MILITARY SPACE RESILIENCY: DEFINITION, MEASUREMENT AND APPLICATION
Northrop Grumman Aerospace Systems

To understand Military Space resiliency we must understand where and how space systems fit within the DoD context. The Quadrennial Defense Review sets a long-term course for the DoD as it assesses the threats and challenges the nation faces and re-balances its strategies, capabilities, and forces to address current conflicts and future threats. Re-balancing the DoD enterprise is an expansive task that looks across the services (Army, Navy, Air Force, Marines), force projections, logistics, and situational awareness capabilities as well as the environment and doctrines that guide the concept of operations and decision making to execute missions/scenarios critical for our national security. An important part of re-balancing is in understanding the resiliency of the DoD’s capabilities to successfully execute these missions/scenarios consistent with desired goals.

To successfully integrate resiliency into this re-balancing effort, we need enterprise communities to work together using a common understanding and dialogue. We need to establish a common approach to measure how we are doing in meeting objectives. And we need clear communication across these communities to allow efficient implementation of resilient enterprise solutions. The goal of this Northrop Grumman Aerospace Systems (NGAS) white paper on space systems resiliency is to lay out a framework with these characteristics:

1) A definition that enables a common understanding and dialogue among community leadership
2) An intuitive and measureable approach that avoids subjective measures
3) Results summarized in simple principles that can be applied to space architecture and acquisition

RESILIENCY DEFINITION AND ENTERPRISE CONTEXT

Air Force Space Command (HQ AFSPC) defines resiliency as “the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges, or adversary actions.” For space systems architectures, both system failures and environmental challenges have well established analytical approaches that calculate system availability to address these issues. In this white paper we concentrate on system resiliency due to adversary threats as these effects are the least understood and likely the most detrimental to DoD systems in support of enterprise mission success. Many adversaries have the resources to develop sophisticated cyber, physical and electronic threats to cripple U.S. space systems. A broader group of adversaries have access to a wide range of readily available commercial technologies that threaten all aspects of a space system – from gateways, satellite ground control, terminals, to space. Threats using off-the-shelf technology are becoming increasingly capable of degrading, disrupting and denying access to space. Especially troubling are the low cost and short cycle times of very effective threats when compared with the investments that are made in DoD space systems. These asymmetric threats (low cost weapon disabling an expensive space system) further encourages adversaries to develop capabilities that can deny us our space advantage using readily available technology that in many cases can be executed without attribution. In light of this, the most difficult future threat we must address are those that can be fielded with much shorter cycle times than the life of the space system (development, deployment and operations life). To stay ahead of these threats, we must develop a thorough understanding of system resiliency and use this understanding to force adversaries’ on a path where the only effective threats are those whose costs begin to approach the costs of the DoD systems they attack. We must move away from dependence on DoD systems that give the adversary an asymmetrical advantage.

Executing missions requires coordinated enterprise-wide efforts (Fig. 1). The enterprise must be system engineered to determine how the many different elements interact to execute missions with the best performance and investment solutions. Given that the DoD buys systems which get integrated together to create the enterprise, the core of resiliency and resiliency analysis is tied to the overall system engineering of the enterprise. A threat to enterprise mission execution is in reality a threat to one or more systems within the enterprise. To effectively evaluate enterprise resiliency, threats (threat systems) are best analyzed at the system level. Each system acquired within the enterprise is comprised of key performance parameters (KPPs) critical to the execution of an effective military capability. KPPs normally define the minimum acceptable performance threshold the system must deliver to the enterprise. In this light, system resiliency is a measure of...
a system’s ability to support the KPPs in the face of adversarial actions. For a threat system to have a successful outcome it needs to ‘break’ a system; compromise the system’s ability to successfully meet its KPPs. System resiliency characterizes these system weak links or ‘breakpoints’ and how the system will be compromised in its support of KPPs and mission execution. This system resiliency construct provides an intuitive, straightforward approach to gaining critical insight into why a system fails and what is required to make the system architecture resilient. Enterprise system engineering is the glue which both identifies the system KPPs as well as defines the effect of the systems on the enterprise capabilities. Different system solutions can be traded one against another to find the most resilient enterprise combination of systems. To effectively re-balance the enterprise, it is extremely important to be able to measure and understand the capability of systems and enterprise solutions, namely how and if the enterprise can successfully execute missions consistent with goals.

**EVALUATING RESILIENCY**

Critical to evaluating resiliency is avoiding subjective solutions that foster independent community approaches resulting in a wide range of differing results. To avoid this, an approach based on commonly accepted engineering disciplines enables communities to integrate their assessments into common positions. Common principles that apply to architectures and acquisitions across communities can be developed and implemented in re-balancing the enterprise. Two broad categories of system resiliency evaluation have been proposed – Analytic Modeling and Deterministic Methods (side-by-side comparisons are shown in Fig. 2).

