Paper #168

Systems Architecting for Survivability: Limitations of Existing Methods for Aerospace Systems

Matthew G. Richards **Daniel E. Hastings**
Donna H. Rhodes **Annalisa L. Weigel**

Massachusetts Institute of Technology
77 Massachusetts Ave. 41-205, Cambridge, MA 02139
Corresponding author's email: mgr@mit.edu

Abstract

Survivability may be defined as the ability of a system to minimize the impact of a finite disturbance on value delivery. This paper reviews existing methods of specifying, evaluating, and verifying survivability for aerospace systems in order to identify opportunities for improvement. First, the systems architecting methods underlying this research are described. Second, survivability challenges within the domain of space system architecture are analyzed for motivation. Third, five limitations of existing methods are discussed: (1) treatment of survivability as a constraint on design, (2) static system threat assessment reports, (3) assumption of independent disturbance encounters, (4) narrow scope of survivability design and analysis, and (5) lack of a value-centric perspective. In conclusion, prescriptions are offered for improving the practice of systems architecting for survivability.

Research Context: System Architecture and Value-Based Design

This paper describes ongoing doctoral research for improving the practice of systems architecting for aerospace systems (Richards, Hastings *et al*. 2007). A standard definition of architecture used by the Department of Defense (2003) is "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time." The process of creating and building architectures is referred to as systems architecting and concerns itself most with system conceptualization, objective definition, and certification for use (Maier and Rechtin 2002).

Within systems architecting, the research is focused on the application of value-based methods to conceptual design. Value, a subjective measure of benefit from a bundle of consequences that is specified by a stakeholder, provides a fundamental metric for relating system properties to desired stakeholder outcomes (Keeney 1992). Empirical evidence suggests that the lifecycle value delivered by systems is primarily determined at the beginning of development programs (Gruhl 1992), highlighting the criticality of good decision making during conceptual design. Conceptual design includes both concept development (*i.e.*, identification of stakeholders, enumeration and evaluation of design alternatives, and selection of one or more concepts for further development) and system-level design (*i.e.*, definition of the architecture, including subsystem decompositions and functional specifications) (Ulrich and Eppinger 2004). Taking the value-centric perspective during conceptual design empowers decision makers to

rigorously evaluate and compare different system concepts in the technical domain (*e.g.*, geosynchronous satellite vis-à-vis low-Earth orbit satellite constellation for a communications mission) using a unifying set of attributes in the value domain (*e.g.*, signal isolation, information rate, information integrity, and data availability) (Shaw, Miller and Hastings 2001).

The value-centric perspective is operationalized in conceptual design through the application of decision theory (*e.g.*, multi-attribute utility theory[1]) to the engineering design process—making cost-benefit tradeoffs explicit in concept selection (Thurston 1990; Keeney and Raiffa 1993). Extending traditional trade studies, which may consider a small number of alternative designs, tradespace exploration builds on this application by adding computer-based parametric models and simulations, enabling comparison of hundreds or thousands of potential architectures (McManus, Hastings and Warmkessel 2004; Ross, Hastings *et al*. 2004). Tradespace exploration avoids the limits of local point solution trades by providing an understanding of the underlying relationship between the decision maker preference structure and potential designs. Applied to system architecture development, tradespace exploration may be used as a quantitative tool for evaluating the benefits, costs, and risks of alternative architectures—informing critical front-end decision making. In addition to evaluating potential technical capabilities, architecture tradespaces may also be used to explore the implications of policy uncertainties (Weigel and Hastings 2004) and changing value perceptions (Ross 2006).

Given that non-traditional design criteria—such as flexibility and robustness, collectively referred to as "ilities"—are increasingly regarded as critical system properties for delivering stakeholder value (Rhodes 2004; McManus and Hastings 2006), ongoing systems engineering research is seeking to establish descriptive taxonomies and prescriptive methods for the incorporation of the ilities in system design (de Weck, de Neufville and Chaize 2004; Fricke and Schulz 2005; Rajan, Van Wie *et al*. 2005; Ross 2006; McManus, Richards *et al*. 2007; Nilchiani and Hastings 2007; Silver and de Weck 2007). Ilities may be defined as temporal system properties that specify the degree to which systems are able to maintain or even improve function in the presence of change.[2] The ilities explicitly recognize that, in addition to meeting requirements in a static context, the performance of system architectures is defined by an ability to deliver value to stakeholders in the presence of changing operational environments, economic markets, and technological developments (Fricke and Schulz 2005). Despite general agreement on their importance, the ilities are neither well-defined nor easily evaluated in isolation.[3] Operationalizing the ilities for value-based design methods such as tradespace exploration is

[1] As a decision aid for multi-criteria assessment of alternatives, multi-attribute utility theory (MAUT) provides a construct for assessing values and subjective probabilities of individuals in the presence of risk or uncertainty (Dyer, Fishburn et al. 1992). Founded upon mathematical theory for utility models (Keeney and Raiffa 1993), MAUT's logical consistency is coupled with a variety of assessment techniques that address the limited cognitive abilities of decision makers. As normative theory that focuses on how decisions ought to be made, MAUT's potential is implicitly recognized by descriptive theories that characterize human decision making (in the absence of such methodological structure) in terms of heuristics and biases (Tversky and Kahneman 1974) as well as bounded rationality (Gigerenzer and Goldstein 1996; Simon 1996).

