3-23-2017

A Framework for Understanding, Prioritizing, and Applying Systems Security Engineering Processes, Activities, and Tasks

Stephen Khou

A FRAMEWORK FOR UNDERSTANDING, PRIORITIZING, AND APPLYING SYSTEMS SECURITY ENGINEERING PROCESSES, ACTIVITIES, AND TASKS

THESIS

Stephen Khou, Captain, USAF

AFIT-ENG-MS-17-M-039

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-17-M-039

A FRAMEWORK FOR UNDERSTANDING, PRIORITIZING, AND APPLYING SYSTEMS SECURITY ENGINEERING PROCESSES, ACTIVITIES, AND TASKS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Stephen Khou, MS

Captain, USAF

March 2017

AFIT-ENG-MS-17-M-039

A FRAMEWORK FOR UNDERSTANDING, PIORITIZING, AND APPLYING SYSTEMS SECURITY ENGINEERING PROCESSES, ACTIVITIES, AND TASKS

THESIS

Stephen Khou, MS

Captain, USAF

Committee Membership:

Major Logan O. Mailloux
Chair

Lieutenant Colonel John M. Pecarina
Member

Mr. Michael A. McEvilley, MS
Member

Abstract

Current systems security practices lack an effective approach to prioritize and tailor systems security efforts to develop and field secure systems in challenging operational environments, which results in business and mission stakeholders becoming more susceptible to an array of disruptive events. This work informs Systems Engineers on recent developments in the field of system security engineering and provides a framework for more fully understanding the application of Systems Security Engineering (SSE) processes, activities, and tasks as described in the recently released National Institute of Standards and Technology (NIST) Special Publication 800-160. This SSE framework uniquely offers a repeatable and tailorable methodology that allows system developers to focus on high Return-on-Investment (RoI) SSE processes, activities, and tasks to more efficiently meet stakeholder protection needs and deliver trustworthy secure systems.

Acknowledgments

My Peers - Thank you for making this past year an enjoyable one

My Instructors - Thank you for the challenges and insights

My Advisors - Thank you for your guidance and trust throughout the year

My Family - Thank you for everything else

Stephen Khou

Table of Contents

A FRAMEWORK FOR UNDERSTANDING, PRIORITIZING, AND APPLYING SYSTEMS SECURITY ENGINEERING PROCESSES, ACTIVITIES, AND TASKS

1. Introduction

1.1. Background

Over the past 50 years, Congress and the DoD have continually explored ways to improve system acquisition outcomes, including improvements to sound management practices, such as realistic cost estimating, prototyping, Systems Engineering (SE), and systems security [3]. Typically, SE and Systems Security Engineering (SSE) are defined and shaped by the context, environment, and situation in which they are embedded where the classical SE/SSE approach is tailored to and works best in situations in which all relevant factors are largely under the control of or can at least be well understood and accommodated by the engineering organization and/or the program manager [4]. Generally speaking, this situation occurs when system and security requirements are relatively well established (between the engineers and the stakeholders), technologies are relatively mature, the system is being developed for a single or relatively homogeneous user community, and at best a single individual has management and funding authority over the program [4].

However, as the dynamicity of these systems present complexities that scale beyond our ability to comprehend, manage, and control, we often find that systems security is not adequately addressed in enterprises or supporting systems, resulting in business and mission stakeholders becoming susceptible to a considerable array of disruptive events [5], [4]. Consequently, special attention is needed to develop more

defensible and survivable systems for uncertain, unpredictable, and challenging operational environments, to include attacks by intelligent and persistent adversaries. Additionally, recent years have seen serious erosion in the ability of U.S. forces to quickly field new weapons systems in response to changing threats, as well as a large increase in the cost of these weapons systems [7]. For example, the military's acquisition cycle for major weapons systems currently take two to three times longer than 30 years ago [7]. While many causes for this trend have been suggested, one common view is that better SE and development planning could help shorten the time required for development [7]. Another key cause of poor acquisition outcomes is the mismatch between the validated capability requirements for a new weapon system and the appropriate SE knowledge, funding, and time that is planned to develop that new system [3]. The Department of Defense's (DoD) three key decision making processes for acquiring weapon systems (requirements determination, resource allocation, and the acquisition management system) are fragmented, making it difficult for the department to achieve a balanced mix of weapon systems that are achievable and affordable and often begin with validated requirements that have not been informed by solid SE practices [3].

As modern systems continue to increase in size and complexity, security is not adequately addressed, resulting in key stakeholders becoming susceptible to attacks from intelligent adversaries and a considerable array of disruptive events [1]. Systems, networks, and sensitive information can be compromised by malicious and inadvertent activities despite best efforts to prevent such events from occurring [2]. These vulnerabilities often result in business and mission losses when assets (i.e., people, processes, and technology) are insufficiently protected; thus, allowing for system faults,

degradation, misuse, abuse, and security violations. Such losses can result in mission failure and financial ruin, as well as, reduced trust from key stakeholders.

1.2. Specific Issue

In order to address this critical systems security gap and meet steadily increasing security needs from the commercial sector, international partners, and the defense industry in a sustainable manner, the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and several other global industry leaders began a collaborative effort to deliver a comprehensive systems-oriented approach to SSE [8]. The ultimate objective of NIST SP 800-160 *Systems Security Engineering* is to address security issues from a stakeholder requirements and protection needs perspective and to use established engineering processes to ensure that such requirements and needs are addressed early in and throughout the life cycle of the system [8]. More specifically, NIST Special Publication 800-160 is aligned with the SE life cycle processes of ISO/IEC/IEEE 15288 and provides "considerations for a multidisciplinary approach in the engineering of trustworthy secure systems" [8].

To maximize the utility of these SSE processes, activities and tasks, it is important to understand that systems-level thinking is required in the bringing together of expertise and perspectives from multiple disciplines, security specialties, and other specialty engineering areas. Moreover, when considering an adversary who is agile, intelligent, determined, and highly competent, a systematic way to identify, assess, and plan for negative impacts, losses, and associated consequences is critical for the Systems Engineer.

1.3. Research Objectives

As current security practices lack effective methodologies to prioritize and address system security issues in complex systems, this research effort aims to identify gaps in current security approaches and apply the NIST SP 800-160 in a rationalized and streamlined process [9]. The research questions to be answered are three-fold:

1. How can SSE be understood and described with respect to established Systems Engineering processes?
2. How can SSE efforts be decomposed into universally applicable systems security domains?
3. How can SSE processes, activities, and tasks be prioritized and applied to diverse classes of systems?

1.4. The Way Ahead

Given the progressive nature of the research questions, this thesis will follow a scholarly, or k-paper, format. In Chapters 2 and 3, the publications "A Foundation for Developing Sustainably Secure Systems" and "Putting the 'Systems' in Security Engineering: An Examination of NIST Special Publication 800-160" provide Systems Engineers and security professionals an update on recent developments in the field of SSE to promote a systematic view of security which ensures networked systems operate properly despite uncertain environments, malicious and non-malicious disruptions, and intelligent adversaries. In addition, these articles offer a brief overview of the NIST SP 800-160, emphasizing a systematic, yet tailorable approach for system security in order to familiarize Systems Engineers with the NIST SP 800-160 and provide a foundation for developing sustainably secure systems [9]. In particular, this section explores how the NIST SP 800-160 can help the Systems Engineer understand what they are getting from

SSE, and emphasizes that Systems Engineers may perform some of the multidisciplinary SSE tasks in collaboration with other engineering team members [9]. In doing so, Chapters 2 and 3 describe current SSE practices with respect to established SE processes as presented in the NIST SP 800-160.

Chapter 4, "System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts," puts further focus on the SSE approach. More specifically, this article provides a comprehensive discussion of SSE concepts, methodologies, and frameworks, in addition to introducing several competing systems security concepts and outlining their respective security domains, noting that the preponderance of existing frameworks are intended for Information Technology (IT) and cybersecurity applications [4]. This article uniquely analyzes the constituent parts of the systems security problem through an SSE perspective by defining seven system agnostic security domains in order to better address the systems security problem holistically [4]. In doing so, this work represents essential knowledge for understanding how to more effectively apply SSE processes for engineering trustworthy and secure systems. By utilizing this concept with well-established SSE activities and tasks, this paper identifies a means for analyzing the SSE approach and understanding where to focus limited resources to maximize the stakeholders' return on investment [4].

In Chapter 5, "A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks," this research looks to incorporate the assessment methods presented in Chapter 4 alongside NIST SP 800-160 to investigate its tailorable nature and explore how to efficiently apply the NIST SP 800-160 to various classes of systems [10]. This work aligns with the goals of the NIST SP 800-160 by examining the

tailorable set of SSE activities and tasks to support critical missions and business operations [8]. By examining the NIST SP 800-160's SSE activities and tasks in relation to the agnostic security domains of chapter 4, this work describes possible prioritization schemes for streamlining demanding security approaches, increasing the manageability of SSE efforts, and lowering implementation costs. Finally, conclusions and future work are presented in Chapter 6.

Bibliography

[1] Government Accountability Office, "Addressing Incentives is Key to Further Reform Efforts," 30 April 2014. [Online]. Available: http://www.gao.gov/assets/670/662837.pdf. [Accessed 25 January 2017].

[2] The MITRE Corporation, Systems Engineering Guide, McLean, VA: The MITRE Corporation, 2014.

[3] L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST Special Publication 800-160," *IEEE Security & Privacy,* vol. 14, no. 4, pp. 76-80, 2016.

[4] S. Khou, L. O. Mailloux, J. M. Pecarina and M. A. McEvilley, "System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts," *IEEE Access,* Accepted February 2017.

[5] Hearings before the Committee on Armed Services, U.S. Senate, 111th Congress, "The Acquisition of Major Weapons Systems by the Department of Defense," 3 March 2009. [Online]. Available: http://www.nationalacademies.org/OCGA/111Session1/testimonies/OCGA_149977. [Accessed 25 January 2017].

[6] J. Bayuk and A. Mostashari, "Measuring Systems Security," *Systems Engineering,* vol. 16, no. 1, pp. 1-14, 2013.

[7] J. Allen, "CERT System and Networks Security Practices," *NCISSE 2001: 5th National Colloquium for Information Systems Security Education,* 2001.

[8] R. Ross, M. McEvilley and J. C. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, 2016.

[9] K. Baldwin, J. Miller, P. Popick and J. Goodnight, "The United States Department of Defense Revitalization of System Security Engineering Through Program Protection," in *Systems Conference (SysCon)*, 2012.

[10] S. Khou, L. O. Mailloux and M. McEvilley, "A Foundation for Developing Sustainably Secure Systems," *Insight,* vol. 19, no. 2, pp. 62-65, July 2016.

[11] S. Khou, L. O. Mailloux, J. M. Pecarina and M. A. McEvilley, "A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks," *IEEE Access,* Submitted February 2017.

2. Introduction to SSE Concepts and the NIST SP 800-160

2.1. Description

This chapter provides a brief introduction to SSE and is intended to familiarize the reader, and in particular Systems Engineers, with the ongoing and recent developments in the field of SSE. The article itself explores the history and vision of SSE and how the NIST SP 800-160 *Systems Security Engineering* can help Systems Engineers understand what they are getting from SSE, and emphasize that Systems Engineers may perform some of the multidisciplinary SSE tasks in collaboration with other engineering team members.

This article lays the initial groundwork for future research by introducing the systems oriented view of SSE and its evolution over the past few decades. In addition, the Authors provide an initial assessment of the draft NIST SP 800-160.

2.2. Publication Details

Title: A Foundation for Developing Sustainably Secure Systems

Publication: INCOSE INSIGHT, Volume 19/Issue 2

Date: July 2016

A Foundation for Developing Sustainably Secure Systems

Stephen Khou, *US Air Force Institute of Technology*, stephenkhou@gmail.com; **Logan O. Mailloux**, *US Air Force Institute of Technology*, Logan.Mailloux@afit.edu; and **Michael McEvilley**, *The MITRE Corporation*, mcevilley@mitre.org

■ **ABSTRACT**
This article is intended to introduce and familiarize systems engineers with ongoing developments in the field of systems security engineering and particularly the effort to develop NIST Special Publication 800-160 *Systems Security Engineering*, which provides security considerations for engineering trustworthy secure systems.

INTRODUCTION

Over the past two years, the INCOSE Systems Security Engineering (SSE) working group has participated in the development of a new National Institute of Standards and Technology (NIST) publication focused on providing a foundation for meeting stakeholder protection needs and security objectives. Unlike most information technology (IT) focused NIST publications, Special Publication 800-160 *Systems Security Engineering* is aligned with the system lifecycle processes of ISO/IEC/IEEE 15288 and provides "Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems" (Ross, McEvilley, and Oren 2016).

In this article, we emphasize a systematic, yet tailorable approach for systems security and familiarize systems engineers with NIST 800-160 in order to provide a foundation for developing sustainably secure systems.[1]

HISTORY OF SYSTEMS SECURITY ENGINEERING (SSE)

Figure 1 depicts a concise history of notable systems-oriented security publications. During the 1970s and 1980s, the United States Department of Defense (DoD) sponsored a number of secure computing efforts that culminated in the Trusted Computer System Evaluation Criteria, (RAND 1970, Anderson 1972, DoD 1983).[2] Despite their focus on computer security, these early efforts recognized the *systems nature* of their work and the first systems-level security standard – Military Standard 1785 – was published in 1989 (DoD 1989). This work was the first to explicitly define a systems approach to security in terms of both its technical and technical management aspects. Additionally, this "vision" reinforces that security must be treated no differently than any other system capability or quality characteristic, and aligns with the broader perspective of systems engineering and its technical and technical management aspects.

"Systems security engineering (SSE) Management is an element of program management that ensures system security tasks are completed. These tasks include developing security requirements and objectives; planning, organizing, identifying, and controlling the efforts that help achieve maximum security and survivability of the system during its lifecycle; and interface with other program elements to make sure security functions integrate effectively into the total systems engineering effort (MIL-STD 1785)."

During the IT bubble of the 1990s and 2000s, these initial system security notions lapsed as researchers concentrated almost exclusively on information assurance, network security and cyber security. However, in 2011 the DoD once again acknowledged its need for an integrated, systems engineering approach for developing secure systems, which led to the DoD's revitalization of SSE through the methodology defined as Program Protection (Baldwin, Miller, Popick, and Goodnight 2012, DoD 2011, DoD 2015).

THE PURPOSE OF NIST 800-160 *SYSTEMS SECURITY ENGINEERING*

While DoD system security efforts served to protect critical information and technologies well, there was no full realization of the systems engineering-focused specialty discipline of SSE as described in MILSTD 1785 (McEvilley 2015). Thus, in 2010 a collaboration by the NIST and the National Security Agency (NSA) to fill this gap materialized in the NIST 800-160, which is best described in its fivefold purpose (Ross, McEvilley, and Oren 2016):

1. To provide a basis to formalize a discipline for systems security engineering in terms of its principles, concepts, and activities;
2. To foster a common mindset to deliver security for any system, regardless of its scope, size, complexity, or stage of the system lifecycle;
3. To provide considerations and to demonstrate how systems security engineering principles, concepts, and activities can be effectively applied to systems engineering processes;

1 The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 initial public draft was made available for comment May 2014. A second public draft was made available in May 2016 for review and comment.

2 Note, the Trusted Computer System Evaluation Criteria matured into the Common Criteria (ISO/IEC 2009) and remains a popular methodology for securing IT systems.

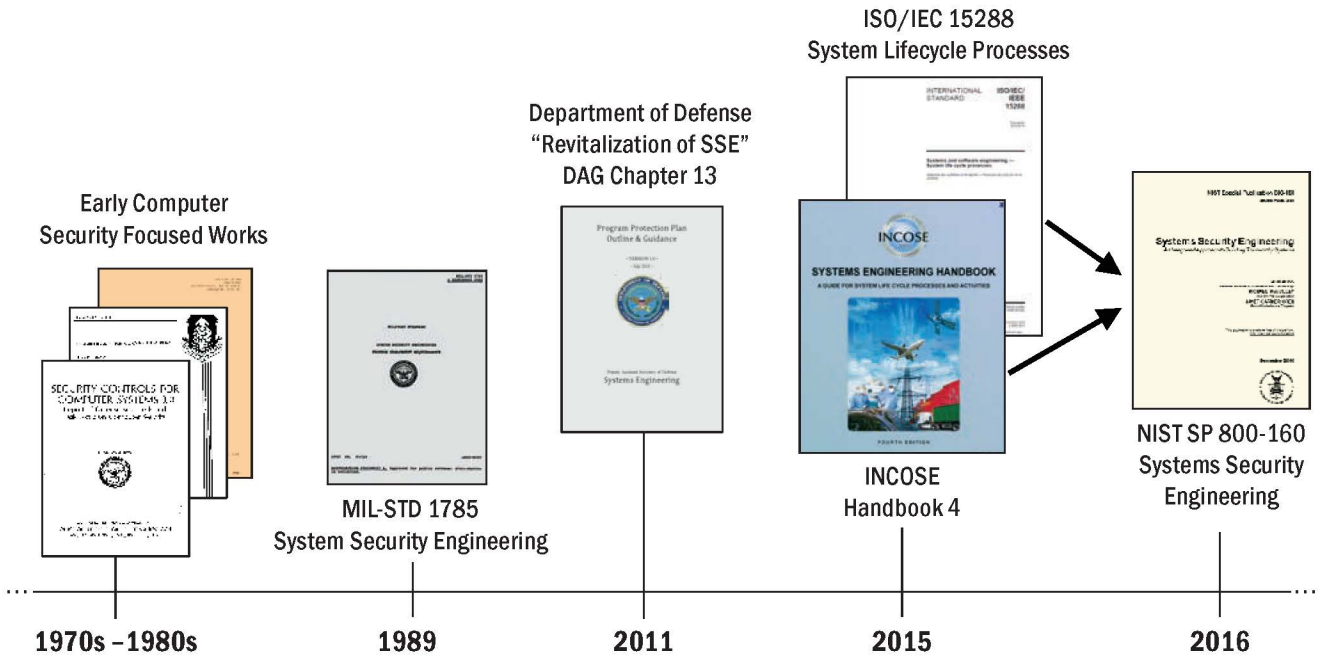


Figure 1. A concise history of Systems Security Engineering (SSE) publications as they contribute to the formalized need for and establishment of a systems security approach based on systems engineering lifecycle processes as used in NIST 800-160

4. To advance the field of systems security engineering by promulgating it as a discipline that can be applied and studied;
5. To serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria.

NIST 800-160 strives to provide a comprehensive description of system-oriented security considerations for application in systems engineering, which makes it the most significant work in the system security field in over a decade (Mailloux, Dove, Garrison, and Biondo 2015).[3] Moreover, the NIST 800-160 is in alignment with both the systems engineering lifecycle processes of the 2015 ISO 15288 standard and INCOSE Systems Engineering Handbook version 4.

WHO SHOULD READ NIST 800-160 *SYSTEMS SECURITY ENGINEERING?*

Table 1 provides a helpful breakdown for systems engineers to understand the tutorial and technical nature of NIST 800-160. While chapters 1 and 2 provide the necessary background to understand SSE, chapter 3 provides a detailed description of the various SSE activities and tasks as they pertain to the 30 systems engineering lifecycle processes from ISO 15288.[4] In particular, these chapters help the systems engineer understand what they are getting from SSE, and emphasize that systems engineers may perform some of the multi-

Table 1. An Outline of NIST SP 800-160, Systems Security Engineering[5]

Section	Description	Pages
Chapter 1	Definition of SSE	7
Chapter 2	SSE Fundamentals	15
Chapter 3	SSE Tasks and Activities	128
Appendix D	Systems Engineering Lifecycle View of SSE Processes	19
Appendix E	SSE Roles & Responsibilities	3
Appendix F	Security Design Principles	15
Appendix G	Engineering and Security Fundamentals	21
Appendix H	System Resiliency	26
Appendix I	Security Requirements Considerations	2
Appendix J	Software Security and Assurance	24
Appendix K	Hardware Security and Assurance	TBD*
Appendix L	System Security Analyses	TBD*
Appendix M	Risk Management Framework	3
* As of NIST SP 800-160 second public draft these sections are not populated.		

3 An excellent survey of SSE is available from Stevens Institute (Bayuk 2010).

4 The SSE activities and tasks described are in the context of the established ISO/IEC/IEEE 15288 phases of the system life cycle, while recognizing that specific acquisition and systems engineering processes may vary in their interpretation.

5 Table 1 is based on the second public draft of the NIST SP 800-160. The ordering and page count may change slightly with the publication of version 1 scheduled for the end of 2016.

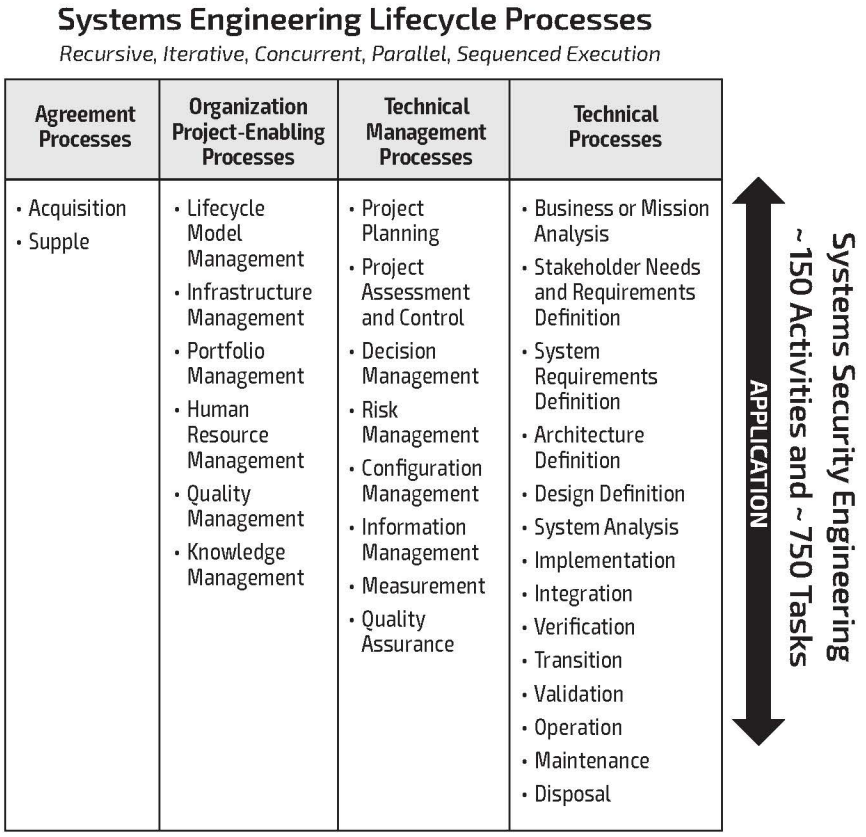


Figure 2. Application of Systems Security Engineering (SSE) activities and tasks to the ISO 15288 systems engineering lifecycle processes. (Figure is modified from NIST SP 800-160. (Ross, McEvilley, and Oren 2016))

disciplinary SSE tasks in collaboration with other engineering team members.

