A Path Towards Cyber Resilient and Secure Systems

Metrics & Measures Framework

Final Whitepaper
April 2016

Prepared by:

Systems Engineering Division

System Security Engineering Committee
Chairs: Holly Dunlap, Raytheon
Beth Wilson, Raytheon

Developmental Test & Evaluation Committee
Chair: Joe Manas, Raytheon

In collaboration with:
INCOSE SSE Committee
Trusted Supplier Steering Group
Mitre AF Cyber Integration

CHANGE HISTORY

Revision	Date	Author	Description

Table of Contents

1 INTRODUCTION

The cyber threat has become one of the greatest asymmetric threats to our national defense and warfighting capabilities. The magnitude of threats and opportunities, as well as its ubiquitous nature, have cemented cyberspace in the global commons as the newest warfighting domain. The United States has maintained military advantage in the other warfighting domains: land, air, sea, and space. The cyberspace domain threatens to undermine all of these domains as systems are interconnected and dependent upon cyberspace technology.

Cybersecurity challenges our ability to ensure unwavering trust in the systems' information confidentiality, integrity, and availability. System security extends a security perspective to systems and the systems engineering process. In order to increase the confidence in the flow of bits and bytes both transmitting and receiving within the system as well as to external systems of systems, we must understand the multiple threat vectors and security specialties focused on minimizing the vulnerabilities and opportunities for adversarial attack.

A holistic approach to system security engineering (SSE) makes use of scientific and engineering principles to deliver assured system-level protection via a single, full-system/full life cycle view of system security. Implemented via the program protection process, SSE can enable managing and balancing risks across the security specialties such as Information Assurance/Cybersecurity, anti-tamper (AT), supply chain, software and hardware assurance , and general program security to provide a system security risk perspective. Taking a holistic approach to system security requires bringing together multiple communities with rich histories introduces varying perspectives, terminologies, taxonomies and methodologies. This diversity provides opportunities and challenges for evaluating the security quality system attributes of metrics and measures. Ultimately, we are committed to providing systems that are resistant to attack, and are resilient when under attack.

2 BACKGROUND

The rapid pace of technology development and the human unconstrained of technical realism has a heighted desire and expectation of seamless, interconnected, agile, and affordable systems. The push for innovation and technology advancement has placed high priorities on system and component performance optimization but limited emphasis on security. This expectation is testing our national defense ability to produce cyber resilient and secure systems which are at least one and at best two generations ahead of our adversaries. As defense system integrators and the extended industrial base designs, develops, test, and field systems, it is imperative that we maintain security at the forefront of our priorities.

In order to do so, the requirements community continually must refine capability requirements to be sensitive to evolving threats. The Joint Capabilities Integration and Development System (JCIDS) Net-Ready (NR) KPP focuses on the interoperability of the interconnected systems. However, operational needs extend far beyond interoperability in a cyber-contested environment. The JROC Manual, revised February 12, 2015, refined the Survivability KPP into a System Survivability KPP to incorporate mandatory requirements for survivability from non-kinetic fires.

As part of Better Buying Power 2.0, USD Acquisition, Technology, and Logistics (AT&L) Mr. Kendall initiated a holistic approach to system security and program protection in a July 18, 2011 memo. Prior to issuance, security was defined and addressed within each security specialty silo leading to inconsistencies and security gaps. This memo signified renewed Department of Defense (DoD) acquisition prioritization of security and expanded information assurance and anti-tamper program protection planning to include supply chain and software assurance (SwA).

Mr. Kendall then codified policy for program protection, including the requirement to submit a Program Protection Plan (PPP) at each acquisition milestone in the following policy instructions:

- Trusted Systems and Networks, DoDI 5200.44 (November 5, 2012),
- Enclosure to DoDI 5000.02, Systems Engineering, (January 7, 2015), and
- Critical Program Information, DoDI 5200.39, (May 28, 2015)

At the same time, the DoD CIO is a co-signature on DoDI 5200.44 and updated the information assurance focus to cybersecurity in the DoDI 8500.01, March 14, 2015, which includes insertion points for PPP. The Director of the Operational Test and Evaluation (DOT&E) Directorate of the Department of Defense (DoD), Dr. J. Michael Gilmore, published a memorandum titled, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs” (August 1, 2014). For decades, unique test ranges have been developed and maintained to represent the operational mission environment to test systems within the conditions in which they must perform. Ranges such as Missile Ranges, Radar Ranges, and Undersea Warfare Ranges mimic the environmental conditions and introduced red team adversarial threats to be able to test the system in a simulated live operational mission environment. Prior to the DOT&E memo, cyber was a significant source of failure during OT&E assessments conducted in FY12 and FY13. Over 400 cybersecurity vulnerabilities were uncovered during the vulnerability

assessment and/or the penetration testing that was conducted during OT. Of those, approximately half were serious (Category 1) vulnerabilities that could allow debilitating compromise to a system. It was those test results that have "*indicated the need to move the discovery and resolution of system vulnerabilities earlier in program development*" [DOT&E 2013 Annual Report, p17]. These cyber system failures occurred in the traditional non-cyber specific ranges when cyber was not the primary focus of the OT&E test plan. The DOT&E memo is the first direction requiring testing for system survivability within the cyber contested environment to assess the system suitability for operational mission effectiveness. This pronounced acquisition tail-end requirement causes a dramatic reverse ripple effect through the systems engineering "V" all the way back to the early system functional capability design requirements.

The strong partnership between OT&E and DT&E ensures the continuity of cybersecurity requirements. DASD (DT&E) Dr. C. David Brown's initiative to "Shift-Left" to focus on earlier developmental testing seeks to improve DT&E to enable programs to find and fix problems earlier in development when fixes are more effective, more efficient, and less costly [DASD (DT&E) FY 2014 Annual Report, p1].

Providing true holistic program protection requires a fully committed government, industry, and academic partnership. The challenge is technically, politically, financially, and procedurally complex. However, many are working to make progress to move us forward to combat our adversaries and minimize their opportunity for malicious effect to our war fighting capabilities. Appendix A includes prior committee work and parallel efforts related to cyber resilient and secure systems which were leveraged where applicable and have been integrated into this paper.

3 KEY PERFORMANCE PARAMETERS

Key Performance Parameters (KPP) are mandatory performance attributes of a system considered critical or essential to the development of an effective capability. KPPs are expressed in terms of Measures of Performance (MOPs) and must be measurable, testable, and affordable. The January 2015 revision to the JCIDS Manual refined the "Survivability" KPP into the "System Survivability" (SS) KPP to incorporate survivability considerations of both kinetic and non-kinetic fires. In doing so the Manual added a requirement to establish cyber survivability as an element of the SS KPP.

