An Actionable Framework for System of Systems and Mission Area Security Engineering

J. Dahmann, G. Rebovich, G. Turner
The MITRE Corporation
Bedford, MA 01730
{jdahmann, grebovic, gturner}at mitre.org

Abstract— **This paper describes an actionable engineering framework for security engineering of a system of systems (SoS). The framework is envisioned as a tool for assessing security risks to critical missions based on the contributing systems and SoS supporting them. An SoS security risk framework is needed to manage the problem of identifying the key elements of risk to SoS missions. The issue is the complexity resulting from the large number of potential logical paths through an SoS that could represent a security risk. Managing this problem then enables the application of security specific analyses to the SoS elements that have been identified as critical. The framework draws on the foundational elements of SoS SE, particularly an understanding of the SoS components, interdependencies and dynamics. The results of the analysis support investment decisions about the constituents of a SoS. The framework is a bridge between the operational and acquisition/engineering communities. While the focus of this framework is on acquisition and engineering materiel solutions, it also accommodates the consideration of non-materiel solutions.**

Keywords—system of systems; system security engineering; critical missions; acquisition; system engineering

I. Introduction

The security threat is real, large and growing. Networks, systems and the missions they enable are at risk from malicious intrusion, supply chain attacks and other threats. These can reduce warfighter effectiveness in key operations and put lives and critical missions at risk. [1, 2]

The overall goal of this effort is to identify repeatable methods to address security risks to systems of systems (SoS) supporting critical missions. The focus is on military defense but may be extensible to other domains where SoS are vulnerable to security risks.

We look at the problem from the point of view of the military mission, the system engineering (SE) and management of the supporting SoS and its constituent systems, as well as the enabling network and other infrastructure.

This paper builds on an earlier activity that identified logical extensions to current DoD SoS SE guidance to incorporate system security engineering (SSE) and base lined SoS SSE state-of-the-practice via interviews of active practitioners [3]. This paper reported on a study to identify logical extensions of SoS SE guidance to address security concerns as part of SoS SE and then based on a set of case studies sought to identify evidence that these extension have been implemented in current SoS activities. The comparison of the current practices with the logical extensions found a general lack of attention to SoS SSE and little evidence of the extensions in practice.

II. Background and Motivation

The US Department of Defense (DoD) is addressing security of new systems by building protection into their acquisition and engineering processes. This is reflected in efforts to inject consideration of threats into the design of systems, motivated by program protection planning (PPP) and other policies which direct investment of resources in system security engineering (SSE) of individual systems. Every system-level acquisition program is required "to identify critical functions and components and manage their risk of compromise" including hardware, software, firmware and information [4], that is, security vulnerabilities of systems are to be addressed as part of systems engineering of the system.

The current US DoD methodology to manage the risk of compromise includes processes to: identify critical system functionality and components; assess threats to and vulnerabilities of the components in operational, program and development environments; and identify and assess countermeasure options.

Building security into newly developed systems is an important step in the right direction. But these systems get fielded as part of a SoS with other systems that have not necessarily been through the same SSE processes. The larger reality is that the number of new systems the DoD fields is miniscule compared to the number of legacy ones and is likely to remain so in the prevailing fiscal environment. The problem then is how to engineer for mission success when most missions will be supported by a SoS composed of constituent systems with very uneven levels of security protection and with the potential for additional vulnerabilities introduced by the SoS configuration. In particular, can we apply the SSE risk-based methodology to systems engineering of SoS to assure mission success?

Guidance for systems engineering of SoS is relatively silent on security. The 2008 Systems Engineering Guide for Systems of Systems [5] states:

> "… more work is needed to better understand the role of SE in SoS not addressed in this guide. This understanding will enable one to better address SE issues that go beyond the initial class of SoS addressed here. These areas include:
>
> - …
> - Systems assurance issues posed by SoS"

Work has been done to show how SoS SE could be logically extended to incorporate SSE but there is little evidence that it is happening in practice [3]. SSE is generally seen as a system-level issue, not that of the end-to-end SoS or mission. At the SoS level, less attention is placed on in-service system protection than new developments. SoS architectures do not typically include security considerations. Security is not normally included in formal SoS agreements and end-to-end security risk management is typically not addressed.