[2] This excludes some non-operational ilities, such as manufacturability, that affect the design of the system but not its operation.

[3] Recognizing that design navigates among functional, physical, and environmental domains (Simon 1996), McManus and Richards et al. (2007) developed the "Ility Space" to characterize the operational ilities as temporal motion along three axes: needs (*i.e.*, value domain), system (*i.e.*, technical domain), and context (*i.e.*, environmental domain).

challenging[4] and the subject of ongoing research. For example, after building a descriptive theory of the systems property of changeability, Ross (2006) developed a prescriptive dynamic tradespace methodology with the associated metrics of Pareto Trace and Filtered Outdegree. In an attempt to improve and build upon the existing theory of changeability, this ongoing research on system survivability focuses on particular challenges posed by dynamic disturbance environments and on how survivability might be better articulated, evaluated, and implemented during the conceptual design of aerospace systems.

Research Motivation: Space System Complexity Has Bred Fragility

"Our spacecraft, which take 5 to 10 years to build, and then last up to 20 in a static hardware condition, will be configured to solve tomorrow's problems using yesterday's technologies." (Brown 2007).

A typical space system architecture is comprised of one or more satellites, launch vehicle(s) for transportation to operating orbits, ground-based control stations, and communications links among these nodes to transfer information to end users. With the exception of select civil space systems such as the Hubble Space Telescope and International Space Station that employ on-orbit servicing, current satellite architectures aim to deliver value over time by developing reliable individual space vehicles that operate in an inaccessible, hostile environment. As a result, attempts to apply flexibility and other ilities to space systems are tightly constrained by the lack of capability to physically service satellites following launch.[5] A distinguishing characteristic of the current U.S. space architecture is a high level of risk aversion stemming from the high cost of space systems combined with the criticality of space mission areas (on the government side) and drive for investor return (on the commercial side). This environment has driven satellite designers toward three common design strategies: redundancy, proven technology, and long operational lives (Long, Richards and Hastings 2007).

The high cost of launching spacecraft combined with a focus on traditional strategic measures of effectiveness in the space industry (*e.g.*, optimize cost-per-function) has driven U.S. space architecture from an era of single-payload, short-lived spacecraft to a current state of multi-payload, long-lived systems. For example, the average design life of active geosynchronous satellites grew from under two years in 1965 to over thirteen years in 2003 (Sullivan 2005). While this design philosophy is justified on the basis on economic arguments associated with the high initial cost of spacecraft and enabled by improvements in supporting subsystems (*e.g.*, ion propulsion), this design philosophy also has many negative implications. For example, noting that space system developments now take five to ten years, Brown (2007) describes how "complexity has bred fragility" in terms of unanticipated modes of failure. Such unanticipated modes of failure include an acquisitions crisis (Young, Hastings and Schneider 2003) where development problems with an individual sensor can cripple the schedule and budget of multi-payload programs (*e.g.*, the National Polar-Orbiting Environmental Satellite System), software-related common-cause failures that circumvent margin and redundancy (Leveson 2004), and uncertain technological change.[6] The consequences of failure for space

[4] Two key challenges make the ilities difficult to represent in a classic tradespace: (1) representation of temporal properties in a static construct and (2) axiomatic restrictions on the incorporation of the ilities in attribute sets (*i.e.*, attributes need to be perceived as independent, yet the ilities are defined by attribute performance over time).

[5] Software uplinks are one enabler of change that is not dependent on physical accessibility.

[6] One downside of long design lifetimes is the inability to update space-based capabilities with modern avionics in a timely manner during an era dictated by "Moore's Law" (*i.e.*, the doubling of processing speed of new computer

architecture reliant upon integral, long-lived satellites is further exacerbated by the growth of military and commercial dependency on space systems (GAO 2002; Ballhaus 2005), identified vulnerabilities in the current architecture (Rumsfeld, Andrews *et al*. 2001), the proliferation of threats (Wilson 2001; Covault 2007), and the weakening of the sanctuary view in military space policy (Mowthorpe 2002; U.S. 2006).