Analytic Modeling approaches seek to identify functions which measure the magnitude of resiliency in a system. Attempts have been made to create functions composed of multiple resiliency tactics or categories. The difficulty in this approach is identifying intuitive and measurable functions that can be validated (yield consistent answers) across the community. Without such measurable and validated functions, this approach becomes a subjective assessment without measure (units) or intuition. Subjective assessments for systems resilience can yield a wide variety of outcomes strongly influenced by preferences and desired outcomes. The larger the set of systems considered the more complex and intensive the analysis becomes. Integrating multiple independent subjective scores together becomes problematic as there are no units or relationships to govern this process. The result is a score which in itself yields little intuition or understanding of the problem. Moreover, subjective approaches are not conducive to moving communities to a common understanding and thus do not foster principles that can be applied to space architecture or acquisition.
Alternatively, a Deterministic method proposed below focuses on characterizing Space system breakpoints using established system engineering disciplines. Space system breakpoints can be identified by defining threat systems that successfully deny its ability to successfully meet its KPPs. Using established system engineering disciplines to define threat systems avoids subjective measures and associated pitfalls. This approach uses the same disciplines that are well understood in characterizing DoD systems and provides strong intuitive, objective and measurable data. This results in a far simpler resiliency assessment to perform, characterize and validate. Common metrics used to characterize systems include the type of system, the cost of the system, and the reliability of the system (successful mission execution). These same metrics can be used to characterize successful threat systems (DoD system breakpoints) and yield very insightful and useful information about a DoD system's resiliency (Fig. 3). This approach can foster common understanding and dialogue among community leadership combined with intuitive and measurable data to help form simple principles that can be applied to space architecture and acquisition.

**DEVELOPING THREAT SYSTEMS – SYSTEM BREAKPOINTS**

For a given scenario and Space system within the enterprise, one can engineer physical, electronic or cyber-based threat systems that can deny the DoD system from meeting their KPPs (Fig. 4). Using established system engineering disciplines one can identify vulnerabilities and techniques that will disable a DoD system. With these vulnerabilities characterized at different susceptibility levels, one can design effective threat elements and a concept of operations that successfully compromises a DoD system's performance. These threat elements can be designed with well defined life spans, operations and maintenance requirements and reliability characteristics. Questions and debate within the community regarding the validity of these threats elements (and threat systems) can be addressed with detailed system designs and performance assessments. Using these system designs, operational, environmental and mitigation probabilities can be determined and combined to yield an individual threat element’s probability of success. These probabilities can be used to calculate the quantity of threat elements required within a concept of operation to provide successful threat system reliability. Threat system reliability may be improved by replicating threat elements or increasing capability of these threat elements. Calculating threat system reliabilities assures apples to apples comparisons using consistent characteristics to define and evaluate different threat systems.

Deterministic system resiliency metrics are best used to establish well defined, verifiable, and intuitive data for assessing trends and finding big resiliency disparities (e.g., low cost threat systems creating highly

---

**Figure 3 System break points characterized using established disciplines**

**Figure 4 Identifying Successful Threat Systems**
asymmetric vulnerabilities). These same metrics can be misleading if used as high fidelity absolute values to choose between systems with very slight differences (i.e., choosing winners in a tight group). Deterministic system resiliency metrics also provide an excellent objective foundation from which to integrate subjective criteria (e.g., politics, personalities, deterrence, attribution, and escalation). This is a very familiar process we experience daily as consumers when we take a deterministic value of a product (cost) and build on it the subjective reasons why we should buy the low, middle or high cost product. Deterministic metrics also allow cost benefit analysis when iterating DoD and threat architectures to assess different resiliency techniques like mitigation and reconstitution. This iteration analysis can also be used to define susceptibility limitations characterizing different threat and DoD system designs (e.g., limitations due to physics).

**System Resiliency Value**

System resiliency is a measure of capability to successfully execute a scenario in the face of threats; it is not a measure of value to determine the best investment. To assess resiliency value, simply comparing successful threat costs to DoD system costs provides significant insight for determining investment value. Successful threat costs represent the cost of the threat system, and system costs represent the cost of the DoD system compromised by the threat. This ratio is proposed as a comparison tool and not as an absolute measure. Again, cost provides a strong intuitive and objective foundation to which subjective criteria can be added. As an example, investing billions of dollars in a DoD system that can be neutralized for a small fraction of the system cost (e.g., $10K jammer) would possess a low system resiliency value compared to a threat system that requires substantially more funds (e.g., $6B ASAT threat system) to have a questionable affect on the system.