The primary purpose of this paper is to present an actionable engineering framework for conducting SSE of a SoS for critical missions. In developing the framework we addressed the following considerations:

- How should risks to a SoS/mission be assessed so they can be countered?
- Can the approach being pursued for systems be adapted to SoS?
- What type of SoS analysis provides the logical foundation for implementation of SoS SSE?
- How can we identify effective approaches to SoS SSE analysis and implementation for priority missions?

III. APPROACH

There are a growing number of techniques to improving mission assurance and many of them are increasing in maturity [6, 7, 8, 9].

Current analytical techniques to protection of systems are based on a methodology which identifies critical components of the system; their risks to persistent threats and vulnerabilities; and options for countermeasures to address the risks.

Security-specific techniques take a somewhat specialized view depending on their original focus (e.g., an operational view of cyber and information technology assets) and tend to assume an understanding of the mission, systems and dependencies rather than explicitly incorporating these knowledge finding activities in their processes.

However, the increased complexity of analyzing an SoS requires an especially clear understanding of the SoS as a critical prerequisite to the application of these approaches. This is particularly true of the SoS components and their interdependencies that are critical to mission outcomes.

How can current analytical techniques be adapted to a SoS and risks to its missions? Our approach has been to:

- Develop a cross-cutting mission area SSE framework to identify risks to critical missions and assess potential solutions
- Identify and storyboard or pilot promising analytical techniques against a detailed DoD test case to evaluate what mix of approaches could support SoS SSE across different situations
- Synthesize the results into an actionable SoS SSE engineering framework based on the system-level approach to SSE

IV. FRAMEWORK OVERVIEW

The purpose of the SoS SSE engineering framework is to provide a structured systems engineering approach to addressing security for SoS supporting missions and technical grounding for investments in security to improve the likelihood of successful mission outcomes.

We envision users of the framework to be organizations responsible for delivery of technically sound mission capabilities, including: system engineering offices responsible for the SoS (e.g., Joint Systems Engineering Integration Office SE); DoD Military Components or Command with mission or portfolio responsibility; and organizations with specific tasking to address risks to key missions. Users of the results of the framework would be decision makers responsible for system improvement investments.

A. Driving Factors

There are a number of factors that drive the need for and shape of a SoS SSE engineering framework. First is the increasing recognition of the persistent threat and its potential impact on mission outcomes, particularly for critical missions. The recognition of the problem and the need for attention at the mission/SoS level are increasing despite the lack of action to this point. Second, progress is being made in protecting systems, but considerable residual risk remains given the large legacy component of fielded assets and the complex interdependencies that exist in SoS supporting missions. While protecting systems is important, it may not be sufficient to assure missions. Third, missions are predominantly supported by fielded systems and any improvements to security need to realistically consider current operational system configurations. Understanding the current systems and operations is key to assessing risks and investment options in systems to improve assurance. A consequence is that any framework needs to bridge the operational and system acquisition/engineering communities, as depicted in figure 1.

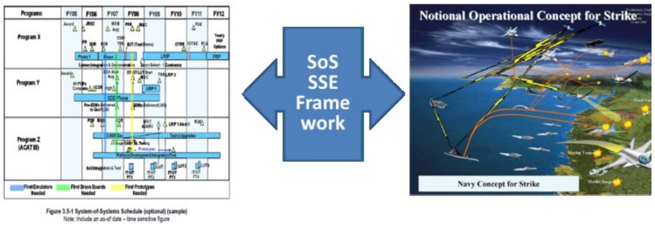

Figure 1. SoS SSE Framework Bridges Acquisition/Engineering and Operational Communities

Fourth, SoS and their support to missions in an operational and threat context constitute a complex environment which challenges the application of system-level approaches to SSE. Therefore, it is important to consider this complexity when identifying security improvements to account for unintended effects, missing actions, and to ensure the desired mission impact. Lastly, the growing inventory of approaches to address system security risks calls for an engineering framework to provide the structure needed to leverage them in a SoS/mission context.

