IEEE Open Journal of the Systems Engineering

Received 1 December 2023; revised 23 February 2024; accepted 8 April 2024. Date of publication 22 April 2024; date of current version 14 May 2024. *(Corresponding author: Giselle Bonilla-Ortiz.)*

Digital Object Identifier 10.1109/OJSE.2024.3391734

Systematic Mapping Study of Systems Security Engineering for Modular Open Systems

GISELLE BONILLA-ORTIZ [1], DINESH VERMA [2], JAMES N. HEAD [1], LU XIAO [2], AND KODUVAYUR SUBBALAKSHMI [2]

[1]Raytheon, Tucson, AZ 85756 USA
[2]Stevens Institute of Technology, Hoboken, NJ 07030 USA

ABSTRACT Modular Open Systems Approach (MOSA), a recent initiative to increase competition in the defense market, has become a directive to new acquisition programs. It is a United States Department of Defense (DoD) initiative for designing composable systems with open standards that can be acquired from independent vendors, while allowing an adaptive response to evolving threats. Implementation of MOSA was signed into law in the National Defense Authorization Act for Fiscal Year 2021, requiring regulations to facilitate DoD's access to and utilization of modular system interfaces and implementation of openness across major acquisition programs. MOSA's objectives include interoperability, technology refresh, increased competition, innovation, and cost savings. Determining an effective strategy to realize this intent is of paramount importance to industry. Current MOSA research focuses on developing guidelines for incorporating modularity and open standards into DoD acquisition. Given the concurrent priority regarding system security and cyber-resilience, there is a gap in open literature regarding architectural and design guidelines focused on security and cyber-resilience requirements for MOSA. This systematic mapping resulted in the selection of 33 relevant research papers. A hybrid approach of inductive and deductive qualitative coding was used as a method of rigor in extracting answers to the research questions.

INDEX TERMS Cyberattacks, interoperability, modular open systems, open architectures, risk management framework (RMF), systems security engineering.

I. INTRODUCTION

Implementation of Modular Open Systems Approach (MOSA) by the United States Department of Defense (DoD) and its contractors is now law as stated in the National Defense Authorization Act for Fiscal Year 2021 [1]. This law requires regulations and guidance to facilitate DoD's access to and utilization of modular system interfaces as well as the implementation of modular open system approaches across major defense and other relevant acquisition programs. The motivation of using MOSA is to improve interoperability, technology refresh, competition, innovation, and cost savings [2]. Because government contractors are required to follow this approach, it is necessary to establish a strategy that also incorporates system security engineering concepts and guidelines into the lifecycle of MOSA-compliant systems.

To develop secure MOSA-compliant systems, it is important that the government and contractors address the vulnerabilities and attacks that could be exacerbated by the attributes of MOSA, such as interoperability, configurability, and open standards. In this article, a systematic mapping study is presented to understand the attack vectors that could affect modular open system as well as the security functions that could be applied to mitigate these attacks. Therefore, the goal of this study is to identify from literature possible attack vectors that pose a threat to modular open systems and the security functions that could be used to mitigate these attack vectors. The main contributions of this study are as follows:

1) an understanding of the attributes that make a system modular and open;
2) the identification of attack vectors that could pose a threat to modular open systems;
3) the identification of security functions to mitigate the identified attacks.

The rest of this article is organized as follows. Section II of this article discusses the methodology used for this study,

© 2024 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

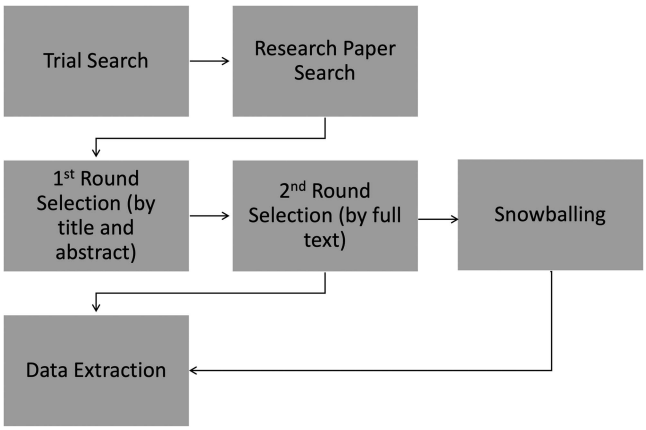


FIGURE 1. Systematic mapping process.

and Section III presents the results of the study. Section IV describes this study's threats to validity. Finally, Section V concludes this article and suggests future directions. Appendices A and B of the Supplementary Material provide the full suite of attack vector and security function data collected during the course of this study.

II. STUDY METHODOLOGY

This section describes the methodology used for this literature review and synthesis study.

A. SYSTEMATIC MAPPING PROTOCOL

The study was conducted using the systematic mapping guidelines proposed by Petersen et al. [3] and the security engineering systematic guidelines proposed by Felderer and Carver [4]. The mapping process performed was also complemented by using the systematic literature review guidelines proposed by Kitechenham [5].

