassel, An approach for modelling interdependent infrastructures in the context of vulnerability analysis, Reliab Eng Syst Saf 95(12) (2010), 1335–1344.

J. Johansson, H. Hassel, and E. Zio, Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems, Reliab Eng Syst Saf 120 (2013), 27–38.

R.S. Kalawsky, Y.T. Joannou, and A. Fayoumi, Using architecture patterns to architect and analyze systems of systems, Conference on Systems Engineering Research, Atlanta, GA, 20–22 March, 2013.

S. Kaplan and B.J. Garrick, On the quantitative definition of risk, Risk Anal 1 (1981), 11–28.

J.C. Knight, Safety critical systems: Challenges and directions, *Proceedings of the 24th International Conference on Software Engineering*, Orlando, FL, 25 May, 2002.

M. Kurant and P. Thiran, Error and attack tolerance of layered complex networks, Phys Rev E 76(2) (2007), 026103-1–026103-5.

F. Landegren, J. Johansson, and O. Samuelsson, "Review of computer based approaches for modeling and simulating critical infrastructures as socio-technical systems," in R.D.J.M. Steenbergen, P.H.A.J.M. Van Gelder, S. Miraglia, et al. (Editors), Safety, Reliability and Risk Analysis,: Beyond the Horizon, (2014) pp. 2047–2054. Available online at http://www.crcnetbase.com/isbn/9781315815596.

J.-C. Laprie, From dependability to resilience, *IEEE International Conference on Dependable Systems and Networks*, 2008, pp. G8–G9.

N. Leveson, *Safeware*, Addison-Wesely, Boston, MA, 1995.

N. Leveson, *Engineering a safer world*, MIT Press, Cambridge, MA, 2012.

N.G. Leveson and J.L. Stolzy, Safety analysis using Petri nets, IEEE Trans Softw Eng 13, 1987, 386–397.

Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabasi, Controllability of complex networks, Nature 473(12) (2011), 167–173.

D. Luzeaux, "Engineering large-scale complex systems," in D. Luzeaux, J.-R. Ruault, and J.-L. Wippler (Editors), *Complex Systems and Systems-of-Systems Engineering*, Wiley, Somerset, NJ, 2011.

A.M. Madni, Integrating humans with software and systems: Technical challenges and a research agenda, Syst Eng 13(3) (2010), 232–245.

A.M. Madni and S. Jackson, Towards a conceptual framework for resilience engineering, IEEE Syst J 3(2) (2009), 181–191.

G.E. Mahnken, Use case histories to energize your HAZOP. Chem Eng Progr 97(3) (2001), 73–78.

M.W. Maier, Architecting principles for system-of-systems, J Syst Eng 1(4) (1998), 267–284.

M.W. Maier and E. Rechtin, *The art of systems architecting*, CRC Press, Boca Raton, FL, 2000.

M. Mane, W.A. Crossley, and Nusawardhana Z., System of systems inspired aircraft sizing and airline resource allocation via decomposition, J Aircr 44(4) (2007) 1222–1235.

M. Mane, D. DeLaurentis, A. Frazho, A Markov perspective on development interdependencies in networks of systems, J Mech Des 133(10) (2011), Article Number: 101009.

K. Marais and A. Weigel, A framework to encourage successful technology transition in civil aviation, *25th Digital Avionics Systems Conference*, Portland, OR, 15–19 October, 2006.

B. Mekdeci, A.M. Ross, D.H. Rhodes, and D.E. Hastings, Controlling change within complex systems through pliability, *Third International Engineering Systems Symposium (CESUN)*, Delft, Holland, 18–20 June, 2012.

S.B. Miles and S.E. Chang, Modeling community recovery from earthquakes, Earthq Spectra 22(2) (2006), 439–458.

M. Modarres, M. Kaminsky, and V. Krivtsov, *Reliability engineering and risk analysis: A practice guide*, Marcel Dekker, New York, NY, 1999.

A.E. Motter and Y.-C. Lai, Cascade-based attacks on complex networks, Phys Rev E 66(6) (2002), 065102-1–065102-4.

R. Neches and A.M. Madni, Towards affordably adaptable and effective systems, Syst Eng 16(2) (2012), 224–234.

D.E. Newman, B. Nkei, B.A. Carreras, I. Dobson, V.E. Lynch, and P. Gradney, Risk assessment in complex interacting infrastructure systems, *38th International Conference on System Sciences*, Big Island, HI, 03–06 January, 2005.