B. Framework Introduction and Foundation

The SoS SSE framework is a five-stage SE process for analyzing a SoS from a mission perspective to identify elements critical to mission outcomes that are at risk. The framework builds on our current understanding of SE as applied to SoS; a growing inventory of approaches to address security risk to systems; and current processes for identifying and addressing changes in systems to support mission success. The framework is based on the recognition that improvements to mission security need to focus on current and projected operational needs and risks to fielded SoS, and targeted changes to fielded system elements judged to have the greatest impact on mission outcomes. The framework is depicted in figure 2.

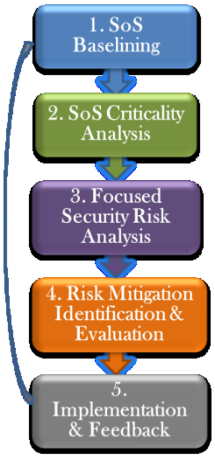

Figure 2. SoS SSE Engineering Framework

The SoS SSE framework is a tailoring of the SoSE Wave Model [10]. Ideally, implementation of SSE would be done as part of SoSE, as depicted in figure 3. This implementer's view of SoS SE is based on iterative implementation of four key steps as shown in the figure. 'Conducting SoS Analysis' is an ongoing SoS SE activity. Security analysis depends on the basic SoS SE analysis and is used this to identify areas for focused security analysis. Risk mitigation is addressed in either evolution of the SoS architecture and/or the constituent systems, changes to which are implemented as part of the normal implementation processes.

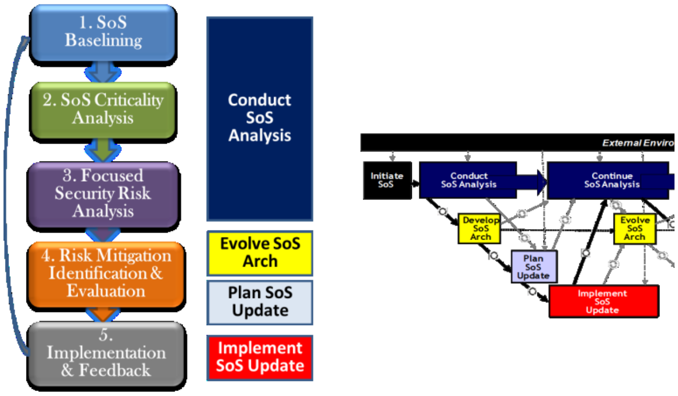

Figure 3. SoS SSE relationship to SoSE Wave Model

The details of the SSE framework stages are described below.

C. SoS Baselining

The objective of SoS baselining is to understand the key elements of the SoS and how they address mission outcomes. SoS elements include mission and enabling infrastructure systems, links and interfaces. Understanding the current configuration of SoS elements and their roles in mission execution is the starting point for improving security to ensure mission effectiveness. There are a growing number of approaches to addressing mission resilience to advanced threats, but to apply them requires a good understanding of the current "brownfield" mission situation, including mission CONOPS and outcomes, end-to-end functionality and performance measures. Steps required to achieve this understanding include describing the current systems and links that comprise the SoS and their relationships, and defining the dynamics of the SoS and the environments which support the mission outcomes. The result is a technical foundation for analysis of critical elements, security risks and mediations. SoS baselining may be straightforward where some type of SoS engineering effort already exists, but if not it may require investment.

There are a variety of approaches for defining and representing the SoS and its mission, including integration and interoperability baselining tools based on mission threads and system data from operational testing, standards-based business process modeling (BPM) techniques for representing activities and sequential relationships, various architecture tools (e.g., DoDAF) for depicting systems and their relationships, and model-based approaches (e.g., UML, SysML) to represent SoS elements, behaviors and relationships.