B. MAPPING REVIEW PROCESS

This section describes the steps involved in the mapping review process, as illustrated in Fig. 1. The publications selected for this research synthesis were published between 2015 and 2021. The systematic mapping protocol was performed between August 2020 and March 2021. An additional update to this study was performed by repeating the protocol between August 2022 and December 2022 for papers published between 2020 and 2022. The selected papers are presented in Table 1.

D. RESEARCH PAPER SELECTION

Inclusion Criteria: The following were the inclusion criteria used in the study.

I1: Paper is peer-reviewed (including peer-reviewed conferences).
I2: Paper addresses both system modularity and security OR discusses security for a modular open system.
I3: Paper was published between 2015 and 2022.

TABLE 1. Search Strings and Selected Research Papers

Database	Search String	Title Selection	Abstract Selection	Full-Text Selection	Comments
IEEE	("modular open system" OR modularity OR modular) AND (security OR cybersecurity OR "information assurance" OR "system integrity") AND (threat OR attack OR vulnerability)	24	12	12	Searched in Journals and Conferences only
SPIE	("modular open system" OR modularity OR modular) AND (security OR cybersecurity OR "information assurance" OR "system integrity") AND (threat OR attack OR vulnerability)	14	10	8	Searched in Journals and Proceedings only
Science Direct	("modular open system" OR modularity OR modular) AND (security OR cybersecurity OR "information assurance") AND (threat OR attack OR vulnerability)	17	9	0	Only accepts eight Booleans. Publications Searched: 1) Computers and Security; 2) Future Generation Computer Systems; 3) Journal of Systems and Software; 4) Procedia Computer Science; 5) Computer Networks; 6) Renewable and Sustainable Energy Reviews; 7) Journal of Information Security and Applications; 8) Information Sciences; 9) Journal of Cleaner Production.
Scopus	("modular open system" OR modularity OR modular) AND (security OR cybersecurity OR "information assurance" OR "system integrity") AND (threat OR attack OR vulnerability)	28	20	7	Document type: article or conference paper. Looked in title, abstract, keywords
Springer Link	("modular open system" OR modularity OR modular) AND (security OR cybersecurity OR "information assurance" OR "system integrity") AND (threat OR attack OR vulnerability)	89	55	4	Searched in: Engineering Articles Computer Science Articles Engineering Conferences Computer Science Conferences.

Exclusion Criteria: The following were the exclusion criteria used in the study.

E1: Paper discusses modularity but not security.
E2: Paper discusses security for nonmodular open systems.
E3: Paper discusses security but not modularity.
E4: Paper is gray literature (i.e., technical report, nonpeer reviewed conference presentation).

E5: Paper is not written in English.

Snowballing: To guarantee that no relevant papers were missed, the snowballing process was applied, in which the references of selected papers were reviewed. Snowballing identified 18 papers, two of which were selected for this study. The papers selected proceeded to the data collection step.

E. DATA EXTRACTION AND SYNTHESIS

To effectively answer the research questions, a data collection form was established as part of the extraction process. In addition, a qualitative coding approach was used to extract data for each of the research questions. This process consisted of inductive qualitative coding where codes were created from emerging data obtained from the research papers and deductive coding, in which an existing theory or framework was used to a priori define the codes to be used as categories during the inspection of the literature. Once definition codebooks were documented for each research question, relevant text from the studies was categorized based on each code, thus providing a systematic count and categorization for each code. To analyze and synthetize the data for the research questions, a combination of descriptive statistics and frequency analysis was used. The results were graphed and tabulated.

F. GOAL AND RESEARCH QUESTIONS

The goal of this systematic research study is to identify and analyze refereed publications that address both security and modularity, with the purpose of identifying attack vectors and security functions for modular open systems. The following research questions are addressed in this study.

RQ1: What attributes of the studied systems make them both modular and open? The purpose of RQ1 is to determine the applicability of the systems presented in the selected research papers, as not all are developed under the umbrella of MOSA but may exhibit the attributes of a modular open system. To determine the attributes as presented in literature, a combination of deductive and inductive qualitative coding was used. A modular and open system attributes codebook was documented by using the definitions of open system, open system architecture, open standards, and open interfaces, as described in [6]. Codes were also added from [7], [8], [9], and [10] using an inductive process as these papers were revised as part of the study.

RQ2: What attack vectors have been presented in the literature for modular open systems? To understand the attack vector patterns presented in literature for modular open systems, the attacks were categorized according to the attack pattern domain categories established by MITRE Corporation's Common Attack Pattern Enumeration and Classification (CAPEC) [11]. These domains are as follows:

1) software;
2) hardware;
3) communications;
4) supply chain;
5) social engineering;
6) physical security.

The CAPEC domains were used as the initial codes to categorize the attacks extracted from literature. A second round of deductive coding was used to further categorize each attack with an attack pattern within its corresponding CAPEC domain.

