Summer 2018

Cybersecurity Architectural Analysis for Complex Cyber-Physical Systems

Martin Trae Span III
United States Air Force Academy

Logan O. Mailloux
Air Force Institute of Technology

Michael R. Grimaila
Air Force Institute of Technology

Cybersecurity Architectural Analysis for Complex Cyber-Physical Systems

Martin "Trae" Span
Logan O. Mailloux
Michael R. Grimaila

ABSTRACT

In the modern military's highly interconnected and technology-reliant operational environment, cybersecurity is rapidly growing in importance. Moreover, as a number of highly publicized attacks have occurred against complex cyber-physical systems such as automobiles and airplanes, cybersecurity is no longer limited to traditional computer systems and IT networks. While architectural analysis approaches are critical to improving cybersecurity, these approaches are often poorly understood and applied in ad hoc fashion. This work addresses these gaps by answering the questions: *1. "What is cybersecurity architectural analysis?"* and *2. "How can architectural analysis be used to more effectively support cybersecurity decision making for complex cyber-physical systems?"* First, a readily understandable description of key architectural concepts and definitions is provided which culminates in a working definition of "cybersecurity architectural analysis," since none is available in the literature. Next, we survey several architectural analysis approaches to provide the reader with an understanding of the various approaches being used across government and industry. Based on our proposed definition, the previously introduced key concepts, and our survey results, we establish desirable characteristics for evaluating cybersecurity architectural analysis approaches. Lastly, each of the surveyed approaches is assessed against the characteristics and areas of future work are identified.

Keywords—cybersecurity; architectural analysis; system architecture; systems security engineering; complex system security

MARTIN "TRAE" SPAN III is an Instructor of Systems Engineering at the United States Air Force Academy (USAFA), Colorado Springs, Colorado. He is commissioned as Captain in the United States Air Force (USAF). He received his undergraduate degree in Systems Engineering in 2012 from USAFA and is a recent distinguished graduate from the Air Force Institute of Technology (AFIT) with a Master of Science in Systems Engineering. He serves as a developmental engineer and holds Department of Defense certifications in systems engineering, science and technology management, test & evaluation, and program management. He has served the USAF as a developmental test engineer responsible for planning and executing complex weapon system test and evaluation. He is a member of IEEE and the Tau Beta Pi Honor Society. Capt. Span's research interests include systems engineering and systems security engineering. He can be contacted at: martin.span.1@us.af.mil

I. INTRODUCTION

The cybersecurity threat is one of the most serious economic and national challenges we face as a nation—economic prosperity in the 21st century depends on cyber [1]. Cyberattacks have grown in frequency and complexity, and it is now commonplace to hear of widespread cyberattacks on personal computers, webservers, and even large company and government personnel databases [2]. Moreover, as the Internet of Things (IoT) continues to grow, the centrality of cyber-physical devices to modern life is increasingly important [3]. Previously, cyber-physical systems such as automobiles and airplanes were relatively simplistic. Astonishingly, the 2017 Ford F-150, a relatively common vehicle, has over 150 million lines of code [4], demonstrating the complexity of modern systems when software is at the core of functionality [3]. For these cyber-enabled systems, adversaries are challenging traditional assumptions that systems are secure due to their relative isolation and uniqueness. Recent examples include a widely-publicized hacking demonstration against a Jeep Cherokee [6]. claims of hacking a commercial airliner [7], and comprehensive reports of vehicle vulnerabilities [3]. In light of this growing threat, it is critical to analyze modern weapon systems for cybersecurity vulnerabilities as directed by the United States Congress to mobilize industry to counter these attacks [9].

Recent Department of Defense (DoD) policy updates have expanded the traditional IT security approaches and mandated cybersecurity assessments for cyber-enabled weapon systems [9], [10], [11], [12]. These revisions dictate that acquisition programs integrate cybersecurity efforts into existing systems engineering processes, and work to ensure

LOGAN O. MAILLOUX (BS 2002, MS 2008, Ph.D. 2015) is an Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio USA. He is commissioned as Lieutenant Colonel in the United States Air Force (USAF) and serves as a computer developmental engineer. He is a Certified Information System Security Professional (CISSP), Certified Systems Engineering Professional (CSEP), and holds Department of Defense certifications in cyberspace operations, systems engineering science and technology management, T&E, and program management. He is a member of IEEE, INCOSE, and ITEA professional societies, as well as, HKN and TBP honor societies. He has served the USAF as a cyberspace operations expert responsible network defense exercises, documenting and training computer security best practices and performing T&E of enterprise resource planning solutions. Lt Col Mailloux's research interests include systems security engineering, quantum key distribution, cyber-physical systems, and complex information systems. He can be contacted at: Logan.Mailloux@us.af.mil

cyber considerations hold equal footing with other requirements and design trade-offs at major acquisition milestones [13].