Systems Security Engineering Processes, Activities, and Tasks

As shown in Figure 2, developing sustainably secure systems requires a "SSE presence" in all systems engineering lifecycle processes. To maximize the utility of these SSE activities and tasks, it is also important to understand that systems-level thinking is required in the bringing together of expertise and perspectives from multiple disciplines, security specialties, and other specialty engineering areas. Moreover, when considering an adversary who is agile, intelligent, determined, and highly competent, a systematic way to identify, assess, and plan for negative impacts, losses, and associated consequences is critical for the systems engineer. In this way, NIST 800-160 provides a repeatable, and tailorable, approach to meet stakeholder's security needs and concerns for major weapon systems, complex control systems, transportation systems, cyber-physical systems, and other specialized systems. In the following paragraphs, the application of SSE is explored with respect to several systems engineering technical processes.[6]

Business or Mission Analysis, Stakeholder Needs and Requirements Definition Processes

During these conceptual systems engineering processes, the systems engineer identifies the security protection needs associated with the stakeholder's business objectives. These security needs must be properly understood and integrated with other functional and non-functional requirements such as performance, safety, agility, reliability, resilience, and survivability. Next, these protection needs transform into security requirements to establish acceptable thresholds for performance and effectiveness, as well as, a basis for capability trades and determination of trustworthiness. Lastly, unique system security viewpoints should inform the analysis of stakeholder needs and aid in the selection of feasible solutions instead of focusing on conformance to ubiquitous security requirements, policies, and protocols (Dove 2009).

System Requirements Definition, Architectural Definition, Design Definition

These processes transform stakeholder requirements into systems security requirements, produce security-oriented architecture and design-level technical descriptions of the system, and inform the security aspects of all technical performance aspects of the system. Well-established system security activities include the development and analysis of architectures and system designs (Bayuk and Horowitz 2011). This phase also includes the identification of verification methods and evidences to assure the satisfaction of security requirements across a spectrum of predictable and emergent behaviors while facing disruption and uncertainty.

Systems Analysis

Systems analysis supports decision making throughout all aspects of the total engineering effort (concept and requirements trades, analysis of alternatives (AoA), requirements validation, architecture trades, design trades, contractor selection trades, risk treatment options and risk treatment selection, and more.). In supporting the systems engineering technical and non-technical processes, SSE has two primary contributions: (1) conduct security-focused analyses when the decision is driven by a security concern; and (2) inform system-level analyses with security-relevant considerations to achieve security-informed decision making.

Implementation, Integration, Verification, Transition, Validation Processes

As systems are being realized and transitioned into the operational environment, analyses to examine susceptibility, determine negative impacts from potential asset losses, and identify consequences across a wide spectrum of potential disruptions is accomplished. These protection analyses should be asset-oriented, occurring at the system level with traceability back to stakeholder business concerns. A key SSE focus during verification and validation is to provide evidence and supporting arguments to demonstrate satisfaction of security claims including system-level emergent properties.

Operations and Maintenance Processes

Perhaps more than other requirements, security, challenges the systems engineer to thoroughly consider the system's operational description where operations and maintenance considerations often constrain requirements, architecture, and design (Dove 2009). Another key aspect is feedback from these phases to early systems engineering processes regarding security incidents,

6 With long system lifetimes and dynamic operational environments, systems engineers should expect to revisit the system lifecycle processes regularly, especially as it pertains to the dynamic nature of security.

abnormalities, emergent behaviors, failures, attacks and associated negative impacts. Without feedback, it is very difficult to identify and differentiate between deficiencies in requirements, architecture, or design and the results of a fault, failure, error, or attack. Moreover, feedback is necessary to improve SSE methods, processes, and techniques.

Disposal Process

This process focuses on the secure storage, handling, disposal and destruction of system elements, and associated intellectual property, sensitive information, and privacy data. Secure disposal is also subject to relevant regulatory constraints and/or contractual agreements.

CONCLUSION

As systems engineers developing increasingly complex systems, we need to be concerned with addressing stakeholder security needs and objectives in a systematic way to deliver trustworthy secure systems. This paper helps systems engineers understand recent developments in the field of SSE which provide an approach to ensure networked systems operate properly despite uncertain environments, malicious and non-malicious disruptions, and intelligent adversaries. ■

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the US Air Force, the US Department of Defense, or the US Government. Author Michael McEvilley's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author. Approved for Public Release; Distribution Unlimited. 16-1653.

REFERENCES

- Anderson, J. P. 1972. Computer Security Technology Planning Study. Bedford, US-MA: US Air Force Electronic Systems Division.
- Baldwin, K., J. Miller, P. Popick, and J. Goodnight. 2012. The US Department of Defense Revitalization of System Security Engineering Through Program Protection. IEEE International Systems Conference (SysCon), Vancouver, CA-BC, 19-22 March: 1-7.
- Bayuk, J. 2010. Systems Security Engineering Final Technical Report. Hoboken, US-NJ: Stevens Institute.
- Bayuk, J. L. and B. M. Horowitz. 2011. "An Architectural Systems Engineering Methodology for Addressing Cyber Security." *Systems Engineering* 14 (3): 294-304.
- DoD. 1983. Department of Defense Standard 5200.28. Trusted Computer System Evaluation Criteria. Washington, US-DC: Department of Defense.
- DoD. 1989. Military Handbook 1785. System Security Engineering Program Management Requirements. Washington, US-DC: Department of Defense.
- DoD. 2011. Program Protection Plan Outline & Guidance. Deputy Assistant Secretary of Defense, Systems Engineering.
- DoD. 2015. Defense Acquisition University. 24-November. Retrieved from Defense Acquisition Guidebook: https://dag.dau.mil/Pages/Default.aspx.
- Dove, R. 2009. "The Interplay of Architecture, Security, and Systems." *INSIGHT*, 12 (2): 7-10.
- ISO/IEC. 2009. Information Technology – Security Techniques – Evaluation Criteria for IT Security.
- Mailloux, L. O., R. Dove, C. Garrison, and R. C. Biondo. 2015. Guidance for Working Group Maintenance of the Systems Engineering Body of Knowledge (SEBoK) with Systems Security Engineering Example. Presented at the Twenty-fifth Annual International Symposium of INCOSE, Seattle, US-WA, 13-16 July: 1004-1019.
- McEvilley, M. 2015. "Towards a Notional Framework for Systems Security Engineering." Presented at the18th Annual Systems Engineering Conference of NDIA. Springfield, US-VA, 26-29 October.
- RAND. 1970. Security Controls for Computer Systems. Washington, US-DC: The RAND Corporation.
- Ross, R., M. McEvilley, and J. C. Oren. 2016. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. National Institute of Standards and Technology.

ABOUT THE AUTHORS

Stephen Khou received his BS in engineering from the School of Engineering and Applied Science, University of Pennsylvania, Philadelphia, in 2009. He is currently pursuing a MS degree in cyber operations from the Computer Science and Computer Engineering Department, Air Force Institute of Technology at Wright-Patterson Air Force Base, as well as a MS degree in systems engineering from the School of Engineering, University of California, Los Angeles. He is also an active duty Captain in the US Air Force.

Logan O. Mailloux (BS 2002, MS 2008, PhD 2015) is an assistant professor at the US Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio, US. He is commissioned as Major in the US Air Force and serves as a computer developmental engineer. He is a certified information system security professional (CISSP), certified systems engineering professional (CSEP), and holds US Department of Defense certifications in cyberspace operations, systems engineering science and technology management, test & evaluation, and program management. He is a member of IEEE, ACM, INCOSE, and ITEA professional societies, as well as, HKN and TBP honor societies. He has served the USAF as a cyberspace operations expert responsible for planning and executing network defense exercises, documenting and training computer security best practices, performing test and evaluation of enterprise resource planning solutions, and maintaining distributed simulation infrastructure. Major Mailloux's research interests include systems security engineering, complex information technology implementations, and quantum key distribution.

Michael McEvilley (BS 1980, MS 1995) is a principal computer scientist in the Systems Engineering Technical Center at The MITRE Corporation, McLean, Virginia, US. He serves as a system assurance lead supporting the US DoD in the acquisition of trustworthy secure and resilient weapons systems. His experience includes requirements analysis for high confidence real-time and embedded systems; safe, secure, dependable computing; security product design assurance evaluation; tactical intelligence computer operations; and most recently, the formalization of multidisciplinary considerations for the engineering of trustworthy secure systems. He is as a co-author of NIST SP 800-160. He is a member of INCOSE and active participant in the INCOSE Systems Security Engineering and Resilient Systems Working Groups. His research interests include system assurance for high confidence systems, integrated engineering methods for safe and secure systems, and systems security engineering.

3. Exploring NIST SP 800-160's Tailorable Design

3.1. Description

This chapter complements the article of chapter 2 and continues to describe the systems-oriented components of NIST SP 800-160. Unlike typical standards that define elaborate prescriptive security methods, checklists, and directives, the NIST SP 800-160 uses tailorable Systems Engineering processes, activities, and tasks to address security engineering considerations early and sustainably throughout the system's life cycle. This article details how to utilize the NIST SP 800-160, from familiarizing top level management with SSE concepts to allowing practitioners to master the specialty domain of SSE by building upon the expanded material provided in NIST SP 800-160.

In this article, the Authors also provide a general overview of the structure of the NIST SP 800-160, elaborating on its tailorability for securing system designs, noting that regardless of system type, size, or complexity, the NIST SP 800-160 offers a customizable "development kit" for engineering trustworthy secure systems. The Authors offer an overview of the NIST SP 800-160 and provide a detailed example of the NIST SP 800-160's tailorable design. Lastly, a research agenda into future efforts regarding the application of established SSE processes, activities, and tasks for the development of complex systems is mentioned.

3.2. Publication Details

Title: Putting the "Systems" in Security Engineering: An Examination of NIST Special Publication 800-160

Publication: IEEE Security & Privacy, Volume 14/Number 4

Date: July/August 2016

Editors: Sean W. Smith, sws@cs.dartmouth.edu | William Enck, whenck@ncsu.edu

Putting the "Systems" in Security Engineering:

An Examination of NIST Special Publication 800-160

Logan O. Mailloux | Air Force Institute of Technology
Michael A. McEvilley | The MITRE Corporation
Stephen Khou and John M. Pecarina | Air Force Institute of Technology

Modern systems are increasingly complex, with extensive infrastructure dependencies and interactive system-of-systems behaviors. As networked systems, they're inherently susceptible to a wide range of malicious and nonmalicious events that can result in unexpected disruptions and unpredictable emergent behaviors. In addition, the dynamicity of these systems present complexities that scale beyond our ability to understand, manage, and protect against all possible events. Therefore, special attention is needed to develop more defensible and survivable systems for operation in uncertain, unpredictable, and challenging environments, to include attacks by intelligent and persistent adversaries as well as instances of abuse and misuse by the intended system users.

To address this critical systems security gap, the US National Institute of Standards and Technology (NIST), National Security Agency (NSA), and several other industry leaders around the world have collaborated in a five-year effort to provide a comprehensive systems-focused description of systems security engineering (SSE). A recent milestone in this effort was the May 2016 announcement of the second public draft release of NIST Special Publication (SP) 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.[1] Unlike other NIST 800-series special publications and other IT-focused security standards, NIST SP 800-160 employs a systems engineering approach to address stakeholder protection needs, to satisfy security requirements, and to demonstrate systems security trustworthiness.[1] More specifically, NIST SP 800-160 provides a comprehensive collection of foundational engineering considerations in the form of SSE activities and tasks based on well-established security principles, concepts, and practices.

In this article, we provide a brief history of SSE, describe the systems-oriented components of NIST SP 800-160, and outline future work regarding the application of SSE activities and tasks for the development of complex systems.

History of SSE

Figure 1 depicts a history of notable systems security works dating back to the 1970s. Initially, the US Department of Defense (DoD) sponsored several security research efforts focused on building and assuring computing systems with the correct level of protection.[2,3]

Copublished by the IEEE Computer and Reliability Societies

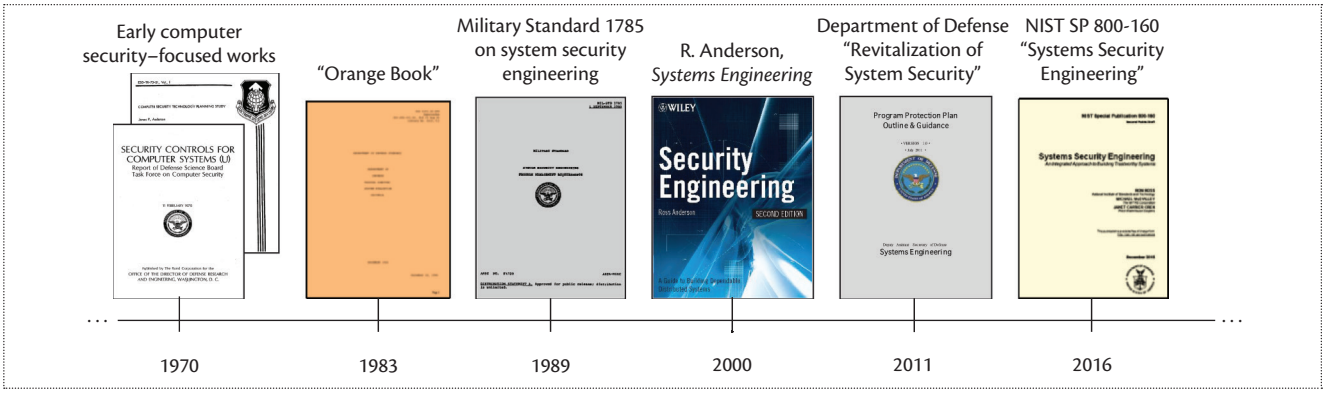


Figure 1. A concise history of systems security engineering (SSE). This timeline captures the major publications that contributed to the formalized need for and establishment of US National Institute of Standards and Technology Special Publication (NIST SP) 800-160.

These works culminated in the "Trusted Computer System Evaluation Criteria," otherwise known as the revered "Orange Book."[4] (Note that the "Trusted Computer System Evaluation Criteria" evolved into the "Common Criteria" and continues to serve as an internationally recognized methodology for evaluating IT products.[5]) Despite their focus on computer security, these early efforts recognized the foundational systems nature of their work: "[P]roviding satisfactory security controls in a computer system is in itself a system design problem … a combination of hardware, software, communication, physical, personnel, and administrative-procedural safeguards."[2] Thus, the specialty domain of systems security was informally born from the culmination of these efforts.

In 1989, the DoD formalized this systems security concept in Military Standard (MIL-STD) 1785, which defined both the technical and managerial aspects of SSE for the first time.[6] While MIL-STD 1785 emphasizes the systematic application of scientific rigor, it also reinforces that security must be treated no differently from any other system capability or quality characteristic:[6]

> Systems Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines as well as the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats.

During the IT bubble of the 1990s and 2000s, these initial systems-oriented security notions lapsed as researchers concentrated almost exclusively on network security and information assurance. During these years of rapid computing advancements, recognized security expert Ross Anderson was one of only a few who continued to build a holistic view of systems security in his seminal work *Security Engineering*.[7]

In 2011, the DoD once again acknowledged its need for an integrated, systems approach for developing secure systems.[8] Accordingly, the Deputy Assistant Secretary of Defense for Systems Engineering led the DoD's revitalization of SSE through the methodology defined as Program Protection.[9,10] Although this effort serves well to bring system security concepts and principles to protect critical program information, technologies, and critical components (that is, the realization of protections for corporate intellectual property and critical capability assets), the specialty discipline of SSE as described in MIL-STD 1785 was never fully realized.[11] This left the security community without a systematic approach to effectively build in security for complex, unprecedented systems.

Why NIST SP 800-160?

To meet steadily increasing systems security needs from the commercial sector, international partners, and the defense industry in a sustainable manner, NIST and NSA began a collaborative effort to deliver a systems-oriented approach to SSE in order to "address security issues from a stakeholder protection needs and requirements perspective."[1] More concretely, NIST SP 800-160 ensures systems security requirements are "addressed with appropriate fidelity and rigor" by aligning with the engineering viewpoint captured in the 30 systems life-cycle processes of ISO/IEC/IEEE 15288.[1,12]

In contrast to typical standards that define elaborate prescriptive security methods, checklists, or the like, NIST SP 800-160 uses the tailorable systems engineering processes to address security engineering considerations early and sustainably throughout the

system's life cycle. Perhaps the best way to understand "why NIST SP 800-160?" is through its fivefold purpose:[1]

- to provide a basis to formalize a discipline for SSE in terms of its principles, concepts, and activities;
- to foster a common mindset to deliver security for any system, regardless of its scope, size, complexity, or stage of the system life cycle;
- to provide considerations and to demonstrate how SSE principles, concepts, and activities can be effectively applied to systems engineering processes;
- to advance the field of SSE by promulgating it as a discipline that can be applied and studied; and
- to serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria.

Consequently, NIST SP 800-160 provides a comprehensive description of SSE, which makes it arguably the most significant work in the systems security field to date.[13] Moreover, it's useful to a wide audience of security-minded professionals from young security specialists to seasoned program managers.

How to Use NIST SP 800-160

Because of NIST SP 800-160's fivefold purpose, its usage and readership are quite broad. Moreover, the publication (not a standard) is written primarily as an SSE reference, organized across 30 system life-cycle processes and not meant to be read from top to bottom. For example, managers required to work with systems security engineers might simply read the seven pages of chapter 1 to become more familiar with SSE. Conversely, those trying to master the specialty domain of SSE will benefit from NIST SP 800-160's detailed chapters and appendixes that clearly explain foundational SSE concepts, such as a systems perspective, active and passive protection capabilities, and security design principles.

In addition, NIST SP 800-160 is well suited to support specialized certifications and educational programs such as the Information Systems Security Engineering concentration of the Certified Information Systems Security Professional or the graduate certificate offered by the US Naval Postgraduate School.[14] This is particularly important for security-minded organizations concerned with systems security training and education. For example, the DoD is trying to educate a large workforce consisting of hundreds of thousands of personnel across the US Army, Navy, Marine Corps, and Air Force.

Furthermore, there are several practical reasons for those already working in the systems security space to read and review NIST SP 800-160. For example, chief security officers will want to become familiar with it to determine how their development life cycle will change, system and software developers might want to revise and refine their existing engineering life cycles, and security researchers (particularly those studying security requirements) will want to become familiar with new engineering recommendations. In addition, systems security researchers will want to closely watch for lessons learned and application gaps in NIST SP 800-160 because these could very well lead to new areas of research.

Building a Systems Perspective

SSE is concerned with the development of a system's security capability and with the protection of sensitive data, information, processes, technologies, and intellectual property throughout the system's entire life cycle. That is, trustworthy systems must be conceptualized, designed, built, operated, sustained, and retired while accounting for and attempting to control asset losses and associated negative consequences. Thus, as Anderson comments, "security engineering is about building systems to remain dependable in the face of malice, error, or mischief."[7] In this regard, SSE has two predominant roles in the larger systems engineering effort:[1]

- engineering the security protection capability of the system, and
- advising on the security aspects of the entire system.

Successful execution of these two roles requires an SSE "presence" throughout all ISO/IEC/IEEE 15288 system life-cycle processes. In this way, NIST SP 800-160 provides a systematic methodology for applying SSE principles, concepts, and practices with an emphasis on capturing security requirements and associated verification measures, engineering security capabilities, and conducting verification and validation activities to provide evidentiary data to support assertions that security claims have been met.

SSE Activities and Tasks

NIST SP 800-160 provides a systematic approach to meeting stakeholders' security needs and objectives through the application of SSE activities and tasks. As Figure 2 shows, NIST SP 800-160 is organized in a three-chapter format with several detailed appendixes. Chapters 1 and 2 introduce the specialty domain of SSE and lay the necessary foundation for executing the SSE-oriented activities and tasks. Chapter 3 is organized into four families of system life-cycle processes (technical, management, project enabling, and

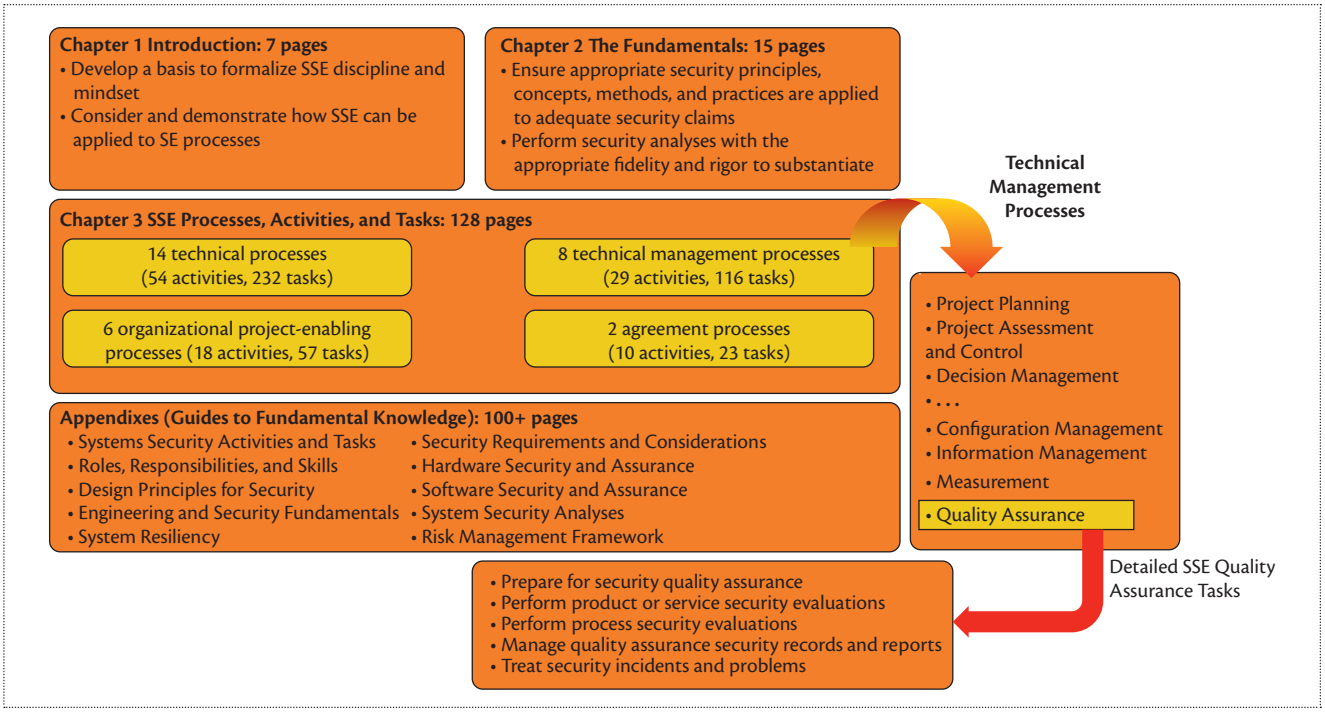


Figure 2. Selective overview of NIST SP 800-160 on SSE. Each process area is further elaborated on in chapter 3 of the publication, providing vast tailorable options to secure system design. For example, the figure outlines the associated tasks to only the Quality Assurance Activity listed under the Technical Management Processes.

agreement) with a total of 111 SSE activities and 428 tasks across the 30 systems engineering life-cycle processes described in ISO/IEC/IEEE 15288.