RQ: What security functions have been proposed in literature to address attack vectors in modular open systems? The security functions collected from the selected papers were categorized using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) security control families [12]. These control families are Access Control, Awareness and Training, Audit and Accountability, Assessment, Authorization and Monitoring, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Program Management, Personnel Security, Personally Identifiable Information Processing and Transparency, Risk Assessment, System and Services Acquisition, System and Communications Protection, System and Information Integrity, and Supply Chain Risk Management. The RMF control families were used as the initial codes to categorize the security functions extracted from literature. A second round of deductive coding was used to further categorize each security function with a security control within its corresponding RMF control family.

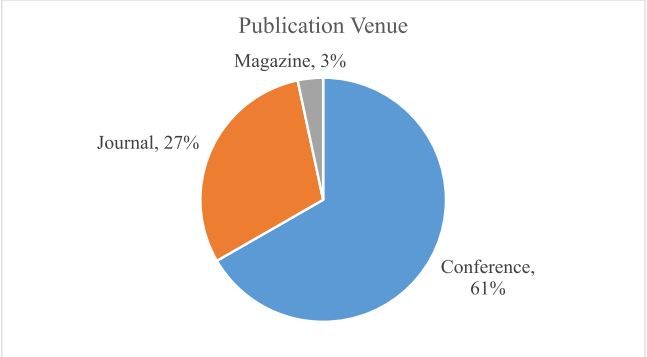


FIGURE 2. Publication venue type.

III. STUDY RESULTS

A total of 33 papers were selected through this systematic mapping study. These are presented in Table II. Most of the selected papers were published in conference proceedings, followed by journal publications and one magazine, as shown in Fig. 2. The papers selected were classified according to the categories proposed by the authors in [4] and [13]. Publications, such as literature reviews and systematic mappings, were not excluded from this study and these categories are included in the classification schema. Most papers fell under the solution proposal category, as shown in Fig. 3. Seven of the papers were classified as evaluation research and seven as validation research. These were further subcategorized as

TABLE 2. Selected Papers

Title	Database	Reference
A secure design-for-test infrastructure for lifetime security of SoCs	IEEE	[14]
Safety and security aware framework for the development of feedback control systems	IEEE	[15]
Designing safe and secure autopilots for the urban environment	IEEE	[16]
Cyber-Physical Systems Security—A Survey	IEEE	[8]
Open Platform Systems Under Scrutiny: A Cybersecurity Analysis of the Device Tree	IEEE	[17]
Cyber Security Concerns Regarding Federated, Partly IMA and Full IMA Implementations	IEEE	[18]
The Need for a Secure Modular Open Systems Approach (MOSA): Building the Case Using Systems Thinking Methodologies	IEEE	[9]
Attacks on Distributed Sequential Control in Manufacturing Automation	IEEE	[19]
A Multicycle Pipelined GCM-Based AUTOSAR Communication ASIP	IEEE	[20]
Cyber-Attacks in Modular Multilevel Converters	IEEE	[21]
Securing Robots: An Integrated Approach for	IEEE	[22]
Security Challenges and Monitoring for the Robotic Operating System (ROS)		
Security Threat Analysis and Treatment Strategy for ORAN	IEEE	[23]
Security Risk Assessment and Risk Treatment for Integrated Modular Communication	Scopus	[24]
Big Missions, Small Solutions Advances and Innovation in Architecture and Technology for Small Satellites	Scopus	[10]
Considerations and examples of a modular open systems approach in defense systems	Scopus	[7]
Security Mechanisms Used in Microservices-Based Systems: A Systematic Mapping	Scopus	[25]
Security Considerations in Modular Mobile Manipulation	Scopus	[26]
Openness and Security Thinking Characteristics for IoT Ecosystems	Scopus	[27]
Railway Defender Kill Chain to Predict and Detect Cyber-Attacks	Scopus	[28]
Mission Systems Open Architecture Science and Technology (MOAST) program	SPIE	[29]
Joint Communications Architecture for Unmanned Systems (JCAUS)	SPIE	[30]
Designing the next generation of sensor systems using the SOSA standard	SPIE	[31]
A systems approach to achieving the benefits of open and modular systems	SPIE	[32]
Chaos engineering experiments in middleware systems using targeted network degradation and automatic fault injection	SPIE	[33]
Protecting publish/subscribe interactions via TLS and a system-wide certificate validation engine	SPIE	[34]
Secure Internet of Things Architecture (SIoTA) on the battlefield	SPIE	[35]
The rise of open architectures in the U.S. Department of Defense	SPIE	[36]
Systematization and security assessment of cyber-physical systems	Springer Link	[37]
Security Challenges in Cyber-Physical Production Systems	Springer Link	[38]
Alignment of safety and security risk assessments for modular production systems	Springer Link	[39]
Enabling a Zero Trust Architecture in Smart Grids Through a Digital Twin	Springer Link	[40]
Integrated Modular Avionics — Past, present, and future	Snowballed	[41]
Towards an Architecture-Centric Approach to Security Analysis	Snowballed	[42]

* Table II Acronyms: System on Chip (SoC), Integrated Modular Avionics (IMA), Galois-Counter Mode (GCM), AUTomotive Open System Architecture (AUTOSAR), application-specific instruction set processor (ASIP), open radio access network (ORAN), Internet of Things (IoT), Sensor Open System Architecture (SOSA), Transport Layer Security (TLS)