For highly complex systems, including DoD weapon systems, architectural analysis is a critical enabler to effective cybersecurity; however, architectural analysis approaches are often poorly understood and applied in ad hoc fashion. This work addresses these gaps by answering the questions:

1. *"What is cybersecurity architectural analysis?"*
2. *"How can architectural analysis be used to more effectively support cybersecurity decision making for cyber-physical systems?"*

This paper examines and proposes answers to the above questions. In Section II, we provide a readily understandable discussion of key concepts and definitions. Section III expands on this foundation and surveys several cybersecurity architecture analysis approaches from government and industry. In Section IV, desirable characteristics for architectural analysis for cybersecurity are identified and mapped to the approaches from Section III. Lastly, Section V summarizes key findings and identifies promising follow-on research areas for increasing the effectiveness of cybersecurity architectural analysis of unprecedented systems, specifically modern complex cyber physical systems.

II. FOUNDATIONAL CONCEPTS AND DEFINITIONS

This section provides a brief historical context for system-level architectural analysis and, more formally, discusses key definitions for cybersecurity architectural analysis.

A. Brief History of System Architecture

Much of the seminal work in the field of architecture analysis was accomplished by Zachman, who proposed the first system architecture—a logical

MICHAEL R. GRIMAILA, PhD, CISM, CISSP (BS 1993, MS 1995, PhD 1999) is Professor and Head of the Systems Engineering and Management department at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. Dr. Grimaila holds the Certified Information Security Manager (CISM), the Certified Information Systems Security Professional (CISSP), and the National Security Agency's INFOSEC Assessment Methodology (IAM) and INFOSEC Evaluation Methodology (IEM) certifications. Dr. Grimaila is a Fellow of the Information Systems Security Association (ISSA), a Senior Member of the Institute for Electrical and Electronics Engineers (IEEE), and is a member of the Association for Computing Machinery (ACM), Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2), Eta Kappa Nu, and Tau Beta Pi. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management, and systems engineering. He can be contacted at Michael.Grimaila@afit.edu.

construct for integrating the complexities of modern information systems [14]. Similarly to the varying levels of abstraction in physical construction plans, Zachman argued that system architectures should be composed of many perspectives in varying levels of detail. Moreover, he insisted that these perspectives (or views) be synchronized across the system, forming one integrated architecture.

Sowa expanded Zachman's work to form the Information Systems Architecture (ISA) framework [15]. Shown in Fig. 1, the ISA employs six interrogatives (what, how, where, who, when, and why) across five levels of detail (scope, business, system, technology, and detailed representations) as a means of expressing relationships to guide complex system development [16]. In this way, the ISA offers a simplified approach to compare and elaborate on the desired capabilities, requirements, components, and functions in an integrated enterprise-level model which enables effective decision making. Note, not all 30 conceptual graphs are required; thus, the ISA is also tailorable. Since its inception, the ISA (commonly known as the Zachman Framework) has been a popular choice for system architects—it has been widely used by system architects for decades, while several other system-level frameworks have incorporated or adopted its tenets [17].

B. Key Definitions

Here we discuss definitions for key terminology used in this work (i.e., "cybersecurity," "architecture," and "analysis"). First, the term "cybersecurity" should be addressed because it is generally the most poorly understood (see sidebar in [16]). Within the DoD, cybersecurity is formally defined as:

> The prevention of damage to, protection of, and restoration of electronic systems to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [19].

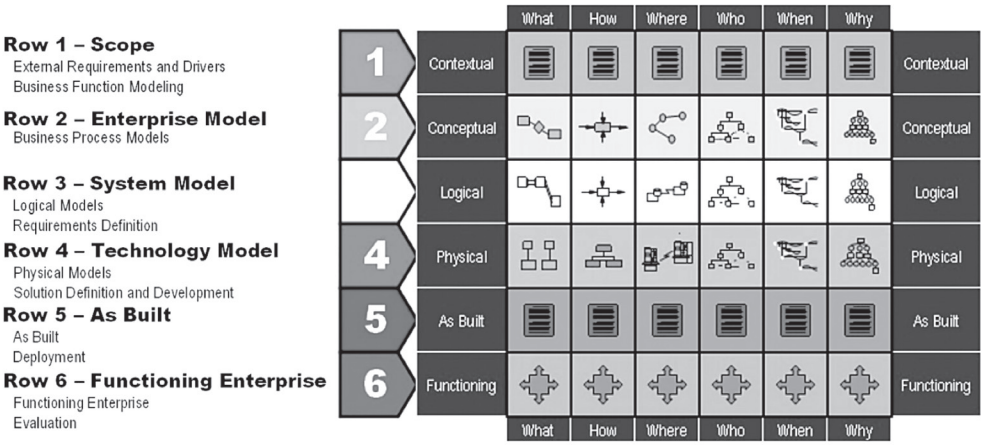

Figure 1. The Zachman Framework for Enterprise Architecture [24].

Despite being often cited, this definition tends to cause confusion because it is packed with domain-specific IT jargon: availability ensures the system is usable as anticipated; integrity is the protection from unauthorized modification; confidentiality is keeping data private; authentication is a validation of the claimed identity; and, nonrepudiation is the ability to prove that an action has taken place. While seemingly comprehensive, the DoD definition is somewhat hindered with legacy terminology; a more practical (i.e., a working) definition of cybersecurity might simply seek to protect critical systems against cyber-based threats [20].

