Adding Resilience to Naval Systems for Mission Success

Timothy J. Allensworth and John G. Schuster

ABSTRACT

This article traces the development and evolution of reliability engineering as applied to complex systems, with an emphasis on naval applications. It further examines the limitations of reliability approaches in mitigating disruptions to modern systems. With rapidly developing technologies, and equally rapid technology obsolescence, historical reliability approaches often are unable to cope with unexpected disruptions to system operations, such as weather, cyberattacks, military and terrorist threats, and the deployment of unmanned autonomous systems, to name a few. In response to these issues, this article examines the potential for a concept called resilience to expand the domain of reliability engineering to include the ability to respond adaptively to and mitigate disruptions in near real time so that the failure of system components will not result in mission failure. Specific examples highlight the practical approaches resilience principles enable to position naval missions for success even in the face of unexpected disruptions.

INTRODUCTION

For nearly three quarters of a century, systems engineering has emphasized reliability in the design of complex naval systems.[1–7] Reliability focuses on quality components that operate without failure.[8] When failures do occur, enhancements to the system are implemented to restore or improve the overall reliability. These techniques have supported the creation of modern technically complex naval marvels, including nuclear submarines, aircraft carriers, surface combatants, aircraft, and satellites. Over the past two decades, increasing system complexity, proliferation of system interconnectivity, introduction of autonomy, and the increasing likelihood of external disruptions or attacks (both kinetic and nonkinetic) have led engineers to question whether reliability alone is sufficient for naval mission success.[9–11] The systems engineering community has begun integrating active approaches that enable systems to withstand and adapt to disruptions in near real time.[12–15] This combination of traditional reliability and active adaptive approaches is called resilience.[14–16] Resilience enables systems to prepare for, withstand, recover from, and adapt to disruption with the goal of increasing the probability of mission success.[17] Adding resilience to naval systems is important to ensure high probabilities of mission success in the growing complexity of operations and evolving threats.

RELIABILITY HISTORY

Reliability, as defined today, is a measure of the probability that a system will perform without failure over a specific time interval, under specified conditions. The most common reliability metric is mean time between failure (MTBF).[18] The concept embodies the principle that systems should be designed so that they do not fail, and reliability approaches attempt to identify and mitigate potential failures before they occur. Critically, reliability procedures emphasize statistical methods to predict and measure failure probabilities in system components (hardware and software).

The pervasiveness of the reliability culture today might suggest that this design ethic is an outgrowth of experiences from an earlier era. However, across a number of histories of reliability, its emergence at the end of World War II was rapid and unanticipated before the war. The proximate cause of this reliability explosion has been primarily identified as the precipitous wartime adoption of complex electronic systems (based on vacuum tube technology) and the corresponding challenges of addressing failures in critical systems (radars, radios, early computers, etc.) once they were deployed.[1,2,6]

Despite the fact that the 18th and 19th centuries had experienced unprecedented technology development driven by the industrial revolution, "by the 1940s, reliability and reliability engineering still did not exist."[1] Waves of new systems such as chronometers, steam-powered ships, railroad engines, automobiles and their assembly lines, airplanes, factories, and vacuum tubes themselves (among other notable examples) predated the requirement for system failure mitigation via statistical analysis.

While it is difficult to explain the absence of a concept such as reliability before its time, a potential defense is that engineers and designers understood that reliable systems and system components were a good thing, but until World War II there had been no major problems with reliability. Mechanical and electrical equipment of the time could perform reliably enough to satisfy users; and when devices might break, they could be repaired rapidly enough to be acceptable. In the 1920s there was no incentive for designing reliability into systems: "There wasn't much planned proactive prevention or economic justification for doing so."[1]

Measures of system performance certainly existed before the war, but they focused on the quality of what was produced, defined as the ability of a delivered product or component to perform an intended job.[1,2] Quality fits with the historical expectations of human-made goods—they will work as expected when new but will need to be maintained or repaired from time to time. Prior to the war the paradigm was that designers were responsible for the system until delivery, and repair people handled maintenance and failures after delivery. For example, early Ford cars came with a repair kit and instruction book so that owners could perform their own maintenance and repairs. Quality measures were augmented by newly developed statistical analysis techniques but were not well accepted in industry at the time. Walter Shewhart from Bell Laboratories developed statistical methods to address quality control problems in industry in the 1920s and 1930s but had difficulty gaining acceptance for his ideas because of the "deep-seated conviction of American production engineers . . . that laws of chance have no proper place among scientific production methods."[19]

Irrespective of why reliability engineering was not developed earlier, the histories of reliability broadly agree that the impetus for its adoption was the early World War II experience with complex electronic systems populated with vacuum tubes. Vacuum tubes were sold in the millions before the war, primarily to enable home radios to flourish across the United States; these radios typically contained ~4 to 10 tubes manufactured with standardized sockets that owners could quickly replace when they eventually burned out. This do-it-yourself repair concept did not spawn a need for reliability engineering since such replacement was familiar to most Americans because of their experience with electric light bulbs.