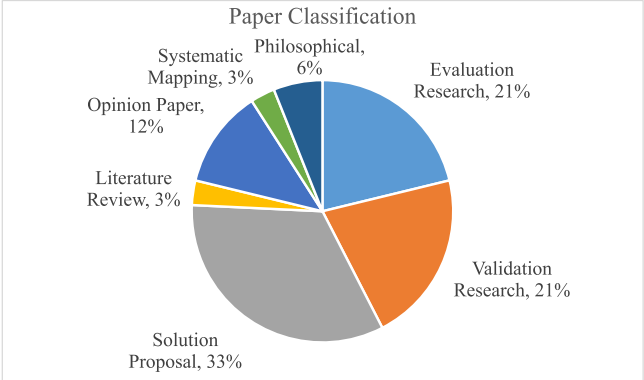


FIGURE 3. Paper classification.

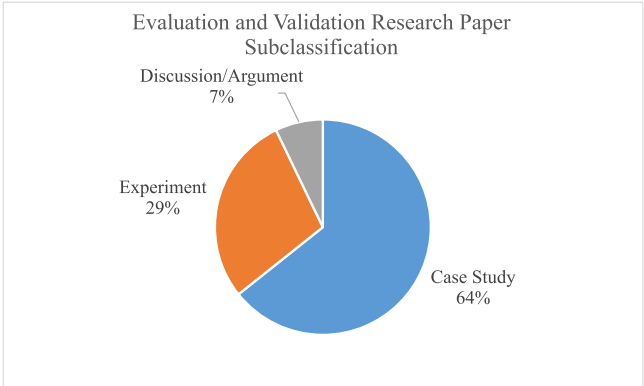


FIGURE 4. Paper subclassification.

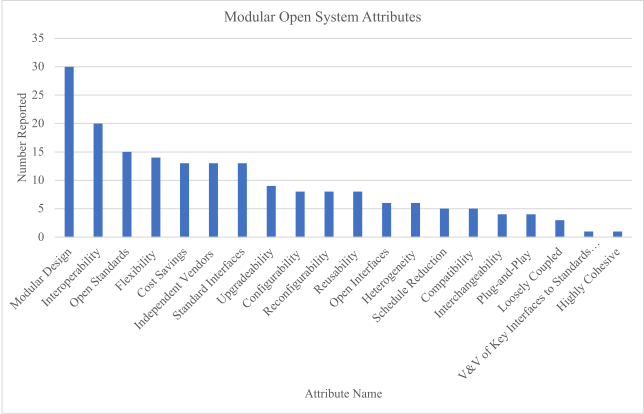


FIGURE 5. Modular system attributes.

case studies, experiments, or discussion/argument papers, as shown in Fig. 4.

A. RQ1 RESULTS: MODULAR OPEN SYSTEM ATTRIBUTES

Fig. 5 presents the modular open system attributes extracted from the selected papers. In the papers selected, modular design was reported 30 times, followed by interoperability

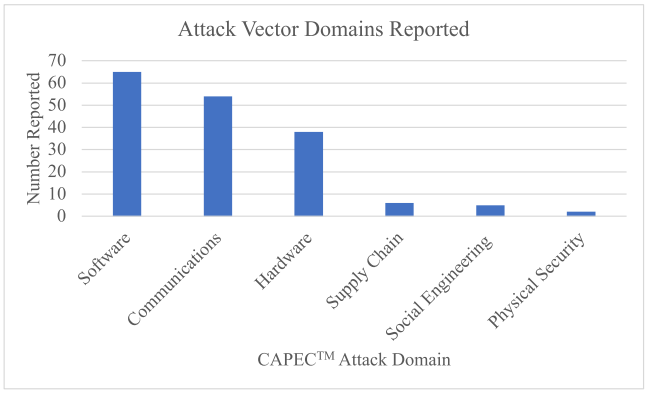


FIGURE 6. Attack vector domains reported.

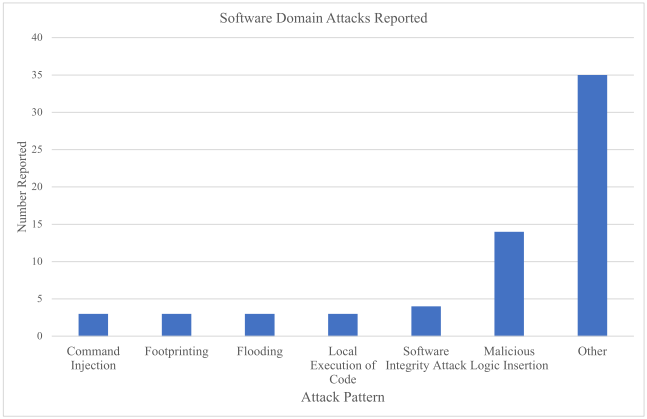


FIGURE 7. Software domain attacks.