The next key term to define is "architecture" (note, we interpret "architecture" synonymously with "system architecture" and/or "system-level architecture"). Perhaps the most classically understood definition of architecture is provided by Maier and Rechtin:

> Structure in terms of components, connections, and constraints of a product, process, or element [21].

This definition offers a holistic view of the system of interest to include technological aspects as well as non-technological aspects, such as processes. In the simplest terms, an architecture merely provides a means for viewing the system of interest from different perspectives. Conversely, in a somewhat physically-driven characterization, ISO/IEC/IEEE 42010 provides the following definition for architecture:

> The fundamental organization of a system, embodied in its components, their relationship to each other and the environment, and the principles governing its design and evolution [22].

Somewhat surprisingly, the DoD provides a progressive definition of system architecture:

> A set of abstractions (or models) that simplify and communicate complex structures, processes, rules, and constraints to improve understanding and implementation [23].

In addition to being readily understandable, this definition alerts the reader to the intrinsic value offered by such architectures in that they serve to simplify communication with, and improve understanding of, key stakeholders (not just engineers). Moreover, this definition implies that architectures are intended to improve the system's implementation. While these value-rich aspects of the definition are a bit atypical, they are useful for helping others to understand what an architecture is and does.

Lastly, the task of identifying a formal definition of "analysis" within the context of a "system architecture" proved more difficult than previous definitions. Often a systems architecture will center on an integrated model of entities and the relationships between them; architectural models serve as a vehicle to bring order, and thus understandability, to the growing complexity associated with complex systems. An architecture-focused definition may read as such:

> Architectural analysis is the activity of discovering important system properties using conceptual and physical models of the system of interest [25].

However, an architecture's purpose is to increase understanding and facilitate better engineering choice [17]. This two-fold purpose is acutely stated by Crawley *et al.*:

> Architectural analysis focuses on understanding both the architecture's function and form to support decision making [26].

It is worth noting the closely related concept of architecture trade-off analysis, which focuses on evaluating and comparing alternative architecture-level designs and attributes (e.g., modifiability, security, performance, reliability, etc. [27].

C. Cybersecurity Architectural Analysis Working Definition

Ultimately, architectural analysis identifies trade-off points among system attributes and facilitates communication among stakeholders (e.g., customers, developers, operators, maintainers). System-level architectural analysis requires consideration of various missions, essential functions, potential components, and desirable attributes, which help to clarify and refine stakeholder needs and, later, requirements. Moreover, integrated architectural analysis provides a robust framework for ongoing and concurrent system design and analysis.

Specific to the cyber domain, architectural analysis should be used to understand cyber dependencies within the functions and form of the system to enable well-informed decisions. This type of structured analysis brings an otherwise unmanageable amount of information under control in support of system security requirements [28]. Architectural

analysis enables system-level programmatic risk management by providing context and functional mapping to the various physical elements of the system. Thus, cybersecurity architectural analysis allows appropriate security mitigations to be applied where needed with rigorous justification.

After considering seminal definitions in the area, and working through the various architectural analysis approaches discussed in Section III, we present a working definition of cybersecurity architectural analysis for consideration:

> The activity of discovering and evaluating the function and form of a system to facilitate cybersecurity decisions. [31]

This definition identifies two key activities, discovery and evaluation, while simultaneously catering to both new development (i.e., a focus on desired capability through functionality) and legacy systems (i.e., a focus on existing system solutions). For new developments, discovery typically implies exploring the business or mission problem space to further understand the desired capability through functional analysis. For existing systems, this process is often conducted in reverse, mapping critical subsystems back to critical functions which support important business operations or mission execution. It is also worth noting that cybersecurity architectural analysis should also help with identifying and understanding how security requirements support the desired capability, which also provides traceability that is often lacking in systems security efforts.

As part of the broader system definition and development effort, cybersecurity architectural analysis should help inform engineering tradeoffs and decision making such as those processes and activities described in ISO/IEC/IEEE 15288.

III. CURRENT CYBERSECURITY ARCHITECTURAL ANALYSIS APPROACHES

In this section, we survey architectural analysis approaches and assess their applicability for complex system cybersecurity. Within the DoD (and its major defense contractors), several approaches (i.e., methods, processes, and tools) have been developed to secure and assess the cybersecurity of complex systems and systems-of-systems. While providing a detailed case study for each approach surveyed in this work would be ideal for a robust assessment, it is just not feasible as some approaches take months if not years to complete. This survey is based on publicly available literature and presentations that focus specifically on architectural analysis for weapon systems.

The predecessor for many cybersecurity architectural analysis approaches is compliance-based Information Assurance (IA), which focuses almost exclusively on applying security controls to computer networks and IT systems. For complex systems, this approach is inadequate as demonstrated by several high profile security breaches [29]. This inadequacy has driven the development of many of the approaches described in this work.