Presented as a tailorable engineering approach to satisfy stakeholder needs, the SSE activities extend the activities and tasks of the parent system's engineering life-cycle processes to directly address security-specific considerations and outcomes. The SSE activities are based on well-established security principles, concepts, methods, and best practices; these are detailed in several of the publication's accompanying appendixes. The detailed SSE tasks are designed to provide substantiated evidence-based confidence to assert that the system and its protective measures behave, interact, and produce outcomes only as specified and, therefore, warrant the trust that stakeholders place in the system. Furthermore, to maximize the utility of the prescribed SSE activities and tasks, it's important to realize that they're each complex undertakings involving close coordination among various domain experts and stakeholders throughout each of the systems engineering processes. This holistic approach serves to build a multidisciplinary approach to engineering secure trustworthy systems.[13]

Applying SSE Activities and Tasks

As systems increase in size and complexity, they become more susceptible to a wide range of malicious and nonmalicious disruptive events.[8] Moreover, critical systems (those with unrecoverable loss consequences) are increasingly characterized by reliance on distributed technologies that provide a range of automated and autonomous capabilities. These systems might include automotive assembly lines, banking and financial systems, communication networks, cyber-physical systems, systems of systems, military weapon systems, and the Internet of Things. Regardless of the system type, size, or complexity, NIST SP 800-160 is applicable, offering a customizable "development kit" for delivering trustworthy secure systems.

Thus, as system security engineers constrained by real-world costs and timelines, we're interested in more fully understanding how to effectively apply the 111 SSE activities and associated 428 tasks of NIST SP 800-160. In future work, we'll study how to best apply the tailorable SSE processes, activities, and tasks to different classes of development (for instance, new acquisitions or legacy systems) and types of systems (for instance, distributed cybersystems, autonomous transportation systems, airliners, satellites, and control systems) to make better-informed security-related tradeoffs.[15] Moreover, we're

interested in examining the level of effort (that is, the number of system security engineers, systems engineers, and other security-minded professionals) necessary to successfully execute the proposed SSE activities and tasks.

SSE is increasingly recognized as an important specialty domain, responsible for the trustworthiness of complex systems. Although several standards and publications exist in the cybersecurity space, NIST SP 800-160 uniquely delivers a systems-oriented approach to ensuring stakeholder security requirements and protection needs are met with appropriate fidelity and rigor. More specifically, the SSE activities and tasks described in NIST SP 800-160 provide a comprehensive set of systems security considerations for engineering more defensible and survivable systems while facing untold disruptions, losses, hazards, and threats. As the most systematic treatment of systems security available to date, NIST SP 800-160 is sure to impact both the theory and practice of SSE as it's adopted and applied across various commercial, government, and military systems. ■

Acknowledgments

This work is an extension of Stephen Khou and his colleagues' "A Foundation for Developing Sustainably Secure Systems," to be published in *Insight*, in 2016. The views expressed by these authors do not reflect the official policy or position of the US Air Force, the US Department of Defense, or the US government. Author Michael A. McEvilley's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author. Approved for Public Release; Distribution Unlimited. 16-1917.

References

1. R. Ross, M. McEvilley and J.C. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," Nat'l Inst. Standards and Technology, 2016.
2. "Security Controls for Computer Systems," The RAND Corporation, 1970.
3. J.P. Anderson, "Computer Security Technology Planning Study," US Air Force Electronic Systems Division, 1972.
4. "Department of Defense Standard 5200.28, Trusted Computer System Evaluation Criteria," US Dept. Defense, 1985.
5. ISO/IEC 15408, "Information Technology—Security Techniques—Evaluation Criteria for IT Security," 2009.
6. "Military Handbook 1785: System Security Engineering Program Management Requirements," US Dept. Defense, 1989.
7. R. Anderson, *Security Engineering*, 2nd ed., Wiley, 2008.
8. K. Baldwin et al., "The United States Department of Defense Revitalization of System Security Engineering through Program Protection," *Proc. IEEE Int'l Systems Conf.* (SysCon 12), 2012, pp. 1–7.
9. "Program Protection Plan Outline & Guidance," Deputy Assistance Secretary of Defense, Systems Engineering, US Dept. Defense, 2011.
10. "Defense Acquisition University," Dept. Defense, 24 Nov. 2015; https://dag.dau.mil/Pages/Default.aspx.
11. J. Bayuk, "Systems Security Engineering Final Technical Report," Stevens Inst., 2010.
12. ISO/IEC/IEEE 15288, "Systems and Software Engineering—System Life Cycle Processes, First Edition 2015-05-15," 2015.
13. L.O. Mailloux et al., "Guidance for Working Group Maintenance of the Systems Engineering Body of Knowledge (SEBoK) with Systems Security Engineering Example," *Proc. INCOSE Int'l Symp.*, 2015; http://dx.doi.org/10.1002/j.2334-5837.2015.00112.x.
14. C. Irvine and T.D. Nguyen, "Educating the Systems Security Engineer's Apprentice," *IEEE Security & Privacy*, vol. 8, no. 4, 2010, pp. 58–61.
15. S. Evans et al., "Risk-Based Systems Security Engineering: Stopping Attacks with Intention," *IEEE Security & Privacy*, vol. 2, no. 6, 2004, pp. 59–62.

Logan O. Mailloux is an assistant professor at the Air Force Institute of Technology (AFIT). Contact him at logan.mailloux@afit.edu.

Michael A. McEvilley is a principal computer scientist in the Systems Engineering Technical Center at The MITRE Corporation. Contact him at mcevilley@mitre.org.

Stephen Khou is a commissioned officer in the US Air Force and masters student at AFIT. Contact him at stephen.khou@us.af.mil.

John M. Pecarina is an assistant professor at AFIT. Contact him at john.pecarina@afit.edu.

4. Universally Applicable Systems Security Domains

4.1. Description

This work introduces SSE concepts, methodologies, and frameworks, as well as discusses several competing systems security concepts and outlining their respective security fields. In doing so, this work analyzes the constituent parts of the systems security problem through a systems security perspective by defining seven system agnostic security domains in order to better address the SSE problem holistically.

These abstracted domains serve as a common baseline for implementing SSE while thoroughly understanding and discussing the system security problem in addition to building confidence in inter-organizational activities such as developing security standards and effective security practices. The utility of these security domains are further amplified as the Authors provide three example prioritization schemes based on the importance (or criticality) of each security domain according to particular system types or classes. This allows organizations to determine which domains are more important and therefore warrant more resources.

As a result, this work represents essential knowledge for understanding how to more effectively apply SSE processes for engineering trustworthy and secure systems. By utilizing this concept with well-established SSE activities and tasks, this effort identifies a means for analyzing the SSE approach and understanding where to focus limited resources to maximize the stakeholders' security and return on investment.

4.2. Publication Details

Title: System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts

Publication: IEEE Access

Date: Accepted February 2017

System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts

S. Khou, L.O. Mailloux, *Member, IEEE,* J. M. Pecarina, and M. A. McEvilley

***Abstract*—As modern systems continue to increase in size and complexity, current systems security practices lack an effective approach to prioritize and tailor systems security efforts to successfully develop and field systems in challenging operational environments. This work uniquely proposes seven system-agnostic security domains which assist in understanding and prioritizing Systems Security Engineering (SSE) efforts. To familiarize the reader with the state-of-the-art in SSE practices, we first provide a comprehensive discussion of foundational SSE concepts, methodologies, and frameworks. Next, the seven system-agnostic security domains are presented for consideration by researchers and practitioners. The domains are intended to be representative of a holistic SSE approach which is universally applicable to multiple systems classes and not just a single system implementation. Lastly, three examples are explored to illustrate the utility of the system-agnostic domains for understanding and prioritizing SSE efforts in Information Technology (IT) systems, Department of Defense (DoD) weapon systems, and cyber-physical systems.**

***Index Terms*—Security Domains, Systems Security Engineering, Systems Engineering, Security Engineering**

I. INTRODUCTION

As modern systems continue to increase in size and complexity, security is not adequately addressed, resulting in key stakeholders becoming susceptible to attacks from intelligent adversaries and a considerable array of disruptive events [40]. These vulnerabilities often result in business and mission losses when assets (i.e., people, processes, and technology) are insufficiently protected; thus, allowing for system faults, degradation, misuse, abuse, and security violations. Such losses can even result in mission failure and financial ruin, as well as, reduced trust from key stakeholders.

In a recent call to arms, Principal Deputy to the Deputy Assistant Secretary of Defense for Systems Engineering Kristen Baldwin stresses the need for integration and formalization of Systems Security Engineering (SSE) methods, processes, and tools into established systems engineering efforts [1]. More specifically, it identifies three key trends which pose serious security challenges to modern programs and systems. The first challenge describes how systems increasingly rely on commercially available technologies; whether open source or proprietary, cost-conscience commercial technologies are seldom manufactured with security in mind [1]. This means, adversaries across the world can purchase, reverse engineer, and identify vulnerabilities in critical systems, sub-systems, and components more easily. The second challenge to systems security is accountability during acquisition. Complex supply chains often obfuscate the point of origin and composition of system components. Furthermore, with multiple tiers of prime contractors, subcontractors, and suppliers, the chain of custody often becomes confusing and misreported. The third challenge is the increasingly complex, dynamic, and interconnectedness of systems (i.e., large Systems-of-Systems with many networked interactions). This results in difficulty proving that systems, across their execution states and modes, are secure. Moreover, extensive dependencies may lead to the concealment of lingering vulnerabilities.

To address the SSE problem holistically, this work proposes seven system-agnostic (or system-neutral) security domains to examine its constituent parts. While the term "domain" may invoke particular implications depending on the context of its use, we use it here to refer to design principles and concepts at a system-agnostic intended for universal applicability across a broad range of systems. This level of abstraction is desirable to promote systems thinking and an overarching view of systems security ideas within the systems engineering specialty domain of SSE [2]. Note that this "systems" approach is in contrast to most security approaches which promote a rather narrow view of specific security concerns within a particular application domain (e.g., mobile computing or cloud storage systems). The domains described in this work discuss issues pertinent to all system types regardless of their application. In doing so, we also hope to help practitioners and researchers uncover additional areas of study, as the introduction of these abstracted domains themselves do not sufficiently solve the overarching issues of SSE complexity and non-uniformity across the spectrum of possible systems; rather, they provide opportunities for expansion of the concept. We stress that the proposed system-agnostic domains are not intended to be formal specifications but merely provide an example of how security domains can be defined and utilized for studying various Systems of Interest (SoI).

Paper submitted December 23, 2016. This work was supported by the Air Force Research Laboratory.

- *S. Khou, L.O. Mailloux, and J. M. Pecarina are with the Air Force Institute of Technology, Wright-Patterson AFB, OH 45433-7765 USA (email: {Stephen.khou}, {logan.mailloux}, {john.pecarina}@afit.edu).*
- *M. A. McEvilley is a principle computer scientist with the MITRE Corporation, McLean, VA 22102 (email: mcevilley@mitre.org).*

The article is organized as follows. In Section II, a comprehensive discussion of SSE concepts, methodologies, and frameworks is provided for the reader. We also outline their respective security domains, noting that the preponderance of existing frameworks are intended for Information Technology (IT) and cybersecurity applications. Section III proposes seven system-agnostic security domains for understanding how to more effectively apply SSE efforts. This work is not intended to provide a new standard, but rather an approach for prioritizing the SSE processes, activities, and tasks as described in the recently published National Institute of Standards and Technology Special Publication (NIST SP) 800-160 *Systems Security Engineering* [14].

Section IV provides example methods and suggestions for developing prioritization schemes based on the importance (or criticality) of each security domain according to the particular SoI type or class. Finally, in Section V, we conclude with a discussion on the implications of our work and outline future research goals. Ultimately, this work seeks to extend the baseline knowledge of systems security engineers and those responsible for executing SSE roles and responsibilities [43].

II. BACKGROUND

In this section, we offer the reader foundational background knowledge on the development of SSE. In doing so, we note that the majority of security literature speaks to security only from an IT or cybersecurity perspective. While systems security has been studied for many decades, a fully encompassing philosophy ensuring that our daily personal and professional activities remain secure has yet to surface due to a lack of fundamental science underlying current security practices [42].

A. History of Systems Security Engineering (SSE)

Early security research efforts by the United States Department of Defense (DoD) focused on the challenge of how to build and assure computing systems with the correct level of protection [6], [34]. These efforts culminated in the Trusted Computer System Evaluation Criteria (TCSEC), commonly referred to as the "Orange Book" in 1983 [4]. Of note, the Orange Book set basic requirements for assessing the effectiveness of security controls built into computer systems and was primarily used to evaluate, classify, and select computer systems for processing, storage, and retrieval of sensitive or classified information. Despite their focus on computer security, early works recognized the foundational *systems* nature of their task [6]. For example, the 1970 Defense Science Board Task Force on Computer Security concluded that providing satisfactory security controls in a computer system is itself a system design problem [6]. Moreover, the board specifically identified security as a systems problem: "a combination of hardware, software, communications, physical, personnel, policy and procedural safeguards" [6].

In 1989, the DoD formalized this systems security concept in Military Standard 1785 (MIL-STD 1785), which defined the technical and managerial aspects of SSE for the first time [7]. Subsequently, the National Security Agency (NSA) created a draft set of secure design principles in 1993, which emerged from a study on rules for system composition [8], [35]. While not a finished effort, the study represented collective wisdom that needed to stand the test of time, and perhaps more importantly, practice. Additionally, in response to recommendations by the US National Research Council in December of 1990 to promulgate comprehensive, generally accepted security principles, the International Information Security Foundation (IISF) began drafting the Generally Accepted System Security Principles (GASSP) [8], [9]. Originally drafted in 1992, it was left unfinished until its adoption by NIST in 1996 (NIST SP 800-14 *Generally Accepted Principles and Practices for Security Information Technology Systems* [10]) and later the Information Systems Security Association in 2003 (*Generally Accepted Information Security Principles* [9]).

B. IT Focused Security Efforts

While initial systems security efforts served to protect information systems well, a holistic systems-oriented view of security was largely overshadowed by the rapid development of network security and information assurance during the IT bubble of the 1990s and early 2000s. In the meantime, other countries began their own initiatives to develop evaluation criteria influenced largely by the concepts presented in the United States' TCSEC. These included the Information Technology Security Evaluation Criteria (ITSEC), published in 1991 by the Commission of the European Communities (largely based on works from France, Germany, the Netherlands, and the United Kingdom) [11], as well as, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), published in 1993 by the Communications Security Establishment [12]. The TCSEC, ITSEC, and CTCPEC efforts eventually culminated in an international collaboration in 1999 to produce ISO/IEC 15408: *Information technology — Security techniques — Evaluation criteria for IT security*, otherwise known as the Common Criteria for Information Technology Security Evaluation (often abbreviated as "Common Criteria" or simply "CC"). The Common Criteria provides a shared set of requirements for the security functionality of IT products and for assurance measures applied to these technologies [13].

C. A Resurgence of Systems-Oriented Security

More recently, a collaborative effort between NIST and NSA was formed in 2010 to continue the systems approach to security MIL-STD 1785 began some 20 years prior. In 2012, the initial public draft of NIST SP 800-160 *Systems Security Engineering* was published (with the full release version published November 2016), providing a comprehensive description of systems-oriented security engineering considerations [2], [14]. Likewise, in 2011 the United States DoD publicly acknowledged the need for an integrated approach for developing secure systems as they revitalized their SSE approach through established methodologies such as Program Protection Planning (i.e., SE processes throughout the system lifecycle) [1], [15]. Similarly, the on-line Guide to the Systems Engineering Body of Knowledge (SEBoK) recognizes that the primary objective of SSE is to apply SE principles and practices during all system development phases in order to minimize (or contain) system vulnerabilities to known and postulated security threats, ensuring that developed systems are adequately protected [16].

D. Modern SSE Concepts and Frameworks

In this section we introduce foundational SSE concepts and review several popular security frameworks. Experience has

shown that systems often exhibit behaviors that are unanticipated in the design process, even when formal design process exists [5]. Fundamental analysis of system security, and thus risk to successful mission execution, requires necessarily anticipating conditions in which the SoI is forced outside its normal operating constraints. Furthermore, these analyses are complicated by the high degree of connectivity between independently managed systems, where formal assessments can be prohibited by the affected systems' management [17].

With regard to the challenge of developing secure systems, security expert Ross Anderson observed that security engineering is about building systems to remain reliable through intentional and unintentional disruption, to include malice, error, or mischief [18]. In the same respect, the need for cyber resiliency has been increasingly recognized in recent years; there is a need for information and communications systems and the missions and business functions which depend on them to be resilient under attacks focused on cyber resources [41]. Thus, SSE has two predominate roles within the larger SE effort:

- Engineering the security functions that provide system security protection
- Engineering the security-driven constraints on the entire system

Note, a possible third role exists in the engineering of protection for life cycle assets as exemplified in aspects of DoD Program Protection [15]. Successful execution of these roles requires a tailored SSE "presence" throughout the 30 SE life cycle processes of ISO/IEC/IEEE 15288 [5]. While meta-engineering SSE methodologies may exist, such as the Systems Security Engineering Capability Maturity Model (SSE-CMM) (which has evolved into ISO/IEC 21827), the majority of security literature speaks to security only from an IT or cybersecurity perspective [44]. For example, two of the most predominantly exercised methodologies and frameworks for understanding, developing, and fielding secure systems are the *Certified Information Systems Security Professional* (CISSP) [19] and the ISO/IEC 27002: *Information technology — Security techniques — Code of practice for information security management* [20]. The CISSP provides a Common Body of Knowledge (CBK) relevant to information security professionals and establishes a common framework for information security terms and principles which allows professionals to discuss, debate, and resolve related matters with a common understanding [19]. Conversely, the ISO/IEC 27002 provides recommendations on IT and cybersecurity management for use by those responsible for initiating, implementing or maintaining IT and cybersecurity security management systems [20].

On the other hand, methodologies like the SSE-CMM deliver the necessary roadmap for adopting organization-wide security engineering practices, but do not specifically point out any tools or techniques that can be used to help reach the goals described in the process areas [44], [45]. They are rather used as a means for engineering organizations to evaluate their existing security engineering practices and define improvements to them [44], [45].

Summarized in Table I, six commonly referenced security frameworks include the United States Department of Health and Human Services 45 Code of Federal Regulations (CFR) Part 95, Subpart: F [21]; ISO/IEC 27002 [20]; Federal Information Processing Standards 200 (FIPS 200) [22]; the International Information System Security Certification Consortium (ISC)2 CISSP CBK [19]; the Department of Homeland Security's (DHS) Transportation Systems Sector-Specific Plan, an annex to their National Infrastructure Protection Plan [23]; and the DHS Catalog of Control Systems Security for protecting critical infrastructure [24]. Collectively, these works outline provisions for establishing a minimum baseline or system-agnostic security considerations (each from their respective area), which are often acknowledged in multiple concepts or frameworks (as described in Section III). While this is not an exhaustive list of all existing security frameworks, it endeavors to be representative sample of these frameworks. In particular, there work offers representation for traditional IT and cybersecurity systems, cyber-physical systems, transportation systems, industrial control systems, and government requirements on similar systems; this subset provides a diverse yet comprehensive sampling of possible systems.

TABLE I
SECURITY FRAMEWORKS

Security Framework	Description
45 CFR Part 95 (1990)	Outlines provisions for establishing minimum standard requirements for the security of all developmental or operational federally funded automatic data processing systems
FIPS 200 (2006)	Addresses the specification of minimum security requirements for federal information and information systems
Transportation Systems Sector-Specific Plan (2010)	Describes collaboratively developed strategies to reduce risks to critical transportation infrastructure and build a set of programs and initiatives to reduce the sector's most significant risks in an efficient, practical, and cost-effective manner
Catalog of Control Systems Security for CIKR (2011)	Presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and non-physical (cyber) attacks and is specifically designed to provide the framework needed to develop sound security standards, guidelines, and best practices
ISO 27002 (2013)	Provides recommendations on IT and cybersecurity management for use by those responsible for initiating, implementing or maintaining IT and cybersecurity security management systems
CISSP (2015)	Establishes a common framework of information security terms and principles which allows for professionals to discuss, debate and resolve related matters with a common understanding

III. EXAMINING THE SYSTEMS SECURITY DOMAINS

This section proposes seven abstracted systems security domains to broadly describe a "system-agnostic" approach for universally understanding and categorizing systems security concerns into distinct domains. In Table II, we map the six frameworks and their associated domains from Table I into seven recommended system-agnostic domains. The abstracted domains are intended to serve as a common baseline for implementing SSE while thoroughly understanding and discussing the systems security problem in addition to building confidence in inter-organizational activities such as developing security standards and effective security practices. These

domains also infer that the complexity and diversity of security needs and domains that contribute to system security is indeed "defense in depth," a commonly applied architecture and design approach which implements a composition of various defenses and countermeasures to provide multiple opportunities to stop an attack using different techniques and/or tools in the event a security control fails [19].

TABLE II
SECURITY DOMAIN ASSOCIATIONS

System-Agnostic Mapping	Associated Security Domains (from the security frameworks listed in Table I)
Compliance	Audit[b,d]; Accountability[b,d]; Planning[b,c,d]; Certification[b]; Accreditation[b]; Assessments[b,d]; Policy[d,e]; Organizational Security[a,d]; Monitoring[d]; Reviewing[d]; Risk Management[d,f]; Compliance[e]
People	Awareness [b,c,d]; Training [b,c,d]; Identification[b]; Authentication[b]; Personnel Security[a,b,d]; Screening[c]; Preparedness[c]; Response[c]; Human Resources[e]
System Resiliency	Contingency Planning[a,b,c]; Disaster Recovery[f]; Management[e,f]; Business Continuity[e,f]
Operations	Emergency Preparedness[a]; Risk Analysis[a]; Access Control[b,d,e,f]; Incident Response[b,d]; System Integrity[b,d]; Information Integrity [b,d]; Risk Assessment[b,c]; Vulnerability Assessment[c]; Software Development Security[f]; Information Management[d,e]; Document Management[d]; Security Program Management[d]; Operations Security[e,f]; Cryptography[e]; Security Engineering[f]; Security Assessment[f]; Security Testing[f]
Physical and Environmental	Physical Security[a,b,c,d,e,f]; Environmental Protection[b,d,e,f]
Asset Management	Equipment Security[a]; Software Security[a]; Data Security[a]; Configuration Management[b,c]; Maintenance[b,d,e]; Media Protection[b,d]; System Acquisition[b,d,e]; Service Acquisition[b,d]; Leveraging Technologies[c]; Cyber Critical Infrastructure Security[c]; System Development[d]; System Maintenance[e]; Media Protection[d]; Asset Management[e,f]; Supplier Relationships[e]
Interconnectivity	Telecommunication Security[e]; System Protection[b,d]; Communication Protection[b,d,e,f]; Network Security[f]
References: a. *45 CFR Part 95* [21], b. *FIPS 200* [22], c. *Transportation Systems Sector-Specific Plan* [23], d. *Catalog of Control Systems Security* [24], e. *ISO 27002* [20], f. *CISSP* [19].	