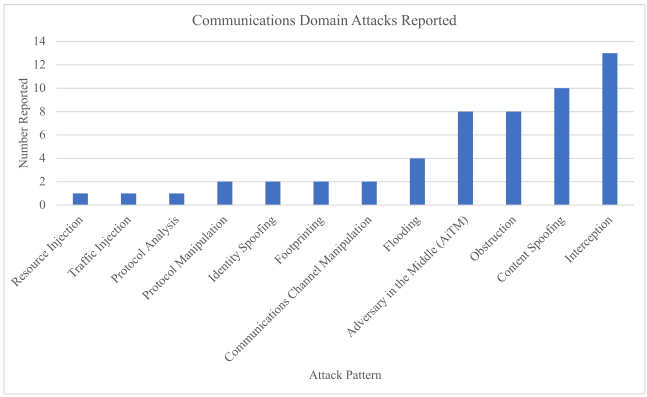


FIGURE 8. Communication domain attacks.

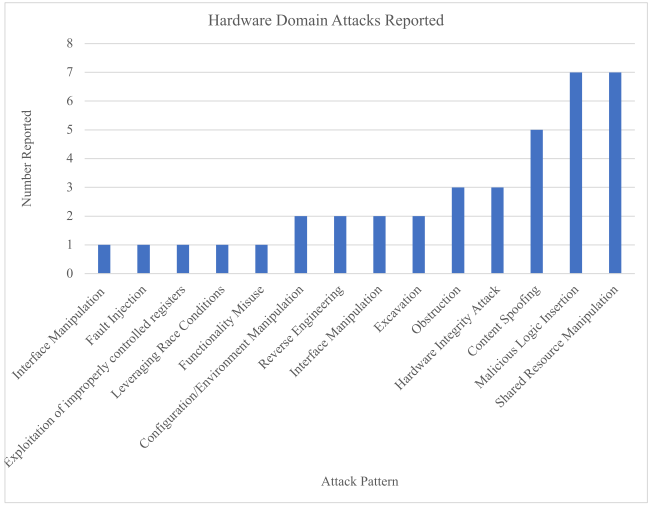


FIGURE 9. Hardware domain attacks.

(20) and open standards (15). RQ1 was utilized as validation that the selected papers pertained to systems under study that possess the characteristics of modular open systems and were appropriate to include in this SMS.

B. RQ2 RESULTS: ATTACK VECTORS

A total of 170 attack vectors were reported across all selected papers. By using qualitative deductive coding, the attack vectors were categorized according to the attack domains established by the CAPEC by the MITRE Corporation. These attack domains are as follows: Software, Hardware, Communications, Supply Chain, Social Engineering, and Physical Security. As shown in Fig. 6, 65 Software attack vectors were reported, 54 Communication attack vectors, followed by 38 Hardware attack vectors and 6 Supply Chain attack vectors.

Of the Attack domains presented, the top four were further analyzed due to being the most relevant to modular open system attacks on common software, common hardware, common communication protocols, and common supply chain interfaces. These attack vectors from the selected literature were categorized by using qualitative deductive coding.

Fig. 7 presents the decomposition of those attacks categorized under the Software domain. Malicious Logic Insertion (14) and Software Integrity (4) attacks were the most reported in the selected literature. Software domain attacks that only appeared once or twice in the literature are represented under the "Other" category. Examples of Software domain attacks in the "Other" category are: code injection, interception, reverse engineering, fuzzing, configuration/environment manipulation, and shared resource manipulation.

The attacks categorized under the Communications domain are shown in Fig. 8. Interception (13) and Content Spoofing (10) were the most reported.

Fig. 9 presents the Hardware domain attacks reported. The top two reported were Malicious Logic Insertion (7) and Shared Resource Manipulation (7).

Finally, the Supply Chain domain attacks are shown in Fig. 10. Modification During Distribution (3) and Modification During Manufacture (2) were the attacks most reported under this domain.

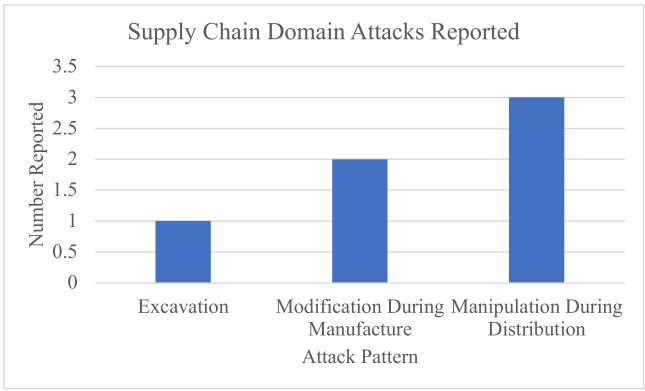


FIGURE 10. Supply Chain domain attacks.