A. Department of Defense Architectural Framework (DoDAF)

The integrated architecture currently in use by the DoD is the DoD Architecture Framework (DoDAF). Its purpose is to manage complexity to enable key decisions through organized information sharing [23]. However, in DoDAF, like many other architecture frameworks, security (or cybersecurity) is not specifically addressed [30]. James Richards, in his work Using the Department of Defense Architecture Framework to Develop Security Requirements [28], proposes a methodology for using DoDAF to derive security requirements. He outlines a process of first building an architectural model of the enterprise, focusing on a core set of views including the OV-5b operational activity model, the DIV-2 logical data model, and the OV-3 operational resource flow matrix. These critical views are used to model security-relevant processes, data, business rules, and communications. Next, he suggests comparing views for compliance and then assessing and refining the architecture. The overall purpose of Richards' approach is to use DoDAF to expose or derive security requirements [28], This approach has not been widely adopted, but his work demonstrates utility for complex cyber-physical systems.

B. Unified Architecture Framework (UAF)

In contrast to the unique solution DoDAF, industry has developed the Unified Architecture Framework (UAF) [31]. Based on industry need, the UAF includes a formal security domain amongst the more common architectural views. The UAF security domain includes views for security taxonomy, structure, connectivity, processes, constraints, and traceability. More specifically, it uses Systems Modeling Language (SysML) class diagrams to identify data types and map them to protections and security controls. As an integrated architecture, it allows security-relevant elements to be mapped to system resources and operations. UAF also capitalizes on the success of model-based sytems engineering (MBSE) efforts to depict and analyze the security properties of a simulation oriented language (SoI) via an executable architecture. Note, UAF is in the final stages of development, so its utility has yet to be fully realized; however, some pathfinder examples of proposed security views demonstrate utility for conducting cybersecurity architectural analysis of complex cyber-physical systems [32].

C. Publically Available Industry Efforts

Major defense contractors often use custom architectural analysis approaches to design and evaluate their system architectures concerning cybersecurity. Although it is likely that most large DoD contractors are working solutions in this area; at the time of this survey, the authors were only exposed to efforts from Raytheon, Northrop Grumman, and Lockheed Martin. Note, Raytheon's Cyber Resiliency Architecture Framework (CRAF) was the only approach with a detailed open-source publication available. Limited information is available on Northrop and Lockheed's approaches.

Raytheon developed CRAF using a DoDAF reference architecture with extensions for specific cyber resilience mappings and metrics [33]. The goal of CRAF is to assess and identify gaps in cyber resiliency by mapping systems, subsystems, and components against prioritized capabilities to identify resilience requirements for critical mission scenarios.

Using failure modes and effects analysis, Northrop Grumman created a risk-based assessment methodology using an integrated architecture modeled in the new UAF to identify cyber risks for their systems [32]. This approach is still under development and is one of the first systems security efforts based on the upcoming UAF standard security views from the Object Management Group (OMG).

Lockheed Martin has created a custom solution titled the Secure Engineering Assurance Model (SEAM) [34]. SEAM is a tailored systems security engineering approach to integrate security into every solution they deliver. This framework provides tailored security considerations and checklists for each program area.

D. Risk Management Framework (RMF) for Cybersecurity

In response to increasing risks against critical infrastructure and information technology systems, the US government enacted the Federal Information Security Management Act of 2002 which established minimum information security requirements for federal information systems, and charged the National Institute of Standards and Technology (NIST) with developing security standards and guidelines to address these growing risks [35]. In response to this requirement, NIST created the Risk Management Framework (RMF) which provided a structured yet flexible process for applying these standards and guidelines [36]. Accordingly, RMF is the mandated approach for addressing cybersecurity in the DoD [11]. In general, this approach applies a prescriptive risk-based methodology to cybersecurity with the goal of identifying, mitigating, and eliminating system vulnerabilities to protect systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Within the U.S. Air Force, the Air Force Life Cycle Management Center is tasked with conducting RMF for legacy weapon systems (designated as the Platform IT (PIT) systems) [37]. This PIT assessment and authorization process consists of six-steps described in the next paragraph [13].

First, the team must categorize the PIT system according to the information displayed, processed, stored, and transmitted along with the classification of the information and associated technologies. Second, security controls are selected (or assigned) based on the impact resulting from the loss of said information (i.e., criticality analysis) [12]. The third step is implementing said controls with consideration for cybersecurity requirements across the entire system development life cycle—although security controls have been historically applied to IT systems, many have been tailored for PIT systems with prescribed overlays [37]. The fourth step is key to the RMF process and assesses the effectiveness of applied

security controls through threat mapping and vulnerability analysis. On a related note, much of the security work conducted today is exclusively focused on this step. Based on the identified vulnerabilities, the fifth step is to produce a risk assessment and mitigation plan, which is then briefed to the Authorization Official for authorization. The sixth step of the RMF process is continuous monitoring of the system with respect to cybersecurity. As the system and threat environment evolve, security control effectiveness needs to be continuously assessed while keeping in mind future changes and cybersecurity impact.

The RMF is the mostly widely implement approach of those surveyed as it is mandatory for DoD information systems to receive an authorization to operate. While this approach has mitigated vulnerabilities, many cite its perceived difficulty, steep learning curve, and IT-centric focus as currently implemented as critiques in its utility for complex cyber-physical systems.

E. Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) and Cyber Hardening Efforts

The Air Force Research Laboratory (AFRL), in conjunction with the Air Force Institute of Technology's (AFIT) Center for Cyberspace Research, developed an Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) Workshop [38]. This weapon-system-specific workshop teaches a thorough analysis approach by systematically identifying and assessing all external inputs and communications paths to and from a weapon system (i.e., an exhaustive boundary analysis of the system's architecture). The primary activities include gathering information, identifying and analyzing access points, finding and analyzing susceptibilities, anticipating attacks, and applying and recommending mitigations and protections. The ACVAM approach requires extensive subject-matter expert (SME) involvement, access to design documents, and detailed operator insight to discover susceptibilities and determine appropriate mitigations to increase mission assurance by eliminating or reducing vulnerability to cyberattacks. [39]

Additionally, AFRL is developing enhanced cyber hardening tools and resiliency instructions [40]. While specific details are not publicly available, the cyber hardening approach was recently briefed to the defense community at large [39]. In general, this approach describes avionics cyber hardening and resiliency concepts and suggests ways to protect avionics and related systems from cyberattack. Moreover, this approach encourages engineers to 'think avionics cyber' using three tenets of cyber protection: focus on what's critical; restrict access to the critical; and detect, react, and adapt [41]. These approaches provide a robust analysis but require technically savvy domain experts to execute, which restricts its utility for a larger group of complex systems.

F. Attack Path Analysis via Automotive Example

Historically, attack path analysis has served the security community well [42]. In a great

example from the automotive domain, Checkoway *et al.,* provide a practical attack path analysis and comprehensive discussion which solidifies the importance of threat modeling as a cybersecurity architectural analysis technique [8]. While this specific example is automobile-centric, many similarities are shared between cyber-physical systems. More specifically, the work details a four-step method of analyses. First, threat model characterization is accomplished through identification of external attack vectors and attack surfaces. Second, vulnerability analysis addresses the accessibility, criticality, and exploitability of potential vulnerabilities. Third, a threat assessment attempts to gauge the attacker's motivation by answering the question of what utility a given attack path has for the attacker. Finally, the approach suggests mitigation actions by synthesizing similarities among vulnerabilities to provide practical recommendations for enhancing the system's cybersecurity.

G. System Theory Process Analysis for Security (STPA-Sec)

In recent work, MIT's System Theory Process Analysis (STPA) approach for safety was extended to focus on security related concerns, known as STPA-Sec [43]. The goal of this approach is to ensure mission-critical functions are maintained in the face of disruption(s). Starting from a strategic viewpoint, system developers and users can proactively shape the operational environment by controlling specified mission critical system risks. This top-down approach elevates the security problem from guarding the system (or network) against all potential attack paths to a higher-level problem of assuring the system's critical functions. The STPA-Sec steps include: identifying unacceptable losses, identifying system hazards (vulnerabilities), drawing the system functional control structure, and identifying unsafe or insecure CAs [43]. This method has been embraced by defense and commercial industries with several favorable case studies [43].

H. Functional Mission Analysis for Cyber (FMA-C)

The DoD has adopted Functional Mission Analysis for Cyber (FMA-C) as an approach to secure operational computer networks [45]. FMA-C is being taught to thousands of airmen to assure critical cyber systems and reduce vulnerabilities. While the structure and content of FMA-C are similar to STPA-Sec, its application is tailored to As-Is Information Technology infrastructures. In practice, Air Force Mission Defense Teams apply FMA-C to fielded cyber systems to identify mission-critical vulnerabilities. It has proved to be a useful tool for understanding and mitigating risks in traditional cyber (i.e., ICT) domains.

I. Other Notable Methodologies

As previously noted, other methodologies and frameworks for systems-level security analysis are sure to exist which are not covered in this work. A few notable works focused on mission assurance are available here [46], [47], [48], and on software here [49], [50].

IV. DESIRABLE CHARACTERISTICS FOR CONDUCTING CYBERSECURITY ARCHITECTURAL ANALYSIS

This section identifies desirable characteristics for cybersecurity architectural analysis and cross-examines the approaches discussed in Section III.

A. Cybersecurity Architectural Analysis Characteristics

The first characteristic is definitional and classifies approaches as either top down or bottom up. Those defined as top down start with analysis at the function level with identification and examination of critical missions and/or capabilities—sometimes operations depending on how the approach is being applied. As is typical of architecting for new systems (and sometimes upgrades), higher-level functional analysis leads to further functional decomposition and allocation to a more specific form (e.g., lower subsystems, elements, or components). These approaches lend themselves to the identification of stakeholder security needs, early trade-offs, thorough security requirements definition, and integration of more holistic security solutions [27].

Conversely, bottom-up approaches begin with the form in mind (i.e., the physical or technological solution) and often focus on perimeter security through boundary analysis [51]. While this approach successfully identifies vulnerabilities in networked components, it is often less useful for protecting systems from intelligent adversaries. For example, Bayuk and Horowitz [52] surmise that perimeter defense tactics are mostly ineffective, and conclude that a top-down, risk-based systems engineering approach to system security should be used instead.