The war required significantly more tubes, in much more complex arrangements and operating in much harsher conditions, leading to significant logistics problems, as described in the following quotes:

- "At the onset of the war, it was discovered that over 50% of the airborne electronics equipment in storage was unable to meet the requirements of the Army Air Core and Navy."[20]
- "For shipboard equipment after the war, it was estimated that half of the electronic equipment was down at any given time."[21]
- "The vacuum tube, the active element that made the wizard war possible, was also the chief source of equipment failure. Tube replacements were required five times as often as all other equipment."[5]
- "During World War II . . . the US Navy was supplying a million replacement parts a year to support 160,000 pieces of equipment."[5]

Much work was done during the war to solve the problems with vacuum tube failures. One example involved several miniature tubes required for the Johns Hopkins University Applied Physics Laboratory (APL)-developed VT fuze. Not only was the fuze complex, but it had to withstand the shock of being fired from a gun. It was ultimately successful, with over 22 million VT fuzes built.[22]

Of course, reliability, like many other new developments that came out of World War II, was birthed by necessity and not from a desire to improve the theoretical performance of systems. Although scientists did not set out to create reliability theory, a seminal document published in 1949 and based on the experiences from World War II [MIL-P-1629 on failure mode, effects, and criticality analysis (FMEA/FMECA)], defined a critical reliability tool that is still being used routinely today.[23]

While MIL-P-1629 was an Army document, the U.S. Navy played a large role in the development of electronic systems (including the VT fuze) and in the establishment of reliability engineering. Much of the government work in reliability both during and after the war involved U.S. naval officers, likely due to the overwhelming presence of naval platforms in the Pacific theater and requirements for ships to operate far from ports for extended time periods. The Navy has been a strong proponent of reliability engineering over the intervening years and remains so today.

In the 1950s, efforts continued to focus on strengthening electronic reliability by improving the reliability of vacuum tubes. The lessons learned from World War II were codified by the rapidly maturing electronics industry (military and commercial) to address the increasing complexity of electronic systems—including computers. The Sperry UNIVAC, for example, used more than 10,000 tubes in the 1950s:

> The early large Sperry vacuum tube computers were reported to fill a large room, consume kilowatts of power, have a 1024 bit memory and fail on the average of about every hour. The Sperry solution was to permit the failed section of the computer to shut off and tubes replaced on the fly.[1]

As reliability theory rapidly matured, numerous technical organizations formed to coordinate and standardize implementation processes across commercial and military efforts, some of which are still active nearly 70 years later. With this exposure in the broader technical community, reliability expanded beyond electronics. (The first National Symposium on Reliability and Quality Control in Electronics was held in 1954, and by 1962, the eighth symposium, the organizers had dropped "in electronics" from the title.) Along with the development of reliability as an engineering discipline, there was a parallel development in tools, manuals, specifications, directives, standards, and contractual requirements (particularly in the military) designed to implement approaches to improve the reliability of complex systems. Similarly, theoretical work on statistical approaches to measuring reliability improvements increased.

These developments continued into the 1960s, but as solid-state electronic devices exploded onto the scene and vacuum tubes simultaneously diminished, the focus of many of the reliability efforts was diverted. Reliability engineering continued to grow in the 1960s, with increasing specialization for application to different kinds of systems and movement away from component reliability to the idea of system reliability. The Cold War and the corresponding development of missiles and spacecraft accelerated the use of reliability techniques. Reliability approaches were adopted by NASA (in part from Germany's early reliability experience with its V-1 and V-2 missile programs) and were credited with a major role in the successes of the Apollo program.[3,24] Reliability physics emerged from physics of failure to better standardize the identification and mitigation of component failures.[3] Reliability growth theory also emerged in the 1960s as a way to track and reduce a system's failure rates over time. Finally, in the 1960s, the concept of system effectiveness emerged, combining notions of reliability with availability. Despite efforts to promote system effectiveness, in the 1970s life cycle costs began to emerge as the military emphasis.[5]

The 1970s were marked by the rise in importance of complex consumer electronic systems and a corresponding decrease in the military's influence on the electronics industry.[5] The consumer electronics industry looked to reliability to protect manufacturers from lawsuits. At the same time, there was also increased interest in system-level reliability and safety as applied to complex systems, particularly in the oil and gas, chemical, and nuclear power industries. This led to the development of probabilistic risk assessments applied for the first time to nuclear power plants.[2] Increasing concerns about the correlation between factory reliability measurements and those the military observed in the field led to testing of requirements in representative environments that simulated field conditions. Finally, in the 1970s came a growing interest in software reliability that, despite progress, remains an area of concern today.[5]

The 1980s saw a renewed emphasis on operational readiness in the military and on quality in the commercial sector. While electronic devices did not become significantly more reliable during this decade, they were used to improve the reliability of mechanical systems such as switches and tuning controls, digital clocks, and electronic ignition and fuel injection systems for automobiles. The automotive industry noted a sharp increase in buyer interest in reliability of cars due in large part to Japanese competition.[3] This competition had been prompted by W. Edwards Deming, who championed statistical quality control prior to World War II. His ideas were not embraced by U.S. manufacturing companies, so in the 1950s he went to Japan, where his theories took root—leading to the Japanese automotive invasion of the United States. Also in the 1980s, the Challenger disaster called into question NASA's previous successes with system reliability and prompted increased interest in statistical risk analysis.

Commercial development of advanced electronic devices containing integrated circuits continued in the

1990s and blossomed with the development and expansion of the internet. The military became interested in COTS applications of hardware but was still tied to standardized military computer systems that could not take advantage of the COTS revolution. In the late 1990s, the U.S. submarine force made a radical decision to replace its existing MILSPEC sonar computers with COTS hardware (known as ARCI, for Acoustic Rapid COTS Insertion) and benefited from a dramatic increase in processing power and a dramatic reduction in the time required to field new processing algorithms.[25] From a reliability perspective, the performance advantages gained from ruggedized COTS computers appeared to greatly outweigh any perceived advantages in quality and configuration control that were intended to accrue from computer standardization in the military. In fact, open-architecture computer systems are being adopted across DoD.