Given that the need to address space architecture fragility has been articulated by national leaders, a critical challenge arises: how best to enhance the survivability of space architecture? For example, are existing satellite survivability practices of hardening individual satellites or constellations applicable to these problems? To what extent might architectural agility be emphasized to address the mismatch between rapidly changing environments and the 15-25 year generational turnover of satellites (GAO 2006)? These questions, as well as insights from survivability engineering and related disciplines, are addressed in the following section.

Existing Responses: Limitations of Current Survivability Methods

"The current state of practice in survivability and security evaluation tends to treat systems and their environments as static and unchanging. However, the survivability and security of systems in fact degrade over time as changes occur in their structures, configurations, and environments, and as knowledge of their vulnerabilities spreads…." (Ellison, Fisher et al. 1999)

Survivability is defined by system engineers as "the capability of a system to avoid or withstand hostile natural and manmade environments without suffering abortive impairment of its ability to accomplish its designated mission" (USAF 2005). Primarily specified as a requirement in military systems (JTCG/AS 2001), survivability is an increasingly important attribute of all aerospace systems which must be robust to environments characterized by system-threatening hazards (GAO 2002). While disturbances may originate from a wide range of man-made and natural environments, a universal challenge confronting system architects is the specification, development, procurement, operation, and maintenance of systems with critical survivability requirements (Neumann 2000). Established disciplines related to survivability engineering include safety engineering (Leveson 1995; Leveson 2002), security engineering[7] (Yurick and Doss 2002), and reliability engineering[8] (Pate-Cornell 1984). Related emerging disciplines include resilience engineering[9] (Sheffi 2005; Hollnagel, Woods and Leveson 2006) and systems assurance[10] (Baldwin, Komaroff and Croll 2006). Safety, defined as "freedom from

---

chips every 18-24 months). This slowdown of the space industry's "clockspeed" limits the agility of satellite operators in capturing emergent terrestrial markets.

[7] Reliability is defined as the probability that a component will perform its intended function "for a prescribed time and under stipulated environmental conditions" (Leveson 1995). Reliability engineering is considered with internal component failures while survivability is considered with external system disturbances.

[8] Security may be defined as "a *system* property that implies protection of the informational, operational, and physical elements from malicious intent" (Laracy and Leveson 2007). Although both disciplines are concerned with hostile malevolent environments, survivability is distinguished from security by excluding threats internal to the system boundary while including hostile natural environments. In addition, enablers of survivability include not only resistance to attack but also robustness under attack and recovery efforts (Ellison, Fisher et al. 1999).

[9] Resilience may be defined as "the ability of a system or organization to react to and recover from disturbances at an early stage, with minimal effect on the dynamic stability" (Hollnagel, Woods and Leveson 2006). Resilience is one enabler of increasing the survivability of systems.

[10] Systems assurance has been defined as "the level of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system" (Baldwin, Komaroff and Croll 2006). While systems assurance is focused on the challenge of validating software

accidents or losses," is perhaps the discipline most closely linked to survivability in that both disciplines seek to minimize hazards *(i.e.*, system and environmental states which will lead to losses) (Leveson 1995). However, whereas the hazards addressed by system safety encompass a broad spectrum of system failures (*e.g.*, from operator errors and component failures to flawed software design, dysfunctional component interactions, and unsafe organizational evolution) that emerge from the interaction of a system with its environment (Leveson 2002), the disturbances considered by survivability are all exogenous to the system and consist of both naturally-occurring and man-made hostile environments (Ball and Atkinson 2006).

Survivability research stems from a long history of naval architecture that sought to prevent the loss of ships from sustained damage and to save lives in the event of a ship sinking (Yurick and Doss 2002). Modern research on survivability engineering is an outgrowth of experience in the First and Second World Wars and became a formal discipline in the domain of combat aircraft. Ball and Atkinson (1995) document the history of combat aircraft survivability engineering from the 1940's to the present day. While the importance of survivability was recognized during the Second World War (*e.g.*, eight major design evolutions made to the B-17 "Flying Fortress" between 1942 and 1945 to enhance survivability), survivability was not specified as a formal design requirement by the military for another 25 years. Before the systems approach for survivability engineering existed, enhancements were made within the context of individual aircraft design disciplines and subsystems (*e.g.*, structures made more resistant to enemy fire, guns and missiles added for self-defense) and relied on combat experience to adapt designs to more survivable states. Following the loss of 5,000 aircraft by the U.S. military in Southeast Asia between 1963 and 1973, the importance of the survivability of military aircraft increased dramatically, and a formal discipline emerged to support the integrated specification, design, and assessment of highly survivable systems (Ball and Atkinson 1995).