Note that systems developers (i.e., practicing Systems Engineers) may partition security into domains with varying detail and specificity. As such, the existing security domains may not map directly to the proposed system-agnostic domains; however, the goal is merely to map the domains as close as possible in order to represent the intention of the domain as described by its framework. For example, the Asset Management domain can be further partitioned into hardware, software, and operating systems to more specifically account for physical material and components (e.g., hard drives, car doors, fuselages, etc.), the mechanisms used to provide functionality to systems (e.g., human-machine interfaces, hardware logic, software applications, etc.), and the platform that the applications reside on (e.g., operating systems, virtual machines, web interfaces, etc.). The problem with this systems security approach, though, is the translation from one framework to another: the concepts are similar but often expressed with varying lexicon. Also, some domains may have interdependencies with other domains that may need to be considered, such as communications and network equipment (Interconnectivity) needing to be managed (Asset Management) and protected (Physical and Environmental security).

A. Compliance

Compliance addresses the security policies of the organization, provides the organization direction, and supports security in accordance with business or mission requirements, alongside applicable legal, statutory, and regulatory requirements. While many believe, security is primarily based on locks and walls to prevent access, there are many times when security depends on deterrence including the possibility of punishment; this is the role of policy and laws [25]. For example, while cars have door locks, it is often the possibility of a thief getting caught and sent to jail, which, while small, is large enough to deter all but the most determined criminals. As such, there are many different forms of punishment to include fines, ostracism, firing, jail, and other creative alternatives that can be incorporated into compliance policies and laws [25].

This domain also serves as an important form of internal control to limit unwanted behaviors from employees and includes investigative measures to determine if an incident has occurred as well as the processes for responding to such incidents. Well-written policies convey to employees what is expected of them, leaving the organization free to focus on other security and management priorities. Additionally, adherence to compliance requirements also helps to maintain a degree of accountability in the eyes of external (and internal) stakeholders.

B. People

Because modern systems currently, and will continue to, depend on people for development and operation, most vulnerabilities tend to occur at the human level [26], [39]. For example, Kevin Mitnick, a computer security consultant once known as the world's most wanted hacker, stated that as "better security technologies, [make] it increasingly difficult to exploit technical vulnerabilities… attackers will turn more and more to exploiting the human element" [26]. His work recognizes that attackers pay more attention to the human element in security than most system developers have, and consequently hackers have managed to successfully exploit this advantage repeatedly with little investment and minimal risk. Therefore, the security roles and responsibilities of employees, contractors and third parties are critically important and should be defined and documented in accordance with the organization's policies and overall competitive strategy. At a minimum, background checks on all potential employees should be conducted in accordance with applicable laws, regulations, and ethics in relation to the business needs and the perceived risks [20].

Furthermore, motivation to comply is often based on the users' understanding of why their actions and behaviors can put organizational assets at risk [26]. Education, training, and certification needs to instill personal and collective responsibility in all users to include security designers, administrators, decision makers, and end users. Note there is a point of distinction to make between education and training:

education is largely about teaching concepts and skills whereas training aims to change behavior through drill, monitoring, feedback, reinforcement, and punishment [26]. By incorporating both security education and training into every task the user does, the organization puts security into the forefront of people's minds on a daily basis, which allows them to focus on the necessary actions to protect themselves, as well as, the organization's data, networks, and systems.

C. *System Resiliency*

The system must also be able to continue its mission during critical failures while protecting its people and assets regardless of internal and external conflict or attacks, unforeseen environmental or operational changes, and system malfunctions [28], [29]. While each component of the system itself may be secure and reliable, demonstrating (or proving) that the whole system is resilient becomes much harder. System Resiliency requires processes to identify and mitigate design, production, test, and field support deficiencies which threaten mission success [27]. Additionally, resiliency with respect to system security also means providing justified confidence that the SoI security functions as only intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system [27].

The complete system must meet stakeholder expectations and needs while also addressing their security concerns by performing traceability of system security requirements. Note that the stakeholder requirements are the results of requirements analysis to transform the informal needs, expectations, and concerns into something that can be delivered. The system requirements transform the stakeholder expression into the technical solution that will be delivered. To be effective, claims should be addressed early and proportionately with stakeholder needs and expected threats. Activities should include a planned systematic set of multi-disciplinary activities to achieve adequate evidence for system resiliency and manage the risk of exploitable vulnerabilities [27]. Incorrectly addressing concerns late in the engineering process could result in the system being misused, resulting in unnecessary costs or delays in full system operations [27].

D. *Operations*

Operations security (and by extension sustainment, maintenance, and logistics) focuses on providing system availability for end users while protecting sensitive data and important resources [19], [20]. From a systems-level perspective, Operations includes the collection of mechanisms and procedures that allow system managers to exercise directive or restrictive influence over the behavior, use, and content of the system; however, due to the prevailing nature of software applications in today's systems, it is important to note that fundamental cybersecurity principals from programs and standards such as the CISSP and the ISO/IEC 27002 have a large impact in securing this domain. Properties such as access control, cryptography, application development, and information security play crucial roles in keeping this domain secure. For example, access control permits management to specify what users or processes can do, which resources they can access, and what operations they can perform on a system [19].

E. *Physical and Environmental*

Physical and environmental security addresses the physical and procedural issues that exist in the environment in which the SoI is to be deployed and operated/sustained. This domain is concerned with the prevention of unauthorized physical access, damage, and interference to the system, as well as measures to prevent loss, damage, theft, or compromise of assets [20]. Some systems may require more physical security considerations than other systems due to a tightly coupled cyber-physical relationship. For example, Industrial Control Systems (ICS) like power plants or waste water treatment plants are considered critical infrastructures which merit higher levels of physical security in order to prevent tampering. Similarly, classified or consolidated IT systems such as military networks and service delivery points may also warrant high levels of physical security due to the sensitive and important nature of the service they provide. Conversely, conventional organizational IT systems (e.g., servers, desktop computers, etc.), may not require significant physical security consideration because these systems are often integrated into larger systems or "businesses" in which physical security has already been provided.

F. *Asset Management*

Asset management describes the assets that the SoI utilizes to operate such as people, intellectual property, system components, and the acquisition of such assets (i.e., supply chain management). This domain encompasses both high-level and more detailed processes, concepts, principles, structures, and standards used to define, design, implement, monitor, and secure/assure operating systems, applications, equipment, and networks [19]. For data components, the domain should also clearly integrate various levels of confidentiality, integrity, and availability to ensure effective operations and adherence to governance. This domain can be further subdivided into three components:

i. Hardware

Of the many components that compose a technological product, and ultimately the system, most contain elements from the broader global market, making it difficult to establish the trustworthiness and security of an end product [30]. As demand drives competition, many companies are forced to outsource in order to lower costs and remain competitive. This can be seen in the U.S. computer manufacturing sector, which in the first half of the decade has declined at an annual rate of 21.8 percent as computer manufacturing has increasingly moved abroad [30]. As manufacturers lose direct control of production quality and product integrity, this outsourcing process can be misused by others to introduce malicious logic into unsuspecting devices. More often than not, hardware failure or cyber-attacks would likely be suspected before malicious hardware, especially since diagnostic tests might not find proof of malicious actions [30]. These devices may also contain hidden backdoors which are equally difficult to detect.

ii. Software

Software (applications or firmware) can also be subject to compromise as complex systems are typically implemented by a large number of developers across a number of companies [1]. In March 2013, a study by the International Data

Corporation found that "at least a third of all PC software is counterfeit" because of its nonphysical nature [30], significantly increasing the potential for malware infection and application performance degradation. Conversely, sometimes vulnerabilities in technology are simply design or implementation mistakes; however, malicious or not, vulnerabilities in software can be, and often are, used for malicious ends, be it cyber-attacks or espionage [36].

iii. Operating Systems

Operating systems are also subject to multiple programmers or outsourcing, which, like in the case of hardware and software, can introduce supply chain compromises. Modern operating systems contain millions of lines of codes with numerous undetected or undetectable vulnerabilities. Because of the crucial role of the operating system in any computing system, the security (or lack thereof) of an operating system has a significant impact on the overall security of the system, including the security of dependent applications (i.e., the software running on the operating system) [31]. Lack of proper control and containment of execution of individual applications in an operating system may lead to attack or break-in from one application to other applications [31].

G. *Interconnectivity*

Communications and network security can be described as the cornerstones of information security, being one of the most central assets to the information environment of any system [38]. Loss of interconnectivity can have devastating consequences on the SoI and its ability to operate, which often leads to mission failure. This domain then refers to not only the transmission methods and security measures used to provide integrity, availability, and confidentiality of data during transfer over private and public communication networks but also the intercommunication between components within a system, such as a vehicle control area network bus which allows microcontrollers and other devices in a vehicle to communicate with each other without the presence of a host computer. Likewise, using the appropriate security protocols ensures that security and integrity of data in transit persist as these protocols are primarily designed to prevent any unauthorized user, application, service, or device from accessing data by implementing various cryptography and encryption techniques.

IV. Example Prioritization Schemes

This section provides three example prioritization schemes (i.e., possible interpretations) using available frameworks to demonstrate the utility of the system-agnostic domains. It is also important to note that many organizations adopt control frameworks to provide a governance structure that is consistent, measurable, standardized, comprehensive, and modular [19]; however, there is often no standard or methodology for determining the "criticality" or importance of such efforts with respect to existing security domains. Thus, information about each domain must be considered and combined by SMEs to get a true understanding of its priority and determine proper courses of action. For example, should developmental and operational tests lack adequate SSE process controls and appropriate design features, planning and engineering efforts could be wasted if vulnerabilities go undiscovered.

Decisions regarding when, where, and how these system-agnostic security domains should be used are best determined by the specific industry sectors and the SMEs associated with those systems. Thus, these examples are not intended to replace the need for applying sound engineering judgment, established best practices, or risk assessments, but rather function as an example use case for further analysis and consideration for engineering complex systems. More specifically, we examine three well-established frameworks and attempt to create mappings from their criticality assessment back to the system-agnostic security domains described in Section III. In this way, we construct prioritization schemes that determine, based on what controls is assumed to matter more for the system or organization, how to organize the security domains in level of importance for the system developer.

Note, the notion of using a weighted priority scheme (i.e., using multiplicative factors to influence the perceived importance of particular categories or domains) allows for a finer level of granularity and detail, but was ultimately omitted in this work in order to minimize the complexity of the issue and prevent possible obfuscation of the necessary components. To provide a broad systems security perspective and demonstrate wide applicability, we addressed security guidance from the conventional IT industry [32], government specific acquisition [15], and critical infrastructure [24]. It must be emphasized again that as these are sample scenarios, the values and order of importance may change depending on the background and expertise of the individual or individuals implementing this concept.

A. *NIST SP 800-53 Revision 4*

The first example is the NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations, consisting of 285 controls in 19 families [32]. This publication provides for the ability to scope and tailor controls to an organization's specific mission (or user requirements) and provides best practice recommendations for information security management by those initiating, implementing, or maintaining information security systems. By categorizing the 19 control families and mapping them back to the proposed security domains, we derive Table III. These 19 control families are listed along the left column of Table III and serve as consideration or control factors to help determine how much a given security domain would impact or influence the system, as determined by the SME. While the NIST SP 800-53r4 provides a holistic approach to information security by providing the breadth and depth of security controls necessary to fundamentally strengthen information systems and the environments in which those systems operate, this assessment looks to apply those same security control families as a set of defined requirements used to satisfy the system-agnostic security domains.

With respect to the sums in Table III, once each control is associated with its respective security domains, we can assert that larger security domain values imply a more weighted or

critical importance to the system utilizing this particular prioritization scheme. For example, the Media Protection control family can apply directly to the Physical and Environmental security domain as well as the Asset Management domain. For this particular scheme then, Compliance should be weighted more heavily than the commonly emphasized Operations security domain. While all security domains are important, this prioritization allows IT-focused organizations to focus their resources more specifically.

B. *Defense Acquisition Guidebook*

In 2012, the Defense Science Board Task Force concluded that the cyber threat was serious and that the United States could not be confident that its critical information and cyber systems would work under sophisticated and well-resourced cyber attacks [40]. While the DoD takes great care to secure the use and operation of its weapon systems, its networks are built on inherently insecure architectures that are increasingly composed of foreign assets [40]. The Defense Acquisition Guidebook (DAG) provides details on integrating classical systems engineering processes for mitigating and managing risks to unprecedented technologies and mission-critical system functionality throughout the acquisition lifecycle [15]. More specifically, Chapter 13 of the DAG (Program Protection) provides detailed procedural steps in performing criticality analysis, the DoD's method by which mission-critical components and information are identified and prioritized. In essence, program protection seeks to defend warfighting capabilities by keeping secret things from getting out and malicious things from getting in [15], [37].

Leveraging this methodology, another example prioritization scheme is generated, as shown in Table IV. Here, the criticality analysis procedural steps are assessed against the security domains, which we treat like critical components and information for mission-critical functions. From these results, we assert that security domains with larger sum values imply more importance to the SoI. In this example, System Resiliency and Asset Management share equally high sum priorities of "3".

C. *SCADA Security Policy Framework*

The final prioritization example uses the Framework for Supervisory Control and Data Acquisition (SCADA) Security Policy, developed by Sandia National Laboratories in an effort to ease the creation of SCADA security policies and ensuring coverage over all critical areas of SCADA security as well as flexibility in developing customized policies for specific operations [33]. Because SCADA systems are often used to control time-critical functions, standard IT security practices may not be particularly suitable for SCADA systems [33].

Although the framework describes a methodology to creating SCADA specific policy documents, the policy itself translates the organization's desired security and reliability control objectives into enforceable direction and behavior for the staff to ensure secure design, implementation, and operation [33]. In this fashion, we strive not to explicitly exclude this type of framework from applicability in our system-agnostic approach. As shown in Table V, we can rationally map each category to the system-agnostic security domains to create a SCADA specific prioritization scheme. Again, the larger the sum value for a security domain implies more importance of that domain to the system. In this example, the domain of most concern is the Asset Management domain with a value of "4".

D. *Implications of the SSE Domains*

Tables III, IV, and V demonstrate that the prioritization orders for the three system frameworks are vastly different from one another given these specific mappings (which

TABLE III
PRIORITY SCHEME FOR NIST SP 800-53R4

NIST SP 800-53r4	Compliance	People	System Resiliency	Operations	Physical and Environmental	Asset Management	Interconnectivity
Access Control	X	X		X			X
Awareness and Training	X	X					
Audit and Accountability	X	X					
Security Assessment and Authorization	X						
Configuration Management	X					X	
Contingency Planning			X				
Identification and Authentication					X		X
Incident Response			X		X		
Maintenance						X	
Media Protection					X	X	
Physical and Environmental Protection					X		
Planning			X				
Program Management	X	X					
Personnel Security		X			X		
Risk Assessment	X						
System and Services Acquisition						X	
System and Communication Protection				X			X
System and Information Integrity				X			X
Privacy Controls					X		X
Sum	**7**	**5**	**3**	**3**	**6**	**4**	**5**

presumably represent the stakeholders' priorities). For example, the NIST SP 800-53r4 prioritizes Compliance whereas the DAG is more inclined to require fairly equal attention in System Resiliency as well as Asset Management. These results show that the proposed system-agnostic security domains can serve as a basis for further developing and tailoring systems specific security frameworks, processes, and requirements efforts. By utilizing and extending this concept with well-established SSE processes, activities, and tasks, we desire to increase understanding of SSE approaches in order to focus limited resources and maximize return on investment.

V. Conclusion and Future Works

This paper provides a comprehensive description of foundational SSE concepts and frameworks for the interested reader, and proposes seven system-agnostic security domains for consideration to prioritize and address system security issues in complex systems. In contrast to the preponderance of "cyber" focused security research, this work focuses more holistically on SSE in order to create a system-agnostic approach for various types and classes of systems to include: cyber-physical, transportation, weapons systems, and other complex systems or systems of systems.

The abstracted domains allow users and practitioners to focus on systems in general as opposed to specific systems designed for a specialized purpose. While more attention to detail can be given by a SME to his/her particular system, this preliminary approach allows for a standard baseline to be created such that new practitioners in the field have a starting guide to developing secure systems of their own. This work could potentially save, at the very least, the initial cost of understanding the majority of non-specialized security requirements, to providing an effective method for prioritizing and quantifying such an approach for systems in development.

In future efforts, we desire to re-evaluate the proposed list of system-agnostic domains and further elaborate on them as well as appending overlooked domains into the current decomposition. We also seek to incorporate our assessment methods alongside NIST SP 800-160 *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* to aid in the development of trustworthy secure systems that are fully capable of supporting critical missions and business operations while meeting stakeholder security objectives and protection needs [14]. Thus, we desire to investigate the tailorable nature of NIST SP 800-160 and explore how to more efficiently apply the SSE processes, activities, and tasks to various SoI (e.g., smart vehicles, major weapon systems, and industrial control systems). Our research goal is to more fully understand an effective systems security approach, increase the manageability of SSE efforts, and provide cost effective SSE solutions.

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

TABLE IV
PRIORITY SCHEME FOR THE DEFENSE ACQUISITION GUIDEBOOK

Defense Acquisition Guidebook	**Compliance**	**People**	**System Resiliency**	**Operations**	**Physical and Environmental**	**Asset Management**	**Interconnectivity**
Missions/Mission-Essential Functions		X	X			X	X
Critical Subsystems, Configuration Items, and Components			X			X	X
Initial Start Conditions			X	X			
Operating Environment	X				X		
Critical Suppliers	X					X	
Sum	**2**	**1**	**3**	**1**	**1**	**3**	**2**

TABLE V
PRIORITY SCHEME FOR THE FRAMEWORK FOR SCADA SECURITY POLICY

SCADA Security Policy Framework	**Compliance**	**People**	**System Resiliency**	**Operations**	**Physical and Environmental**	**Asset Management**	**Interconnectivity**
Data Security						X	X
Platform Security				X	X	X	
Communication Security				X			X
Personnel Security		X			X		
Configuration Management	X					X	
Audit	X	X					
Applications			X	X		X	
Physical Security					X		
Manual Operations		X	X				
Sum	**2**	**3**	**2**	**3**	**3**	**4**	**2**

REFERENCES

[1] K. Baldwin, J. Miller, P. Popick and J. Goodnight, "The United States Dept of Defense Revitalization of System Security Engineering Through Program Protection," in Systems Conference (SysCon), 2012.

[2] L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST SP 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.

[3] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann and P. Sommerlad, Security Patterns: Integrating Security and Systems Engineering, West Sussex: John Wiley & Sons Ltd, 2006.

[4] DoD, "Dept of Defense Standard 5200.28. Trusted Computer System Evaluation Criteria," Dept of Defense, Washington, D.C., 1983.

[5] S. Khou, L. O. Mailloux and M. McEvilley, "A Foundation for Developing Sustainably Secure Systems," INSIGHT, vol. 19, no. 2, pp. 62-65, July 2016.

[6] Defense Science Board Task Force, "Security Controls for Computer Systems," The Rand Corporation, Washington, D.C., 1970.

[7] DoD, "Military Handbook 1785. System security engineering program management requirements," Dept of Defense, Washington, DC, 1989.

[8] P. G. Neumann, "Principled Assuredly Trustworthy Composable Architectures," SRI International, Menlo Park, CA, 2004.

[9] "GAISP - Generally Accepted Information Security Principles," Information Systems Security Association, 2004.

[10] M. Swanson and B. Guttman, "NIST SP 800-14 Generally Accepted Principles and Practices for Security Information Technology Systems," NIST, Gaithersburg, MD, 1996.

[11] ITSEC, "Information Technology Security Evaluation Criteria," Commission of the European Communities, 1991.

[12] CTCPEC, "The Canadian Trusted Computer Product Evaluation Criteria," Communications Security Establishment, Canada, 1993.

[13] "ISO/IEC 15408 - Information technology — Security techniques — Evaluation criteria for IT security," International Organization for Standardization/International Electrotechnical Commission, Switzerland, 1999.

[14] R. Ross, M. McEvilley and J. C. Oren, "NIST SP 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, 2016.

[15] DAU, "Defense Acquisition Guidebook," Defense Acquisition University/Dept of Defense, Ft. Belvoir, VA, 2010.

[16] SEBoK authors, "Security Engineering," The Trustees of the Stevens Institute of Technology, Hoboken, NJ, 2015.

[17] M. Branagan, R. Dawson and D. Longley, "Security Risk Analysis for Complex Systems," in Information Systems Security Association, 2006.

[18] R. Anderson, Security Engineering, 2nd ed., Indianapolis, Indiana: Wiley Publishing, Inc, 2008.

[19] H. F. Tipton and K. Henry, Official $(ISC)^2$ guide to the CISSP CBK, Boston: Auerbach Publications, 2015.

[20] "ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management.," International Organization for Standardization/International Electrotechnical Commission, Switzerland, 2013.

[21] HHS, "45 CFR 95.621 - ADP Reviews," United States Dept of Health and Human Services, 1990.

[22] FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," National Institute of Standards and Technology, Gaithersburg, MD, 2006.

[23] DHS, "Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection," Dept of Homeland Security, Washington, D.C., 2010.

[24] DHS, "Catalog of Control Systems Security: Recommendations for Standards Developers," Dept of Homeland Security, Washington, D.C., 2011.

[25] B. Lampson, "Usable Security: How to Get It," Communications of the ACM, vol. 52, no. 11, pp. 25-27, 2009.

[26] M. A. Sasse and I. Flechais, "Usable Security: Why Do We Need It? How Do We Get It?," in Security and Usability: Designing secure systems that people can use, Sebastopol, O'Reilly, 2005, pp. 13-30.

[27] NDIA, "Engineering for System Assurance," National Defense Industrial Association, Arlington, VA, 2008.

[28] The MITRE Corporation, "Systems Engineering Guide," The MITRE Corporation, McLean, VA, 2014.

[29] NATO, "Engineering for System Assurance in NATO Programs," NATO Standardization Agency, Washington, D.C., 2010.

[30] D. Inserra and S. P. Bucci, "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Backgrounder, 6 March 2014.

[31] C.-Q. Yang, "Operating System Security and Secure Operating Systems," SANS Institute, 2003.

[32] NIST, "NIST SP 800-53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Dept of Commerce , Washington, D.C., 2013.