The next key characteristic is whether the approach should be driven by threats or vulnerabilities. Prior research suggests that the foundation for improving system security starts with an analysis of potential threats, which leads to more appropriate security requirements for implementation [42]. This is intuitive; without first understanding the adversary—system-specific threats (and their rapid agility)—it is difficult, or impossible, to defend against them. Understanding and modeling the threat becomes a critical prerequisite for generating and developing secure systems [53]. Once the model has been developed and validated, vulnerability analysis is the logical follow-on. With the threats understood, the system architecture can be analyzed for vulnerable access points through techniques such as attack path analysis and/or red teaming.

While acknowledging the rapidly changing nature of threats, the exercise of red teaming and brainstorming potential attack paths is a helpful critical thinking exercise for ensuring sound cybersecurity practices. Moreover, threat modeling and vulnerability analysis typically form the foundation for cybersecurity architectural analysis. While threat modeling alone does not ensure cybersecurity, rigorous threat modeling and vulnerability analysis are helpful for ensuring the security of realized systems. However, more focus should be applied to providing security solutions and not just focused on identifying problems.

In today's highly-contested cyberspace environment, documentation-based engineering is largely ineffective against dynamic adversaries [42]. Developing a successful response to a dynamic adversary necessitates the tools and methods used to develop countermeasures be, in kind, dynamic. In response to these complexities, Model-Based Systems Engineering (MBSE) offers an integrated modeling approach capable of mapping desired capabilities to functions (and even components), as well as providing traceability and fit-for-purpose views to enable more effective decision-making [54]. In a recent effort, Apvrille and Roudier proposed SysML-Sec, an injection of security considerations into SysML to foster integration between system designers and security experts [55]. SysML-Sec and more generally MBSE approaches enable security-focused computer simulations of a potential system architecture. These executable architectures provide tremendous value by providing insights into early design trade-off analysis [56]. While MBSE requires significant initial investment in tools and training, it significantly increases the depth of possible architectural analysis, especially in executable architectures.

B. Assesment of Architectural Analysis Approaches

Table I provides a consolidated assessment (i.e., a mapping) of the proposed architectural analysis characteristics to the surveyed approaches from Section III. This mapping seeks to provide a consolidated reference for differentiating approaches to inform the user and assist in selecting an appropriate cybersecurity architectural approach which meets the stakeholders' needs. Consideration is given to each approaches' usability, scalability, and tool availability. The ideal approach will also easily facilitate modeling and simulation studies to perform early design feasibility studies and support trade-off analysis (i.e., MBSE).

In general, bottom-up approaches are relatively systematic; however, historically they have not produced secure systems and tended to scale poorly. Top-down approaches have the benefit of being more scalable, but they often require a high level of tool proficiency to effectively model (thus, the potential of MBSE to systems security is largely missed). While vulnerability analysis is inherent in every approach, a threat- based approach is less so. This aspect is crucial because effectively safeguarding unprecedented, and complex systems require more than a good architectural tool or technique – a holistic engineering approach that embraces all aspects of security (e.g., people, processes, policy, technology, feasibility, cost, etc.) is required [57], [58].

V. CONCLUSIONS AND FUTURE WORK

The practice of architectural analysis is not new; however, in the context of complex cyber-physical systems, the role of architectural analysis with respect to cybersecurity is not well understood. Moreover, given cybersecurity's widespread interest, it was surprising to find a general lack of understanding or consistency regarding what it means to conduct architectural analysis for cybersecurity while surveying the literature. Thus, this work

	Top Down	Bottom Up	Threat Driven	Vul. Based	MBSE Integrated	MBSE Executable	Tool Based
DoDAF+ Richards	X[1]			X	X	X[4]	X
CRAF	X[1]		X	X	X	X	X
UAF Security	X			X	X	X[4]	X
ACVAM		X	X	X			
STPA-Sec	X[2]			X			
RMF		X[5]	X	X	X[3]		

1. Promotes a top-down approach after mission functions are identified (i.e., does not include mission thread analysis).
2. Approach begins at a higher level than other approaches examined (i.e., includes mission thread analysis) and includes lower level analysis.
3. Suggests using MBSE, but not required and often not considered.
4. Would require pairing with additional modeling and simulation plugin.
5. RMF is intended to be a top-down approach but is often applied bottom-up using security control compliance based on system type.

Table 1: Architectural Approaches to Characteristics Mapping

briefly surveys key architectural analysis concepts and provides a timely and widely applicable working definition of "cybersecurity architectural analysis" for the community to consider. Next, a survey of several cybersecurity architectural analysis approaches from industry and government is provided, along with an assessment of their applicability for complex cyber-physical systems according to several desirable characteristics. These results help practitioners and researchers understand how to achieve more effective cybersecurity architectural analysis efforts to develop secure systems according to stakeholders needs.