Since 2000, reliability programs in industry and the military have continued unabated. However, in the military, questions are being raised about the practical impact of reliability approaches, particularly in the discrepancies between system requirements and operational testing attributed to reliability, availability, and maintainability (RAM) issues. In 2005, the *DoD Guide for Achieving Reliability, Availability, and Maintainability* was published, detailing these problems along with recommended solutions.[9] These included placing more emphasis on the existing reliability tools and developing new metrics, such as mission success, which addressed prioritizing and remediating failures that could cause mission aborts. A subsequent 2007 Defense Science Board (DSB) study focused on problems with "Initial Operations Test and Evaluation (IOT&E)," and its major recommendation stated, in part: "The single most important step necessary to correct high suitability failure rates is to ensure programs are formulated to execute a viable systems engineering strategy from the beginning, including a robust RAM program." In its report, the DSB defined reliability as "the probability of carrying out a mission without a mission-critical failure," further emphasizing the connection between reliability and mission success.[26]

Military instructions and requirements have been continually updated to emphasize reliability of systems after the 2005 DoD guide. In the 2009 release of the RAM cost rationale report (RAM-C),[27] mission success and reliability were formally tied together: "The probability of mission success and effectiveness is then assessed based on system reliability."[27] The Navy has taken a particular interest in its reliability and maintainability engineering (R&ME) policies:

> Since 2011, the Naval Sea Systems Command (NAVSEA) has undertaken a focused effort to revitalize reliability and maintainability engineering (R&ME) and institutionalize formal R&ME policy, standards, practice and processes for all NAVSEA programs.[28]

This in part was a reaction to *Reliability Analysis, Planning, Tracking, and Reporting*, DTM-11-003, signed by the Office of the Secretary of Defense on 21 March 2011, which requires all DoD components "to immediately enhance reliability" by "institutionaliz[ing] reliability planning methods and reporting."[29] The DoD memo was in response to the recommendations from the DSB report. Mission success has continued to remain important, as the 2015 release of DoD Instruction 5000.02, *Operation of the Defense Acquisition System*,[11] through the current August 2017 update states: "DoD's highest priority is to provide warfighters involved in conflict or preparing for imminent contingency operations with the capabilities urgently needed to overcome unforeseen threats, achieve mission success, and reduce risk of casualties."[11] The 2017 revision of the RAM-C[10] broadened considerations beyond just reliability to mitigate degraders and achieve mission success, stating: "Identify any significant degraders to availability and mission success and the top drivers [of] O&S [operating and support] costs along with any actions in process to mitigate these."

The many histories of reliability, as well as the multitude of requirements documents, testify to the widespread acceptance of reliability principles. However, the success of reliability analysis in improving performance often depends on the details of the technologies addressed. For example, early reliability applications to vacuum tubes assisted in selecting the "good" tubes in a batch but did little to improve the fundamental reliability of vacuum tube technology. As solid-state electronic components became dominant, electronics reliability increased rapidly, but not because of reliability analysis. As one researcher said in 1960, "the factor of ten by which reliability has improved in the past 10 years is far less attributable to our papers on reliability than to the invention of transistors."[5] A few known limitations of reliability are:[7,30]

- Data supporting reliability metrics lag technology development. It is difficult to either measure or predict reliability metrics such as MTBF for new technologies.
- In the longer term, aging effects can impact MTBF data. Reliability statistics for a system change over time, often in unexpected ways. Hence, over the last 15 years, the reliability community has been moving away from MTBF and toward time-dependent metrics.
- To collect data for continuous reliability improvement, large data sets are required, resulting in the need for reliability growth programs.
- Reliability is intended to work where requirements, system design, and the environment are unchanging. It is difficult to apply DoD standards for reli-

ability principles when the system or environment is changing. More complex physics-of-failure and Markov models are required.

- Software reliability remains a challenge. New requirements to address unknown and ever-changing cyber threats greatly complicate this problem.
- Reliability is not a good predictor of near-term mission success. It is designed to estimate average probabilities of failure over time, not to ensure success in a single mission.
- Reliability procedures need to be tailored to different systems and environments. There is no single reliability approach to system design and no guarantee that any particular level of reliability will be achieved.

Problems with the reliability process are not arguments against the use of reliability to understand system performance; however, they do suggest that reliability can be improved.

Inherently reliable systems can still fail on occasion and result in mission abort. Moreover, any system, no matter how reliable, can fail in the face of unforeseen disruptions. While reliability remains vital to system performance, the increasing pace of changing threats and technology development (cyber, hypersonics, artificial intelligence, etc.) necessitates a more active and adaptive augmentation to ensure mission success. This is especially important for naval platforms with long life expectancies, which must survive in future battles far beyond what was envisioned when they were built. Resilience can add this capability by focusing on functional performance and rapid restoration of functions in the face of disruptions.

RESILIENCE FRAMEWORK

Resilience has been accepted by the broader engineering community and is becoming more formalized as an approach within engineering standards and practices.[13,16,31–33] Successful approaches from across engineering communities can be leveraged as a framework for adding resilience to naval systems. Two useful concepts that have been tailored to improve portions of naval system performance are the 4Rs[34] and the performance recovery idea[13] of enabling recovery and adaptability. These concepts have been useful in applying resilience to hydraulic, mechanical, and electrical systems; computer and network applications; positioning, navigation, and timing (PNT) systems; accessible and nonaccessible systems; and unmanned systems.