[33] D. Kilman and J. Stamp, "Framework for SCADA security policy," Sandia National Laboratories, Albuquerque, NM, 2005.

[34] J.P. Anderson.. "Computer Security Technology Planning Study", United States Air Force Electronic Systems Division. Bedford, MA, 1972

[35] P. Boudra, Jr.. "Report on rules of system composition: Principles of secure system design", NSA, Information Systems Security Organization, March 1993.

[36] "Mandiant APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 2013.

[37] M. Reed, "System Security Engineering for Program Protection and Cybersecurity," 18th Annual NDIA Systems Engineering Conference, Springfield, VA,October 2015

[38] J. Bayuk and A. Mostashari, "Measuring systems security," Systems Engineering, vol 16, no 1, pp. 1-14, 2013

[39] J. M. Narkevicius, "Making People the Center of Systems Security," INSIGHT, vol. 14, no. 2, pp. 32-35, July 2011.

[40] Defense Science Board Task Force, "Reslient Military Systems and the Advanced Cyber Threat," Defence Science Board, Washington, D.C., January 2013.

[41] D. J. Bodeau and R. Graubart, "Cyber Resliliency Engineering Framework," The MITRE Corporation, Bedford, MA, 2011

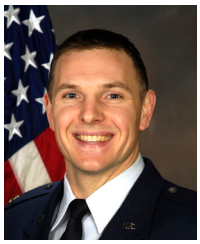
[42] P. McDaniel, B. Rivera, and A. Swami, "Toward a Science of Secure Environments," IEEE Security & Privacy, vol. 12, no. 4, pp. 68-70, 2014.

[43] C. Irvine, T. D. Nguyen. "Educating the Systems Security Engineer's Apprentice," IEEE Security & Privacy, vol. 8, no. 4, pp. 58-61, 2010.

[44] "ISO/IEC 21827nformation technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM)," International Organization for Standardization/International Electrotechnical Commission, Switzerland, 2008.

[45] J. Dahmann, G. Rebovich, M. McEvilley, and G.Turner, "Security Engineering in a System of Systems Environment," *IEEE SysCon International*, 2013

Stephen Khou (BS 2009, MS 2016) is a Masters student at the US Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio, US. He is commissioned as a Captain in the United States Air Force and serves as a cyberspace operations expert.



Logan O Mailloux, CISSP, CSEP (BS 2002, MS 2008, PhD 2015) is a commissioned officer in the United States Air Force and Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. His research interests include system security engineering, complex information technology systems, and quantum key distribution systems. He is a member of INCOSE, ITEA, IEEE, ACM, Tau Beta Pi, and Eta Kappa Nu.

John M Pecarina (BS 2001, MS 2008, PhD 2013) is a commissioned officer in the United States Air Force and Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. His research interests include distributed systems, image retrieval and object detection, pattern detection in workflow management systems, and data security.

Michael McEvilley (BS 1980, MS 1995) is a principal computer scientist in the Systems Engineering Technical Center at The MITRE Corporation, McLean, Virginia, US. He serves as a system assurance lead supporting the US DoD in the acquisition of trustworthy secure and resilient weapons systems. He is a co-author of NIST SP 800-160.

5. A Framework for Prioritizing SSE Processes, Activities, and Tasks

5.1. Description

While there are many excellent security frameworks and methodologies available, there are few references written to equip the Systems Engineer to intelligently engage the established security community. This paper provides a framework for more fully understanding and prioritizing the application of SSE processes, activities, and tasks as described in the NIST SP 800-160. This work extends the system agnostic domains concepts introduced in chapter 4 by presenting a methodology which examines, maps, and prioritizes the SSE processes, activities, and tasks to the system agnostic domains.

This paper studies explicit relationships between processes and activities as noted in the NIST SP 800-160 and highlights areas of interest within the NIST SP 800-160 for the Systems Engineer. This mapping affords the Systems Engineer another opportunity at further tailoring the NIST SP 800-160 to their specific needs. The resulting SSE framework offers a repeatable and tailorable methodology which allows system developers to systematically focus on particular SSE processes, activities, and tasks in order to support critical missions and business operations while also meeting stakeholder security objectives and protection needs. This framework creates a bridge between experts and those looking to apply state of the art SSE practices by offering a prioritization tool to reduce some of the decision-makers' required knowledge and time.

5.2. Publication Details

Title: A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks

Publication: IEEE Access

Date: Submitted February 2017

A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks

S. Khou, L.O. Mailloux, *Member, IEEE*, J. M. Pecarina, and M. A. McEvilley

***Abstract*—This paper provides a framework for more fully understanding the application of Systems Security Engineering (SSE) processes, activities, and tasks as described in the National Institute of Standards and Technology (NIST) Special Publication 800-160. First, a Systems Engineering perspective to the security problem is described with an emphasis on related systems-oriented security methodologies. Next, a proposed SSE framework is presented; most importantly, it allows stakeholders to tailor and prioritize their SSE efforts based on protection needs. Lastly, three example prioritizations are detailed to illustrate the framework's applicability to various systems types (conventional IT, cyber-physical, and major weapon systems). The SSE framework (included online) offers a repeatable and tailorable methodology which allows system developers to focus on high Return-on-Investment (RoI) SSE processes, activities, and tasks to more efficiently meet stakeholder protection needs.**

***Index Terms*—Systems Security Engineering, Systems Engineering, Security Engineering, Security Framework**

I. INTRODUCTION

Current security practices lack effective methodologies to prioritize and address system security issues in complex systems [1], [27]. In their recent call to arms, the Principal Deputy to the Deputy Assistant Secretary of Defense for Systems Engineering Kristen Baldwin *et al.* stressed the need for integration and formalization of security methods, processes, and tools into established Systems Engineering (SE) processes, specifically citing that one of the major challenges to modern programs and systems was the increasingly complex, dynamic, and interconnected interactions of systems [3]. This challenge complicates the ability to understand and prove that complex systems and Systems-of-Systems (SoS), across their execution states and modes, are secure.

To address this problem, the National Institute of Standards and Technology Special Publication (NIST SP) 800-160 *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* aims to aid in developing trustworthy secure systems that are fully capable of supporting critical missions and business operations while meeting stakeholder security objectives and protection needs [1]. Yet the SSE processes activities and tasks in NIST SP 800-160 must be applied to diverse classes of systems.

This research seeks to provide a System Security Engineering (SSE) framework that offers a repeatable and tailorable methodology to system developers, allowing them to focus SSE processes, activities, and tasks to more efficiently meet stakeholder protection needs. By doing so, we make the following contributions:

- A provision for mapping the SSE processes and activities to the system agnostic security domains introduced in [2]
- A systematic application of SSE processes, activities, and tasks to diverse classes of systems
- A graphical analysis on the tightly coupled nature of the SSE processes as presented in the NIST SP 800-160

In Section II, a discussion of existing SSE concepts, methodologies, and frameworks is provided for the reader. Section III explores the SSE process relationships through graphical analysis clustering. This application identifies and outlines the explicit relationships between processes and activities presented in the NIST SP 800-160. Section IV introduces the SSE application framework by discussing domain-to-process associations and mappings. Section V provides a brief commentary on the implications of these domain mappings and the ability to express particular areas of interest in the NIST SP 800-160 for the Systems Engineer given their own specific domain prioritization. It also provides three examples which utilize the framework presented in Sections III and IV to prioritize SSE efforts. Finally, in Section VI, we conclude with a discussion on the interpretations of our work and discuss how this research agenda can be further explored with respect to the NIST SP 800-160. This work also seeks to extend the baseline knowledge of practicing systems security engineers and those responsible for SSE roles and responsibilities [5]. Note, this work extends the author's previous work [2], [6], [7].

Paper submitted February 01, 2017.

- *S. Khou, L.O. Mailloux, and J. M. Pecarina are with the Air Force Institute of Technology, Wright-Patterson AFB, OH 45433-7765 USA (email: {Stephen.khou}, {logan.mailloux}, {john.pecarina}@afit.edu).*
- *M. A. McEvilley is a principle computer scientist with the MITRE Corporation, McLean, VA 22102 (email: mcevilley@mitre.org).*

II. BACKGROUND

Despite their focus on computer security, early works recognized the foundational systems nature of their task [6]. For example, the 1970 Defense Science Board Task Force on Computer Security concluded that providing satisfactory security controls in a computer system is itself a system design problem [31]. Moreover, the board specifically identified security as a systems problem: "a combination of hardware, software, communications, physical, personnel, policy, and procedural safeguards" [31].

As modern systems continue to increase in size and complexity, systems security is not adequately addressed, resulting in business and mission stakeholders becoming more susceptible to a considerable array of disruptive events [1]. This is because the majority of security literature speaks to security only from an IT or cybersecurity perspective, (e.g., Trusted Computer System Evaluation Criteria (TCSEC) [8], Information Technology Security Evaluation Criteria (ITSEC) [9], Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [10], and ISO/IEC 15408: *Information technology — Security techniques — Evaluation criteria for IT security* [11]).

Initially sponsored by the National Security Agency (NSA) and developed by the International Systems Security Engineering Association (ISSEA), the Systems Security Engineering Capability Maturity Model (SSE-CMM), which has evolved into ISO/IEC 21827, describes essential characteristics of engineering security processes that should exist in an organization in order to ensure quality security engineering [32], [34]. The SSE-CMM establishes a framework for measuring and improving performance in the application of security engineering principles; it can be used by engineering organizations to evaluate and refine security engineering practices, by customers to evaluate a provider's security engineering capability, and by SE evaluation organizations to establish organizational capability-based confidences [33], [34].

While the SSE-CMM delivers the necessary roadmap for adopting organization-wide security engineering practices, it does not specifically point out any tools or techniques that can be used to help reach the goals described in the process areas; rather, it is used as a means for engineering organizations to evaluate their security engineering practices and define improvements to them [33], [34].

Another groundbreaking work, Ross Anderson's *Security Engineering: A Guide to Building Dependable Distributed Systems* describes the interaction between technical engineering basics, security, human psychology, and usability [21]. At more than one thousand pages, this comprehensive volume details how to develop systems that stay dependable whether faced with error or malice. As security spans a wide gamut of disciplines, this book tries to bridge the gap between the various disciplines while avoiding unnecessary technical details and providing much emphasis on what can go wrong and what one can learn from those situations. While it does not specifically present a "systems-oriented" view of security, it highlights numerous security considerations for a number of distributed systems and successfully covers a wide range of practical security issues quite well.

In addition, a risk-based methodology for addressing security concerns in systems via the Program Protection Plan (PPP) [3] had been developed and applied as the basis for system security engineering for US Department of Defense (DoD) systems. In 2011, the DoD publicly acknowledged the need for an integrated approach for developing secure systems as they revitalized their SSE approach through the PPP [3], [25]. By identifying critical system components and assessing threats and vulnerabilities of these components, the Systems Engineer can identify and address countermeasure options for the system. By considering these risks in early concepts, requirements, and design trades for systems, SSE is being integrated into SE of systems [3], [35].

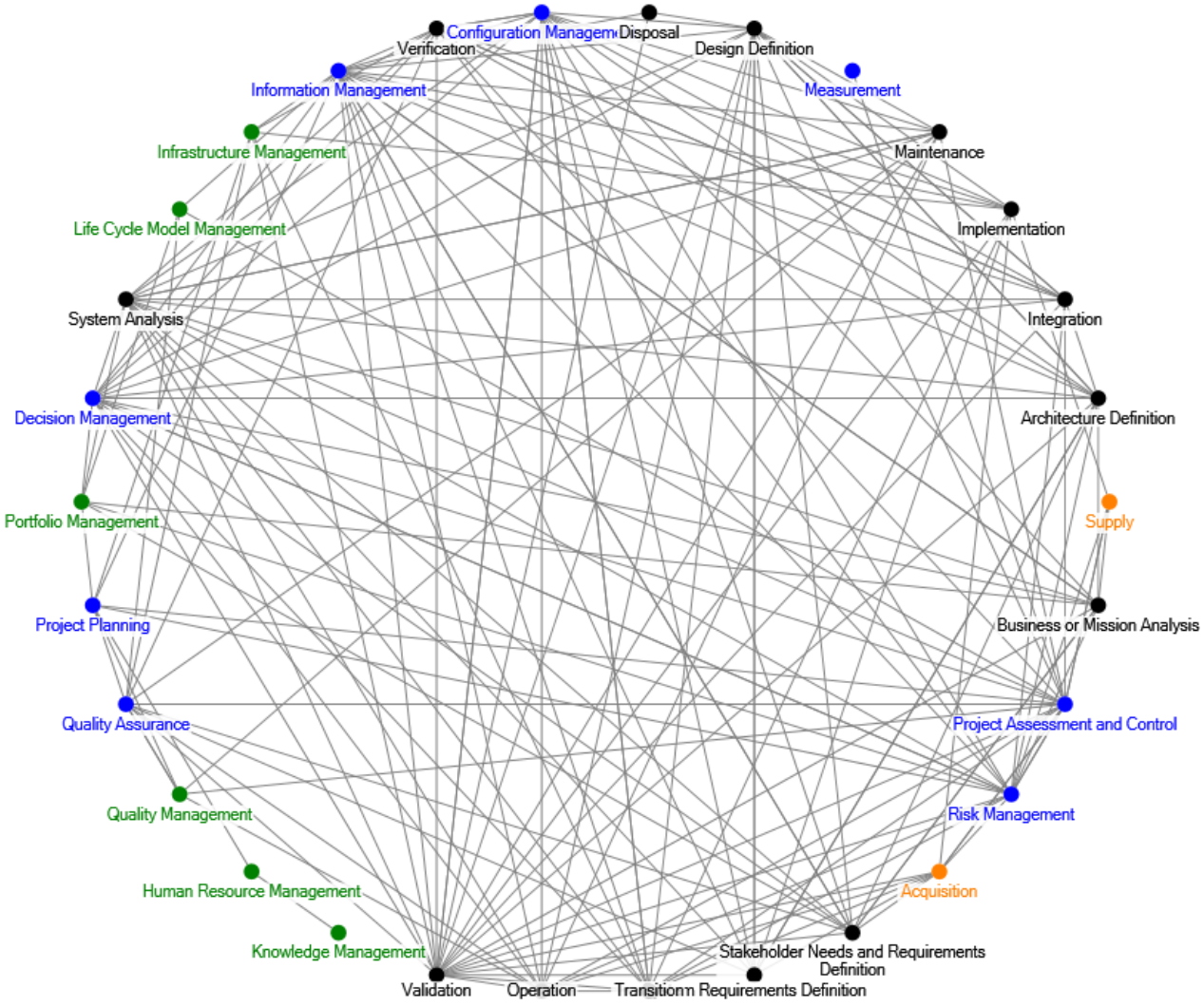
Other security frameworks, such as those used to develop the seven abstracted security domains described in [2], include the United States Department of Health and Human Services 45 Code of Federal Regulations (CFR) Part 95, Subpart: F [12]; ISO/IEC 27002 [13]; Federal Information Processing Standards 200 (FIPS 200) [14]; the International Information System Security Certification Consortium $(ISC)^2$ CISSP CBK [15]; the Department of Homeland Security's (DHS) Transportation Systems Sector-Specific Plan, an annex to their National Infrastructure Protection Plan [16]; and the DHS Catalog of Control Systems Security for protecting critical infrastructure [17]. These works outline provisions for establishing minimum baseline or system-level security considerations for their respective areas.

While there are many excellent security frameworks and methodologies available, there are few references written to equip the Systems Engineer to intelligently engage the established security community. Of the SSE literature available, only a few promote a systematic approach to SSE. Furthermore, due to the constant emergence of new threats and technologies, adopting organization wide standardization of security concepts and practices is becoming more critical.

Of noteworthy importance is NIST SP 800-160, which provides a systematic approach to security for Systems Engineers and is framed around the widely accepted international standard ISO/IEC/IEEE 15288 [4]. Published in November of 2016, after 5 years of effort and significant reviews by subject matter experts, it is arguably the most comprehensive statement on SSE to date, providing foundational engineering considerations in the form of SSE processes, activities, and tasks based on well-established security principles, concepts, and practices. More concretely, NIST SP 800-160 is not a standard, prescriptive checklist, or formalized evaluation criteria – it is a multidisciplinary engineering approach which "ensures [security] requirements and needs are addressed with appropriate fidelity and rigor" [4]. For an overview of NIST SP 800-160, please see [6], [7].

III. INHERENT RELATIONSHIPS BETWEEN SSE PROCESSES

In this work, we map the relationships between the processes as described in the NIST SP 800-160, noting that we assume a non-directional relationship between the processes. The NIST SP 800-160 identifies and describes 30 SSE processes, 111 activities, and 428 tasks. While each process and its supporting activities and tasks can be executed as a standalone procedure, it is often the case that each process (or



The colors partition the processes into their respective families: black represents the Technical Processes, Blue represents the Technical Management Processes, Green represents the Organization Project-Enabling Processes, and Orange represents the Agreement Processes

.FIG. 1: RELATIONSHIP GRAPH OF SYSTEMS SECURITY ENGINEERING PROCESSES AS OUTLINED IN NIST SP 800-160.

one of its activities) has a connection, or relationship, with another process. The NIST SP 800-160 explicitly connects several of these processes and activities to other processes and activities, either as inputs or outcomes of those processes and activities.

Mapping these explicit relationships, Table A-1 (see Appendix A) shows that many of the processes are tightly coupled and that no process is completely isolated from any other process. In other words, each process outcome influences or is influenced by another process, and may not necessarily be in the same process family. Fig. 1 details a relationship graph (also known as a social graph) that depicts the connective network between the processes of Table A-1 [30]. As is evident in the relationship graph, all processes are connected in some fashion to another process.

In analyzing the relationship between these processes, we examine clustering coefficient, as shown in Table 1. In graph theory, the clustering coefficient is a measure of the degree to which nodes in a graph tend to cluster together; it is a real number between 0 and 1 in which 0 represents no clustering and 1 represents maximal clustering [38]. More specifically, evidence suggests that in most real-world networks, and in particular social networks, nodes tend to create tightly knit groups characterized by a relatively high density of ties; this likelihood tends to be greater than the average probability of a tie randomly established between two nodes [36], [37]. The clustering coefficient of a graph is based on a local clustering coefficient for each node

$$C_i = \frac{\text{number of triangles connected to node } i}{\text{number of triples centered around node } i} \quad (1)$$

where a triple centered around node i is a set of two edges connected to node i. Using NodeXL to calculate the clustering coefficient for each process (treating them as nodes with respect to Fig. 1), we generate the values in Table 1 [30].

The results point to the notion that 27 of the 30 processes have some varying degree of connectedness with the other processes, with 20 of those processes having a clustering coefficient of 0.5 or higher. In other words, when applying any

of the SSE processes to a particular system, the system developer must account for possible related processes in order to maximize the development effort. We note that the clustering coefficient for *Measurement*, *Human Resource Management*, and *Knowledge Management* is 0, a value we expect and corresponds directly to the number of connections each process makes in Fig. 1 (and relationships identified in Table A-1). A value of 0 does not necessarily mean there are no connections for that node (this could instead be interpreted as a less complete neighborhood around that particular node).

TABLE 1: CLUSTERING COEFFICIENTS FOR SSE PROCESSES ORDERED BY VALUE FROM GREATEST TO LEAST.

Processes (Nodes)	Clustering Coefficient
Disposal	1.000
Integration	0.867
Quality Management	0.800
Architecture Definition	0.773
Business or Mission Analysis	0.689
Maintenance	0.689
Transition	0.667
Decision Management	0.650
Configuration Management	0.633
Operation	0.628
Verification	0.621
Infrastructure Management	0.619
Design Definition	0.590
System Requirements Definition	0.583
System Analysis	0.583
Stakeholder Needs/Req Definition	0.564
Acquisition	0.536
Implementation	0.533
Risk Management	0.525
Validation	0.500
Portfolio Management	0.476
Information Management	0.415
Project Assessment and Control	0.375
Quality Assurance	0.345
Supply	0.333
Project Planning	0.286
Life Cycle Model Management	0.167
Measurement	0.000
Human Resource Management	0.000
Knowledge Management	0.000

IV. DOMAIN-TO-PROCESS ASSOCIATIONS

In order to study the efficient application of the SSE processes, we utilize the seven abstracted system security domains (Compliance, People, System Resiliency, Operations, Physical and Environmental, Asset Management, and Interconnectivity) from [2]. These domains were developed using existing and well-established security frameworks, extracting common elements described across many fields and specialties without being too restrictive to one specific system.

The utility of these domains allows systems to be partitioned into their most basic security considerations when developing or modifying systems through the use of a priority scheme [2]. In order to better define the connection between the system agnostic security domains and SSE, we map each domain with possible SSE processes and activities from the NIST SP 800-160. In doing so, we create a customizable framework for stakeholders and Systems Engineers to tailor and prioritize their SSE efforts based on protection needs.

Utilizing past and present experiences and efforts of systems-related works such as [3], [4] and security-related works including [5], [6], [7], we interpret the NIST SP 800-160 literature descriptions of the 30 processes and 111 activities and match each activity to the corresponding system agnostic security domain(s) [2] most closely associated with that activity to build Table B-1 (see Appendix B). We map the activities here because we determined that the processes themselves do not provide enough detail for association whereas the tasks are perhaps too detailed for our purposes. The results are normalized on a scale from 0 to 1, with 0 having no association or relation and 1 being highly associated or having a strong relation between the domain and the process in question. That is, the more activities that are associated to a given domain, the higher the correlation value of the parent process or "hit rate" for that domain. We assume that each positive association (i.e., each connection between a domain and an activity) increases the overall relationship between that domain and the activity's parent process. Note that as this mapping is the authors' preliminary effort at correlating between the domains and the literature, the information presented in the table may not necessarily be complete or entirely correct in its current form. It serves as an initial baseline for discussion, and may be complicated by the high degree of connectivity between independently managed systems where formal assessments can often be prohibited by the affected systems' management [23]. Additional elaboration or evaluation is needed as future efforts continue.

In Table 2, the SSE naming convention, as described by the NIST SP 800-160, is established for the system life cycle processes [4]. Each process is identified by a two-character designation.

Plotting the developed relationships into a radar chart (shown in Figs. 2, 3, 4, and 5), we are able to observe the relative values (or levels of associativity) between each domain and the NIST SP 800-160 SSE processes. This allows us to infer, given no previous bias (i.e., we assume that all processes, activities, and tasks were given similar and fair assessment by the authors and reviewers of NIST SP 800-160 and are equally important in the SSE approach), what specific process areas to explore given a specific domain of interest. Because the system life cycle processes are organized and grouped into four families in the NIST SP 800-160, the radar charts are organized as such to provide a similar perspective. Fig. 2 is the Technical Processes, Fig. 3 is the Technical Management Processes, Fig. 4 is the Organization Project-Enabling Processes, and Fig. 5 is the Agreement Processes. Note, because the Agreement Processes family only contains two processes, Fig. 5 is displayed with the information in reverse to better display the result.