D. SoS Criticality Analysis

The objective of the SoS criticality analysis is to identify the key elements of the SoS essential to mission outcomes. Since comprehensive protection of an end-to-end SoS is generally not tractable, a way to identify critical SoS elements and manage complexity is needed. At this stage, the identification of critical elements is done independent of any risks or threats to them. Risk/threat analysis is the focus of the security risk analysis stage. Complexity inherent in the SoS and the role SoS elements play in mission execution determine criticality of SoS elements which drive protection priorities.

Various representation and analysis approaches can be applied to help establish critical SoS elements and evaluate how potential changes to them might impact mission assurance. SoS criticality analysis consists of three interacting activities, as depicted in figure 4 and described below.

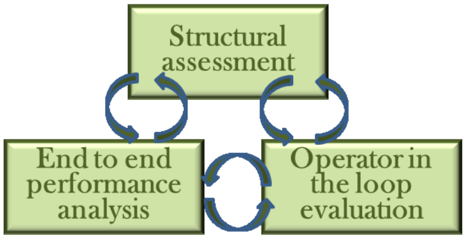
Structural assessment
End to end performance analysis
Operator in the loop evaluation

Figure 4. SoS Criticality Analysis Activities

1) Structural Assessment: The purpose of the structural assessment is to identify the elements of the SoS that are clearly critical to the mission and those that are clearly not critical, as a starting point for the SoS criticality analysis. Starting with the baseline SoS description, the first step is to define the end-to-end systems flows and dependencies required to execute the mission. Based on an analysis of the structure of the SoS architecture, the next step is to identify those elements which are clearly critical path for mission success and those that are not and can be ruled out from further criticality analysis. The product or outcome of the structural assessment is an initial identification of elements of the SoS that are potentially critical to mission outcomes.

Tools and technical approaches for structural assessment include: lessons learned from operations/user inputs; business process models, architecture representations and analyses and functional dependency network analysis (FDNA) [11]. Operator and user inputs are a good starting point. They may reveal considerations not otherwise apparent. However, they require other methods to validate them. BPMs provide an activity/system sequence representation of an end-to-end mission thread which supports analysis of flows, paths through nodes and dependencies. DODAF data include structural descriptions of the mission elements and relationships. Tools like System Architect provide capabilities to conduct analysis of SoS elements. FDNA is a methodology that can be used to model and measure the operational effectiveness of a mission network. It provides a method to assess the ability of a network to operate effectively if one or more of its entities or entity chains degrade, fail or are eliminated due to adverse events.

2) End-to-End Performance Analysis: The end-to-end performance analysis is done to understand the SoS behavior and the effects of loss of, incursions or disruptions to critical elements on mission outcomes. The first step is to identify an appropriate model or simulation to represent the SoS critical missions, a set of scenarios which reflect the mission context, the mission objectives and metrics for measures of performance and effectiveness. This may include discrete event simulations (e.g., EADSIM, JIMM), agent-based models, or other operations/systems analysis environments used to address other mission-level issues in specific mission areas. The next step is to represent the end-to-end mission thread, including systems and their behaviors, in a realistic operational context to simulate the mission in a selected set of scenarios. A series of simulations would be run, starting with a base case to assess nominal mission performance and effectiveness, followed by excursions in which changes to critical SoS elements are made to evaluate impacts on mission performance and effectiveness. When there are a sizable number of critical SoS elements, an analysis of experiments may need to be conducted first to scope the set of excursions required to identify key elements for detailed mission performance and effectiveness analysis. Capabilities like the MITRE Elastic Goal-Directed Simulation Framework (MEG) could be employed to support these analyses. MEG supports simulation-based optimization and other advanced design of experiment methods for legacy simulations [12]. The product or outcome of the end-to-end performance analysis is a set of priority SoS elements to be analyzed for security risk to the mission. The results may indicate the need for additional structural analysis or provide data needed for structural analysis techniques (e.g., FDNA).