In *The Fundamentals of Aircraft Combat Survivability Analysis and Design*, Ball (2003) describes the current state-of-the-art in survivability engineering. Design for survivability involves two elements (1) increasing the ability of systems to avoid disturbances (*i.e.*, reduce susceptibility) and (2) increasing the ability of systems to withstand disturbances (*i.e.*, reduce vulnerability). During the conceptual design of military aerospace systems today, a System Threat Assessment Report (STAR) is issued by a service intelligence agency as an estimate of the operational, physical, and technological environment in which the system is expected to function. The STAR is the authoritative document from which survivability requirements are derived—specifying threat force levels as well as enemy doctrine, strategy, and tactics. Following issuance of the STAR, survivability assessments of design alternatives are performed at the engagement, mission, and campaign levels. For example, at the engagement level, the probability of an aircraft surviving a one-on-one engagement from a single shot from a single weapon is calculated using an event tree. Five probability assignments are used to assess system susceptibility—P[weapon is active], P[sensor detects], P[fire control solution is obtained], P[weapon intercepts], P[weapon hits]—and one probability assignment is used to assess system vulnerability—P[weapon hit disrupts critical components]. The probability of surviving the engagement is computed as the complement of the joint probability of these six assigned values. This same process is applied at the mission and campaign level by allowing multiple shots from multiple weapons. In order to abstract away the complexity associated with dependent shot

---

security in military systems given the complex, international supply webs characteristic of all modern information systems, survivability engineering is focused on the design of systems robust to operational disturbances.

outcome probabilities (*e.g.*, increased aircraft susceptibility and vulnerability if one of an aircraft's four engines is destroyed by a previous engagement), independent shot outcomes are assumed. The reliance of Ball's methodology on probabilistic risk assessment (Bedford and Cooke 2001) for combat aircraft is shared by the threat evaluation methodology for satellites documented in the U.S. Air Force Space and Missile Systems Center's *Systems Engineering Primer and Handbook* (USAF 2005).

From a value-based design perspective, the current principles and methods governing the articulation of survivability in aerospace system conceptual design are inadequate along several dimensions. In particular, five limitations are found: (1) treatment of survivability as a constraint rather than an active trade in the design process, (2) static nature of system threat assessment reports despite changing operational environments, (3) reliance on probabilistic risk assessment and its underlying assumptions, (4) limited scope of survivability design and analysis, and (5) inability to consider alternative value-delivery mechanisms.

Treatment of survivability as a constraint. The first limitation, the treatment of survivability as a constraint rather than an active trade in the design process, reduces the design space available to designers before conceptual design has even begun. While specifying a minimum level of survivability may be appropriate for the design of piloted aircraft, the wisdom of specifying survivability as a constraint on the design of unmanned aerial vehicles and satellites *a priori* is less clear because survivability versus quantity trade-offs may reveal more valuable system designs (Jeffcoat 2003). Since the beginning of the space era, incorporating survivability as a parameter in system-level trade studies (*e.g.*, with lifecycle cost and stakeholder utility) has proven challenging. The first reconnaissance satellite program, CORONA,[11] provides a revealing example (Wheelon 1997). Fearing the vulnerability of CORONA satellites to attack by the Soviet Union, a wide range of defensive measures were examined by the Central Intelligence Agency (CIA), including inflating and deploying decoy balloons and orbit-adjust maneuvers (Wheelon 1965). However, CORONA protection was never implemented because of the payload weight required, mutual forbearance towards space warfare (once the Soviets developed their own reconnaissance capabilities), and an inability to trade film weight (*i.e.*, performance) with survivability measures.

Static threat assessment reports. The second limitation of existing survivability methods is attributed to the static nature of the System Threat Assessment Report. Upheld as the authoritative description of a system's operational hazards and the document from which survivability requirements are derived, the STAR suffers from the potential for obsolescence before system end-of-life. For example, the life span of a combat aircraft from program inception (when the STAR is issued) to removal from service might stretch beyond 50 years (Ball 2003). A similar disconnect exists for space system design given the long gestation period and operational life of satellites. Furthermore, practitioners admit that "selected operational scenarios are not likely to truly represent future conflicts," "unanticipated technological developments will affect combat operations," and "adversaries in real conflicts will adapt to our capabilities in unanticipated ways" (Anderson and Williamsen 2007). Given that survivability is an inherently dynamic property (Ellison, Fisher *et al*. 1999), it is troubling that current methods rely on static assumptions.

[11] The CORONA program refers to a series of 145 photo reconnaissance satellites launched to low Earth orbit between 1960 and 1972, providing the "backbone of US intelligence capability for 12 precarious years" (Wheelon 1997).