TABLE 2: PROCESS NAMES AND DESIGNATORS.

ID	Process	ID	Process
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

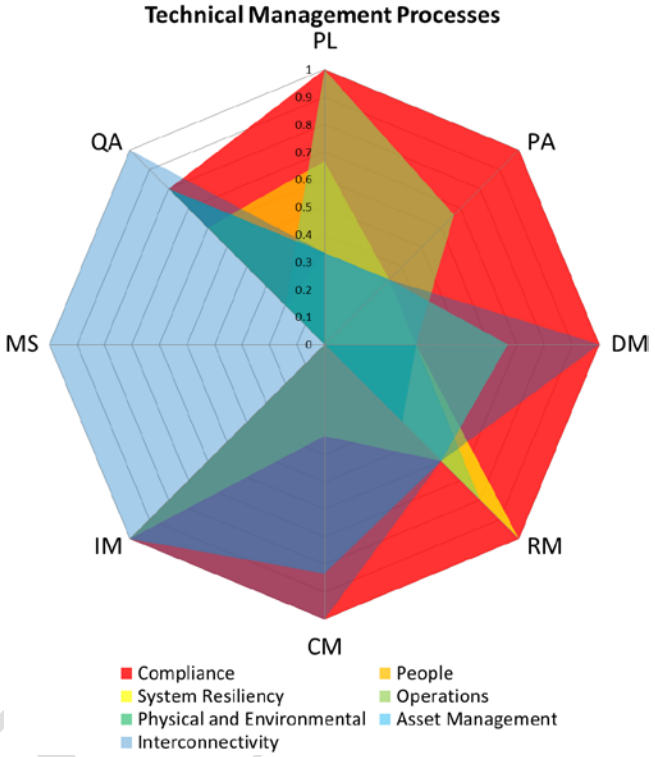


FIG. 3: CONSOLIDATED OVERVIEW OF SSE DOMAIN ASSOCIATIONS WITH SSE TECHNICAL MANAGEMENT PROCESSES.

FIG. 2: CONSOLIDATED OVERVIEW OF SSE DOMAIN ASSOCIATIONS WITH SSE TECHNICAL PROCESSES.

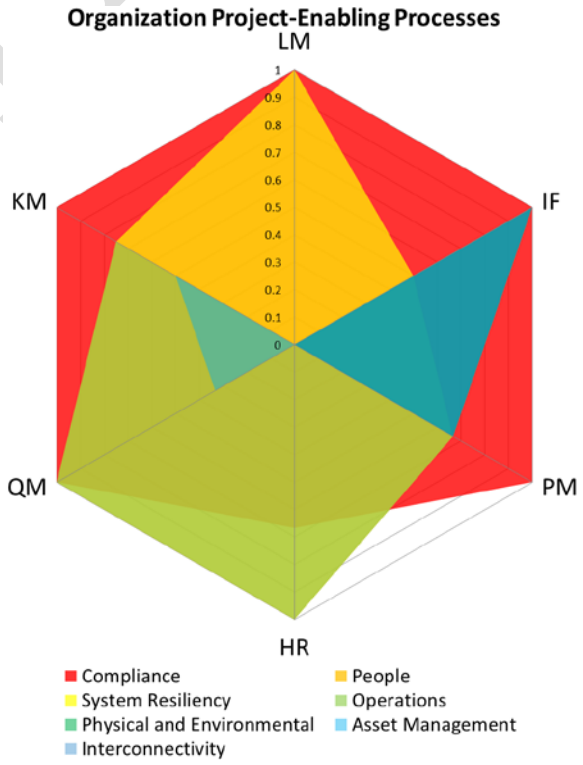


FIG. 4: CONSOLIDATED OVERVIEW OF SSE DOMAIN ASSOCIATIONS WITH SSE ORGANIZATION PROJECT-ENABLING PROCESSES.

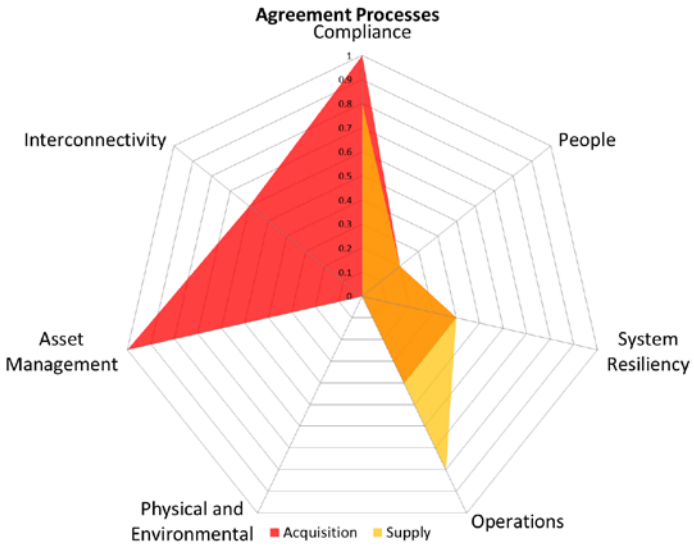


FIG. 5: CONSOLIDATED OVERVIEW OF SSE DOMAIN ASSOCIATIONS WITH SSE AGREEMENT PROCESSES.

To better understand Figs. 2–5, consider a scenario in which the stakeholder (or project manager) considers Physical and Environmental Security to be the system's highest security concern. From Fig. 2, we note that the Technical Process that most closely concerns the Physical and Environmental Security domain is *Maintenance*, with *Architecture Definition*, *Integration*, *Verification*, *Transition*, and *Validation* falling closely behind. Continuing with Figs. 3 and 4, we can see that the Technical Management Processes that most closely concerns the Physical and Environmental Security domain is *Quality Assurance* while the Organization Project-Enabling Processes point to *Quality Management*. The Agreement Processes, from Fig. 5, shows no association to Physical and Environmental Security. These processes have the highest correlation or "hit rate" values for their specific process family. Consequently, from the initial list of 30 SSE processes, the Physical and Environment Security domain has narrowed the system security engineer's focus down to eight first level SSE processes of concern, as shown in Table 3.

We can then use Fig. 1 (and Table A-1) to determine the processes related to these eight. Accounting for the duplicates in the additional processes provided, our final list of processes associated with the Physical and Environmental Security domain include: *Maintenance*, *Architecture Definition*, *Integration*, *Verification*, *Transition*, *Validation*, *Quality Management*, *Quality Assurance*, *Project Assessment and Control*, *Decision Management*, *Risk Management*, *Configuration Management*, *Information Management*, *Life Cycle Model Management*, and *Infrastructure Management* processes. Of these 15 processes, the first eight were determined directly by the domain association to the NIST SP 800-160 whereas the remaining seven were obtained using explicit process relationships identified in Table A-1.

TABLE 3: SUMMARY OF THE PHYSICAL AND ENVIRONMENTAL SECURITY DOMAIN ASSOCIATED PROCESSES AND THEIR RELATED PROCESSES.

First Level Processes	Related Processes
Maintenance	Validation; Operation; Design Management; Configuration Management; Information Management; Quality Assurance; Quality Management
Architecture Definition	Validation; Decision Management; Risk Management; Configuration Management; Information Management
Integration	Verification; Validation; Project Assessment and Control; Decision Management; Risk Management; Configuration Management; Information Management
Verification	Validation; Project Assessment and Control; Decision Management; Risk Management; Configuration Management; Information Management; Quality Assurance
Transition	Validation; Operation; Project Assessment and Control; Decision Management; Risk Management; Configuration Management; Information Management
Validation	Project Assessment and Control; Decision Management; Risk Management; Configuration Management; Information Management; Quality Assurance
Quality Management	Project Planning; Project Assessment and Control; Quality Assurance
Quality Assurance	Information Management; Life Cycle Model Management; Infrastructure Management

V. IMPLICATIONS AND APPLICATION EXAMPLES

The mapping of the system agonistic domains to the SSE processes via its activities marks an attempt to focus the Systems Engineer to specific issues or considerations during system development. The more associated activities a process has to a domain, the higher the chance that the process will outweigh other processes in terms of importance using this methodology. In doing so, this approach provides a repeatable mechanism for the engineer to quickly determine the most important SSE processes (in the context of their particular system) when using the NIST SP 800-160 as a guideline for secure system development. Of important note is that not all of the activities and tasks in a particular process map directly to a domain, but rather provide a starting point for focusing when developing and maintaining systems. Similarly, tasks and activities in "non-important" (remaining) processes should also be considered when time and resources allow as this approach provides a foundational approach to the issue, rather than an all-encompassing solution.

For example, while the first level processes (those determined using the domain-to-process mappings) determined by domain association should take precedence based on the system's own criticality factors, the related processes (or second level processes) add an additional layer of consideration for developing sustainably secure systems. Moreover, duplicate process listings do not necessarily indicate that those processes are more important or that more resources should be allocated towards those process areas; they are a byproduct of various associations and relations that each process shares with other processes. Further examination and analysis needs to be conducted in order to provide an accurate interpretation of the nature of duplicate processes.

Next, the three examples provided in [2] (conventional IT industry [24], government specific acquisition [25], and critical infrastructure [26]) are extended through the use of the methodologies outlined in Sections III and IV. Decisions regarding when, where, and how these system agnostic

security domains and their interpretations should be used are best determined by the specific industry sectors and the Subject Matter Experts (SMEs) associated with those systems. Thus, these examples are not intended to replace the need for applying sound engineering judgment, established best practices, or risk assessments, but rather function as example use cases for further analysis and consideration for engineering complex systems. In this way, it was possible to construct prioritization schemes that determine, based on what controls is assumed to matter more for the system or organization, how to organize the security domains in level of importance for the system developer [2].

A. NIST SP 800-53 Revision 4

The first example is the NIST SP 800-53R4 *Security and Privacy Controls for Federal Information Systems and Organizations*, consisting of 285 controls in 19 families [24]. This publication provides for the ability to scope and tailor controls to an organization's specific mission (or user requirements) and provides best practice recommendations for information security management by those initiating, implementing, or maintaining information security systems. Using the NIST SP 800-53R4 prioritization scheme [2], the domains list by "order of importance" are: Compliance; Physical and Environmental; People and Interconnectivity; Asset Management; and System Resiliency and Operations. Applying the domain-to-process methodology to the Compliance domain, we determine the associated processes from each of the families, summarized in Table 4. Figs. 6, 7, and 8 display modified versions of Figs. 2, 3, and 4, highlighting only the domain of interest (Compliance).

Similar to the sample scenario, highlighting the processes in the relationship graph allows us to extrapolate another level deeper into related processes. Accounting for duplicates, the list of related processes reduces down to (in no particular order): *Stakeholder Needs and Requirements Definition*, *System Analysis*, *Maintenance*, *Supply*, *Quality Assurance*, *Human Resource Management*, and *Measurement*. Table 5 shows the finalized list of first level processes obtained by using the domain-to-process mapping methodology as well as the second level related processes from the associated relationship graph. It should be again noted that the first level processes, given the methodology provided, should take precedence over the related processes in terms of time and resources due to the direct relationship that the first level processes have with the domain, as opposed to the acquired relationship of the related processes.

TABLE 4: NIST SP 800-5R4 FIRST LEVEL PROCESSES.

Process Families	Compliance
Technical Processes	Business or Mission Analysis; System Requirements Definition; Architecture Definition; Design Definition; Implementation; Integration; Verification; Transition; Validation; Operation; Disposal
Technical Management Processes	Project Planning; Project Assessment and Control; Decision Management; Risk Management; Configuration Management; Information Management
Organization Project-Enabling Processes	Life Cycle Model Management; Infrastructure Management; Portfolio Management; Quality Management; Knowledge Management
Agreement Processes	Acquisition

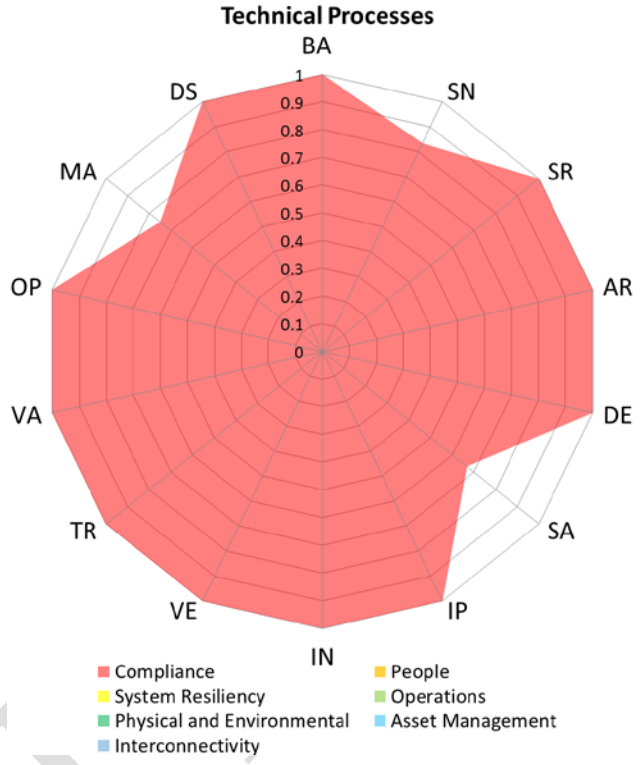


FIG. 6: OVERVIEW OF COMPLIANCE DOMAIN ASSOCIATIONS WITH SSE TECHNICAL PROCESSES.

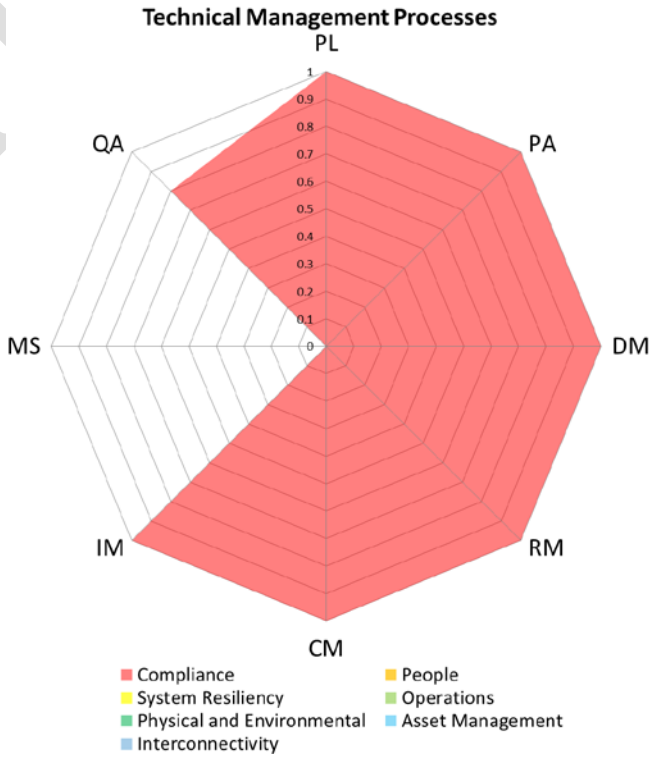


FIG. 7: OVERVIEW OF COMPLIANCE DOMAIN ASSOCIATIONS WITH SSE TECHNICAL MANAGEMENT PROCESSES.

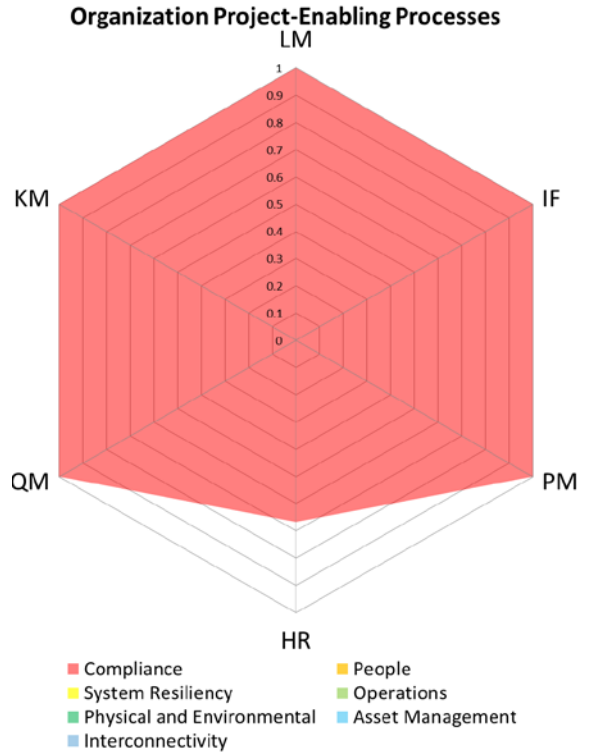


FIG. 8: OVERVIEW OF COMPLIANCE DOMAIN ASSOCIATIONS WITH SSE ORGANIZATION PROJECT-ENABLING PROCESSES.

TABLE 5: CONSOLIDATED LIST OF NIST SP 800-53R4 SUGGESTED PROCESSES.

First Level Processes (by domain association)	Related Processes (by explicit relationship)
Business or Mission Analysis	Stakeholder Needs and Requirements Definition
System Requirements Definition	System Analysis
Architecture Definition	Maintenance
Design Definition	Supply
Implementation	Quality Assurance
Integration	Human Resource Management
Verification	Measurement
Transition	
Validation	
Operation	
Disposal	
Project Planning	
Project Assessment and Control	
Decision Management	
Risk Management	
Configuration Management	
Information Management	
Life Cycle Model Management	
Infrastructure Management	
Portfolio Management	
Quality Management	
Knowledge Management	
Acquisition	

In this example, 23 of the 30 processes are identified by the Compliance domain. Adding in the related processes, all 30 are identified. This, however, does not mean that Compliance should be considered the most important of all domains. Conversely, it identifies that this specific domain reaches across all processes and activities in some manner and should be further scrutinized and evaluated for its specific system. It also points to an area in the methodology that requires additional research and considerations in order to provide the user more actionable items and results.

B. *Defense Acquisition Guidebook*

The next example examines Chapter 13 of the Defense Acquisition Guidebook (DAG) [25], which provides detailed procedural steps in performing criticality analysis, the Department of Defense's (DoD) method by which mission-critical components and information are identified and prioritized. In essence, this program protection concept seeks to defend warfighting capabilities by keeping secret things from getting out and malicious things from getting in [25], [22]. The DAG provides details on integrating classical Systems Engineering processes for mitigating and managing risks to unprecedented technologies and mission-critical system functionality throughout the acquisition lifecycle [25].

Using the DAG prioritization scheme from [2], the domains list by "order of importance" are: System Resiliency and Asset Management; Compliance and Interconnectivity; and finally People, Operations, and Physical and Environmental. Applying the domain-to-process methodology to the System Resiliency and Asset Management domains, we can determine the associated processes from each of the families, summarized in Table 6. Figs. 9, 10, and 11 display modified versions of Figs. 2, 3, and 4, highlighting only the domains of interest (System Resiliency and Asset Management). Note that System Resiliency and Asset Management were prioritized equally in the aforementioned scheme.

Exploring the processes in the relationship graph and accounting for duplicates, the list of related processes reduces down to (in no particular order): *Decision Management, Configuration Management, Stakeholder Needs and Requirements Definition; System Requirements Definition, System Analysis, Operation, Disposal, Supply, Project Assessment and Control, Quality Assurance, Quality Management,* and *Business or Mission Analysis.* Table 7 shows the finalized list of first level processes obtained by using the domain-to-process mapping methodology as well as the second level related processes from the associated relationship graph.

In this example, we identified that 25 of the 30 processes should have some consideration based on the prioritization of System Resiliency and Asset Management. Perhaps more realistically, an initial approach could focus directly on the 13 first level processes (and perhaps even prioritize those processes themselves to determine which has more importance in the context of the system) and only attempt to address the related processes as needed or as time and resources allow.

For instance, we can construct a new "hybrid" graph that provides additional information by aggregating the domains' values (or the values of their process "hit rates"). Figs. 12, 13, and 14 show that by focusing on the processes in this manner, we can narrow the list to: *Validation*, *Verification*, *Risk Management*, and *Infrastructure Management*. This is not to say that these processes are of more importance; rather, these processes have a higher correlation value given our particular association scheme and may prove to be a reasonable starting point for considering the large number of identified processes.

TABLE 6: DAG FIRST LEVEL PROCESSES.

Process Families	System Resiliency	Asset Management
Technical Processes	Verification; Validation	Architecture Definition; Design Definition; Implementation; Integration; Verification; Transition; Validation; Maintenance
Technical Management Processes	Risk Management	Information Management
Organization Project-Enabling Processes	Life Cycle Model Management	Infrastructure Management
Agreement Processes	N/A	Acquisition

FIG. 9: OVERVIEW OF SYSTEM RESILIENCY AND ASSET MANAGEMENT DOMAIN ASSOCIATIONS WITH SSE TECHNICAL PROCESSES.

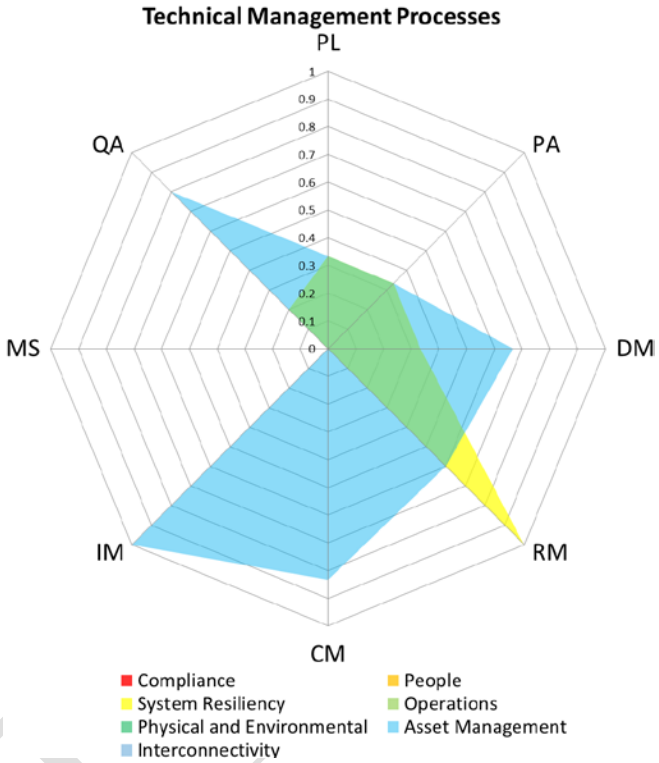


FIG. 10: OVERVIEW OF SYSTEM RESILIENCY AND ASSET MANAGEMENT DOMAIN ASSOCIATIONS WITH SSE TECHNICAL MANAGEMENT PROCESSES.