Cyber survivability KPP values are intended establish the performance threshold and objective values for a capability solution, and are derived from the operational requirements of the system, scenario-based assumptions for its operational use, and the planned logistical support to sustain it.

As defined in the JCIDS Manual:

The SS KPP is intended to ensure the system maintains critical capabilities under applicable threat environments. The SS KPP may include reducing a system's likelihood of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability, and countermeasures; reducing the system's vulnerability if hit by hostile fire, through attributes such as armor and redundancy of critical components; enabling operation in degraded EM, space, or cyber environments; and allowing the system to survive and continue to operate in, or after exposure to, a CBRN environment, if required. In SoS approaches, it may also include resiliency attributes pertaining to the ability of the broader architecture to complete the mission despite the loss of individual systems.

Purpose. SS KPP attributes are those that contribute to the survivability of a system's capabilities from kinetic and non-kinetic fires. These include attributes which support:

(1) Reduced likelihood of being hit by kinetic or non-kinetic fires.
(2) Reduced vulnerability if hit by kinetic or non-kinetic fires, including cyber effects.
(3) Resiliency of the overall force (broader than a single system architecture) to complete the mission despite the loss of individual platforms.
(a) Resilience is the ability of the collection of systems to support the functions necessary for mission success in spite of hostile action or under adverse conditions.
(b) An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities.
(c) Include whether or not the system must be able to survive and operate in, or after exposure to, CBRN environments in accordance with reference uuuu. If the system is covered under reference vvvv, nuclear survivability attributes must be designated as part of the SS KPP.
(d) Include whether or not the system must be able to survive and operate in a cyber-contested environment or after exposure to cyber threats which prevent the completion of critical operational missions by destruction, corruption, denial, or exposure of information transmitted, processed, or stored.

The SS KPP along with recent cybersecurity guidance are signposts of resiliency and cybersecurity system requirements that will be flowed to contractors. As the government is working to mature these requirements and values are being extracted from guidance, we offer an industry perspective as we prepare to respond.

4 CYBER RESILIENCY IN THE SYSTEMS ENGINEERING PROCESS

Identification of operational Measures of Effectiveness (MOEs), Measures of Performance (MOPs), and Key Performance Parameters (KPPs) as discussed in the previous section, are very important for architecture. Direct measures of mission performance can be used for measuring cyber resiliency also, such as maintaining minimum values of mission KPPs and MOEs in the presence of threats of various types (kinetic, cyber, etc.) and varying severities. Figure 1 identifies the types of metrics for resiliency that can be used at each phase of the systems engineering process, in addition to the typical performance measures. The ultimate goal is to have acceptable risk that the mission will succeed, hence the higher level architecture resiliency metrics are defined in terms of risk or likelihood of mission success.

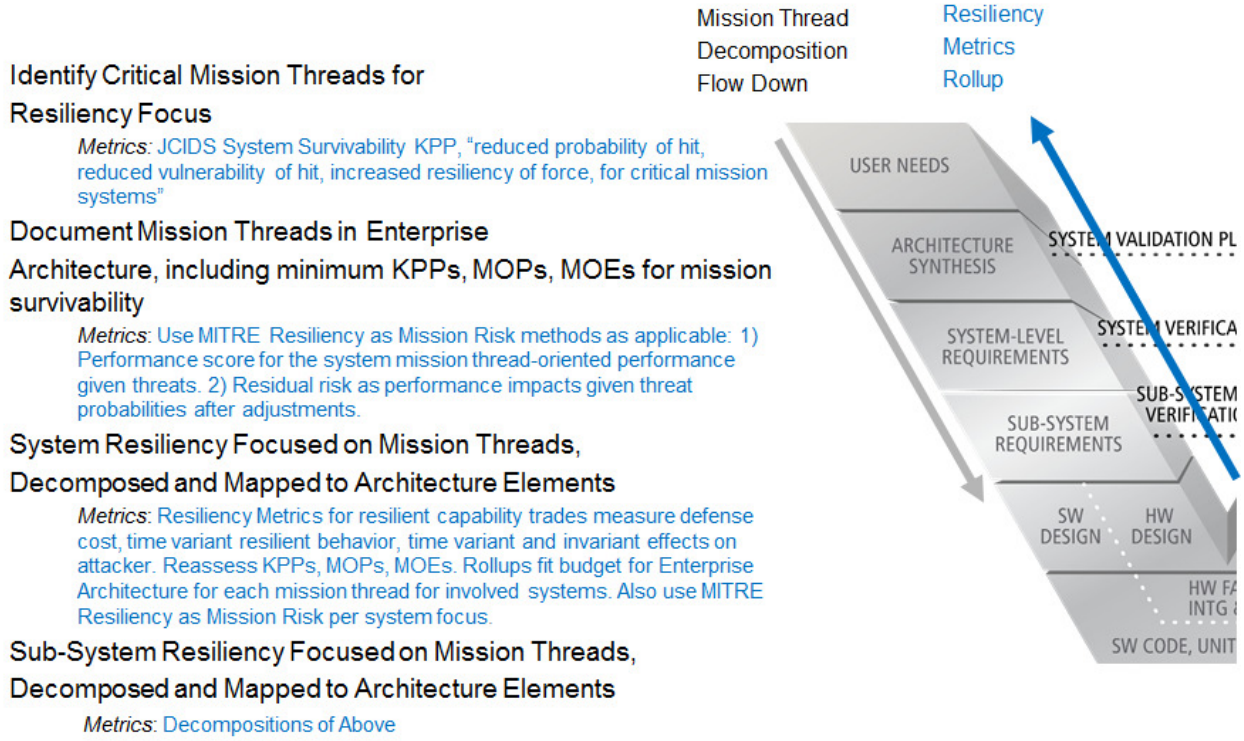


Figure 1: Cyber Resiliency Metrics on the Left Side of the "V"

The metrics become more specific going farther down the "V", and at the lower architecture levels are primarily focused on metrics to help with trades. For this reason, each metric may not directly roll up into the higher level metrics, but the trades/decisions made at the lower architecture levels may affect the higher level overall metric measurements. The selection of the appropriate metrics and the level that they are used will vary based upon the resiliency techniques being evaluated and/or the desired effects on the threat vectors [Marra 2013]. As an example, the use of redundant or vendor diverse systems to increase mission resiliency is traded at the enterprise architecture level, rather than at the system architecture level.

The identification, evaluation and further decomposition of the critical mission threads occurs at each architecture phase. This allows for cyber resiliency to be considered as appropriate for each phase.