The 4Rs

Robustness, redundancy, rapidity, and resourcefulness[34] serve as system characterization guidelines to help identify a broad spectrum of failure mitigations and/or judge the resilience of a system design.

- **Robustness**—the ability of the system and system elements to withstand external shocks without significant loss of performance
- **Redundancy**—the extent to which the system and other elements satisfy and sustain functional requirements in the event of a disturbance
- **Rapidity**—the ability to recover, contain losses, and avoid future disruptions
- **Resourcefulness**—the ability to diagnose and prioritize problems and to initiate solutions by identifying and monitoring all resources, including economic, technical, and social information

These terms are used to generate failure mitigation solutions to correct critical system-failure modes. In this application, systems are discussed in terms of their components—the hardware or software elements that populate the system—and their functions—the events that describe what the system does to conduct operations.

Robustness and redundancy encompass the traditional reliability concepts. Rapidity focuses on the expeditious restoration of mission functions by augmenting maintainability and repair approaches. Resourcefulness integrates the functions (including the operators) into the systems engineering design. When the 4Rs are applied to mitigate failures, the number and types of potential solutions increase dramatically over typical component improvements. Solutions can be applied to changing physical systems, system functions, procedures (normal, abnormal, and emergency), and training. By addressing the concerns through prevention and responsiveness over the whole system, at both the component and functional levels, rather than in stovepiped areas, the spectrum of solutions increases, improving cost–benefit analysis.

For example, a procedural and training solution that enables rapid recovery from a component failure with minor disruption to mission objectives can increase the likelihood of mission success without improving component reliability. If that approach can be implemented quickly (and at relatively low cost), it will have a large near-term cost benefit and will still be able to leverage longer-term component reliability improvements. This approach provides an immediate mission improvement that can also remain effective in providing a rapid functional restoration as future system improvements are incorporated.

Alternatively, when comparing two systems of similar performance, the 4Rs can be used to evaluate each system's ability to meet mission objectives in the face of external disruptions. The 4Rs provide guidelines for posing questions to help identify failure modes: Does the

design offer redundancy to component failures? Can the system identify, block, and/or adapt to cyberattacks? Is the design able to withstand and rapidly restore necessary functions after kinetic attacks and shocks? Can the system be easily recovered after failure (reboot, rebuild, rewire, hot-swap, etc.)? Does the system enable flexibility of operations should the environment change, empowering operational resourcefulness?

The Performance Recovery Concept

Another useful construct in implementing resilience is the performance recovery concept. Critical component failures in complex systems can often result in complete loss of functionality, ending in mission failure. This is considered a brittle failure of mission performance. Critical component failures, malfunctions, or external disruptions can all result in the mission ending. Reliability has a proven approach to mitigating component failures but does not routinely address or analyze external disruptions that lead to failures. Resilience aims to mitigate critical failure modes, regardless of the cause, to support graceful degradations of performance followed by an expeditious recovery[35] that enables missions to continue.

Field repairs and maintainability address sustainability but do not generally look to address rapid restoration of functions that improve the success of the current mission. Typically, a large inventory is required to ensure that enough functioning systems are available to meet operational needs. With fewer and fewer ships, submarines, and aircraft, rapid restoration of the available units is crucial. Important distinctions between the performance recovery of resilience and traditional maintainability and repair are the recovery time and functional performance restoration (not necessarily 100% component repair) to enable continued operations immediately.

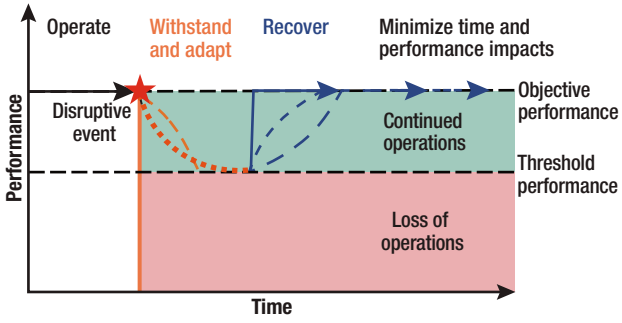


Figure 1. The performance recovery concept: performance versus time. After a disruptive event, as long as operational threshold performance is maintained, continuity is achieved. Design modifications to improve the probability of mission success can be implemented to aid prevention, minimize performance degradation, and/or enhance recovery. Resilience approaches attempt to minimize both the performance degradation and the duration of the recovery after an event.

Figure 1 considers performance of the system along with a disruptive event. After normal performance across the black horizontal line, a disruption occurs, resulting in the orange degradation curves. If an instantaneous loss of performance occurs, the design is considered brittle; the vertical line depicts a loss of performance. A system that has a backup mode of operation, resulting in reduced operations, can degrade at different rates (the dotted and dashed orange curves in Fig. 1). If redundancy is not an option to maintain system performance, consideration should be given to failure mitigation strategies that enable a more graceful degradation result. These approaches can help better enable the blue recovery portion of the performance recovery concept.

A system's quick recovery from the disruption without effecting mission operations achieves the rapidity concept of resilience. Minimizing the time it takes to recover and maximizing performance after recovery is the goal. At times a rapid recovery to a less-than-optimal state (reduced status) is more advantageous to mission success than a longer recovery to the objective performance level. Graceful failures afford operators time to assess and determine the best course of action, enabling more resourcefulness within the system. Metrics begin to emerge from the plot to help assess system resilience. Objective and threshold performance levels enable different recovery procedures for operators to choose from based on the situation. Designs that enable a slower functional performance degradation provide more time for assessments, enabling better decision-making. Reducing the time between failure and recovery becomes an important measure of rapidity that is central to the performance recovery concept.