Assumption of independent disturbance encounters. Negative implications of the third limitation—relying on probabilistic risk assessment (PRA) and its underlying assumptions—have been well-documented in the system safety literature (Leveson 1995; Leveson 2002). The fundamental issue with PRA is that, although it is intended as a systematic methodology to measure risk in complex systems, two of its key underlying assumptions (in practice) may not hold for complex systems: that all probability distributions are known and that system components are independent (Harper, Thornton and Szygenda 2007). In *Normal Accidents*, Perrow (1999) finds that failures may also arise from unanticipated, dysfunctional interactions among components and then subsequently be exacerbated by the rapid propagation of local failures due to tight coupling in complex systems. These findings are consistent with the system safety literature which points out additional flaws, such as the limits of redundancy given common-cause failures (Pate-Cornell, Dillon and Guikema 2004); problems with using historical data as a representative sample of current failure probabilities; and narrow focus of PRA on immediate physical failures (Leveson 2002). These criticisms of PRA are equally valid for existing survivability engineering methods (Ball 2003) that assume linear, independent weapon encounters despite the existence of nonlinear, dependent failure modes.

Narrow scope of survivability design and analysis. The fourth limitation is the limited scope of survivability design and analysis. Since survivability engineering was established as a formal design discipline in the 1960's, a tremendous amount of progress has been made to improve the survivability of individual elements in aerospace system architecture (Nordin and Kong 1999; Paterson 1999). Less progress has been made at the architecture-level where systems tend to evolve in an ad-hoc manner—accommodating constraints from legacy systems and forming temporary coalitions to support emergent missions.[12] More generally, architecting for survivability is a poorly understood, socio-technical issue, increasingly relevant to all engineering systems. For example, despite the recognized criticality of low-probability, high-consequence events (Leveson 1995; Sheffi 2005), modeling these events, evaluating the benefits of protective measures, and internalizing the role of operational behavior, human factors, and supporting infrastructures is the subject of ongoing research (Leveson, Daouk *et al.* 2004). Furthermore, existing models of highly survivable system architecture from the Cold War (*e.g.*, Nuclear Command and Control System) are not readily applied given the virtually unlimited resources allocated to such systems in that era. In analyzing the shortcomings of current methods for the specification, development, procurement, operation, and maintenance of systems and networks with critical survivability requirements, Neumann (2000) succinctly describes the state of the discipline:

> *"The currently existing evaluation criteria frameworks are not yet comprehensively suitable for evaluating highly survivable systems and networks.... There is almost no experience in evaluating systems having a collection of independent criteria that might contribute to survivability...." (Neumann 2000)*

In the space domain, the need for a comprehensive survivability architecture is particularly critical given the interdependencies among spacecraft, ground stations, and communications links (Shellans and Matoush 1992). However, existing design and analysis methodologies

[12] For example, a host of integration problems occurred during Desert Storm as satellite systems were deployed for the first time in support of tactical operations in a large-scale conflict. Older platforms were used for missions for which they were not designed, including strategic missile-warning satellites for Scud detection (Spires 2001).

address survivability at only the satellite or constellation level rather than higher levels in the system architecture (*e.g.*, Air Force mission area).

Lack of a value-centric perspective. The fifth limitation of existing survivability design methodologies is the lack of a value-centric perspective. Success of a system is dependent on how much value it is perceived to deliver to its stakeholders. Value, in this sense, is considered to be synonymous with net benefit (*i.e.*, received benefits less costs for receiving those benefits). Unless the stakeholders care about the mechanism by which value is delivered, which is rare, the system is free to deliver value by many possible means. In terms of survivability, utilization of value as a unifying metric may also enable evaluation of protection measures at various levels in the system architecture (*e.g.*, explore cost-benefit tradeoff of increasing hardness of individual satellite *vis-à-vis* investing in reconstitution capability). Taking the value-centric perspective, system designers are freed to consider multiple paths to achieve the same value delivery (Ross 2006). This is particularly useful for considering survivability issues when original value delivery mechanisms may be blocked due to a disturbance.

Conclusion

In addition to meeting requirements in a static context, the performance of system architectures is increasingly defined by an ability to deliver value to stakeholders in the presence of changing operational environments, economic markets, and technological developments. As temporal system properties that reflect the degree to which systems are able to maintain or even improve function in the presence of change, the ilities constitute a rich research area for improving value delivery over the lifecycle of systems. Applicable across engineering domains, the ilities are particularly critical to aerospace systems which are characterized by high cost, long lifecycles, high complexity, interdependencies with other systems, and dynamic operational contexts. Although survivability is an emergent system property that arises from interactions among components and between a system and its environment, conventional approaches to survivability engineering are often reductionist in nature (*i.e.*, focused only on selected properties of subsystems or modules in isolation). Furthermore, existing survivability engineering methodologies are normally based on domain-specific operating scenarios and presupposed disturbances rather than a general theory with indeterminate threats. As a result, current methods do not allow system architects to communicate trades among cost, utility, and survivability to senior decision makers.