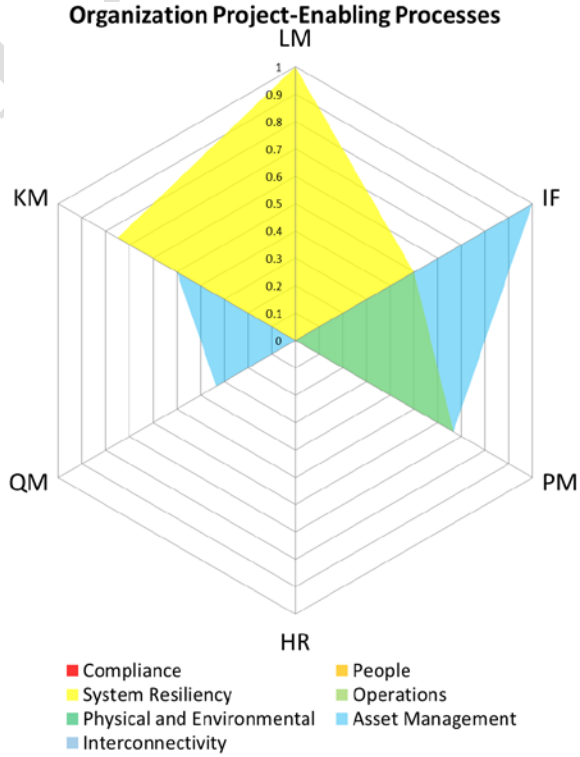


FIG. 11: OVERVIEW OF SYSTEM RESILIENCY AND ASSET MANAGEMENT DOMAIN ASSOCIATIONS WITH SSE ORG. PROJECT-ENABLING PROCESSES.

TABLE 7: CONSOLIDATED LIST OF DAG SUGGESTED PROCESSES.

First Level Processes (by domain association)	Related Processes (by explicit relationship)
Architecture Definition	Decision Management
Design Definition	Configuration Management
Implementation	Stakeholder Needs and Requirements
Integration	Definition System Requirements
Verification	Definition
Transition	System Analysis
Validation	Operation
Maintenance	Disposal
Risk Management	Supply
Information Management	Project Assessment and Control
Life Cycle Model Management	Quality Assurance
Infrastructure Management	Quality Management
Acquisition	Business or Mission Analysis

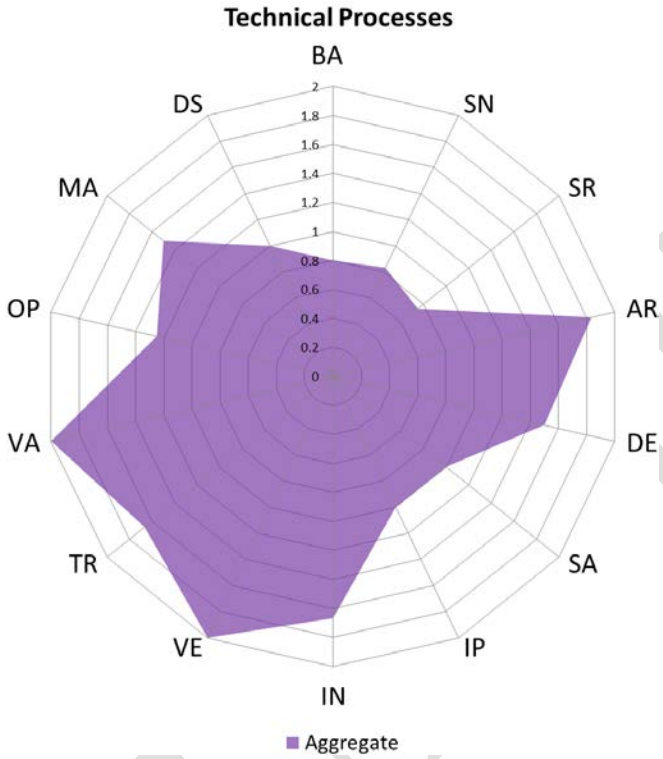


FIG. 12: AGGREGATED OVERVIEW OF DOMAIN ASSOCIATIONS WITH SSE TECHNICAL PROCESSES.

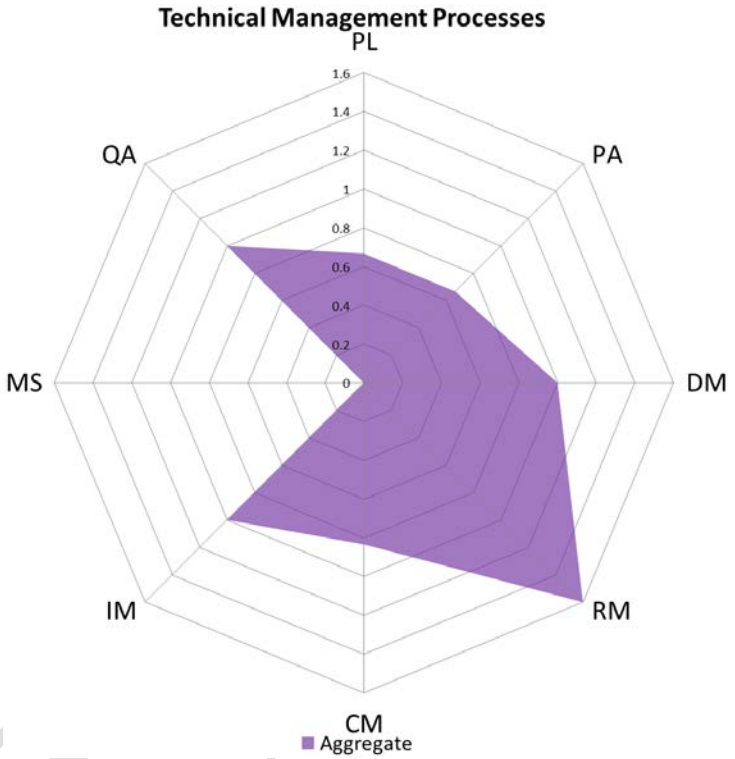


FIG. 13: AGGREGATED OVERVIEW OF DOMAIN ASSOCIATIONS WITH SSE TECHNICAL MANAGEMENT PROCESSES.

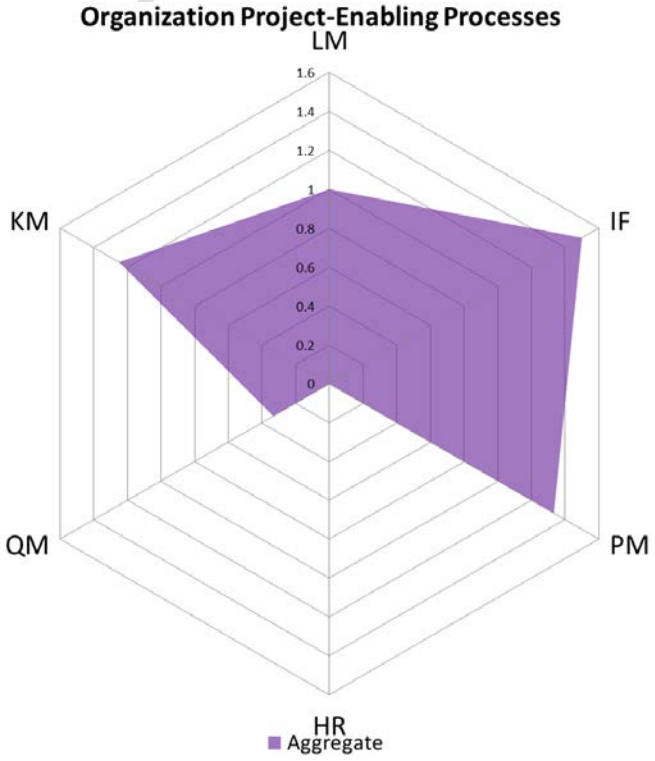


FIG. 14: AGGREGATED OVERVIEW OF DOMAIN ASSOCIATIONS WITH SSE ORGANIZATION PROJECT-ENABLING PROCESSES.

C. SCADA Security Policy Framework

The final prioritization example uses the Framework for Supervisory Control and Data Acquisition (SCADA) Security Policy, developed by Sandia National Laboratories in an effort to ease the creation of SCADA security policies and ensuring coverage over all critical areas of SCADA security as well as flexibility in developing customized policies for specific operations [26]. The domains list by "order of importance" for this example are: Asset Management; People, Operations, Physical and Environmental; and finally Compliance, System Resiliency, and Interconnectivity [2]. Applying the same methodology as before to the Asset Management domain gives us Table 8 and Figs. 15, 16, and 17. Similarly, Table 9 summarizes the second level related processes.

In this example, 11 of the 30 processes are identified, providing the Systems Engineer a reasonable starting point in tailoring the NIST SP 800-160 toward developing a verifiably secure SCADA system. Like before, the 14 related processes provide supplementary direction for secure development, given additional time and resources.

TABLE 8: SCADA FRAMEWORK FIRST LEVEL PROCESSES.

Process Families	Asset Management
Technical Processes	Architecture Definition; Design Definition; Implementation; Integration; Verification; Transition; Validation; Maintenance
Technical Management Processes	Information Management
Organization Project-Enabling Processes	Infrastructure Management
Agreement Processes	Acquisition

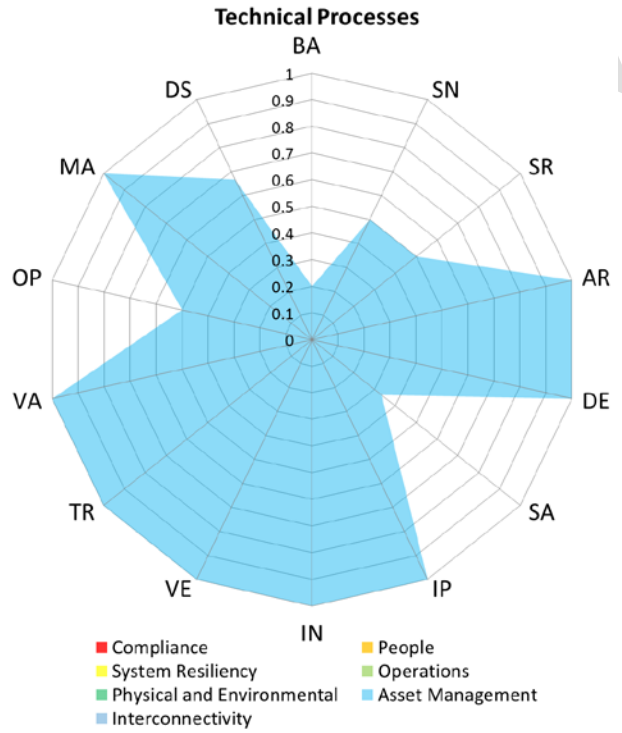


FIG. 15: OVERVIEW OF ASSET MANAGEMENT DOMAIN ASSOCIATIONS WITH SSE TECHNICAL PROCESSES.

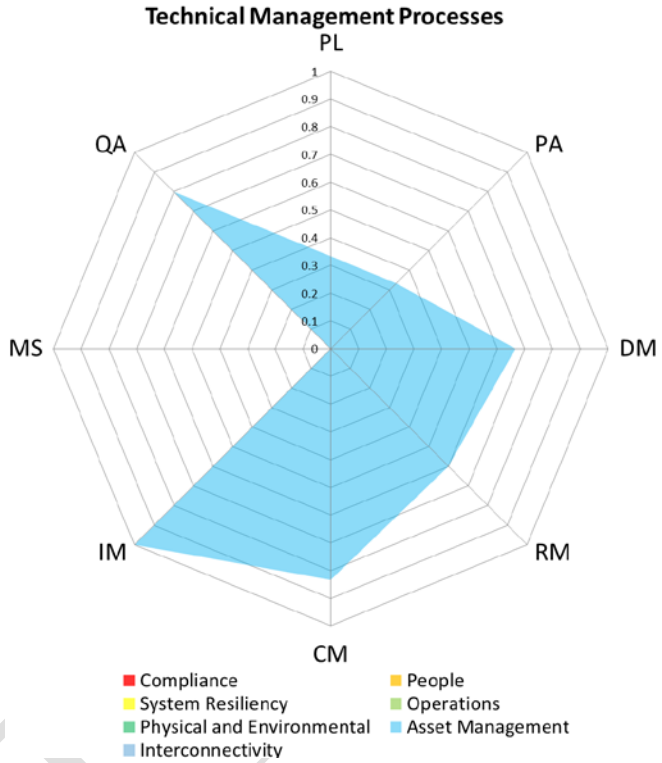


FIG. 16: OVERVIEW OF ASSET MANAGEMENT DOMAIN ASSOCIATIONS WITH SSE TECHNICAL MANAGEMENT PROCESSES.

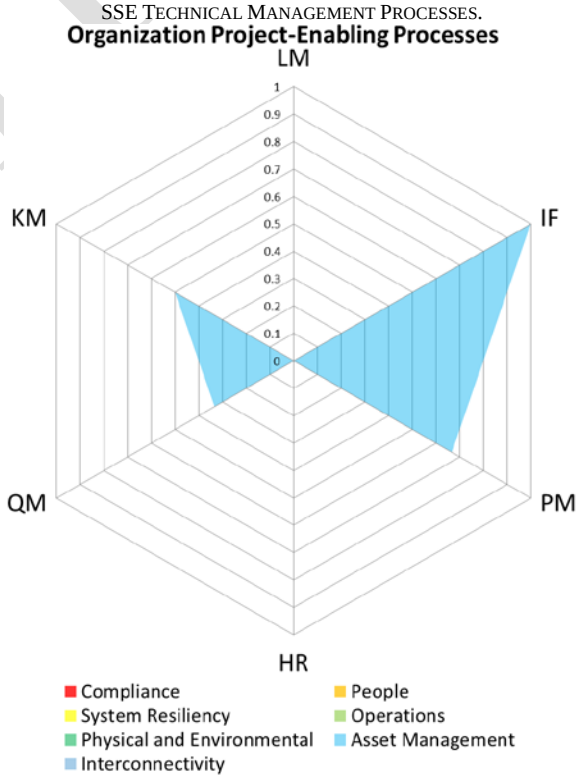


FIG. 17: OVERVIEW OF ASSET MANAGEMENT DOMAIN ASSOCIATIONS WITH SSE ORGANIZATION PROJECT-ENABLING PROCESSES.

TABLE 9: CONSOLIDATED LIST OF SCADA FRAMEWORK SUGGESTED PROCESSES.

First Level Processes (by domain association)	Related Processes (by explicit relationship)
Architecture Definition	Decision Management
Design Definition	Risk Management
Implementation	Configuration Management
Integration	Stakeholder Needs and Requirements Definition
Verification	System Requirements Definition
Transition	System Analysis
Validation	Operation
Maintenance	Disposal
Information Management	Supply
Infrastructure Management	Project Assessment and Control
Acquisition	Quality Assurance
	Quality Management
	Business or Mission Analysis

D. *Observations*

These three examples demonstrate that the "most important" processes when tailoring the NIST SP 800-160 for the three system frameworks are vastly different from one another given the specific prioritization mappings (which presumably represent the stakeholders' priorities).

We also noted that in the first example, the NIST SP 800-53R4, that Compliance was the dominant domain of interest given the prioritization scheme presented in [2]. With it, all 30 processes were highlighted as being associated with the domain through first level and second level relationships. While this result may not provide initial actionable information for the Systems Engineer, it does offer substantiation that Compliance plays a role in all SSE activities and must be considered under most, if not all, circumstances. Motivation to comply is often based on the users' understanding of why their actions and behaviors can put organizational assets at risk [28].

The second example using the DAG emphasized the fact that prioritizing multiple domains may initially highlight too many processes of interest for the Systems Engineer. By aggregating their associative sums, however, we were able to identify which processes appeared more consistently across the various domains and able to offer the Systems Engineer a more targeted approach at tailorability, identifying four of the 30 processes. The final example, the Sandia National Labs SCADA Framework, initially highlighted 11 of the 30 processes for consideration. By focusing on these 11, the Systems Engineer can prioritize their SSE efforts to develop a verifiably secure system with an emphasis on Asset Management security.

VI. CONCLUSION

As current security practices often lack effective methodologies to determine, prioritize, and address system security issues in complex systems, this paper proposes an innovative approach towards the efficient application of SSE processes, activities, and tasks. It does so by offering a mapping to the processes and activities listed in the NIST SP 800-160 as well as providing direct relationships between the processes and activities to allow for further development opportunities for the Systems Engineer. Finally, this work demonstrates the utility of the domain-to-process mappings with three example scenarios.

While the tools and expertise that enable systems engineers to obtain information about the events such as attack paths, likelihood of successful compromise, and the nature and severity of the event exists, information about the potential risk to a system is not readily available using any tools or software [29]. Some prioritization can be performed, but uses the human decision-maker's internal knowledge that is different for each decision-maker; this requires proficient domain knowledge and substantial time [29]. Our proposed framework attempts to create a bridge between the experts and those looking to eventually delve into SSE practices by offering an initial tool for prioritization that complements much of the decision-maker's required knowledge and time through this initial research.

In future work, we desire to further analyze the domain-to-process mapping and relationship in order to better depict a more accurate (and more correct) correlation between the system agnostic domains and the NIST SP 800-160. Additionally, we hope to apply this methodology and framework to a working system, such as a vehicle or avionics system, in order to test its validity and adjust our framework based on these real-world findings. Finally, we would like to be able to provide additional insight into duplicate process listings, as this current effort (save for the second example) treats all processes equally for the purposes of this research activity. Doing so may provide a more detailed approach at domain criticality or process importance for the Systems Engineer and brings us closer to fully understanding an effective systems security approach, increase the manageability of SSE efforts, and provide cost effective SSE solutions.

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

REFERENCES

[1] J. Bayuk and A. Mostashari, "Measuring Systems Security," *Systems Engineering*, vol. 16, no. 1, pp. 1-14, 2013.

[2] S. Khou, L. O. Mailloux, J. M. Pecarina and M. A. McEvilley, "System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts," *Submited to IEEE Access December 2016*.

[3] K. Baldwin, J. Miller, P. Popick and J. Goodnight, "The United States Department of Defense Revitalization of System Security Engineering Through Program Protection," *IEEE Systems Conference (SysCon)*, 2012.

[4] R. Ross, M. McEvilley and J. C. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, 2016.

[5] C. Irvine and T. D. Nguyen, "Educating the Systems Security Engineer's Apprentice," *IEEE Security & Privacy*, vol. 8, no. 4, pp. 58-61, July/August 2010.

[6] S. Khou, L. O. Mailloux and M. A. McEvilley, "A Foundation for Developing Sustainably Secure Systems," *INSIGHT*, vol. 19, no. 2, pp. 62-65, July 2016.

[7] L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST Special Publication 800-160," *IEEE Security & Privacy*, vol. 14, no. 4, pp. 76-80, 2016.

[8] DoD, "Department of Defense Standard 5200.28. Trusted Computer System Evaluation Criteria," Department of Defense, Washington, D.C., 1983.

[9] ITSEC, "Information Technology Security Evaluation Criteria," Commission of the European Communities, 1991.

[10] CTCPEC, "The Canadian Trusted Computer Product Evaluation Criteria," Communications Security Establishment, Canada, 1993.

[11] ISO/IEC, "ISO/IEC 15408: Information technology -- Security techniques -- Evaluation criteria for IT security," International Organization for Standardization/International Electrotechincal Commission, Switzerland, 2009.

[12] HHS, "45 CFR 95.621 - ADP Reviews," United States Department of Health and Human Services, 1990.

[13] "ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management.," International Organization for Standardization/International Electrotechnical Commission, Switzerland, 2013.

[14] FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," National Institute of Standards and Technology, Gaithersburg, MD, 2006.

[15] H. F. Tipton and K. Henry, Official (ISC)2 guide to the CISSP CBK, Boston: Auerbach Publications, 2015.

[16] DHS, "Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection," Department of Homeland Security, Washington, D.C., 2010.

[17] DHS, "Catalog of Control Systems Security: Recommendations for Standards Developers," Department of Homeland Security, Washington, D.C., 2011.

[18] The MITRE Corporation, Systems Engineering Guide, McLean, VA: The MITRE Corporation, 2014.

[19] SEBoK authors, "Security Engineering," The Trustees of the Stevens Institute of Technology, Hoboken, NJ, 2015.

[20] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann and P. Sommerlad, Security Patterns: Integrating Security and Systems Engineering, West Sussex: John Wiley & Sons Ltd, 2006.

[21] R. Anderson, Security Engineering, 2nd ed., Indianapolis, Indiana: Wiley Publishing, Inc, 2008.

[22] M. Reed, "System Security Engineering for Program Protection and Cybersecurity," in *18th Annual NDIA Systems Engineering Conference*, Springfield, VA , 2015.

[23] M. Branagan, R. Dawson and D. Longley, "Security Risk Analysis for Complex Systems," in *ISSA*, 2006.

[24] NIST, "NIST SP 800-53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce , Washington, D.C., 2013.

[25] DAU, "Defense Acquisition Guidebook," Defense Acquisition University/Department of Defense, Ft. Belvoir, VA, 2010.

[26] D. Kilman and J. Stamp, "Framework for SCADA security policy," Sandia National Laboratories, Albuquerque, NM, 2005.

[27] Defense Science Board Task Force, "Resilent Military Systems and the Advanced Cyber Threat," Defense Science Board, Washington, D.C, 2013.

[28] M. A. Sasse and I. Flechais, "Usable Security: Why Do We Need It? How Do We Get It?," in *Security and Usability: Designing secure systems that people can use*, Sebastopol, O'Reilly, 2005, pp. 13-30.

[29] A. Kim and M. H. Kang, "Determining Asset Criticality for Cyber Defense," Naval Research Laboratory, Washington, D.C., 2011.

[30] *NodeXL: Network Overview, Discover, and Exploration for Excel*, Social Media Research Foundation, April 2103, retrieved October 13, 2016.

[31] Defense Science Board Task Force, "Security Controls for Computer Systems," The Rand Corporation, Washington, D.C., 1970.

[32] M. Pazos-Revilla and A. Siraj, "Tools and techniques for SSE-CMM implementation," *12th World Multi-Conference on Systemics, Cybernetics, and Informatics*, 2008.

[33] D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering processes for the development of secure information systems," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 244-253, February 2007.

[34] "ISO/IEC 21827: Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM)," International Organization for Standardization/International Electrotechnical Commission, Switzerland, 2008.

[35] J. Dahmann, G. Rebovich, M. McEvilley, and G.Turner, "Security Engineering in a System of Systems Environment," *IEEE SysCon International*, 2013

[36] P.W. Holland and S. Leinhardt, "Transitivity in structural models of small groups," *Comparative Group Studies*, vol.2, pp. 107-124, May 1971.

[37] D.J. Watts and S.J. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440-442, June 1998.

[38] M. Hazewinkel, ed., "Graph Theory," *Encyclopedia of Mathematics*, Springer, 2001.

Stephen Khou (BS 2009, MS 2016) is a Masters student at the US Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio, US. He is commissioned as a Captain in the United States Air Force and serves as a cyberspace operations expert.