RESILIENCE ENABLING NAVAL MISSION SUCCESS

Resilience emerged in systems engineering to address recovery of the system of systems in civil infrastructure after natural disasters.[14,32] The 4Rs were initially introduced in civil engineering designs to endure earthquakes.[15] The fundamental goals of resilience are to reduce operational risk and enable expeditious recovery after a casualty, shock, or attack on the system. It was realized that the same concepts could be employed across many systems engineering domains beyond utilities, infrastructure, and civil engineering, including nuclear safety,[36,37] SAE and IEEE documentation,[33,38] aerospace (Federal Aviation Administration safety[39,40] and spacecraft[12,41]), and cyber and network applications.[31,42–44] Resilience expanded the engineering approach from a static quality and prevention of component failure to include addressing disruptions and attacks on and within the system.

Infrastructure engineers and managers were early adopters of resilience, using it to minimize impacts of natural disasters. Experience and studies have illustrated that traditional reliability, redundancy, and protections were insufficient in the face of disruptive events.[13,32,34] The resilience approach added adaptable response plans leveraging interconnectivity and shared resources to restore essential capabilities. Traditional protection measures were thereby enhanced through rapid coordinated response forces, mobile and robust communications networks, novel supply deployment, and critical spare management. The National Institute of Standards and Technology (NIST) has established community resilience[32] guidance to support local governments, port operations, and communities in implementing these concepts.

These same concepts should also be implemented for naval surface and submerged combatants. For example, the naval cities at sea (such as the aircraft carrier USS *Stennis*) can also be enhanced by the application of resilience approaches and adaptable response plans in the face of disruptions. Recently additive manufacturing capabilities and the necessary associated crew training were provided on USS *Stennis*. The Chief of Naval Operations and Naval Sea Systems Command, NAVSEA 05, both highlighted how this first-of-a-kind capability better enables the ship to continue operating.[45,46] As one example, the crew was able to build a replacement for a failed communications mast rotary joint that did not have an onboard spare. With the 3-D-printed part, repairs that otherwise would have taken 4–8 weeks were made in less than a day. While the temporary repair was likely less reliable than the original part, the ability to rapidly restore functionality allowed the ship to expeditiously return to full operating capacity.[46]

Cyber and networking engineers were also early adopters of these techniques, employing resilience concepts to combat the rapidly evolving and growing number of cyberattacks.[31,42–44] Just as infrastructure designs cannot prevent natural disasters, neither can firewall designs alone prevent cyberattacks. The traditional protective approaches of static firewalls, passwords, and antivirus libraries, while important, are insufficient to protect a complex network. More active resilience approaches have been adopted, including automated responses and rapid recovery tools to quickly isolate, adapt, and restore network operations. NIST, the U.S. Computer Emergency Readiness Team (US-CERT), and many others have developed cyber resilience frameworks to define this approach. As naval systems become more distributed and networked (both onboard and across the Fleet; see Fig. 2 for a notional network), cyber resilience applications are critical to empowering these systems to face the evolving challenges of cyberattacks.

NASA is well known for building reliable space systems that employ superior components and inherent