"Use of a cyber resilience architecture framework as a reference architecture is desirable both during the initial concept and architecture phases of new systems and systems of systems and for the evaluation of existing systems and systems of systems for cyber resilience" [Hassell, 2015]. As an example, the Raytheon Cyber Resiliency Architecture Framework (CRAF) was designed to be tailored and integrated with a mission systems or enterprise architecture to provide a resilience overlay. For new architectures, the CRAF may be used as a base if desired or integrated with other reference architectures and tailored. Using an architecture framework such as this, combined with metrics for trades and evaluation, can provide a means to evaluate system architectures for resilience. For a more detailed discussion of how to use an architecture framework for resiliency assessments, please refer to [Hassell 2015].

The goal of active cyber defenses is to minimize the magnitude of the attacker's effect, increase the cost to the attacker, increase the uncertainty that the attack was successful, and increase the chance of detection and attribution. Active defenses such as cyber maneuver [Beraud 2011] and reconstitution [Sood 2009] can support these goals. An example of metrics assessing active defenses which have a direct effect on attacker operations are shown in Figure **2**, illustrating reconstitution capability metrics to be used for trades. There are several aspects to be considered in the trades, including the effect on the attacker [Sandoval 2010], cost of the defense in resources (e.g. equipment, operations, bandwidth etc.), and configuration aspects of the defense, such as timing of the active defense. Note that not all the lowest level metrics are illustrated in the figure below, since the metrics taxonomy expands into additional levels. Also, the metrics used for the specific trade must be tailored as appropriate as some of them may not apply.

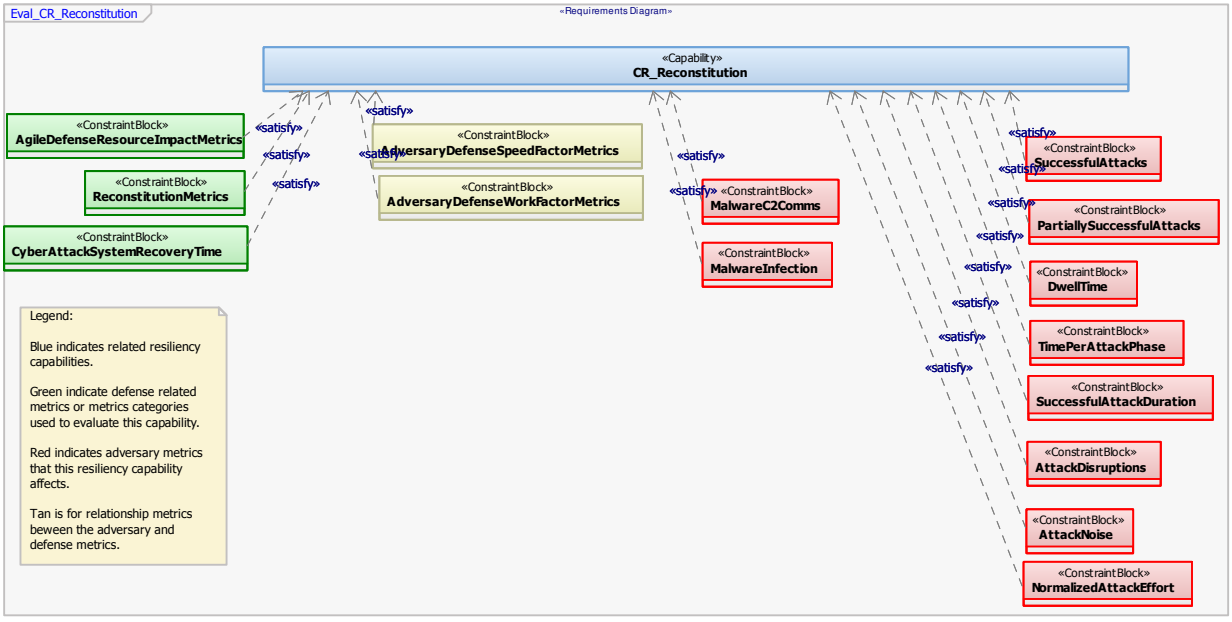


Figure 2: Example Reconstitution Metrics for Trades

5 A CASE FOR CHANGE

Contracts are awarded on technical merit, past performance, and cost. If security relevant requirements are not crisply defined with metrics and measures, system security quality attributes will be traded away to system technical capability and a more affordable solution. Today progress is being made as the presence of security relevant requirements in contract statement of work language is increasing and maturing. However, system security and program protection have not yet made it into the contract award evaluation criteria. To encourage progress, the NDIA SSE Committee led a two year collaborative effort with the NDIA DT&E Committee, INCOSE SSE Committee, Trusted Supplier Steering Group, and Mitre to provide an industry perspective.

To make progress towards developing a system security metrics and measures framework, we began to address the problem not as defense contractors and systems designers but from the warfighter's perspective.

The warfighter wants capabilities and isn't (nor should they be) concerned with system requirements (SCRM, Cyber Controls, etc). At the end of the day, the warfighter simply wants a system that has the capability to be:

- Resistant to kinetic and non-kinetic attack
- Resilient when under attack

Building from the warfighter perspective, we see strong alignment with the newly re-defined System Survivability KPP to include survivability in a cyber-contested environment.

Although resiliency has not been a part of the holistic approach to program protection, the government, industry, and academia have been advancing research and development since the mid 1990's that should be leveraged and incorporated into the mix of countermeasures and capabilities.

It is proposed that the overall system security and program protection attributes contribute to the system survivability in a mission threat environment. In the current state, each security specialty is limited in their ability to directly translate their impact and support of the SS KPP. Without having a common security relevant metric and normalized figure of merit, security gaps and seams are also more difficult to identify, analyze, and address.

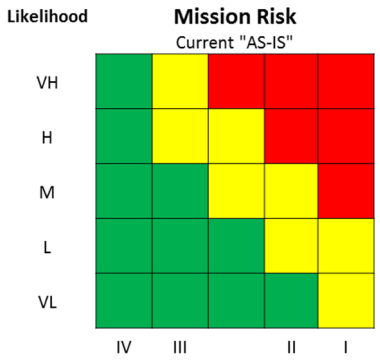
Since each security specialty has a unique set of threats, vulnerabilities, and countermeasures, a common metric is needed to be able to compare, contrast, and balance solutions across the security specialties. A common thread across all security specialties is risk. What is the likely impact or risk to the mission?

If we are able to communicate in terms of risk consistently across the security specialties, this would help to alleviate some of the intense technical intellectual discomfort many feel when talking about or referencing a specialty that is less familiar. It is overly optimistic to expect individual customers, academics, or industry contractors to have technical depth in each security specialty.