Logan O Mailloux, CISSP, CSEP (BS 2002, MS 2008, PhD 2015) is a commissioned officer in the United States Air Force and Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. His research interests include system security engineering, complex information technology systems, and quantum key distribution systems. He is a member of INCOSE, ITEA, IEEE, ACM, Tau Beta Pi, and Eta Kappa Nu.

John M Pecarina (BS 2001, MS 2008, PhD 2013) is a commissioned officer in the United States Air Force and Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. His research interests include distributed systems, image retrieval and object detection, pattern detection in workflow management systems, and data security.

Michael McEvilley (BS 1980, MS 1995) is a principal computer scientist in the Systems Engineering Technical Center at The MITRE Corporation, McLean, Virginia, US. He serves as a system assurance lead supporting the US DoD in the acquisition of trustworthy secure and resilient weapons systems. He is a co-author of NIST SP 800-160.

APPENDIX A

TABLE A-1: INTERRELATIONSHIPS OF SYSTEMS SECURITY ENGINEERING PROCESSES AS IDENTIFIED IN NIST SP 800-160.

	Business or Mission Analysis	Stakeholder Needs/Req Definition	System Requirements Definition	Architecture Definition	Design Definition	System Analysis	Implementation	Integration	Verification	Transition	Validation	Operation	Maintenance	Disposal	Project Planning	Project Assessment and Control	Decision Management	Risk Management	Configuration Management	Information Management	Measurement	Quality Assurance	Life Cycle Model Management	Infrastructure Management	Portfolio Management	Human Resource Management	Quality Management	Knowledge Management	Acquisition	Supply
Business or Mission Analysis		x				x					x						x	x	x	x										
Stakeholder Needs/ Req Definition	x					x					x						x		x	x										
System Req Definition				x	x	x	x				x								x	x										
Architecture Definition	x	x	x	x	x	x					x						x	x	x	x										
Design Definition		x	x	x		x	x	x		x	x	x	x	x					x	x										
System Analysis											x								x	x										
Implementation									x		x								x	x				x				x	x	
Integration				x	x	x			x		x					x	x	x	x	x										
Verification			x								x					x	x	x	x	x		x								
Transition						x	x				x	x				x	x	x	x	x										
Validation						x										x	x	x	x	x		x								
Operation											x					x	x	x	x	x		x								
Maintenance						x					x	x					x		x	x		x					x			
Disposal											x																			
Project Planning																x				x				x		x				
Project Assessment and Control					x	x											x	x			x	x	x						x	x
Decision Management						x												x		x										
Risk Management						x									x	x	x			x										
Configuration Management						x			x	x	x						x	x												
Information Management	x	x																	x											
Measurement																														
Quality Assurance		x	x																	x			x	x						
Life Cycle Model Management																				x										
Infrastructure Management									x	x	x									x										
Portfolio Management	x	x				x									x		x	x					x							
Human Resource Management																														
Quality Management															x	x						x								
Knowledge Management																										x				
Acquisition		x	x							x	x	x				x		x												
Supply	x															x		x												

APPENDIX B

TABLE B-1: NORMALIZED DOMAIN-TO-PROCESS ASSOCIATIONS.

	Compliance	People	System Resiliency	Operations	Physical and Environmental	Asset Management	Interconnectivity
Technical Processes							
Business or Mission Analysis	1	0.2	0.6	0.6	0.2	0.2	0.4
Prepare for the security aspects of business or mission analysis	x						
Define the security aspects of the problem or opportunity space	x		X	x			
Characterize the security aspects of the solution space	x	x	x	x	x	x	x
Evaluate and select solution classes	x		x	x			
Manage the security aspects of business or mission analysis	x						x
Stakeholder Needs and Requirements Definition	0.83	0.67	0.33	0.67	033	0.5	0.67
Prepare for stakeholder protection needs and security requirements definition	x	x					
Define stakeholder protection needs	x	x	x	x	x	x	x
Develop the security aspects of operational and other life cycle concepts		x		x			x
Transform stakeholder protection needs into security requirements	x	x	x	x	x	x	x
Analyze stakeholder security requirements	x			x			
Manage stakeholder protection needs and security requirements definition	x					x	x
System Requirements Definition	1	0.25	0.25	0.75	0.5	0.5	0.5
Prepare for system security requirements definition	x			x	x		
Define system security requirements	x	x	x	x	x	x	x
Analyze system security in system requirements	x			x			
Manage system security requirements	x					x	x
Architecture Definition	1	0.5	0.83	0.83	0.67	1	1
Prepare for architecture definition from the security viewpoint	x	x	x	x		x	x
Develop security viewpoints of the architecture	x	x	x	x	x	x	x
Develop security models and security views of candidate architectures	x	x	x	x	x	x	x
Relate security views of the architecture to design	x		x	x	x	x	x
Select candidate architecture	x		x	x	x	x	x
Manage the security view of the selected architecture	x					x	x
Design Definition	1	0.25	0.5	0.75	0.25	1	0.75
Prepare for security design definition	x		x	x		x	x
Establish security design characteristics and enablers for each system element	x	x	x	x	x	x	x
Assess the alternatives for obtaining security-relevant system elements	x			x		x	
Manage the security design	x					x	x
System Analysis	0.67	0.33	0.67	0.67	0	0.33	0.67
Prepare for the security aspects of system analysis	x	x	x	x			
Perform the security aspects of system analysis			x	x			x
Manage the security aspects of system analysis	x					x	x
Implementation	1	0.33	0	0.33	0.33	1	1
Prepare for the security aspects of implementation	x				x	x	x
Perform the security aspects of implementation	x	x		x		x	x
Manage results of the security aspects of implementation	x					x	x
Integration	1	0.33	0.67	0.67	0.67	1	1
Prepare for the security aspects of integration	x				x	x	x
Perform the security aspects of integration	x	x	x	x	x	x	x
Manage results of the security aspects of integration	x		x	x		x	x
Verification	1	0.67	1	1	0.67	1	1
Prepare for the security aspects of verification	x	x	x	x	x	x	x
Perform security-focused verification	x	x	x	x	x	x	x
Manage results of security-focused verification	x		x	x		x	x
Transition	1	0.67	0.67	0.67	0.67	1	1
Prepare for the security aspects of transition	x	x			x	x	x
Perform the security aspects of transition	x	x	x	x	x	x	x
Manage results of the security aspects of transition	x		x	x		x	x
Validation	1	0.67	1	1	0.67	1	1
Prepare for the security aspects of validation	x	x	x	x	x	x	x
Perform security-focused validation	x	x	x	x	x	x	x
Manage results of security-focused validation	x		x	x		x	x

Operation	1	1	0.75	0.75	0.5	0.5	0.5
Prepare for secure operation	x	x	x	x			
Perform secure operation	x	x	x	x	x	x	x
Manage results of secure operation	x	x	x	x	x	x	x
Support security needs of customers	x	x					
Maintenance	0.75	0.25	0.5	0.75	0.75	1	0.75
Prepare for the security aspects of maintenance	x			x	x	x	
Perform the security aspects of maintenance	x	x	x	x	x	x	x
Perform the security aspects of logistics support						x	x
Manage results of the security aspects of maintenance and logistics	x		x	x	x	x	x
Disposal	1	0.67	0.33	0.33	0.33	0.67	1
Prepare for the security aspects of disposal	x	x				x	x
Perform the security aspects of disposal	x	x	x	x	x	x	x
Finalize the security aspects of disposal	x						x
Technical Management Processes							
Project Planning	1	0.67	0.33	1	0.33	0.33	0.33
Define the security aspects of the project	x			x			
Plan the security aspects of the project and technical management	x	x	x	x	x	x	x
Activate the security aspects of the project	x	x		x			
Project Assessment and Control	1	0.33	0.33	0.67	0	0.33	0.33
Plan for the security aspects of project assessment and control	x		x	x			
Assess the security aspects of the project	x			x			
Control the security aspects of the project	x	x				x	x
Decision Management	1	0.67	0.33	0.33	0.33	0.67	1
Prepare for decisions with security implications	x	x				x	x
Analyze the security aspects of decision information	x	x	x	x	x	x	x
Make and manage security decisions	x						x
Risk Management	1	0.6	1	0.8	0.4	0.6	0.6
Plan security risk management	x		x	x		x	
Manage the security aspects of the risk profile	x		x				x
Analyze security risk	x	x	x	x	x	x	x
Treat security risk	x	x	x	x	x	x	x
Monitor security risk	x	x	x	x			
Configuration Management	1	0.33	0	0	0	0.83	1
Plan for the security aspects of configuration management	x	x				x	x
Perform the security aspects of configuration identification	x	x				x	x
Perform security configuration change management	x					x	x
Perform security configuration status accounting	x					x	x
Perform security configuration evaluation	x					x	x
Perform the security aspects of release control	x						x
Information Management	1	1	0	0	0	1	1
Prepare for the security aspects of information management	x	x				x	x
Perform the security aspects of information management	x	x				x	x
Measurement	0	0	0	0	0	0	1
Prepare for security measurement							x
Perform security measurement							x
Quality Assurance	0.8	0.6	0.2	0.2	0.8	0.8	1
Prepare for security quality assurance	x	x	x	x	x	x	x
Perform product or service security evaluations					x	x	x
Perform process security evaluations	x	x			x	x	x
Manage quality assurance security records and reports	x						x
Treat security incidents and problems	x	x			x	x	x
Organization Project-Enabling Processes							
Life Cycle Model Management	1	0	1	0	0	0	0
Establish the security aspects of the process	x		x				
Assess the security aspects of the process	x		x				
Improve the security aspects of the process	x		x				
Infrastructure Management	1	0.5	0.5	1	1	1	1
Establish the secure infrastructure	x			x	x	x	x
Maintain the secure infrastructure	x	x	x	x	x	x	x
Portfolio Management	1	0.67	0.67	0.67	0.67	0.67	0.67
Define and authorize the security aspects of projects	x	x	x	x	x	x	x
Evaluate the security aspects of the portfolio of projects	x	x	x	x	x	x	x
Terminate projects	x						
Human Resource Management	0.67	1	0	1	0	0	0
Identify systems security engineering skills		x		x			
Develop systems security engineering skills	x	x		x			
Acquire and provide systems security engineering skills to projects	x	x		x			

Quality Management	1	1	0	1	0	0.33	0.33
Plan security quality management	x	x		x		x	
Assess security quality management	x	x		x			
Perform security quality management corrective and preventive actions	x	x		x			x
Knowledge Management	1	0.75	0.75	0.75	0	0.5	0
Plan security knowledge management	x	x	x	x		x	
Share security knowledge and skills throughout the organization	x	x	x	x			
Share security knowledge assets throughout the organization	x	x	x	x		x	
Manage security knowledge, skills, and knowledge assets	x						
Agreement Processes							
Acquisition	1	0.2	0.4	0.4	0	1	0.6
Prepare for security aspects of the acquisition	x		x	x		x	
Advertise the acquisition and select the supplier to conform with the security aspects of the acquisition	x	x				x	x
Establish and maintain the security aspects of agreements	x					x	x
Monitor the security aspects of agreements	x		x	x		x	x
Accept the product or service	x					x	
Supply	0.8	0.2	0.4	0.8	0	0.6	0
Prepare for the security aspects of the supply	x		x	x		x	
Respond to a solicitation		x		x		x	
Establish and maintain the security aspects of agreements	x		x	x			
Execute the security aspects of agreements	x						
Deliver and support the security aspects of the product or service	x			x		x	

6. Discussion

6.1. Conclusions of Research

In examining SSE concepts and developing a framework for understanding, prioritizing, and applying SSE processes, activities, and tasks, the intended purpose of this research effort endeavored to address three research questions:

1. How can SSE be understood and described with respect to established Systems Engineering processes?
2. How can SSE efforts be decomposed into universally applicable systems security domains?
3. How can SSE processes, activities, and tasks be prioritized and applied to diverse classes of systems?

In order to answer the first question, a comprehensive overview of prevailing SSE concepts and practices is required. To determine the current status of SSE, it is imperative to appreciate the historical context under which SSE was developed and to understand its evolution over the years in order to satisfy various requirements. The articles "A Foundation for Developing Sustainably Secure Systems" and "Putting the 'Systems' in Security Engineering" discusses the history of notable systems-oriented security publications and its culmination in the NIST SP 800-160 [1], [2].

With the historical context discussed, these two articles proceed to elaborate on developing a multidisciplinary engineering approach which ensures security requirements and needs are addressed with appropriate fidelity and rigor by aligning with the 30 Systems Engineering life cycle processes of ISO/IEC/IEEE 15288 (discussed in the NIST

SP 800-160) to address system security considerations throughout the entire system life cycle [3].

The second research question is answered in the article "System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts," where seven abstracted systems security domains are proposed to broadly describe a "universal" approach for understanding and categorizing systems security concerns into distinct domains. The article also demonstrates the utility of the proposed system agnostic domains with three example prioritization schemes based on the importance (or criticality) of each security domain, allowing an organization to determine which domains are more important and therefore warrant more resources. For example, three well-established security frameworks (Cyber, ICS, and DoD) were examined and used to create mappings from their particular characteristics and system properties back to the system agnostic security domains. This research effort resulted in the construction of prioritization schemes that determine how to organize the security domains in level of importance for the system developer based on what controls are assumed to matter more for the system or organization [4]. In doing so, the researchers' work provides essential knowledge for understanding how to more effectively apply SSE processes for engineering trustworthy and secure systems.

In response to the third research question, the researcher looked into how SSE processes, activities, and tasks can be systematically applied to diverse classes of systems. In the article "A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks," several existing frameworks were explored and introduced discussions for effectively applying the SSE processes, activities, and tasks

described in the NIST SP 800-160 were introduced. The first involved a graphical analysis on the tightly coupled nature of the SSE processes as presented in the NIST SP 800-160, while the second provided an initial provision for mapping the SSE processes and activities to the system agnostic security domains introduced in [4]. As a result, this work uniquely offers a systematic application of SSE processes, activities, and tasks to diverse classes of systems, culminating in a repeatable and tailorable methodology which allows system developers to focus on high return on investment SSE processes, activities, and tasks to more efficiently meet stakeholder protection needs.

6.2. Significance of Research

With the development of increasingly complex systems, Systems Engineers need to be concerned with addressing stakeholder security needs and objectives in a systematic way to deliver trustworthy secure systems. This research offers the community a look into recent developments in the field of SSE in order to provide an approach which ensures networked systems operate properly despite uncertain environments, malicious and non-malicious disruptions, and intelligent adversaries. While the NIST SP 800-160 delivers a first-of-its-kind, systems-oriented approach to ensuring stakeholder security requirements and protection needs are met with appropriate fidelity and rigor [2], this research provides a directed methodology for efficiently applying the NIST SP 800-160. Additionally, in recommending the seven systems agnostic security domains, this research provides an approach for universally understanding and categorizing systems security concerns [4]. These abstracted domains serve as a common baseline for implementing SSE while thoroughly understanding and discussing the system security

problem in addition to building confidence in inter-organizational activities such as developing security standards and effective security practices [4].

While the tools and expertise that enable Systems Engineers to obtain information about security events such as attack paths, likelihood of successful compromise, and the nature and severity of the event exists, information about the potential risk to a system is not readily available using any tools or software [6]. Thus deductions are drawn, primarily from the human decision-maker's internal knowledge, which is different for each decision-maker, requires expert domain knowledge, substantial time, and is error prone [6]. The proposed framework attempts to create a bridge between experts and those looking to apply state of the art SSE practices by offering a prioritization tool to reduce some of the decision-makers' required knowledge and time.

Furthermore, of the three key decision making processes for acquiring DoD weapon systems (requirements determination, resource allocation, and the acquisition management system), this framework focuses most directly on resource allocation by offering a systematic application of SSE processes, activities, and tasks to allow system developers more efficiently meet stakeholder protection needs and providing a prioritized approach to securing major weapon systems, some of which cost hundreds of millions or billions of dollars to design, develop, and field [7].

6.3. Recommendations for Future Research

The initial designs for this research were heavily constrained by available time and resources for what is primarily a proof of concept. In laying the foundation for this system agnostic framework, however, an opportunity is created for further analysis and

research in this topic. One such consideration for additional investigation, for example, would be applying this methodology and framework to a working system, such as a vehicle or avionics system, in order to test its validity and update the framework based on these real-world findings. With initiatives such as the U.S. Air Force's Task Force Cyber Secure (designed to synchronize multiple efforts and studies attempting to address cybersecurity and focus operations to increasing robustness and resilience of critical Air Force systems for core missions in and through cyberspace), using this framework in a government program office or commercial sector may provide a more detailed understanding of domain criticality or process importance for the Systems Engineer and potentially brings us closer to fully developing an effective systems security approach to increase the manageability of SSE efforts and provide cost effective SSE solutions [7], [8].

Another consideration would be the reevaluation of the current list of seven system agnostic domains. The present list is only merely interpretation of the most important aspects of current systems and existing security frameworks. Further elaboration or additional domains could, and should, be considered when using this original concept for continuing research to create a more accurate (and more correct) correlation between the system agnostic domains and the NIST SP 800-160, especially if viable applications and results could be gained from the aforementioned real-work applications. Likewise, future research could reevaluate the current domain-to-process mapping. The provided mapping is only one possible constructive effort and may not necessarily be the most correct mapping. Further analysis or different interpretations would likely produce results that provide value to the system developer. In addition, the

current mapping is constructed by associating domains to processes via their activities. Another possible construction would be to examine the tasks associated with the activities and conduct that particular mapping. This would provide an opportunity to study whether or not the change in mapping would produce any noticeable results in the final framework.

Finally, while this research offers Systems Engineers the ability to efficiently prioritize and apply vetted SSE processes and activities in order to maximize return on investment and minimize the costs associated with it, the current research lacks a suitable metric for measuring the efficiency being claimed by the thesis. Developing or adopting an appropriate metric for analysis would provide increased validity to the framework. Possible metrics that should be examined include level of security and/or costs as a result of implementing the framework.

Bibliography

[1] S. Khou, L. O. Mailloux and M. McEvilley, "A Foundation for Developing Sustainably Secure Systems," Insight, vol. 19, no. 2, pp. 62-65, July 2016.

[2] L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST Special Publication 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.

[3] R. Ross, M. McEvilley and J. C. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, 2016.

[4] S. Khou, L. O. Mailloux, J. M. Pecarina and M. A. McEvilley, "System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts," IEEE Access, Accepted February 2017.

[5] S. Khou, L. O. Mailloux, J. M. Pecarina and M. A. McEvilley, "A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks," IEEE Access, Submitted February 2017.

[6] A. Kim and M. H. Kang, "Determining Asset Criticality for Cyber Defense," Naval Research Laboratory, Washington, D.C., 2011.

[7] Government Accountability Office, "Addressing Incentives is Key to Further Reform Efforts," 30 April 2014. [Online]. Available: http://www.gao.gov/assets/670/662837.pdf. [Accessed 25 January 2017].

[8] U.S. Air Force, "Task Force Cyber Secure," 2016. [Online]. Available: http://www.afitc-event.com/wp-content/uploads/2016/10/Task-Force-Cyber-Secure.pdf. [Accessed 25 January 2017].

Prologue

Lastly, some insights and lessons learned throughout the research process to other students. Systems Engineering, and to a further extent, Systems Security Engineering, are very broad areas of study with no hard guidelines or check lists to ensure that complete understanding and applicability is guaranteed. As a student of the Computer Science and Computer Engineering Department with a Bachelor's in Computer Telecommunications Engineering, a Master's in System Engineering, and an AFIT curriculum in Cyber Operations, I found myself with a unique opportunity to tackling this research area. With a detailed understanding of the technical aspects of IT, and cyber, and security systems, coupled alongside a comprehensive familiarity of systems procurement and development, identifying a need for and following through with this area of research was still quite difficult at times.

For those lacking a similar background, however, don't fret. In fact, your varied experiences and points of views could bring novel insight and provide new understanding to SSE research that I could never have thought possible. While a good SE understanding provides much of the underlying foundation needed to follow-on this work, having a good understanding at the way "traditional" engineers think and process information (such as in Computer Engineering, Electrical Engineering, Mechanical Engineering, Security Engineering) also has its benefits. To this, I recommend at least browsing through Ross Anderson's book, *Security Engineering*, as it provides not only a high level overview of security applications to a variety of important systems, but also an in-depth understanding on critical topics such as technical engineering basics, specialized protection mechanisms, security psychology, policy, and much more. Additionally, the

Defense Acquisition Guidebook, particularly Chapter 13 on Program Protection, provides valuable SE and technical insight into how the DoD focuses on systems and systems security.

Secondly, regarding concept of, this research was very conceptual (especially at the onset), providing very little confirmation of correctness or success level. It was not until the final article that there was an actual new product being developed (the framework) that provided any real sense of completion or accomplishment. From this experience, I recommend not letting the absence of tangible results in the early- and mid-research timeframes discourage you, but help set a path for discussion between you and your research advisor or committee in determining what success ultimately means to you.

Finally, while coursework largely depends on the student's curriculum and degree program and usually encompasses the first half of your time at AFIT, starting work on your thesis during this first half, no matter how trivial (such as gathering, reading, and documenting background works related to your thesis), allows you to more evenly allocate the workload throughout the entire program, rather than forcing you to sharply increase the effort in order to meet mandatory deadlines. Building a large buffer towards to the end of your time at AFIT by focusing on work earlier rather than later allows you to avoid much of the stress and pressure many students end up dealing with by focusing only on coursework during the beginning. That isn't to say, however, that you shouldn't focus on your coursework and grades; it's just as important as finishing up your thesis!

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
23-03-2017	Master's Thesis	March 2016 – March 2017

TITLE AND SUBTITLE

A Framework for Understanding, Prioritizing, and Applying Systems Security Engineering Processes, Activities, and Tasks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Khou, Stephen, Captain, USAF

5d. PROJECT NUMBER
17G409

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT-ENG-MS-17-M-039

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory, Information Systems Division
1864 4th St, Wright-Patterson AFB, OH 45433
Phone: 937-587-7670 / Email: Jason.bryant.8@us.af.mil
ATTN: Jason Bryant

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RISM

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
Current systems security practices lack an effective approach to prioritize and tailor systems security efforts to develop and field secure systems in challenging operational environments, which results in business and mission stakeholders becoming more susceptible to an array of disruptive events. This work informs Systems Engineers on recent developments in the field of system security engineering and provides a framework for more fully understanding the application of Systems Security Engineering (SSE) processes, activities, and tasks as described in the recently released National Institute of Standards and Technology (NIST) Special Publication 800-160. This SSE framework uniquely offers a repeatable and tailorable methodology that allows system developers to focus on high Return-on-Investment (RoI) SSE processes, activities, and tasks to more efficiently meet stakeholder protection needs and deliver trustworthy secure systems.

15. SUBJECT TERMS
Systems Security Engineering, Systems Engineering, Security Engineering, Security Domains

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Major Logan O. Mailloux, AFIT/ENV
U	U	U	UU	68	19b. TELEPHONE NUMBER *(Include area code)* 937-255-3636 ext. 3348 Logan.Mailloux@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18