While there are several promising cybersecurity architectural approaches, each with unique aspects to be more fully explored, standardized approaches such as UAF paired with MBSE hold promise and have a wider acceptance than some alternatives. In the near term, the authors have chosen to explore STPA-Sec to more fully understand its utility as

a relatively simple architectural analysis approach to assist in the development of safe, secure, and resilient military systems. Specifically, the authors are executing a detailed case study for a next-generation aircraft refueling system. This case study focuses on understanding the utility of the STPA-Sec approach for eliciting cybersecurity and resiliency requirements when developing complex military systems (i.e., unprecedented cyber-physical systems of systems). Ultimately, continued research in this field will enable more effective and efficient cybersecurity architectural analysis for complex systems regardless of the application domain.

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 United States Government.

ACKNOWLEDGMENTS

This work was supported by the U.S. Air Force, Air Force Institute of Technology, Cyberspace Center for Research, Wright-Patterson Air Force Base, Ohio, United States of America.

NOTES

1. White House, "Remarks by the President on Securing our Nation's Cyber Infrastructure," White House Press, 2009.

2. P. Singer and A. Friedman, Cybersecurity and Cyberwar, New York: Oxford, 2014.

3. Y. Liu, Y. Peng, B. Wang, S. Yao and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica,* vol. 4, no. 1, 27-40, 2017.

4. R. Saracco, "Guess What Requires 150 Million lines of Code," EIT Digital, January 13, 2016, [Online], Available: https://www.eitdigital.eu/news-events/blog/article/guess-what-requires-150-million-lines-of-code/, accessed February 2017.

5. R. Charette, "IEEE Spectrum: This Car Runs on Code," February 1, 2009. [Online]. Available: http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, accessed June 1, 2017.

6. A. Greenberg, "Wired," Wired Magazine, July 21, 2015, [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, accessed April 25, 2017.

7. E. Perez, "CNN," CNN, May 18, 2015, [Online]. Available: http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/, accessed April 25, 2017.

8. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security Symposium, 2011.

9. United States Congress, "Nation Defense Authorization Act 2016 Section 1647," November 25, 2015, [Online]. Available: https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf, accessed June 1, 2017.

10. Department Of Defense, "DoDI 8500.01 Cybersecurity," 2014.

11. Department of Defense, "DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)," 2014.

12. Department of Defense, "Defense Acquisition Guidebook Chapter 9 Program Protection," April 5, 2017, [Online]. Available: https://www.dau.mil/tools/dag/Pages/DAG-Page-Viewer.aspx?source=https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/Chapter%209%20Program%20Protection.aspx, accessed June 1, 2017.

13. Department Of Defense, "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle," October 30, 2015, [Online]. Available: https://acc.dau.mil/adl/en-US/721696/file/81323/Cybersecurity%20Guidebook%20v1.10%20signed.pdf, accessed June 1, 2017.

14. J. A. Zachman, "A Framework for Information Systems Architecture," IBM Systems Journal 26, vol. 26, no. 3, 276-292, 1987.

15. J. F. Sowa and J. A. Zachman, "Extending and Formalizing the Framework for Information Systems Architecture," *IBM Systems Journal,* vol. 31, no. 3, 590-616, 1992.

16. J. Zachman, "The Zachman Framework Evolution," April 1, 2011, [Online]. Available: https://www.zachman.com/ea-articles-reference/54-the-zachman-framework-evolution, accessed May 11, 2017.

17. A. Tang, J. Han and P. Chen, "A Comparative Analysis of Architecture Frameworks," *IEEE Computer Society: Proceedings of the 11th Asia-Pacific Software Engineering Conference,* vol. 4, no. 1530-1362, 1-8, 2004.

18. C. Paulsen, "Cybersecuring Small Businesses," *IEEE Computer,* vol. 49, no. 8, 92-97, 2016.

19. Department Of Defense, "DoDI 8500.01 Cybersecurity," 2014.

20. G. Hurlburt, "Good Enough Security: The Best We'll Ever Have," *IEEE Computer,* 98-101, 2016.

21. M. W. Maier and E. Rechtin, The Art of Systems Architecting, CRC Press, 2009.

22. ISO/IEC/IEEE 42010, "Systems and Software Engineering: Architecture Description," 2011.

23. Department of Defense, "Department of Defense Architecture Framework," 2010.

24. J. Zachman, "Wikipedia," May 5, 2010, [Online], accessed May 10, 2017.

25. R. N. Taylor, N. Medvidovic and E. Dashofy, Software architecture: foundations, theory, and practice., Wiley Publishing, 2009.

26. E. Crawley, B. Cameron and D. Selva, System Architecture, Hoboken: Pearson, 2016.

NOTES

27. R. Ross, M. McEvilley and J. Oren, "NIST Special Publication 800-160: Systems Security Engineering," National Institute of Standards and Technology, Washington DC, 2016.

28. J. E. Richards, "Using the Department of Defense Architecture Framework to Develop Security Requirements," 2014. [Online]. Available: sans.org, accessed February 2017.