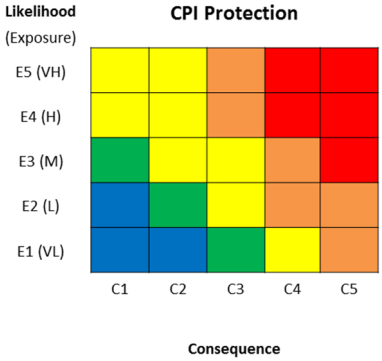
Today, there are diverse methods and guidance that may work within a particular security specialty but do not immediately translate across security specialties.

For example:

DAG Ch13 Program Protection Risk Assessment Guidance



Critical Program Information (CPI) Protection Guidance



In this example, the DAG Ch13 Program Protection Risk assessment guidance has 3 levels of risk. CPI has 5 levels of risk. How do we effectively translate or relate risk within one security specialty to another? If measuring across security specialties is a challenge, how can the value-add associated with security reasonably be expected to survive the engineering trade space?

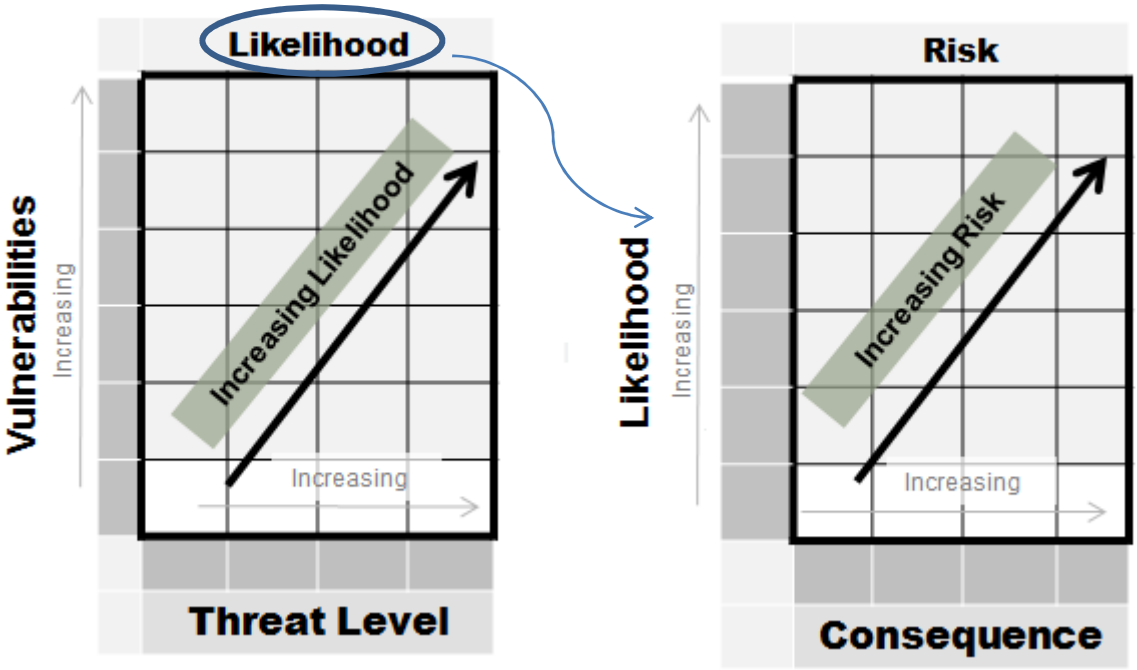
6 METRICS AND MEASURES

Metrics and measures are needed to evaluate one security solution against another. This approach includes integrating multiple security specialties into the system solution. If we were able to have a consistent metric for risk with tailored definitions of how to determine risk by security specialty, then we could make notable progress in managing and balancing risk across the security specialties.

In general terms, evaluating risks looks something like:

Threats x Vulnerabilities = Likelihood

Likelihood x Impact = Risk



However, different security specialty communities may use a slightly modified process to evaluate risk but follows the general concept. For example: the CPI community uses the term "Exposure" to define the likelihood.

Although threats and vulnerabilities are unique to each security specialty, it is proposed that consistent levels of threats, vulnerabilities, likelihood, and impact be developed.

As consistent levels are developed, bringing together definitions also helps to align and enrich the understanding of the levels. For example the DOD AT Guidelines v. 2.1, Criticality Level Characteristic definitions have been added to the MIL-STD 882E Severity and DAG CH13 Consequence definitions for one level of severity. See Appendix B Impact Definitions for a full set of definitions.

Impact (Consequence or Severity) Levels		
Description	Severity Category	Mishap Result Criteria
Catastrophic	MIL-STD-882 **1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
	C5	If ANY ONE of these characteristics exists: • Loss of Superiority/Movement in Relevant Battlespace • Loss of Most System Capability which Adversely Impacts Combat Effectiveness • Long term Technology Advantage over peer competitor • No suitable replacement projected/in-development
	System Mission Impact **I**	Results in a total compromise of system mission capability

Another safety concept that may be valuable to the security community is the evaluation of control for software.

Mil-STD 882 states:

> 4.4 Software contribution to system risk. The assessment of risk for software, and consequently software-controlled or software-intensive systems, cannot rely solely on the risk severity and probability. Determining the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware. Therefore, another approach shall be used for the assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware.

Safety evaluates the level of control and severity as follows:

Control x Severity = Level of Rigor (LOR).

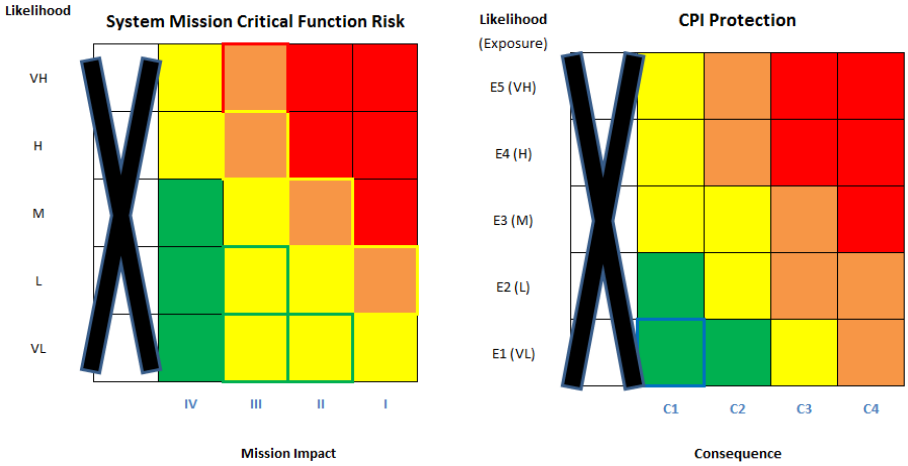
Note that the resultant is the Level of Rigor (LOR) and not risk. The added benefit of the resultant level of rigor or level of protection required directly corresponds to the actions required for risk mitigation. However, if the level of rigor in the case of software or the level of protection for CPI, is not performed or implemented, then the associated level of security specialty risk contributes to the system security risk. For specific detailed definitions for the relationship between SwCI, Risk Level, LOR Tasks, and Risk Assessment / Acceptance, see MIL-STD 882E.