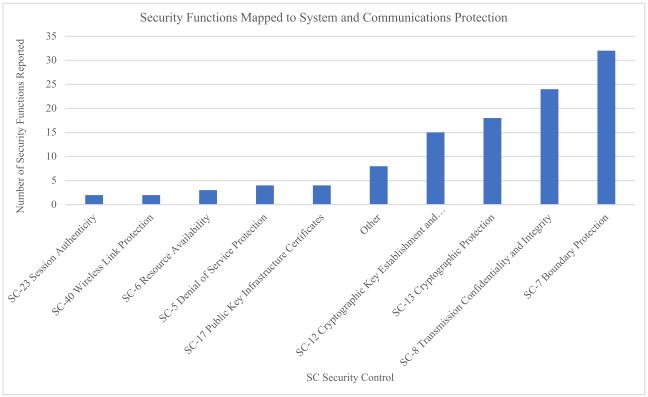


FIGURE 12. Security functions mapped to System and Communications Protection.

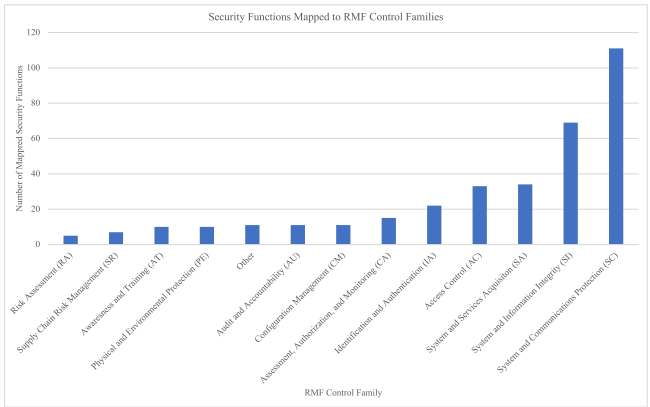


FIGURE 11. Security functions reported.

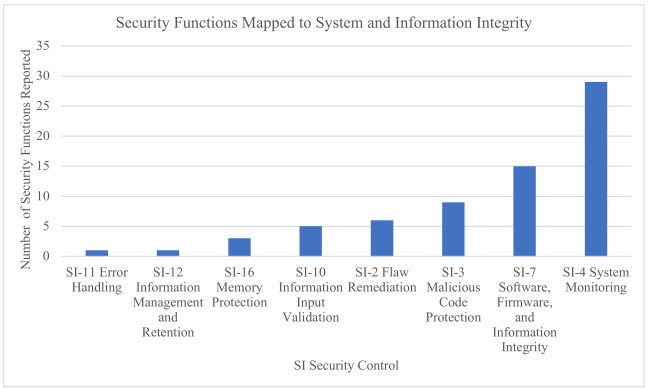


FIGURE 13. Security functions mapped to System and Information Integrity.

C. RQ3 RESULTS: SECURITY FUNCTIONS

A total of 349 security functions were reported. By using qualitative deductive coding, these security functions were categorized using the NIST RMF security control families. Fig. 11 shows the results of this categorization. The top four control families represented were System and Communication Protection (112), System and Information Integrity (69), System and Services Acquisition (34), and Access Control (33). The Personnel Security and Personally Identifiable Information Processing and Transparency control families are excluded from Fig. 11 because no security functions were mapped to those categories.

The top four control families were further analyzed, and the security functions obtained from the selected literature were further categorized. Fig. 12 presents the decomposition of the System and Communications Protection controls. Most of the security functions in this category (32) mapped to SC-7 Boundary Protection, SC-8 Transmission Confidentiality, and Integrity (24), followed by SC-13 Cryptographic Protection (13).

Fig. 13 presents the further decomposition of the System and Information Integrity controls. Most security functions fell under the category of SI-4 System Monitoring (24) followed by SI-7 Software, Hardware, and Information Integrity, followed by (15) and SI-3 Malicious Code Protection (9).

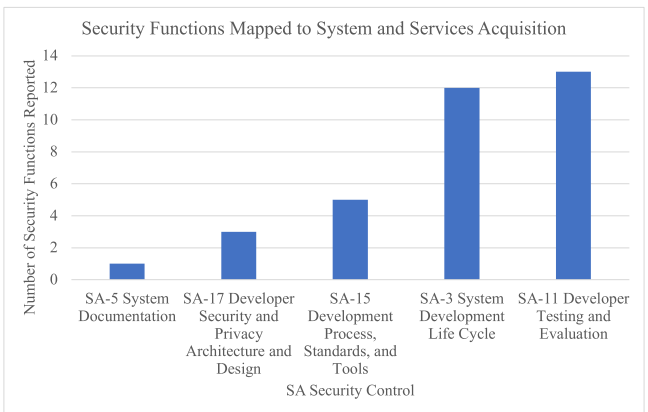


FIGURE 14. Security functions mapped to System and Services Acquisition.

Fig. 14 presents the security functions mapped into System and Services Acquisition. Most of the functions were mapped to SA-11 Developer Testing and Evaluation (13), followed by

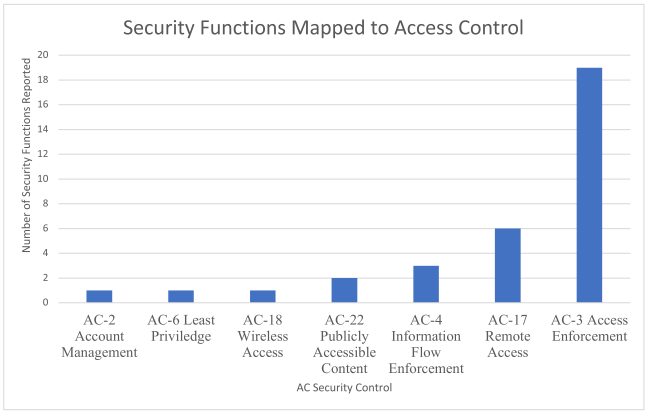


FIGURE 15. Security functions mapped to access control.