Given the limitations of existing survivability design methods for aerospace systems (*i.e.*, treatment of survivability as a constraint on design, static system threat assessment reports, assumption of independent weapon encounters, limited scope, and exclusive focus on physical integrity), there is a need for a design method that (1) incorporates survivability as an active trade in the design process, (2) captures the dynamics of operational environments over the entire lifecycle of systems, (3) captures path dependencies of system susceptibility and vulnerability to disturbances, (4) extends in scope to architecture-level survivability assessments, and (5) takes a value-centric perspective to allow alternative value-delivery mechanisms in the tradespace. Recent research on how decision makers can recognize and evaluate dynamically relevant designs, including Multi-Attribute Tradespace Exploration (Ross, Hastings *et al.* 2004) and Epoch-Era Analysis (Ross 2006), offers a theoretical foundation for the development of an improved design methodology for survivability.

Acknowledgements

Funding for this work was provided by the Systems Engineering Advancement Research Initiative (SEAri) at the Massachusetts Institute of Technology (MIT). Positioned within MIT's Engineering Systems Division (ESD), SEAri (http://seari.mit.edu) brings together a set of sponsored research projects and a consortium of systems engineering leaders from industry, government, and academia. SEAri gratefully acknowledges the support of MIT's Program on Emerging Technologies (PoET), an interdisciplinary research effort of the National Science Foundation.

References

Anderson, T. and J. Williamsen (2007). "Force Protection Evaluation for Combat Aircraft Crews." *48th AIAA Structures, Structural Dynamics, and Materials Conference*, Honolulu, HI.

Baldwin, K., M. Komaroff and P. Croll (2006). "Systems Assurance - Deliverying Mission Success in the Face of Developing Threats." *A White Paper from NDIA Systems Assurance Committee*.

Ball, R. (2003). The Fundamentals of Aircraft Combat Survivability Analysis and Design. Reston, American Institute of Aeronautics and Astronautics.

Ball, R. and D. Atkinson (1995). "A History of the Survivability Design of Military Aircraft." *36th AIAA Structures, Structural Dynamics and Materials Conference*, New Orleans, LA.

Ball, R. and D. Atkinson (2006). "Designing for Survivability." *Aircraft Survivability,* Fall 2006: 26-29.

Ballhaus, W. (2005). "Successes and Challenges in Transforming National Security Space." *43rd Aerospace Sciences Meeting*, Reno, NV.

Bedford, T. and R. Cooke (2001). Probabilistic Risk Analysis: Foundations and Methods. Cambridge, Cambridge University Press.

Brown, O. (2007). "Speech by Dr. Owen Brown on Fractionated Spacecraft." Anaheim, CA.

Covault, C. (2007). "Space Control: Chinese anti-satellite weapon test will intensify funding and global policy debate on the military uses of space." *Aviation Week and Space Technology*, 22 January 2007, pp. 24-25.

de Weck, O., R. de Neufville and M. Chaize (2004). "Staged Deployment of Communications Satellite Constellations in Low Earth Orbit." *Journal of Aerospace Computing, Information, and Communication,* 1(3): 119-136.

DoD (2003). "Department of Defense Architecture Framework: Version 1.0." *DoD Architecture Framework Working Group*.

Dyer, J., P. Fishburn, R. Steuer, J. Wallenius and S. Zionts (1992). "Multiple Criteria Decision Making, Multiattribute Utility Theory: The Next Ten Years." *Management Science,* 38(5): 645-654.

Ellison, R., D. Fisher, R. Linger, H. Lipson, T. Longstaff and N. Mead (1999). "Survivable Network Systems: An Emerging Discipline." *Carnegie Mellon Software Engineering Institute*.

Fricke, E. and A. Schulz (2005). "Design for Changeability (DfC): Principles to Enable Changes in Systems Throughout Their Entire Lifecycle." *Systems Engineering,* 8(4): 342-359.

GAO (2002). "Critical Infrastructure: Commercial Satellite Security Should Be More Fully Addressed." *Report to U.S. Senate, Government Accounting Office*.

GAO (2006). "Space Acquisitions: DoD Needs a Departmentwide Strategy for Pursuing Low-Cost, Responsive Tactical Space Capabilities." *U.S. Government Accountability Office*. Report