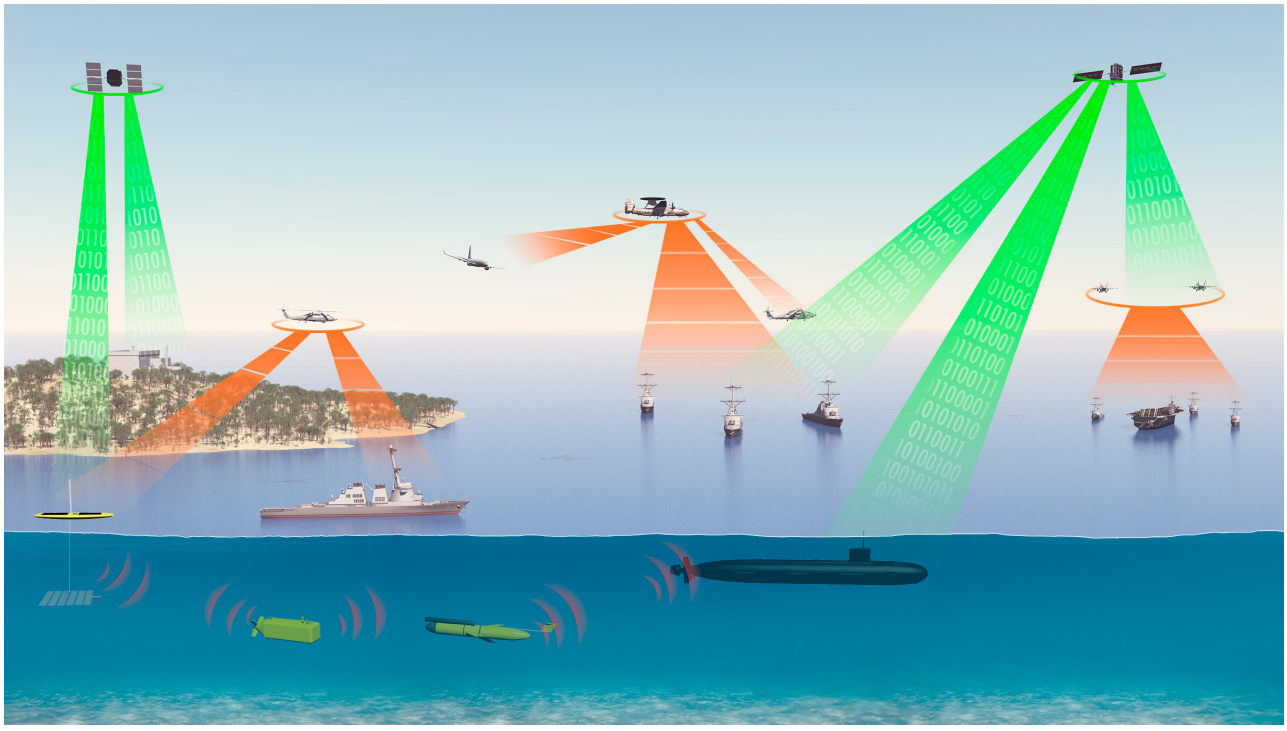


Figure 2. Notional interconnected naval network. The increasing system complexity, proliferation of system interconnectivity, and introduction of autonomy combined with the increasing likelihood of external disruptions or cyberattacks argue for the application of resilience in engineering.

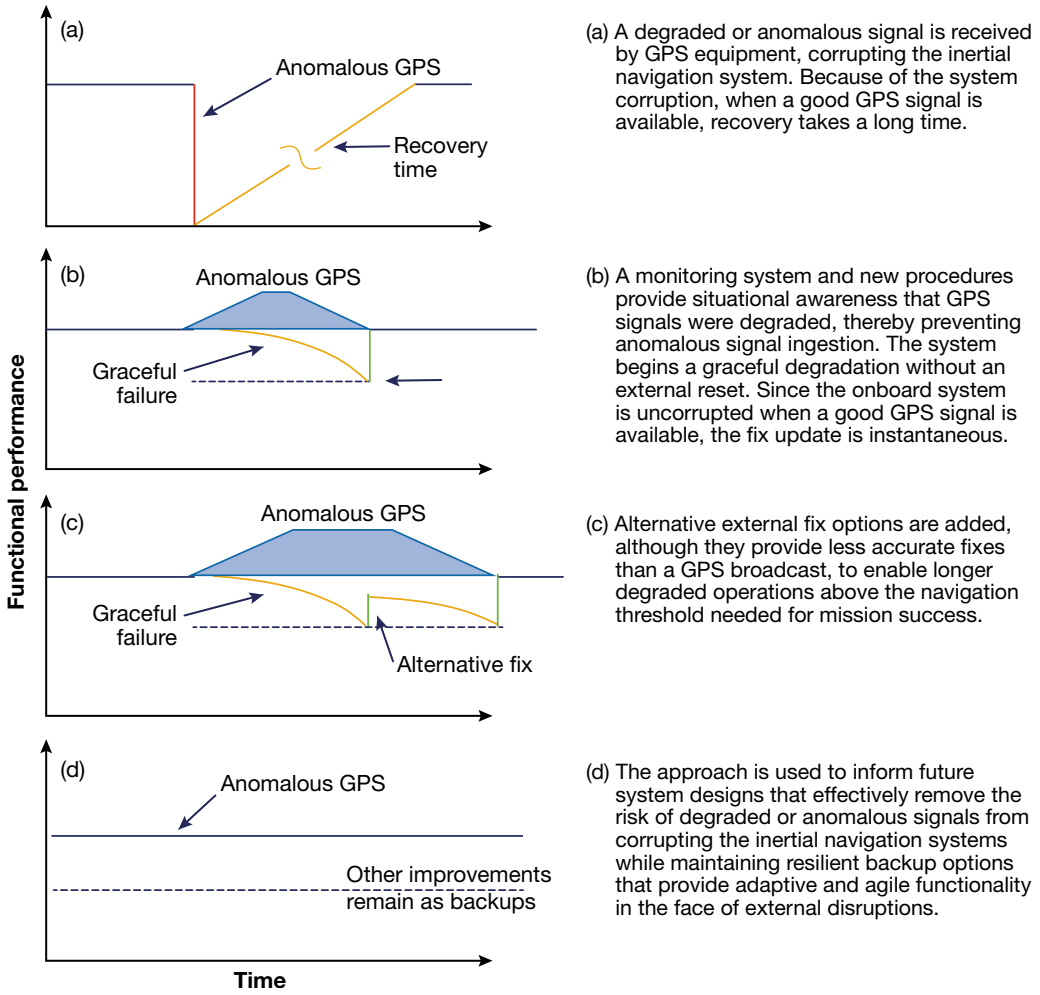


Figure 3. PNT application of performance recovery concept.

system redundancy. Describing next-generation spacecraft, NASA recently stated:

> The increasingly complex interconnectivity of these elements introduces new vulnerabilities within space systems that are sometimes impossible to predict. In that context, one key property of the [future] respective system is its resilience to unforeseen events.[12]

A similar conclusion can be drawn for any future unmanned/autonomous system or any complex system with semiautonomous support to human operators. As naval systems include and integrate additional semiautonomous and fully autonomous systems, resilience is needed to ensure mission success.

PNT systems have become ever more vulnerable to external attacks, despite that components have become increasingly reliable. Although these systems perform reliably, they are susceptible to spoofing, jamming, and other kinds of attacks. New resilient PNT solutions seek to actively monitor and mitigate disruptions regardless of their cause to better enable continued operations and improve the likelihood of mission success. PNT is still required for naval operations regardless of the disruption, whether it is jamming, spoofing, or loss of GPS broadcast. In the *American Practical Navigator,* Bowditch stated that "prudent mariners use all means available to determine their position," understanding that the reliability and accuracy of systems varied greatly even in 1799. In the spirit of Bowditch, today's PNT systems require new resilient solutions to be agile and adaptive to face modern external disruptions and use "all means available" to ensure navigational mission success.

