A Snapshot of Engineering for Resilience at APL: Guest Editor's Introduction

Timothy J. Allensworth

ABSTRACT

Today's systems are increasingly complex and interconnected and face ever more sophisticated threats to their ability to operate successfully. It is no longer enough for systems to be robust and reliable; they must also be resilient. Resilience is particularly vital for systems that provide our critical infrastructure and protect our national security and the lives of those defending it. Although reliability and risk concepts have been codified in systems engineering for decades, resilience is a relatively new concept for the systems engineering community. Because of this recent emergence, the definition of the term/concept is evolving. However, most definitions center on the ability to provide required capability in the face of adversity or disruption. Of course, this is a broad definition, and the potential applications of resilience concepts are equally broad. The articles in this issue provide a glimpse into work being done at the Johns Hopkins University Applied Physics Laboratory (APL) to develop and measure resilience approaches to ensure that our systems are able to respond to adverse events in real time, enabling them to succeed in their missions, whether on land, at sea, or in space.

INTRODUCTION

Every day we rely on systems of many sorts—from computers, phones, and the Internet of Things enabling us to quickly conduct daily tasks to vast systems of systems that protect our national assets, infrastructure, and security. These systems are becoming increasingly complex and interconnected while at the same time facing rapidly evolving engineering and external environments. We must pursue a means of balancing the traditional long-term goal of improving component reliability with the near-term goal of ensuring mission success so that our systems are better able to respond to, or bounce back from, failures as they occur in real time. Incorporating resilience into systems engineering practices expands the performance analysis framework beyond that of traditional approaches, allowing us to model and measure how our systems will respond during adverse events and ultimately improving their ability to continue performing during such events.

Concepts related to resilience—for example, reliability, robustness, redundancy—are not new in the systems engineering community. However, the last decade has seen the community coalesce around the concept of resilience and the application and formalization of resilience processes. Although the definition of resilience is evolving, in broad terms it is defined as a system's ability to provide required capability in the face of adversity. Strategies for implementing resilience are based on "avoiding, withstanding, recovering from and evolving and adapting to adversity."[1] Resilience is particularly important for DoD, NASA, the Department of Homeland Security, the National Security Agency, and other government agencies responsible for critical missions that must succeed even in the face of disruptions.

Resilience methodologies encompass reliability design considerations but also incorporate active system responses to adapt to and overcome disruptions that would otherwise cause operations to fail. When systems are able to withstand and rapidly recover from adverse events (e.g., component failure, weather, physical attacks, or cyberattacks), they can maintain critical operational functions, increasing the likelihood of overall mission success. Focusing on functionality of the full system, rather than of components, expands the set of design options to include, for example, operational resourcefulness (human interaction and autonomy) and rapid restoration that enables recovery from failures in near real time. Considering both preventing and recovering from faults strengthens the functional linkage between logistics, procedures, user training, and operational expertise on the one hand and physical systems, subsystems, and components on the other.

APL design teams are adding resilience techniques to their systems engineering toolboxes. As Fred Rosa Jr., a retired Coast Guard rear admiral and APL senior advisor for homeland security, stated, "In one way or another, 'resilience' plays into almost everything APL does."[2] This issue of the *Johns Hopkins APL Technical Digest* provides a snapshot of how Laboratory teams are developing, applying, and measuring resilience techniques to solve important systems engineering challenges across multiple domains, exploring the potential payoffs of incorporating resilience into cyber, unmanned, and autonomous systems operating everywhere from undersea to outer space.

THE ARTICLES

"Operationalizing Critical Infrastructure Resilience" considers the impacts of catastrophic events on our national critical infrastructure. Potentially catastrophic events include natural and human-caused disasters (e.g., extreme weather, earthquakes, and terrorist attacks) or disruptive forces (e.g., pandemic, financial disturbances, or cyberattacks). The authors describe an approach for achieving functional resilience by leveraging collective action principles to systematically strengthen community preparedness, response, and resourcefulness by using the resilience implementation process (RIP). The RIP is a general methodology that can help public- or private-sector stakeholders at the local, state, and national levels to operationalize resilience.

"How Would Bowditch Navigate Today? The Centuries-Old Quest for Resilience in Navigation" explores resilience in navigation, looking back to Nathaniel Bowditch, often heralded as the founder of modern maritime navigation, and his 1802 publication of *The New American Practical Navigator*. The article then reviews the modern age of GPS. The impressive reliability and accuracy of GPS appeared to solve navigation problems completely; however, recent concerns regarding its availability and integrity necessitate that resilient designs be incorporated into GPS systems. The article explores how the art and science of navigation has evolved since the time of Bowditch but at the same time is marked by many of the same challenges. It concludes by postulating how Bowditch might achieve resilience in navigation today.