SA-3 System Development Lifecycle (12) and SA-15 Development Process, Standards, and Tools (5).

Finally, Fig. 15 below shows the breakdown for the reported security functions mapped to Access Control. Most of the functions were mapped to AC-3 Access Enforcement (19), AC-17 Remote Access (6), and AC-4 Information Flow Enforcement (3).

IV. THREATS TO VALIDITY

This section describes the threats to validity for this study and the steps taken to mitigate them. The threats to validity classification used therein are motivated by the threats to validity map performed by Zhou et al. [43].

A. CONSTRUCT VALIDITY

Construct validity refers to the selection of the appropriate measurements for the concepts studied by this research [43] and how well these concepts and their indicators have been defined [44]. In this study, threats to construct validity include the restricted timeframe of the study selection and the potential of incomplete search terms and inadequate qualitative codes definitions.

The papers used in this study were published between 2015 and 2022. This study was initially performed between August 2020 and March 2021, and to mitigate the exclusion of relevant recent research, the protocol was repeated between August 2022 and December 2022. The search terms were defined based on modular and open system concepts and tested via a trial search as shown in Fig. 1. One database in particular, Science Direct, only accepted eight Booleans, which prohibited using the exact search phrase and for repeatability, this was documented in Table I. The search performed between August and December 2022 also included the synonym terms "open architecture" and "open system architecture," which uncovered additional studies dated to early 2020, however it is possible that relevant studies in the 2015–2019 timeframe were missed.

To systematically categorize the responses to the research questions, definition codebooks were created for each of the qualitative code categories used to extract the modular open system attributes, attack vectors, and security functions from the literature. This mitigates the threat of inadequate qualitative code definitions and improves the repeatability of the study. As previously shown, literature definitions of open system architecture and modular systems definitions were used to create the modular open system code definitions. MITRE's CAPEC and RMF control families were used to define codes for the attack vectors and security functions.

B. INTERNAL VALIDITY

Internal validity refers to whether this study provides sufficient evidence to support its claims [45]. In this study, threats to internal validity include the potential bias in study selection, unsatisfactory data synthesis, and subjective interpretation of the extracted data.

Only one researcher was involved in developing the systematic mapping study protocol and then performing the study. However, detailed exclusion and inclusion criteria were defined and reviewed by the researcher's advisory committee. This helped mitigate the subjectivity of study selection. In addition, and given that not all papers were specific to modular open systems, RQ1 served as validation for the selected papers. This question pertained to assessing the modular and open system attributes of the systems under study in each of the selected papers. Snowballing was also used to capture any papers not initially discovered during the database search.

A protocol for data extraction and synthesis using qualitative coding was also defined. This mitigates any bias during these phases, as specific definition codebooks were defined for the data extracted. The interpretation of the data is presented as is from the data extraction in graph format to allow for the accurate presentation of the number of attack vectors and security functions recorded from the selected literature.

C. EXTERNAL VALIDITY

External validity refers to how well the results of this study can be generalized [45]. This threat can particularly affect the generalizability of the results to systems that are compliant with DoD's MOSA requirements and DoD open architecture systems because not all the papers selected are specific to MOSA open standards. However, this threat is mitigated by the results obtained from RQ1 assessment of modular open attributes of the systems under study. That being said, the results can also be generalized to a multitude of systems, such as cyber physical systems, SCADA, and Internet of Things.

D. CONCLUSION VALIDITY

Conclusion validity refers to the degree to which conclusions reached in this study are reasonable given the data collected [45]. In addition, it deals with how the protocol of this study can be repeated to obtain the same results [43]. Threats to conclusion validity include the misclassification of the papers selected for the study, researcher bias in data extraction, and the potential of subjective interpretation of the data extracted.

To mitigate paper misclassification, specific definitions were leveraged from [4] and [13]. Inductive qualitative coding and deductive qualitative coding were used to lessen the risk of data extraction bias. Each paper was read and relevant text for modular open system attributes, attack vectors, and security functions were categorized according to the definition codebooks for each of the research questions. Again, only one researcher developed the protocol and conducted the study and may affect the subjectivity of the study's conclusion.

V. CONCLUSION

The primary findings of this study are discussed in this section.

A. MODULAR OPEN SYSTEM ATTRIBUTES

The modular open system attributes reported the most in the selected studies were modular design, interoperability, and open standards. Notably, the attributes of flexibility, acquisition from independent vendors, and standard interfaces were also frequently mentioned. The security analysis on these systems under study applies to modular open systems given the attributes described and allows for the researcher to extrapolate attack vectors that potentially threaten modular open systems. In addition, it can be argued that the security functions identified through this study will have applicability in protecting modular open systems from these attack vectors.