The fundamental function of positioning, navigating, and maintaining time is needed regardless of the failure mode. As an example of applying the resilience methodology, a diverse team was established to generate a broad spectrum of solutions to enable continued operations during simulated adverse GPS environments (Fig. 3). Mitigations were generated to prevent degraded or anomalous signals from reaching the PNT components, and then additional navigation sources were used to enable continued mission operations, although positions were not as accurate as those provided by GPS. The lessons learned were then used to inform future

system changes to improve overall performance while maintaining the resilient monitoring and restoration mitigations developed.

CONCLUSION

The application of reliability has morphed over the last century to support the creation of modern technically complex naval marvels. Nevertheless, increasing system complexity and interconnectivity, proliferation of autonomous vehicles, and the growing unpredictability of external disruptions have raised questions within DoD, and the engineering communities writ large, on how systems will meet the needs of operations today and in the future. Designers of future systems should supplement traditional reliability methodologies with more active approaches, enabling systems to withstand and adapt to disruptions in near real time. Resilience offers a framework that can be leveraged for systems, especially those with complex integrations that need to succeed in challenging and changing environments. Adding resilience to naval systems is important to ensure high probabilities of mission success during increasingly complex operations and in the face of evolving threats.

REFERENCES

[1]McLinn, J., "History of Reliability," American Society of Quality, Reliability & Risk Division, https://www.asqrd.org/home/history-of-reliability/ (accessed 22 Apr 2019).

[2]Saleh, J. H., and Marais, K., "Highlights from the Early (and Pre-) History of Reliability Engineering," *Reliab. Eng. Syst. Safe.* **91**(2), 249–256 (2006).

[3]Knight, C. R., "Four Decades of Reliability Progress," in *Proc. Annual Reliability and Maintainability Symp.*, Orlando, FL, pp. 156–160 (1991).

[4]Ryerson, C. M., "The Reliability and Quality Control Field from Its Inception to the Present," in *Proc. IRE*, section 25, pp. 1321–1338 (1962).

[5]Coppola, A., "Reliability Engineering of Electronic Equipment, A Historical Perspective," *IEEE Trans. Reliab.* **R-33**(1), 29–35 (1984).

[6]Zio, E., "Reliability Engineering: Old Problems and New Challenges," *Reliab. Eng. Syst. Safe.* **94**(2), 125–141 (2009).

[7]Bhamare, S., Yadav, O., and Rathore, A., "Evolution of Reliability Engineering Discipline over the Last Six Decades: A Comprehensive Review," *Int. J. Reliab. Safe.* **1**(4), 377–410 (2007).

[8]SEBoK contributors, "Resilience (Glossary)," in *SEBoK*, https://www.sebokwiki.org/w/index.php?title=Resilience_(glossary)&oldid=55022 (last revised 19 Oct 2018).

[9]U.S. Department of Defense, *DoD Guide for Achieving Reliability, Availability, and Maintainability*, DoD, Washington, DC (3 Aug 2005).

[10]Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report Outline Guidance*, Version 1.0, DoD, Washington DC (28 Feb 2017).

[11]Department of Defense, "Systems Engineering," Chap. 3, *Operation of the Defense Acquisition System*, Instruction 5000.02, DoD, Washington, DC (7 Jan 2015, updated 10 Aug 2017).

[12]NASA, SBIR, Phase 1 Solicitation, H6.02 Resilient Autonomous Systems (2017).

[13]Ayyub, B., "Practical Resilience Metrics for Planning, Design, and Decision Making," *ASCE ASME J. Risk Uncertain. Eng. Syst. A. Civ. Eng.* **1**(3), 1–11 (2015).

[14]Hollnagel, E., Woods, D. D., and Leveson, N. (eds.), *Resilience Engineering: Concepts and Precepts*, CRC Press, Boca Raton, FL (2006).

[15]Jackson, S., and Ferris, T., *Resilience Principles for Engineered Systems*, *Syst. Eng.* **16**(2), 152–164 (2013).

[16]International Council on Systems Engineering (INCOSE), "Resilient Systems Working Group," https://www.incose.org/incose-member-resources/working-groups/analytic/resilient-systems (accessed 25 Mar 2019).

[17]Committee on Increasing National Resilience to Hazards and Disasters and Committee on Science, Engineering, and Public Policy, *Disaster Resilience: A National Imperative*, Washington, DC, National Academies Press (2012).

[18]SEBoK contributors, "Reliability, Availability, and Maintainability," in *SEBoK*, https://www.sebokwiki.org/w/index.php?title=Reliability,_Availability,_and_Maintainability&oldid=54519 (last revised 16 Oct 2018).

[19]Freeman, H. A., "Statistical Methods for Quality Control," *Mech. Eng.* 261–262 (1936).

[20]Thomas, M. U., *Reliability and Warranties: Methods for Product Development and Quality Improvement*, CRC, New York (2006).

[21]Evans, R. A., "Electronics Reliability: A Personal View," *IEEE Trans. Reliab.* **47**(3), SP329–SP332 (1998).

[22]Hinman, W. S., and Brunetti, C. "Radio Proximity Fuze Design," Research Paper RP1723, *J. Res. Natl. Bur. Stand.* **37**, 1–13 (1946).