The U.S. DoD has many complex systems that must remain operationally relevant for decades while satisfying multiple stakeholders with diverse preferences. As these systems reach the end of their service lives, stakeholders need a robust methodology for determining the best course of action to ensure mission success. Illustrating how resilience modeling and analysis can support critical decisions regarding acquisition and lifetime extension of complex systems, the authors of "A Hybrid Resilience Framework to Apply Stakeholder Preferences to Aircraft Fleets" describe how they adapted a resilience framework to a squadron of training aircraft. The methodology utilized a simulation of time-series functional data, generating an analytical model, to address end-of-service-life concerns for an aging system.

Reliability has been emphasized in the design of complex naval systems since World War II. A system is reliable if it has quality components that operate successfully. When failures do occur, engineers implement enhancements to the system to restore or improve the overall reliability of the system. Over the past two decades, the systems engineering community has begun integrating active approaches that enable systems to withstand and adapt to disruptions in near real time. This combination of traditional reliability and active adaptive approaches is called resilience. "Adding Resilience to Naval Systems for Mission Success" traces the development and evolution of reliability engineering as applied to complex systems, with an emphasis on naval applications. The authors examine the potential benefits of adding the ability to mitigate and adaptively respond to disruptions in near real time to increase system resilience and improve the likelihood of mission success.

Fault management is a critical element in ensuring the resilience of any complex system but is particularly important for a system like Parker Solar Probe, NASA's historic mission to "touch" the sun. Fault management can be defined as the functional requirements that enable detection, isolation, and recovery from events that upset nominal operations. Since the spacecraft is unable to maintain continuous contact with the ground control during much of its encounter with the sun, the autonomy must be resilient enough to detect and correct any faults. The article "Integrating Reliability Engineering with Fault Management to Create Resilient Space Systems" describes the expanded failure modes and effects analysis approach used to inform the development of the Parker Solar Probe spacecraft, which APL designed, built, and operates. The effort improved the development team's ability to determine critical functional failures and incorporated the responses by failure effect into the model, resulting in a more resilient spacecraft design.

Probabilistic risk assessment (PRA) helps uncover what can go wrong, how likely it is to go wrong, the consequences of the failure, and the credibility of the results presented—information leaders need to make decisions. The Nuclear Regulatory Commission has used PRA since the 1970s to quantify safety risks at nuclear power plants, and today PRA is being used in the defense, petrochemical, and offshore oil drilling industries. APL has used PRA techniques to solve challenges for many sponsors, including NASA, the Missile Defense Agency, Naval Sea Systems Command, and the U.S. Air Force. The article "Quantifying System Resilience Using Probabilistic Risk Assessment Techniques" explores system resilience as a risk proposition of the mission succeeding and applies PRA techniques developed over the past three decades to characterize design impacts on mission success. The article discusses how PRA can be applied to quantify system resilience, focusing on two aspects: scenario development and uncertainty quantification.

"Virtually Connecting Corpsmen, Providers, and Patients to Increase Readiness" describes the collaboration between engineers from APL and the Navy Bureau of Medicine and Surgery to implement a new care delivery model for active-duty service members. In this resilience application, a proof-of-concept system improving accessibility to knowledge and expertise demonstrated the ability to augment a shortage of medical professionals necessary to provide adequate care for patients, particularly in rural areas. The approach leveraged the resourcefulness and adaptability of Navy corpsmen, providing a way for them to practice and refine their skills while also providing much-needed care to patients, and then supplemented their abilities with a new connected health care system. Building on the successful initial implementation in a clinic-based environment, the next step looks to strengthen force capabilities in a field-based environment.

As mentioned, recent years have seen increasing interest in creating systems that are not only reliable but also resilient—capable of responding in real time to changes in their environment so that they can continue to operate. The authors of "Using Resilience to Inform Autonomous System Reliability Assessment: A Concept for Autonomous Ships" propose using a resilience-based engineering approach to enhance reliability analysis of complex autonomous systems. The concepts build on traditional reliability approaches, adding focus on achieving the desired performance metrics of resilience. A key consideration in evaluating a system's resilience is assessing its functional responses to unanticipated disturbances.

"Search-Based Testing Methods for Evaluating the Resilience of Autonomous Unmanned Underwater Vehicles" also describes an approach for improving the resilience of autonomous systems. This approach characterizes an unmanned underwater vehicle's ability to perform a mission across a wide range of dynamic and uncertain environments. To improve a system's resilience, engineers need to understand the way it adapts to, withstands, and responds to uncertainty and external disruptions, and how those responses impact mission success. However, the state space required to test all possible operational scenarios the autonomous system might encounter is impossible to achieve through limited real-world testing. The proposed model approach generates and tests performance boundaries to identify the critical moments when small environmental disruptions result in large changes in system behavior. Determining a system's resilience to disruptions provides valuable feedback to design and test engineers, enabling improvements to the system's operational performance.