See Appendix C for Software Control Categories MilStd 882E and Appendix D for Software Criticality and Levels of Rigor.

The most significant barrier to communicating across the security specialties is the variation in the risk scale. The risk scale varies from 1-3 as indicated in the Program Protection DAG Ch13 Guidance to 1-5 as indicated in the AT Guidelines for CPI. In analyzing approaches to evaluating risk, System Safety MilStd 882E was also considered as it has been matured and is widely accepted.

In an effort to bring the communities together, it is recommended to establish a consistent risk range notionally of 1-4 with 4 being the highest level of risk and 1 being the lowest level of risk. Using a scale of 1-4 removes the lower end of the range for those communities that currently use 1-5. The lower "1" risk in a scale of 5 was defined as no security relevant risk. We recommend expanding the risk range by 1 in the DAG ch13 PPP

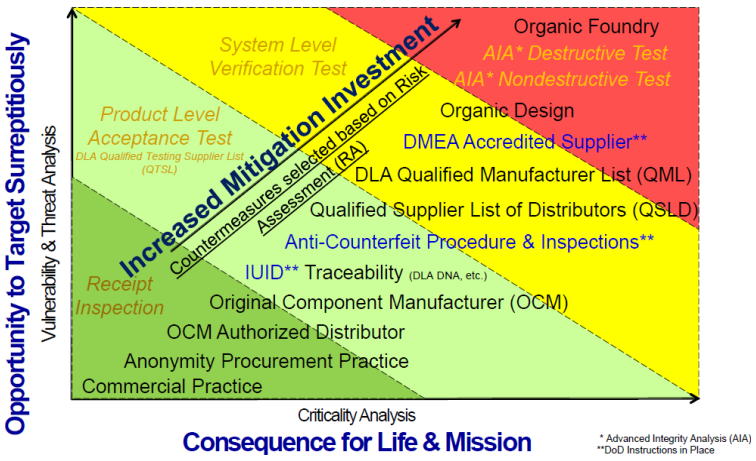
Outline Guidance to then allow for alignment of security specially risk mitigation. Below shows a notional modified PPP System Mission Critical Function Risk cube and a notional modified CPI Protection risk cube. Coordinates with different perimeter color than the area color is an indication of the transition of the current guidance state (perimeter color) to the future proposed notional state (fill color).

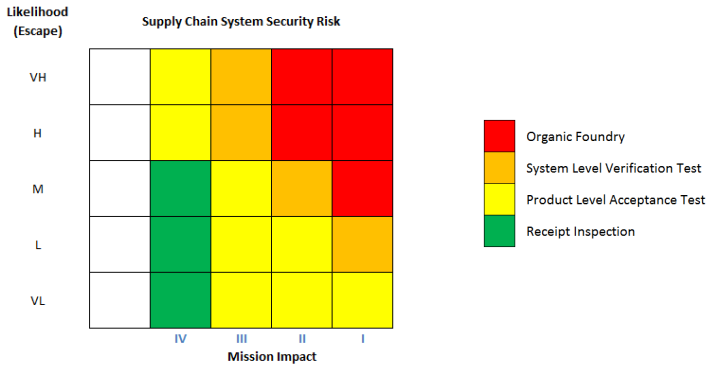


Critical components is addressed using the general PPP System Mission Critical Risk process but does not currently does not have a specific unique risk cube. The 2014 NDIA SE Conference presentation by DASD(SE) Trusted Microelectronics, Raymond Shanahan, could be leveraged to establish the supply chain levels of rigor to correspond to levels of risk.

The risk analysis for supply chain is in terms of the likelihood of escape. How likely is it that a counterfeit component or a maliciously modified component will be missed when implementing standard best practice operating procedures? The likelihood of escape is a function of the design complexity, physical gate size, and gate quantity. As the design complexity, physical gate size, and gate quantity increases, the difficulty or level of effort to validate and verify the component authenticity and integrity also increases.

Supply Chain Risk Countermeasures



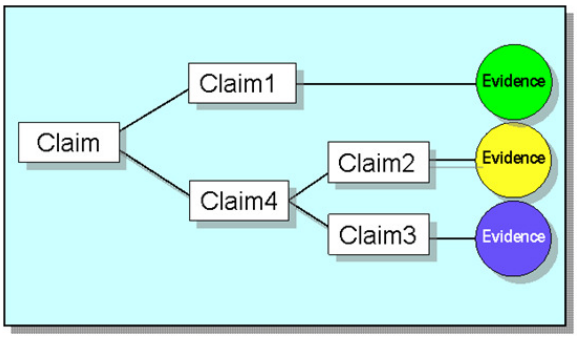


The DASD(SE) "PPP Outline and Guidance," Version 1, July 2011, requires applicable systems as described in DoDI 5200.44 to employ cost-effective countermeasures to mitigate the risk of intentional compromise of microcircuits and other CC that would result in a Criticality Level I (total mission failure) or Level II (significant/unacceptable mission degradation) impact, as determined by the criticality analysis performed by the Program Management Office (PMO). This guidance as written does not address the mid to high probability with the mid to lower level impact risk. It is proposed that a graded approach be considered with risk levels. The risk acceptance level could be determined by each program's risk appetite and affordability parameters. The risk levels broaden the spectrum of required levels of rigor to include lower impact levels but with higher probabilities.

7 CYBER RESILIENT & SYSTEM SECURITY ASSURANCE CASE MODEL

The Software Engineering Institute defines an assurance case as a means to structure the reasoning that engineers use implicitly to gain confidence that systems will work as expected. It also becomes a key element in the documentation of the system and provides a map to more detailed information.

The activities required to construct an assurance case are largely those that a conscientious developer of mission-critical systems would normally undertake. But the assurance case, and the assurance plan, highlights factors relating to system dependability in a reviewable form. An assurance case requires arguments linking evidence with claims of conformance to dependability-related requirements.