Open Group, The Open Group Architectural Framework Version 9.1, 2011, http://www.opengroup.org/togaf/, accessed January 21, 2015.

M. Ouyang, L. Dueñas-Osorio, and X. Min, A three-stage resilience analysis framework for urban infrastructure systems, Struct Saf 36 (1) (2012), 23–31.

N. Paltrinieri, A. Tugnoli, S. Bonvicini, and V. Cozzani, Atypical scenarios identification by the DyPASI procedure: Application to LNG, Chem Eng Trans 24, (2011), 1171–1176.

R. Pant, K. Barker, and C.W. Zobel, Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors, Reliab Eng Syst Saf 125, (2013), 92–102.

J. Park, T.P. Seager, P.S.C. Rao, M. Convertino, and I. Linkov, Integrating risk and resilience approaches to catastrophe management in engineering systems, Risk Anal 33(3) (2013), 356–367.

K.G. Provan and P. Kenis, Modes of network governance: Structure, management, and effectiveness, J Public Adm Res Theory 18(2) (2008), 229–252.

N. Rasmussen, *Reactor safety study (WASH-1400)*, US Nuclear Regulatory Commission, NUREG-75/014, 1975.

M. Rausand and A. Høyland, *System reliability theory: Models, statistical methods, and applications*, Wiley Interscience, Hoboken, NJ, 2004.

D.A. Reed, K.C. Kapur, and R.D. Christie, Methodology for assessing the resilience of networked infrastructure, IEEE Syst J 3(2) (2009), 174–180.

C.S. Renschler, A.E. Frazier, L.A. Arendt, G.P. Cimellaro, A.M. Reinhorn, and M. Bruneau, Developing the "PEOPLES" resilience framework for defining and measuring disaster resilience at the community scale, *9th US and 10th Canadian Conference on Earthquake Engineering*, Toronto, Canada, 25–29 July, 2010.

Resilience Alliance, 2001, http://www.resalliance.org/, accessed January 22, 2015.

M.G. Richards, A.M. Ross, N.B. Shah, and D.E. Hastings, Metrics for evaluating survivability in dynamic multi-attribute tradespace exploration, J Spacecr Rockets 46(5) (2009), 1049–1064.

S.M. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, *37th Hawaii International Conference on System Sciences*, Big Island, HI, 05–08 January, 2004.

B.W. Robinson, Application of hazard and operability studies to a wide range of industries and activities, Qual Reliab Eng Int 11(6) (1995), 399–402.

A. Rose, Economic resilience to natural and man-made disasters: Multi-disciplinary origins and contextual dimensions, Environ Hazards 7(4) (2007), 383–398.

W. Rouse, Multi-level socio-technical modeling, Systems Engineering Research Center Project #44, 2012, http://www.sercuarc.org/projects/view/34, accessed April 3, 2014.

J. Ruault, F. Vanderhaegen, and D. Luzeaux, Sociotechnical systems resilience. INCOSE International Symposium 22(1) (2012), 339–354.

E.T. Ryan, D.R. Jacques, and J.M. Colombi, An ontological framework for clarifying flexibiliy-related terminology via literature survey, Syst Eng 16(1) (2013), 99–109.

J.H. Saleh, K.B. Marais, and F.M. Favaró, System safety principles: A multidisciplinary engineering perspective, J Loss Prev Process Ind 29, (2014), 283–294.

J.H. Saleh, G. Mark, and N.C. Jordan, Flexibility: A multidisciplinary literature review and a research agenda for designing flexible engineering systems, J Eng Des 20(3) (2009), 307–323.

SEI, CERT Resiliency Engineering Framework, Software Engineering Institute, 2009, http://www.cert.org/resiliency engineering/, accessed September 1, 2013.

S. Sheard and A. Mostashari, A framework for system resilience discussions, *18th Annual International Symposium of INCOSE*, Utrecht, the Netherlands, 15–19 June, 2008.

Y. Sheffi and J.B. Rice, A supply chain view of the resilient enterprise, Sloan Manage Rev 47(1) (2005), 41–48.

M. Shinozuka, S.E. Chang, T.-C. Cheng, M. Feng, T.D. O'Rourke, M.A. Saadeghvaziri, X. Dong, X. Jin, Y. Wang and P. Shi, "Resilience of integrated power and water systems," in *MCEER Research Progress and Accomplishments: 2003–2004*, Buffalo, NY, 2004, pp. 65–86.