It is extremely important to note that a system or architecture with low life cycle cost but lacking in resiliency (i.e., easily and readily rendered useless by an adversary), provides poor resiliency value compared with a highly robust system or architecture that may have a higher life cycle cost, but is capable of maintaining a useful level of performance in the face of attacks by a sophisticated near peer adversary. Additionally, trying to achieve a high system resiliency value by combining multiple systems with low system resiliency values, while seemingly intuitive, is unlikely to improve resiliency value in the face of adversarial threats. Multiple systems may provide additional value from natural threats, but provide little additional value in the face of an intelligent adversary directly targeting system weak links (Fig. 5). These principles are extremely important in understanding system resiliency and how it applies to space systems design and acquisition. This philosophy goes against much of the common thinking with regard to system of systems resiliency. This is likely because many view natural and adversarial threats through a similar lens when they are really very different problems.

**Initial Resiliency Findings**

A primary finding we observed in our initial analysis is the large system resiliency gap that exists between systems that are affected by ground-based threats and those that are not. Space systems (ground or space nodes) that can be successfully attacked with ground-based physical, electronic or cyber threats are significantly more vulnerable due to the proliferation of available low cost, or easy to develop ground based threat systems. These systems allow adversaries to follow an asymmetric low cost, high impact threat escalation strategy, providing the opportunity, possibly without attribution, for multiple mobile threats that are nearly impossible to find and eliminate in a timely manner. Low cost threats can easily be bought in large
quantities, enabling effective training and experimentation to determine best practices and designs. Large quantities of affordable threat elements also enable strategies that employ significant reinforcements available to deal with mitigation issues through rapid reconstitution and recovery. Low cost threats are available to many adversaries and can be used in coordinated attacks across multiple system nodes (e.g., primary and redundant uplink stations). Systems that eliminate vulnerabilities to these low cost or easy to develop ground-based threats drive adversaries to space-based threat systems that begin to approach the costs of creating DoD Space systems. Space-based threat systems are expensive (especially with comparable reliabilities to ground-based threat systems) and more attributable. Such systems force adversaries to follow a high cost threat escalation path before they achieve any significant threat objectives. Very few adversaries have the sophisticated capabilities or wealth to pursue this threat path. Additionally, if a DoD system can force the adversary to attack at higher ‘plateaus of resiliency’, they force the adversary to create substantially more difficult, more expensive, time intensive and attributable threat systems to be successful. Higher ‘plateaus of resiliency’ can be achieved with systems that employ multiple nodes, nodes in multiple orbits, nodes that are maneuverable and/or nodes that can be reconstituted making threat attacks successively more difficult to achieve. ‘Plateaus of resiliency’ and the threat vulnerability gap are illustrated by plotting threat system costs for various classes of DoD systems (Fig. 6). DoD systems with space or ground nodes vulnerable to ground-based threats require only modest threat system costs ($Millions) to compromise system performance (left of Fig. 6). Systems vulnerable only to space-based threats require expensive threat systems ($Billions) to compromise system performance (right side of Fig. 6). These ‘plateaus of resiliency’ findings yield strong guiding architecture principles that can be used designing highly resilient DoD systems.

The First Principle is to design systems that must eliminate vulnerabilities to ground-based threats. This eliminates the asymmetric threat environment removing most adversaries and moving the system resiliency magnitudes higher. It is this characteristic that predominately enables the possibility of a day without space. The Second Principle is to design and acquire low cost satellite nodes that enable the system to affordably move to the highest plateau. These nodes must still provide meaningful capability such that the system is affordable, manageable and meets the required KPPs. These principles must be intuitively understood and applied to the enterprise across community’s architectures and acquisitions if system and enterprise resiliency is to be strengthened. These principles mandate a rethinking of the broader space architecture and the duplication of systems to achieve affordable resilient capability.

CONCLUSIONS

Faced with a highly-constrained defense budget and a world where adversaries have increasing access to more capable and sophisticated threats that can be used against U.S. space systems, it is critical that the Government and Industry identify cost-effective investments that enable our systems to resiliently and successfully execute key missions maintaining national security. NGAS has developed a space resiliency context and framework to help forge a common understanding and ensure investments deliver the required value for system architectures, designs and acquisition. The assessment results have been organized into a set of guiding principles that can also be applied to system architectures, designs and acquisition.

For more information, please contact:
Northrop Grumman Aerospace Systems
Gregory Edlund
gregory.edlund@ngc.com