[23]Zhu, Y.-M., "Software Failure Modes and Effects Analysis," Chap. 2, *Failure-Modes-Based Software Reading*, SpringerBriefs in Computer Science, Springer, Cham, Switzerland (2017).

[24]Childers, F. M., *History of Reliability and Quality Assurance at Kennedy Space Center*, KSC Historical Report No. 20 (KHR-20), KSC, Kennedy Space Center, FL (Feb 2004).

[25]Boudreau, M., "Acoustic Rapid COTS Insertion: A Case Study in Modular Open Systems Approach for Spiral Development," in *Proc. IEEE Conf. on System of Systems Engineering*, San Antonio, TX, pp. 1–6 (2007).

[26]Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Developmental Test & Evaluation*, DoD, Washington, DC (May 2008).

[27]Office of the Secretary of Defense in Collaboration with the Joint Staff, *Department of Defense Reliability, Availability, Maintainability, and Cost Rationale Report Manual*, DoD, Washington, DC (1 June 2009).

[28]Dube, P. T., and Greenhalgh Lubas, D., "NAVSEA Reliability and Maintainability Engineering," in *Proc. 2016 Annual Reliability and Maintainability Symp. (RAMS)*, Tucson, AZ, pp. 1–6 (2016).

[29]Office of the Undersecretary of Defense, *Reliability Analysis, Planning, Tracking, and Reporting*, Directive Type Memorandum (DTM) 11-003, DoD, Washington, DC (21 Mar 2011).

[30]Barnard, A., "Why You Cannot Predict Electronic Product Reliability," in *Proc. International Applied Reliability Symp. Europe*, Warsaw, Poland, pp. 1–47 (2012).

[31]Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., and Scarfone, K., *Guide for Cybersecurity Event Recovery*, Special Publication SP 800-184, NIST, Gaithersburg, MD (Dec 2016).

[32]NIST, "Resilience," https://www.nist.gov/topics/resilience (accessed 25 Mar 2019).

[33]*Configuration Management Standard EIA649C*, SAE International, Warrendale, PA (2 Feb 2019).

[34]Tierney, K., and Bruneau, M., "Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction," *TR News* **250**, 14–17 (2007).

[35]Ayyub, B. M., *Risk Analysis in Engineering and Economics*, CRC Press, Boca Raton, FL (2014).

[36]Tran, H. T., Balchanos, M., Domerçant, J. C., and Mavris, D. N., "A Framework for the Quantitative Assessment of Performance-Based System Resilience," *Reliab. Eng. Syst. Safe.* **158**, 73–84 (2017).

[37]Dessavre, D. G., Ramirez-Marquez, J. E., and Barker, K., "Multidimensional Approach to Complex System Resilience Analysis," *Reliab. Eng. Syst. Safe.* **149**, 34–43 (2016).

[38]IEEE, *Proc. 2017 Resilience Week (RWS)*, Wilmington, DE, https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8070887 (2017).

[39]Palumbo, R., and Filippone, E., "A Quantitative Approach to Resilience Engineering for the Future ATM System: Case Study Results," in *Proc. Twelfth USA/Europe Air Traffic Management Research and Development Seminar* (ATM2017), Seattle, WA, pp. 1–9 (2017).

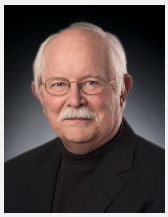
[40]Editor, "SAE Tech Standards for GPS/eLoran," https://rntfnd.org/2017/09/28/sae-tech-standards-for-eloran/ (28 Sep 2017).

[41]Owens, A., "Quantifying the Value of Resilience in Long-Duration Space Systems," https://www.nasa.gov/content/quantifying-the-value-of-resilience-in-long-duration-space-systems/ (8 Dec 2014).

[42]Department of Defense Science Board, *Task Force Report: Resilient Military Systems and Advanced Cyber Threat*, DoD, Washington, DC (Jan 2013).
[43]Bodeau, D., and Graubart, R., *Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines*, Report MTR170001, MITRE, Bedford, MA (Jan 2017).
[44]U.S. Computer Emergency Readiness Team (US-CERT), "Assessments: Cyber Resilience Review (CRR)," https://www.us-cert.gov/ccubedvp/assessments (accessed 25 Mar 2019).
[45]Moroney, J., "CNO Visits the John C. Stennis Carrier Strike Group at Sea," U.S. Navy press release, story number NNS190120-01, 20 Jan 2019, https://www.navy.mil/submit/display.asp?story_id=108359.
[46]Leonard, J., "Stennis Engineers Use 3D Printer to Make Repairs to Critical Systems," *Military News*, 7 Jan 2019, https://www.militarynews.com/news/stennis-engineers-use-d-printer-to-make-repairs-to-critical/article_b30882c6-1294-11e9-b493-0738bc919b8a.html.

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.



John G. Schuster, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

John G. Schuster is a member of APL's Principal Professional Staff. Since joining APL in 2004, he has served as a member of the Laboratory's Science and Technology Council and has participated on numerous internal and external panels and committees. Before retiring from the federal government, John served as an Senior Executive Service (SES) in the Navy Department directing the Submarine Security and Technology Branch of the Submarine Warfare Division in the Office of the Chief of Naval Operations. He holds a B.S. in space science and an M.S. in fluid mechanics from Catholic University. He is a recognized authority in underwater acoustics and anti-submarine warfare. His e-mail address is john.schuster@jhuapl.edu.