29. P. Singer and A. Friedman, Cybersecurity and Cyberwar, New York: Oxford, 2014.

30. L. Ertaul and J. Hao, "Enterprise Security Planning with Department of Defense Architecture Framework (DODAF)".

31. Object Management Group, "Unified Architecture Framework Profile," OMG, 2016.

32. T. Hambrick and M. Tolbert, "Unified Architecture Framework Profile-Systems Engineering Method for Security Architectures-NMWS 17," May 21, 2017, [Online]. Available: https://nmws2017.com/agenda, accessed May 21, 2017.

33. S. Hassell, "Using DoDAF and Metrics for Evaluation of the Resilience of Systems, Systems of System, and Networks Against Cyber Threats," *INCOSE INSIGHT,* vol. 18, no. 1, 26-28, 2015.

34. P. Nejib and D. Beyer, "Secure Engineering Assurance Model," June 11, 2014, [Online]. Available: http://www.incose.org/docs/default-source/enchantment/140611beyernajib-lockeedseam.pdf?sfvrsn=2, accessed June 8, 2017.

35. "E-Government Act of 2002. Pub. L. No. 107-347, 116 Stat. 2899," December 17, 2002, [Online]. Available: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, accessed January 30, 2018].

36. R. Ross, "Managing Enterprise Security Risk with NIST Standards," *Computer,* 88-91, August 20, 2007.

37. AFLCMC/EZAS, "Aircraft Cybersecurity Risk Management Framework," May 19, 2014, [Online]. Available: http://www.mys5.org/Proceedings/2014/Day_2_S5_2014/2014-S5-Day2-12_VanNorman.pdf, accessed May 2017.

38. Air Force Institute of Technology Center for Cyberspace Research, "Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) Workshop," Air Force Research Laboratory, December 1, 2015. [Online]. Available: https://www.afit.edu/ccr/page.cfm?page=1184&tabname=Tab2, accessed May 1, 2017.

39. Air Force Research Laboratory, "Air Force Research Lab Avionics Vulnerability Assessment and Mitigation Efforts," in *Ohio Cyber Dialogue with Industry,* Dayton, 2017.

40. K. Osborn, "BattleSpace IT - Air Force: An F-16 could be vulnerable to cyber attack," Defense Systems, October 18, 2016, [Online]. Available: https://defensesystems.com/articles/2016/10/18/cyber.aspx, accessed May 2017.

41. J. Hughes and G. Cybenko, "Three tenets for secure cyber-physical system design and assessment," in *SPIE Defense+ Security,* 2014.

42. J. Cleland-Huang, T. Denning, T. Kohno, F. Shull and S. Weber, "Keeping Ahead of Our Adversaries," *IEEE Software,* vol. 33, no. 3, 24-28, 2016.

43. W. Young and N. G. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," *Communications of the ACM,* vol. 57, no. 2, 31-35, 2014.

44. Massachusetts Institute of Technology, "MIT Partnership for a Systems Approach to Safety," March 27, 2017, [Online]. Available: http://psas.scripts.mit.edu/home/stamp-workshop-2017/, accessed June 8, 2017.

45. Air Force Cyber College, "Top-down Purpose-based Cybersecurity," 2015, [Online]. Available: https://www.sans.org/summit-archives/file/summit-archive-1492176717.pdf, accessed January 1, 2018.

46. G. Hastings, L. Montella and J. Watters, "MITRE Crown Jewels Analysis," The MITRE Corporation, 2009.

47. H. G. Goldman, "Building secure, resilient architectures for cyber mission assurance," The MITRE Corporation, 2010.

48. C. Alberts and A. Dorofee, "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," 2005.

49. C. Alberts, C. Woody and A. Dorofee, "Introduction to the Security Engineering Risk Analysis (SERA) Framework," 2014.

50. Software Engineering Institute, "Security Engineering Risk Analysis (SERA)," CERT- Carnegie Mellon University, November 1, 2015, [Online]. Available: https://www.cert.org/cybersecurity-engineering/research/security-engineering-risk-analysis.cfm?, accessed May 1, 2017.

NOTES

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

52. J. Bayuk and B. Horowitz, "An Architectural Systems Engineering Methodology for Addressing Cyber Security," *Systems Engineering,* vol. 14, no. 3, 294-304, 2011.

53. A. Shostack, Threat modeling: Designing for security, John Wiley & Sons, 2014.

54. A. Ramos, J. Ferreira and J. Barceló, "Model-based systems engineering: An emerging approach for modern systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C* (Applications and Reviews), vol. 42 , no. 1, 101-111, 2012.

55. L. Apvrille and Y. Roudier, "Towards the Model-Driven Engineering of Secure yet Safe Embedded Systems," *Electronic Proceedings in Theoretical Computer Science,* vol. 148, no. 2, 15-30, 2014.

56. J. A. Estefan, "Survey of Model-Based Systems Engineering (MBSE) Methodologies," International Counsel On Systems Engineering (INCOSE), 2008.

57. J. Eloff and M. Eloff, "Information Security Architecture," *Computer Fraud and Security,* vol. 11, 10-16, 2005.

58. T. Patterson, "Holistic Security: Why Doing More Can Cost You Less and Lower Your Risk," *Computer Fraud and Security,* 13-15, 2003.