N. Siu, Risk assessment for dynamic systems: An overview, Reliab Eng Syst Saf 43(1) (1994), 43–73.

J.P.G. Sterbenz, E.K. Cetinkaya, M.A. Hameed, A. Jabbar, and J.P. Rohrer, Modelling and analysis of network resilience, *International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India, 2011.

N.R. Storey, *Safety critical computer systems*, Addison-Wesley. Boston, MA. 1996.

W.A.H. Thissen, and P.M. Herder, "System of system perspectives on infrastructures," in M., Jamshidi (Editor), *System of Systems Engineering—Principles and Applications*, CRC Press. Boca Raton, FL, 2009.

K. Tierney and M. Bruneau, Conceptualizing and measuring resilience, TR News, 2007, http://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf, accessed March 1, 2014.

P. Trucco, E. Cagno, and M.D. Ambroggi, Dynamic functional modeling of vulnerability and interoperability of critical infrastructures, Reliab Eng Syst Saf 105 (2012), 51–63.

TTCP, Recommended practices: System of systems considerations in the engineering of systems, The Technical

Cooperation Program (TTCP) Technical Report, 2014, http://www.acq.osd.mil/se/docs/TTCP-Final-Report-SoS-Recommended-Practices.pdf, accessed January 18, 2015.

P. Uday and K. Marais, Exploiting stand-in redundancy to improve resilience in a system-of-systems (SoS), *Conference on Systems Engineering Research*, Atlanta, GA, 20–22 March, 2013.

P. Uday and K. Marais, Resilience-based system importance measures for system-of-systems, *Conference on Systems Engineering Research*, Redondo Beach, CA, 21–22 March, 2014.

M. Ulieru, Design for resilience of networked critical infrastructures, *IEEE International Conference on Digital Ecosystems and Technologies*, Cairns, Australia, 21–23 February, 2007.

R. Vaidhyanathan and V. Venkatasubramianian, Digraph-based models for automated HAZOP analysis, Reliab Eng Syst Saf 33(49) (1995), 33–49.

M.L. Wald, The blackout that exposed the flaws in the grid, New York Times, 11 November 2013, http://www.nytimes.com/2013/11/11/booming/the-blackout-that-exposed-the-flaws-in-the-grid.html?pagewanted = all&_r = 0, accessed October 1, 2014.

P. Weber and L. Jouffe, Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN), Reliab Eng Syst Saf 91(2) (2006), 149–162.

WEC, Building resilience in supply chains, World Economic Forum, 2013, http://www.weforum.org/reports/building-resilience-supply-chains, accessed October 1, 2014.

B.E. White, Fostering intra-organizational communication of enterprise systems engineering practices, *National Defense Industrial Association (NDIA) 9th Annual Systems Engineering Conference*, San Diego, CA, 23–26 October, 2006.

J.C. Whitson and J.E. Ramirez-Marquez, Resiliency as a component importance measure in network reliability. Reliab Eng Syst Saf 94(10) (2009), 1685–1693.

X.-L. Xu, Y.-Q. Qu, S. Guan, Y.-M. Jiang, and D.-R. He, Interconnecting Bilayer Networks, Europhys Lett 93(6), (2011), 68002-p1–68002-p6.

W.J. Zhang and Y. Lin, On the principle of design of resilient systems—Application to enterprise information systems, Enterp Inform Syst 4(2) (2010), 99–110.

E. Zio and E. Ferrario, A framework for the system-of-systems analysis of the risk for a safety-critical plant exposed to external events, Reliab Eng Syst Saf 114, (2013), 114–125.

C.W. Zobel, Representing perceived tradeoffs in defining disaster resilience, Decis Support Syst 50(2) (2011), 394–403.

Payuna Uday was a doctoral student in the School of Aeronautics and Astronautics at Purdue University. Her research focused on studying and designing resilience in system-of-systems. After graduating, she entered the aviation consulting industry. She holds a B. Tech. in electronics and communication engineering from the National Institute of Technology in Trichy, India. She received her master's degree from Purdue University and her research involved evaluating the environmental mitigation potential of operational changes in aviation.

Karen Marais is an Associate Professor in the School of Aeronautics and Astronautics at Purdue University. Her research interests include risk assessment and environmental impacts analysis of complex socio-technical systems in general, and aerospace systems in particular. She holds a B. Eng. in electrical and electronic engineering from the University of Stellenbosch and a B.Sc. in mathematics from the University of South Africa. She also holds a master's degree in space-based radar from MIT. She received her Ph.D. from the Department of Aeronautics and Astronautics at MIT in 2005.