In bringing together security specialties for program protection, a rigid defined traditional test and evaluation criteria is woefully inadequate. It is proposed that a Cyber Resilient and System Security Assurance Case Model be used to assess a program's system security posture and overall program protection. The Cyber Resilient and System Security Assurance Case may also provide valuable evidence to contribute to evaluating a system's survivability, KPP. The Cyber Resilient and System Security Assurance Case would allow for a structured argument to be developed to include the system functional decomposition, criticality analysis, and evidence of countermeasures or risk mitigations leveraged such as: technologies, tools, techniques, processes, expertise, and testing. The assurance model will help to visually trace how decisions were made, what risks were accepted, what considerations were evaluated, and what was actually implemented.

Fully embracing the cybersecurity shift-left to test earlier in the systems engineering product development lifecycle concept is applicable to all the security specialties. It is proposed that the Cyber Resilient and System Security Assurance Case be integrated into the Test and Evaluation Master Plan (TEMP). The PPP or contractor PPiP and TEMP should be closely tied together. The Chief Developmental Tester (CDT) should support the Chief Engineer/Lead Systems Engineer in PPP requirements development to include assessing PPP requirements for adequacy and testability. As the chair of the Test and Evaluation Working Integrated Product Team (T&E WIPT), the CDT should seek opportunities to improve efficiency by integrating Cyber Resilient and System Security Assurance Case verification into other planned DT&E events.

8 CONCLUSION

As defense system integrators and the extended industrial base designs, develops, test, and field systems, it is imperative that we maintain security within the forefront of our priorities. As defense contractors, our actions are powerfully driven by legal contractual requirements. We struggle to conduct system security solution trades that include requirements ambiguity. As individuals, we want to provide the greatest and most advanced trusted capability to the war fighter as quickly as possible. However, we all work within a cost competitive and customer budget constrained environment. Therefore, crisp well defined requirements matter as does a compelling evidence-based demonstration of why the delivered system can and should be trusted. As defense systems integrators, we want to propose solutions that will be evaluated against known qualitative and quantitative measurable criteria. As business professionals we require work to stay in business and to stay in business we must win contracts. The challenge is technically, politically, financially, and procedurally complex. Providing true holistic program protection requires a fully committed government, industry, and academic partnership

The next steps included a review and discussion of the notional concepts presented in the paper with government partners. Both government and industry believe that a project to focus on developing the system security risks contributions to the program technical performance risk would be valuable to raise the attention and impact of security to the overall system risks which need to be monitored and assessed throughout the product development lifecycle. Additional concepts for consideration to system security engineering and holistic program protection are summarized below.

Summary of Concepts Presented

1. PPP alignment to support the System Survivability (SS) KPP
2. Add design for cyber resiliency at the architectural level as a countermeasure to holistic program protection
3. Risk
    I. Common risk scale and normalized figures of merit across security specialties
    II. Common levels for threats, vulnerabilities, likelihood, and impact.
    III. Level of rigor concept and if not implemented system security specialty risk contribution to system security risk.
        i. SCRM example of leveraging this concept
4. Cyber Resilient and Secure Systems Assurance Case

9 REFERENCES

[Bodeau, 2013] Bodeau, D., Graubart, R. "Cyber Resiliency Assessment: Enabling Architectural Improvement", MITRE, May 2013.

[Beraud, 2011] Beraud, P., Cruz, A., Hassell, S. and Meadows, S. "Using Cyber Maneuver to Improve Network Resiliency", Military Communications Conference [MILCOM] 2011, Baltimore MA, November 8-10, 2011.

[DoD, 2011] "Program Protection Plan Outline & Guidance", Version 1.0, Deputy Assistant Secretary of Defense Systems Engineering, July 2011

[DoD, 2015] "PM Guidebook for Integrating the Cyber Security Risk Management Framework into the System Acquisition Lifecycle", Version 1.0, May 2015

[DoDI, 2014] 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014

[DOT&E, 2013] "Director, Operational Test and Evaluation, FY2013 Annual Report", Michael J. Gilmore

[ENISA, 2011] "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report", ENISA (European Network and Information Security Agency), February 2011

[Gilmore, 2014] Gilmore, M., "Procedures for Operational Test and Evaluation of Cyber security in Acquisition Programs", Office of the Secretary of Defense, August, 2014.

[Goldman, 2010] Goldman, H., "Building Secure, Resilient Architectures for Cyber Mission Assurance", Secure and Resilient Cyber Architectures Conference, McLean, VA, October, 2010.

[Hassell, 2012] Hassell, S., Beraud, B., Cruz, A., Ganga, G., Martin, S., Toennies, J., Vazquez, P., Wright, G., Gomez, D., Pietryka, F., Srivastava, N., Hester, T., Hyde, D., Mastropietro, B., "Evaluating Network Cyber Resiliency Methods using Cyber Threat, Vulnerability and Defense Modeling and Simulation", Proceedings of Milcom, November 2012.

[Hassell, 2015] Hassell, S., Case, R., Ganga, G., Martin, S.R., Marra, S. and Eck, C., "Using DoDAF and Metrics for Evaluation of the Resilience of Systems, Systems of Systems and Networks Against Cyber Threats", INCOSE INSIGHT, Volume 18, issue 1, April 2015, p.26-28.

[JCIDS, 2015] Manual For The Operation Of The Joint Capabilities Integration And Development System (JCIDS) 12 February 2015 – Enclosure D Appendix C

[King, 2011] Dr. Steven E. King, "Cyber S&T Priority Steering Council Research Roadmap for the National Defense Industrial Association Disruptive Technologies Conference", November 2011.

[Marra, 2013] Marra, S., Hassell, S., Eck, C., Moody, J., Martin, S., Ganga, G., Harward, K., Rickard, E., Sandoval, J., Brown, J., "Cyber Resiliency Metrics for Discussion", Proceedings of the MITRE Cyber Resiliency Workshop, 2013.

[Musman, 2014] Musman, S., Agbolosu-Amison, S., "A Measurable Definition of Resiliency Using "Mission Risk" as a Metric", February 2014, MITRE

[OSD, 2014] Deputy Assistant Secretary of Defense for Systems Engineering and Department of Defense Chief Information Officer, "Trusted Systems and Networks (TSN) Analysis", June 2014

[Pal, 2006] "Intrusion Tolerance by Unpredictability and Adaptation", http://itua.bbn.com/

[Sandoval, 2010] Sandoval, J. and Hassell, S. "Measurement, Identification and Calculation of Cyber Defense Metrics", Military Communications Conference (MILCOM) 2010, San Jose CA, October 31, 2010 – November 3, 2010.

[Sood] http://cs.gmu.edu/~asood/scit

APPENDIX A. PARALLEL EFFORTS AND PRIOR COMMITTEE WORK

NDIA DT&E Committee Integrating Testing (2009): Integrated testing is the collaborative planning and execution of contractor, developmental, and operational testing to provide shared data to support independent analysis across the test program. The NDIA Systems Engineering Division DT&E Committee developed a framework to integrate the people, planning, and data to streamline the test program and introduce operational realism early in to the program.