All the systems discussed are required to successfully perform their missions under threat and during extreme conditions. One threat, the cyberattack, is increasingly frequent and complex. Ensuring that our military systems are resilient in the face of cyberattacks is a challenging but necessary task. The U.S. Government Accountability Office recently reported that "weapon systems cybersecurity assessments identified mission-critical vulnerabilities."[3] An article in this issue of the *Digest*, "Resilience in the Face of Cyberattacks: Cyber Resilience Guidance for Military Systems," proposes 10 principles that operational forces and system acquisition organizations should consider to ensure that their systems are resilient and able to perform their missions in the face of cyber threats. The approach emphasizes a resilient framework that increases the likelihood that systems will continue to perform despite cyberattacks or disturbances.

The next article in this issue, "Cyber Resilience for Navy Tactical Platforms," discusses design and operational aspects of adding resilience to modern warships and aircraft that are dependent on cyber systems. The article considers modern U.S. Navy platforms' warfighting capabilities that require cyber systems to perform critical mission operations. Preventing, adapting, and recovering from disruptions or attacks on computing, networking, and/or autonomy systems increases the resilience of not only those subsystems but also of the physical systems that prevent vessel damage or danger to the crew. The authors offer design considerations that are best implemented in the design phase for new systems and a prioritized list of functions to be reviewed and upgraded in existing systems.

Another method for addressing cyber vulnerabilities is described in the article "Diversity as an Enabler for Cyber Resilience," which argues for software diversity in the construction of highly dependable and resilient computer systems. Specifically, the article addresses the potential benefit of employing cyber diversity as a defensive measure against attacks. The authors cite one well-known example illustrating the importance of software diversity: in the loss of the Ariane 5 rocket, an unhandled software exception caused the backup processor to fail, and the primary processor failed immediately afterward as a result of the same error. The authors examine several novel methods of differentiating diversified sets of programs to increase the resilience of computer systems to errors, regardless of whether the errors stem from fatigue of hardware components, design mistakes, software defects, or malicious adversarial activity.

The articles described thus far have outlined many methods for incorporating resilience into our critical systems. But how do we measure whether these methods are effective? Currently, there is no agreed-upon quantitative method for measuring resilience. "Analyzing System Resilience to Adversary Kinetic and Cyber Actions" describes a method to characterize resilient approaches through the loss and restoration responses caused by off-nominal conditions. APL developed a framework to quantify system resilience and establish a risk profile by identifying the set of threats and analyzing the potential system responses. This framework provides metrics for resilience that are consistent with current definitions and constructs within the space community and addresses the challenges laid out in policy documents. The framework is a cost-effective assessment tool in that it enables an analytical level of effort that is commensurate with the acceptable level of uncertainty and leverages existing modeling and simulation tools. While the measurement approach was applied to space architectures, the framework is domain agnostic and can be implemented in other systems engineering areas.

CONCLUSION

The performance improvements resilience brings to systems engineering are far reaching. APL teams from diverse disciplines are at the forefront of applying resilient approaches and methods in systems engineering processes, and this issue provides just a glimpse of that work. APL's efforts in this burgeoning field are improving the performance of complex systems operating in the harshest environments and facing the most extreme threats, increasing the ability of these systems to withstand and bounce back from disruptions across physical and cyber domains spanning from outer space to subsea warfare.

REFERENCES

[1] SEBoK contributors, "System Resilience," in *SEBoK*, https://www.sebokwiki.org/wiki/System_Resilience (last revised 2 June 2019).

[2] Campbell, P., "Johns Hopkins APL and Northeastern University Join Forces to Conduct Resilience and Security Studies," press release, APL, Laurel, MD (8 Apr 2019), https://www.jhuapl.edu/Press-Release/190408.

[3] U.S. Government Accountability Office, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO, Washington, DC (2018).

Timothy J. Allensworth, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Timothy J. Allensworth is a member of the Senior Professional Staff working in the Ocean Engineering Program at APL. He is the assistant program manager for advanced capabilities within the Ocean Systems and Engineering Group. His interests include submarine communications and navigation, undersea sensor technologies, and advanced processing techniques such as machine learning. He received a B.S. in aerospace engineering from Purdue University, qualified as a submarine officer aboard USS *Annapolis* and as a nuclear engineering officer through Naval Reactors, and holds an M.S. in applied physics from Johns Hopkins University. His e-mail address is timothy.allensworth@jhuapl.edu.