to the Chairman, Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives, GAO-06-449, March 2006.
Gigerenzer, G. and D. Goldstein (1996). "Reasoning the Fast and Frugal Way: Models of Bounded Rationality." *Psychological Review,* 103(4): 650-669.
Gruhl, W. (1992). "Lessons Learned, Cost/Schedule Assessment Guide." *Internal presentation*, NASA Comptroller's Office.
Harper, M., M. Thornton and S. Szygenda (2007). "Disaster Tolerant Systems Engineering for Critical Infrastructure Protection." *1st IEEE Systems Conference*, Honolulu, HI.
Hollnagel, E., D. Woods and N. Leveson (2006). Resilience Engineering: Concepts and Precepts. Hampshire, UK, Ashgate.
Jeffcoat, D. (2003). "The Survivability Versus Quantity Trade-Off for Unmanned Aerial Vehicles." *2nd AIAA Unmanned Systems Conference*, San Diego, CA.
JTCG/AS (2001). Aerospace Systems Survivability Handbook. Arlington, VA, Joint Technical Coordinating Group on Aircraft Survivability.
Keeney, R. (1992). Value-Focused Thinking: A Path to Creative Decisionmaking. Cambridge, Harvard University Press.
Keeney, R. and H. Raiffa (1993). Decisions with Multiple Objectives: Preferences and Value Tradeoffs. Cambridge, Cambridge University Press.
Laracy, J. and N. Leveson (2007). "Applying STAMP to Critical Infrastructure Protection." *IEEE Conference on Technologies for Homeland Security*, Boston, MA.
Leveson, N. (1995). Safeware: System Safety and Computers. Boston, Addison-Wesley.
Leveson, N. (2002). System Safety Engineering: Back to the Future. Cambridge, MIT Department of Aeronautics and Astronautics.
Leveson, N. (2004). "Role of Software in Spacecraft Accidents." *Journal of Spacecraft and Rockets,* 41(4).
Leveson, N., M. Daouk, N. Dulac and K. Marais (2004). "A Systems Theoretic Approach to Safety Engineering." *MIT Engineering Systems Symposium*, Cambridge, MA.
Long, A., M. Richards and D. Hastings (2007). "On-Orbit Servicing: A New Value Proposition for Satellite Design and Operation." *Journal of Spacecraft and Rockets,* 44(4): 964-976.
Maier, M. and E. Rechtin (2002). The Art of Systems Architecting. Boca Raton, CRC Press.
McManus, H. and D. Hastings (2006). "A Framework for Understanding Uncertainty and its Mitigation and Exploitation in Complex Systems." *IEEE Engineering Management Review,* 34(3): 81-94.
McManus, H., D. Hastings and J. Warmkessel (2004). "New Methods for Rapid Architecture Selection and Conceptual Design." *Journal of Spacecraft and Rockets,* 41(1): 10-19.
McManus, H., M. Richards, A. Ross and D. Hastings (2007). "A Framework for Incorporating "ilities" in Tradespace Studies." *AIAA Space 2007*, Long Beach, CA.
Mowthorpe, M. (2002). "US Military Space Policy 1945-92." *Space Policy,* 18(1): 25-36.
Neumann, P. (2000). "Practical Architectures for Survivable Systems and Networks." *Prepared by SRI International for the U.S. Army Research Laboratory*.
Nilchiani, R. and D. Hastings (2007). "Measuring the Value of Flexibility in Space Systems: A Six-Element Framework." *Systems Engineering,* 10(1): 26-44.
Nordin, P. and M. Kong (1999). Chapter 8.2 Hardness and Survivability Requirements. Space Mission Analysis and Design. El Segundo, Microcosm Press.
Pate-Cornell, M. (1984). "Fault Trees vs. Event Trees in Reliability Analysis." *Risk Analysis,* 4(3): 177-186.