NDIA DT&E Committee Developmental Tester (2014): The Chief Developmental Tester role was introduced in 2011 to coordinate DT&E activities, provide insight into contractor activities, oversee test and evaluation activities, and inform the government Program Manager about contractor DT&E results. The NDIA DT&E Committee reviewed the service policies for the new role to propose a model for industry interaction to provide a comprehensive test strategy for programs.

INCOSE SSE Working Group: Systems Security Engineering is ultimately a systems engineering responsibility. The working group has defined the systems security engineering practices throughout the lifecycle and promoted systems security activities as part of the systems engineering process. The working group collaborates with other working groups to bring the systems security perspective to other systems engineering practices (e.g. Systems of Systems, Agile, Resilient Systems, Competency)

2014 Recommendations for Cybersecurity DT&E Guidelines: The NDIA DT&E Committee provided an industry perspective on the Cyber DT&E guidelines to address roles and responsibilities, Program Protection Planning, testing techniques, and test optimization.

- 2014 NDIA 3 day PPP Workshop:
    - Senior Executive Leadership presentations from OSD, Military Service, and Prime Defense System Integrators
    - (3) Breakout sessions
        - Metrics & Measures
        - Integration of Security Specialties
        - Contracting for SSE & DT&E
    - Prioritized list of challenges
        - Metrics & Measures
        - Balancing risk and solutions which address cost vs capability
        - Ill-defined SSE & PPP requirements in SOW language
        - Absence of well-defined SSE Competencies
        - Shared liability & Risk Boundary

- 2014 NDIA 1 day Metrics and Measures Workshop:
  - Goal per discussion is to develop a framework for metrics and measures to characterize the security "goodness" of a system. – System Security Risk.
  - Framing the problem for mission impact and mission success.
  - What is measurable?
    - SwA Discussion
      - SOAR Report – Measuring Cyber Security Report
    - Draft Air Force Program Protection Metrics Scorecard w/ binary responses.
    - Need for a common scale & normalized figures of merit
    - Risk is a common thread across all security specialties.
  - What can we learn from the safety community?
    - Assurance models
- 2015 NDIA SSE Committee Meetings April:

  Expanded the metrics & measures project to include NDIA DT&E Committee
  - Expanding holistic program protection to include cyber resiliency within the system architecture
  - Trusted Supplier Steering Group
  - Cyber DT&E shift left
  - Relationship and synergies between PPP & TEMP
- 2015 NDIA SSE Committee Meetings June:
  - Solidified key concepts for metrics & measures
  - Developed outline

APPENDIX B. IMPACT DEFINITIONS

Impact (Consequence or Severity) Levels		
Description	Severity Category	Mishap Result Criteria
Catastrophic	MIL-STD-882 1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
	C5	If ANY ONE of these characteristics exists: • Loss of Superiority/Movement in Relevant Battlespace • Loss of Most System Capability which Adversely Impacts Combat Effectiveness • Long term Technology Advantage over peer competitor • No suitable replacement projected/in-development
	System Mission Impact I	Results in a total compromise of system mission capability
Critical	MIL-STD-882 2	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
	C4	If ANY ONE of these characteristics exists: • Loss of Battlespace advantage (parity) • Loss of Some System Capability which Adversely Impacts Combat Effectiveness • Moderate Technology Advantage over competition • Potential moderate timeline required for a suitable replacement
	System Mission Impact II	Results in unacceptable compromise of system mission capability or significant system mission degradation.
Marginal	MIL-STD-882 3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
	C3	If ANY ONE of these characteristics exists: • Loss of Military Advantage; Capability Could be Replaced by Military Systems with Equivalent Capabilities • Minor Loss of System Capability Degrading Combat Effectiveness from Primary Mode of Operation • Midterm Technology Advantage over competition • Potential mid timeline required for a suitable replacement
	System Mission Impact III	Results in partial compromise of system mission or partial system mission degradation.
Negligible	MIL-STD-882 4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, monetary loss less than $100K, or
	C2	If ANY ONE of these characteristics exists: • Little or No Direct Loss of Military Advantage • Little to No Direct Loss of System Capability Degrading Combat Effectiveness • Minimal Technology Advantage over competition • Near-term replacement can be fielded < 3 years
	System Mission Impact IV	Results in little or no compromise of system mission capability.
	MIL-STD-882 5	N/A
	C1	If ANY ONE of these characteristics exists: • Loss of System Capability easily mitigated by changes in CONOPS / Tactics • Comparable technology easily available to peer / near-peer competitors
	System Mission Impact	N/A

APPENDIX C. SOFTWARE CONTROL CATEGORIES MIL-STD 882E

Software Control Categories (Leveraged from Safety MIL-STD 882E and modified for Security)		
Level	Name	Description
1	Autonomous (AT)	Software functionality that exercises autonomous control authority over potentially ~~safety~~ **security**-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard. *(This definition includes complex system/software functionality with multiple subsystems, interacting parallel processors, multiple interfaces, and ~~safety~~ **security**-critical functions that are time critical.)*
2	Semi-Autonomous (SAT)	Software functionality that exercises control authority over potentially ~~safety~~ **security**-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent ~~safety~~ **security** mechanisms to mitigate or control the mishap or hazard. *(This definition includes the control of moderately complex system/software functionality, no parallel processing, or few interfaces, but other ~~safety~~ **security** systems/mechanisms can partially mitigate. System and software fault detection and annunciation notifies the control entity of the need for required ~~safety~~ **security** actions.)* Software item that displays ~~safety~~ **security**-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence. *(This definition assumes that the ~~safety~~ **security**-critical display information may be time-critical, but the time available does not exceed the time required for adequate control entity response and hazard control.)*
3	Redundant Fault Tolerant (RFT)	Software functionality that issues commands over ~~safety~~ **security**-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition. *(This definition assumes that there is adequate fault detection, annunciation, tolerance, and system recovery to prevent the hazard occurrence if software fails, malfunctions, or degrades. There are redundant sources of ~~safety~~ **security**-significant information, and mitigating functionality can respond within any time-critical period.)* Software that generates information of a ~~safety~~ **security**-critical nature used to make critical decisions. The system includes several redundant, independent fault tolerant mechanisms for each hazardous condition, detection and display.
4	Influential	Software generates information of a ~~safety~~ **security**-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap.
5	No ~~Safety~~ **Security** Impact (NSI)	Software functionality that does not possess command or control authority over ~~safety~~ **security**-significant hardware systems, subsystems, or components and does not provide ~~safety~~ **security**-significant information. Software does not provide ~~safety~~ **security**-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of ~~safety~~ **security**-significant or time sensitive data.