3) Operator in the Loop Evaluation: The operator in the loop (OIL) evaluation is intended to get a realistic perspective on critical elements in an operational context via simulation exercises (SIMEX), operational exercises or observations of operations. Techniques may range from observing operations or operational exercises to collecting, analyzing and assessing data from a structured OIL experiment on the critical elements identified in the structural and performance analyses. The idea is to put a spotlight on the real-time human dimension of potential solutions or operational workarounds that may not be illuminated by other analysis approaches. OIL results may provide data and insights to better assess the nature of critical SoS elements and their solutions. They may also indicate a need for additional structural or performance analyses.

E. Focused Security Risk Analysis

The objective of the focused security risk analysis is to determine whether the elements critical to the mission are really at risk or adequately protected. This is done by employing currently available system-level threat, vulnerability and impact analysis approaches. The threat assessment determines the threats to a critical element in the particular mission context. The vulnerability assessment looks at how protected the element is to the threat, using the results of system-level program protection planning performed at the time the system was tested. The product of the risk analysis is a characterization of the nature and severity of the security risks for each critical system element. It provides the basis for establishing the priority areas to improve assurance of mission outcomes.

F. Risk Mitigation Identification and Evaluation

The objective of risk mitigation and identification is to identify, evaluate and recommend a suite of risk mitigation changes to the SoS. The changes may be to the SoS architecture, the constituent systems, SoS links and interfaces, or to non-materiel aspects of the SoS concepts of operations, tactics, techniques and procedures). Identification of changes draws on the growing knowledge base of countermeasures, best practices and design patterns. Evaluation leverages the methods used to identify critical SoS elements to assess predicted impact of options, including the composite set of options needed to improve mission outcomes.

In this stage, the system engineer identifies options for addressing risks and evaluates them for impact on mission outcomes, technical feasibility, affordability, etc., including the dependencies among the set of composite solution options. Selection of approaches depends on system-level considerations, including technical feasibility and cost given the state of the legacy system(s), timing for implementation given system(s) development plans, and capacity for implementing changes given available engineering staff and competing user needs.

Assessing the right mix of mitigations across the set of SoS critical elements to provide the required level of mission assurance may require additional analysis using the methods employed during criticality analysis. Other portfolio analysis approaches can also be applied to understand the right mix of investments to achieve the best return on investment or mission outcome value. The product of this stage is a plan for the composite set of changes to systems to improve security of SoS for achieving mission outcomes.

G. Implementation and Feedback

The objective of implementation is to execute the changes in systems resulting from the preceding steps to improve mission outcomes. This includes planning, implementation, integration and testing of changes to systems and their impacts on the SoS and mission assurance. Implementation of materiel solutions is largely a system-level activity. It is usually accomplished as part of system development, upgrade or technology refresh. Feedback is an ongoing process given the dynamic nature of SoS and the threat.

Implementation is executed as part of the normal acquisition processes as changes in systems are implemented, tested and fielded. The SoS-level action in this stage is to monitor system implementation to identify and address issues which could impact the SoS. For example, technical issues in one system that could impact another need to be identified early and options for mitigating effects developed and implemented to assure continuity of operations. The changes to systems are reflected in an updated SoS baseline for further analysis and action, as needed. The ultimate product of this process is update(s) to systems to increase the security of the end-to-end SoS and reduced risk to mission outcomes.

V. SoS SSE Framework as a Bridge

Earlier in the discussion we noted that any SSE framework needed to bridge the operational and system acquisition and engineering communities. The bridge between operations and systems engineering is essential for security and other aspects of a critical mission in a highly uncertain and fiscally constrained environment. A more detailed view of the relationship is depicted in figure 5.