Pate-Cornell, M., R. Dillon and S. Guikema (2004). "On the Limitations of Redundancies in the Improvement of System Reliability." *Risk Analysis,* 24(6): 1423-1436.
Paterson, J. (1999). "Overview of Low Observable Technology and Its Effects on Combat Aircraft Survivability." *Journal of Aircraft,* 36(2): 380-388.
Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies. Princeton, Princeton University Press.
Rajan, P., M. Van Wie, M. Campbell, K. Wood and K. Otto (2005). "An Empirical Foundation for Product Flexibility." *Design Studies,* 26(4): 405-438.
Rhodes, D. (2004). "Report on Air Force/LAI Workshop on Systems Engineering for Robustness." Arlington, VA.
Richards, M., D. Hastings, D. Rhodes and A. Weigel (2007). "Defining Survivability for Engineering Systems." *5th Conference on Systems Engineering Research*, Hoboken, NJ.
Ross, A. (2006). "Managing Unarticulated Value: Changeability in Multi-Attribute Tradespace Exploration." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.
Ross, A., D. Hastings, J. Warmkessel and N. Diller (2004). "Multi-Attribute Tradespace Exploration as Front End for Effective Space System Design." *Journal of Spacecraft and Rockets,* 41(1): 20-28.
Rumsfeld, D., D. Andrews, R. Davis, H. Estes, R. Fogleman, J. Garner, W. Graham, C. Horner, D. Jeremiah, T. Moorman, D. Necessary, G. Otis and M. Wallop (2001). "Report of the Commission to Assess United States National Security Space Management and Organization."
Shaw, G., D. Miller and D. Hastings (2001). "Development of the Quantitative Generalized Information Network Analysis Methodology for Satellite Systems." *Journal of Spacecraft and Rockets,* 38(2): 257-269.
Sheffi, Y. (2005). The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. Cambridge, The MIT Press.
Shellans, M. and W. Matoush (1992). "Designing Survivable Space Systems." *Aerospace America*, 38.
Silver, M. and O. de Weck (2007). "Time-Expanded Decision Networks: A Framework for Designing Evolvable Complex Systems." *Systems Engineering,* 10(2): 167-186.
Simon, H. (1996). The Sciences of the Artificial. Cambridge, The MIT Press.
Spires, D. (2001). Horizons: A Half Century of Air Force Space Leadership. Maxwell Air Force Base, Air University Press.
Sullivan, B. (2005). "Technical and Economic Feasibility of Telerobotic On-Orbit Satellite Servicing." Doctoral dissertation, Department of Aerospace Engineering, University of Maryland, College Park, MD.
Thurston, D. (1990). "Multiattribute Utility Analysis in Design Management." *IEEE Transactions on Engineering Management,* 37(4): 296-301.
Tversky, A. and D. Kahneman (1974). "Judgement Under Uncertainty: Heuristics and Biases." *Science,* 185(4157): 1124-1131.
U.S. (2006). "U.S. National Space Policy." *White House Office of Science and Technology Policy, Released 31 August.*,
Ulrich, K. and S. Eppinger (2004). Product Design and Development. Boston, McGraw Hill.
USAF (2005). "SMC Systems Engineering Primer and Handbook." *Space & Missile Systems Center, U.S. Air Force*.

Weigel, A. and D. Hastings (2004). "Measuring the Value of Designing for Future Downward Budget Instabilities." *Journal of Spacecraft and Rockets,* 41(1): 111-119.

Wheelon, A. (1965). "Vulnerability of the CORONA System to Soviet Countermeasures." Memo to the Director of Central Intelligence, 16 September 1965.

Wheelon, A. (1997). "CORONA: The First Reconnaissance Satellites." *Physics Today*, February 1997, pp. 24-30.

Wilson, T. (2001). "Threats to United States Space Capabilities." prepared for the Commission to Assess United States National Security Space Management and Organization, January 2001.

Young, T., D. Hastings and W. Schneider (2003). "Report of the Defense Science Board / Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs." *Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics*. Washington, DC.

Yurick, W. and D. Doss (2002). "A Survivability-Over-Security (SOS) Approach to Holistic Cyber-Ecosystem Assurance." *IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY.

Biographies

Matthew Richards is a graduate student at MIT pursuing a Ph.D. in Engineering Systems. As a research assistant for SEAri, his current research is focused on survivable system architecture, value-robust design, and tradespace exploration of complex systems. Matt's work experience includes Mars rover mission design at the Jet Propulsion Laboratory (JPL) and systems engineering support on two autonomous vehicle programs for the Defense Advanced Research Projects Agency. From MIT, Matt has B.S. and M.S. degrees in Aerospace Engineering (2004, 2006) and an M.S. degree in Technology and Policy (2006).

Daniel Hastings is a Professor of Aeronautics and Astronautics and Engineering Systems at MIT. Dr. Hastings has taught courses and seminars in plasma physics, rocket propulsion, advanced space power and propulsion systems, aerospace policy, technology and policy, and space systems engineering. He served as chief scientist to the U.S. Air Force from 1997 to 1999, as director of ESD from 2004 to 2005, and is a former chair of the Air Force Scientific Advisory Board. Dr. Hastings is a Fellow of the International Council on Systems Engineering (INCOSE).

Donna Rhodes is a Senior Lecturer and Principal Research Scientist in ESD. Previously, Dr. Rhodes held senior management positions in several corporations. She is a co-founder of SEAri, directing its research program and advising graduate students. Dr. Rhodes is a Past President, Fellow, and Founder of INCOSE, and director of the SEANET doctoral student network. She has published numerous papers in the field of systems engineering. Her research focuses on architecting and design of complex systems, systems-of-systems, and enterprises. She holds a M.S. and a Ph.D. in Systems Science from the T.J. Watson School of Engineering at Binghamton University.

Annalisa Weigel is an Assistant Professor of Aeronautics and Astronautics and Engineering Systems at MIT. Dr. Weigel's teaching and research areas are focused on space system architecture and design, systems engineering, aerospace policy, and finance. As an engineer at Adroit Systems from 1995-1998, she worked in support of the DoD Space Architect Office during its stand-up and initial space system architecture design studies in the areas of satellite communications, satellite operations, and launch on demand. After completing her Ph.D. at MIT, Dr. Weigel worked for a year as a research associate at Lehman Brothers in New York.