APPENDIX D. SECURITY SOFTWARE CRITICALITY LEVELS

Risk	SW Criticality Level	Level of Rigor Tasks
	SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth ~~safety~~ **security**-specific testing.
	SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth ~~safety~~ **security**-specific testing.
	SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth ~~safety~~ **security**-specific testing.
	SwCI 4	Program shall conduct ~~safety~~ **security**-specific testing.
	SwCI 5	Once assessed by ~~safety~~ **software assurance** engineering as Not ~~Safety~~ **Security**, then no ~~safety~~ **security** specific analysis or verification is required.

APPENDIX E. ABREVIATIONS AND ACRONYMS

Abbreviation/ Acronym	Definition
AT	Anti-tamper
CA	Criticality Analysis
COCOM	Combatant Command
CPI	Critical Program Information
CRAF	Cyber Resiliency Architecture Framework
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
FOSS	Free and Open Source
GOTS	Government-Off-The-Shelf
IA	Information Assurance
IP	Internet Protocol
JCIDS	Joint Capabilities Integration and Development System
KPPs	Key Performance Parameters
MOEs	Measures of Effectiveness
MOMA	Method of Objective Mission Analysis
MOPs	Measures of Performance
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
PM	Program Manager
PPP	Program Protection Plan
QA	Quality Attribute – “ility”
RFI	Request for Information
SE	Systems Engineering
SEI	Software Engineering Institute – Carnegie Mellon University
SS	System Survivability (the JCIDS KPP)
TBD	To Be Determined
TPMs	Technical Performance Measures
TSN	Trusted Systems and Network – DoD Analysis Method

APPENDIX F. JCIDS MANUAL FEB 2015 APPENDIX C ENCLOSURE D

This appendix contains most of JCIDS Appendix C Enclosure D, which defines the Survivability KPP. All references not believed to be useful or applicable have been removed. The removed information is primarily Chemical, Biological, Radiological, and Nuclear (CBRN) focused. The author of this report assumes that references to "non-kinetic" apply whether or not 'cyber" is explicitly mentioned. Notes in brackets document applications of the KPP to help understand cyber resiliency.

APPENDIX C TO ENCLOSURE D
CONTENT GUIDE FOR THE SYSTEM SURVIVABILITY KPP

1. Overview

a. Purpose. SS KPP attributes are those that contribute to the survivability of a system's capabilities from kinetic and non-kinetic fires. These include attributes which support:

(1) Reduced likelihood of being hit by kinetic or non-kinetic fires.

(2) Reduced vulnerability if hit by kinetic or non-kinetic fires, including cyber effects.

(3) Resiliency of the overall force (broader than a single system architecture) to complete the mission despite the loss of individual platforms. *[Note the mission focus here rather than systems focus]*.

(a) Resilience is the ability of the collection of systems to support the functions necessary for mission success in spite of hostile action or under adverse conditions.

(b) An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities.

(d) Include whether or not the system must be able to survive and operate in a cyber-contested environment or after exposure to cyber threats which prevent the completion of critical operational missions by destruction, corruption, denial, or exposure of information transmitted, processed, or stored.

b. Synergy/overlap with FP KPP. The SS KPP may include some of the same attributes as those in the FP KPP, but the emphasis is on maintaining the mission capabilities of the system through the applicable threat environment rather than protecting system occupants or other personnel.

c. Exclusion of Offensive Capabilities. Offensive capabilities that are primarily intended to defeat adversary forces before they can engage non-adversary forces are not included in the SS KPP.

d. Tailoring of Standards. For attributes listed below which have an associated standard identified, compliance with the standard is expected unless specific operational context for the capability solution indicates that a higher or lower standard of system survivability is more appropriate. In cases where a deviation from the standard is appropriate, the SS KPP will identify the tailored levels of system survivability required, along with rationale as to why the operational context makes a different level of system survivability appropriate.

2. Potential Attributes or Considerations. Depending upon the aspect of system survivability addressed by the attribute, these may be applicable to the overall system, only applicable to certain subsystems, or applicable at different levels of survivability to different parts of the system.

a. For reduced probability of hit. Reduced likelihood of being hit by kinetic or non-kinetic fires: *[This applies to evasive cyber resiliency capabilities such as moving target defenses, randomized responses, deception etc.]*

(1) Situational awareness, such as missile warning, laser warning, radar warning, or hostile fire indication capabilities.
(2) Speed.
(3) Maneuverability.
(4) Visual, acoustic, and/or electronic detectability, including EM spectrum control.
(5) System countermeasures, such as RF jammers, laser dazzers, and expendable dispensing systems.
(6) Accurate engagement - lethal and non-lethal.
(7) Electronic protection.
(8) Access control.

b. For reduced vulnerability if hit. Reduced vulnerability of critical system components or structures (i.e., radars, weaponry, or command & control devices) if hit by kinetic or non-kinetic fires.

(1) Durability – inherent ability of components or structures to withstand hit/blast/flood/shock for kinetic fires, or resistance to EM or cyber effects from non-kinetic fires.
(2) Added protection – armor for components or structures without sufficient durability to survive kinetic fires, or shielding/hardening for components without sufficient resistance to EM or cyber effects from nonkinetic fires.
(3) Redundancy – ability of individual components or structures to be compromised, from kinetic or non-kinetic fires, without loss of the system's capabilities.

c. For increased resiliency of the force

(1) Robust architecture – ensuring capabilities remain available despite losses of specific numbers of systems, or losses of specific enabling systems.

(a) Systems dependent upon Positioning Navigation and Timing (PNT) capabilities shall be compliant with PNT survivability policies in reference bbbbb, or obtain a waiver in accordance with the process outlined therein.

(b) Survivability under loss of other enabling systems may be governed by other policies and will be evaluated on a case-by-case basis.

(2) Networked – ensuring data remains available despite losses of specific numbers of systems, or losses of specific enabling systems.

(4) Survival and operation in a cyber-contested environment or after exposure to cyber threats, if applicable to the operational context:

(a) In accordance with reference ccccc, state the system's cybersecurity categorization for availability, integrity, and confidentiality and whether the system is an applicable system in accordance with reference ddddd.

(b) If cyber survivability is required, include appropriate cyber attributes in the SS KPP based on applicable cybersecurity controls as directed by reference ccccc and strength of implementation required to protect against cyber threats likely to be encountered in the operational environment.

(c) If applicable, address operational and maintenance issues related to ensuring continuing resilience against cyber threats.

3. Proponent. The SS KPP proponent is the Protection FCB. For questions, please contact the Protection FCB at 703-693-7116.