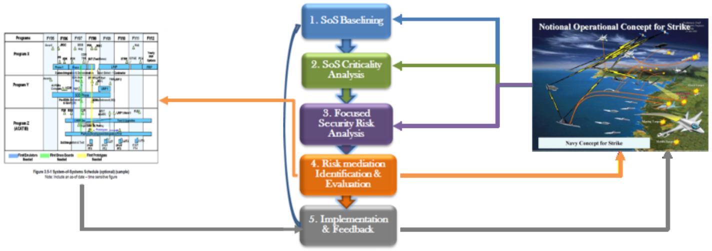
1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk mediation Identification & Evaluation
5. Implementation & Feedback
Notional Operational Concept for Strike
Navy Concept for Strike
Programs
Program X
Program Y
Program Z (ACAT III)
Figure 3.5-1 System-of-Systems Schedule (optional) (sample)
Note: Include an as-of date – time sensitive figure

Figure 5. SoS SSE Framework as Bridge between Acquisition/Engineering and Operations Bigger

The operations community provides the baseline configuration and operational dynamics of the SoS as a foundation for SoS base lining and criticality analysis. They also provide system threats and vulnerabilities for the analysis of SoS critical operational elements during the focused security risk analysis. Risk mitigation identification and evaluation develops options for operational fixes (materiel and non-materiel) and acquisition fixes (materiel) to existing constituent systems. The options need to be constrained by what is actually executable by systems and would represent a balance. Lastly, the acquisition community implements the fixes which are then fielded.

VI. Summary

The purpose of this paper has been to address the security of SoS in support of critical missions. Existing guidance for SoSE is relatively silent on security and there is little evidence that SoS SSE is happening in practice.

In developing an actionable SoS SSE framework we identified a growing number of techniques to improve mission assurance, including security-specific approaches and more general SoS/mission analysis approaches. We assessed promising techniques using a DoD test case as a basis for framework development.

The SoS SSE framework is a five-stage tailoring of the SoSE wave model to analyze a SoS from a mission perspective and identify and address critical elements for security risks to mission outcomes. The framework focuses on current and projected operational needs of and risks to SoS and targeted changes in fielded system elements with the greatest impact on mission outcomes. It builds on our current understanding of SoSE; a growing inventory of approaches to address system-level security risks; and current processes for identifying and addressing system changes to support mission success. The framework is a bridge between the acquisition/engineering and operational communities.

VII. Potential Next Steps

There are several potential next steps to mature the concepts presented in this paper. First would be to conduct detailed pilots of the promising framework analysis approaches against multiple test cases. The goal would be to develop greater insight into the mix of approaches needed to support SoS SSE across different situations. Second would be to revisit the SoS programs interviewed in the SoS SSE base lining activity to vet or pilot the framework within their environments. Third would be to team with operational users of e.g., a combatant command to determine how much of what kind of information is needed to do useful assessments of in-service constituents of a SoS, since availability of comprehensive data for in-service systems is always a concern.

.

References

[1] Department of Defense Strategy for Operating in Cyberspace. July 2011, pp. 2-4.

[2] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD AT&L), Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. January 2013, chapter 2.

[3] J. Dahmann, G. Rebovich, M. McEvilley and G. Turner, “Security Engineering in a System of Systems Environment,” 2013 IEEE International Systems Conference Proceedings, April 2013, pp. 364-369.

[4] Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, Department of Defense Instruction 5200.44, 2012.

[5] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD AT&L), 2008, Systems Engineering Guide for Systems of Systems, Washington, DC: Pentagon, (2008).

[6] Critical Program Information (CPI) Protection Within the Department of Defense, Department of Defnese Instruction 5200.39, 2010.

[7] Defense Acquisition Guidebook, Program protection, chapter 13. 2013.

[8] National Institute of Standards and Technology Special Publications, 800 Series, 2013.

[9] Critical Program Information (CPI) Protection Within the Department of Defense, DoD Instruction 5200.39, 2008.

[10] J. Dahmann, G. Rebovich, R. Lowry, J. Lane and K. Baldwin, “An Implementers view of Systems Engineering for Systems of Systems,” 2011 IEEE International Systems Conference Proceedings, April 2011, pp. 212-217.

[11] C. A. Pinto and P. R. Garvey, Advanced Risk Analysis in Engineering Enterprise Systems, New York, NY: CRC Press, 2012.

[12] E. H. Page, L. Litwin, M. T. McMahon, B. Wickham, M. Shadid, and E. Chang, “Goal-Directed Grid-Enabled Computing for Legacy Simulations,” 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing Conference Proceedings, May 2012, pp. 873-879.

.