B. ATTACK VECTORS

As shown earlier, the attack vectors presented in the selected papers were categorized according to the CAPEC attack domains. Most of the attacks fell under the Software domain, and were further categorized mostly as Malicious Logic Insertion, such as malware, that would aim to steal private information [8], execute denial of service attacks to affect system availability [16] and attack from other modules in the system [24], [25]. Some Software domain attacks were further categorized as Software Integrity attacks, notably attack vectors that exploit system updates, software uploads, and reprogramming, whether by unwitting or malicious users [8], [10], [22], [26].

Communications domain followed Software in number of attacks reported. Most of these were further categorized as interception and content spoofing. Examples of interception attacks found in the literature were eavesdropping on private data or credentials [8], [19], [35], interception of transmitted information [18], and monitoring sensor data [38]. Examples of content spoofing are radar data spoofing [16], spoofing attacks on address resolution protocol in SCADA systems [8], GPS/global navigation satellite systems (GNSS) navigation data spoofing [18], and speedometer data spoofing [20].

A number of Hardware domain and supply chain domain attacks were also recorded. Hardware domain attacks were mostly categorized as Malicious Logic Insertion and Shared Resource Manipulation. Examples are attacks, such as hardware trojans [14], [16], [37], data manipulation in memory [16] and infected memory [8], extraction attacks from direct memory access, peripheral address manipulation [17], and power system disruption [18]. Manipulation During Manufacture and Manipulation During Distribution were notable attack vectors within the Supply Chain domain. Examples include malicious microcontrollers in which a supplier inserts a hardware trojan [14] and infected counterfeit parts [9], [18], [26].

C. SECURITY FUNCTIONS

It may not come as a surprise that most of the security functions reported in the selected papers could be categorized under the RMF system and communications protection control family. One particularly important attribute of modular open systems is the adherence to open interface standards by the modules composing the system. SC-7 Boundary Protection, SC-8 Transmission Confidentiality and Integrity, and SC-13 Cryptographic Protection were the top three controls extracted in this family. Protecting information being transmitted across the standard open interfaces, with or without cryptographic protection, is an important mechanism discussed in literature [8], [18], [20], [23], [24], [26], [28], [30], [35]. Understanding the boundaries of the modular open system (such as trusted/untrusted modules [29], critical and noncritical module boundaries [8], and multilevel security [8], [30], [31]) enables the selection of the correct security mechanisms to protect data being transmitted across those boundaries and maintaining the integrity of modules within a trusted boundary.

The top three controls in this family were SI-4 System Monitoring, SI-7 Software, Firmware and Information Integrity and SI-3 Malicious Code Protection. Mechanisms presented in the research papers, such as securely booting the system [17], [35], [41], monitoring the system environment for intrusion [8], [24], [28], [31], cryptographically securing data and verifying their integrity [8], [31], [37], verifying software integrity [28], [31], and protecting against malicious code and malicious software updates [24], [26] fall into these three categories. These security functions complement the SC-7, SC-8, and SC-13 security functions because they establish the known integrity state of the system and monitor that this state is not compromised during the operational lifecycle of the system by malicious software or other attacks.

SA-11 Developer Testing and Evaluation and SA-3 System Development Lifecycle were the top two control categories extracted for this family. SA-11 covers functions from literature, such as risk management [27], security assessments and testing [8], [18], fuzzing [22], [42], and penetration testing and static code analysis [42]. Security functions that fall under SA-3 are secure integration of components into the system [8], rapid upgrades [7], [10], technology refresh (of security modules or compromised non-security modules) [7], [30], and securing the design and manufacturing lifecycle process of a system [8], [18].

Notably, security functions that mapped to AC-3 Access Enforcement were the most reported under the Access Control family. Some examples are access management for commissioning, maintenance, and reprogramming [26], access

controls for smart grids and industrial control systems [8], access control on cyber-physical production systems [38], and role-based access control on railway systems [28].

In conclusion, a systematic literature mapping study was conducted to identify attack vectors and security functions for modular open systems. In total, 33 research papers were selected after an extensive search in several databases. Inductive qualitative coding and deductive qualitative coding were used to categorize the attack vectors and security functions. Several results and analyses were discussed. Mainly, the attack vectors were categorized, and this showed that most fell under the Software, Communications, and Hardware CAPEC attack domains. The attacks were further categorized as attack patterns within the top domains. Security functions were also extracted from the literature, and these were categorized using the RMF control families, concluding that most security functions were of the System and Communications Protection, System and Information Integrity and System and Services Acquisition, and Access Control families. Furthermore, the top controls for each family were also discussed and analyzed.

VI. FUTURE WORK

This systematic study was the first step in setting the problem space for understanding attack vectors relevant to modular open systems to then identify the potential mitigations to these attacks. The study synthesized the key findings of 33 selected research papers. There are several questions left unanswered, however. Further analysis should be conducted on mapping the identified attack vectors to the identified security functions with the purpose of pinpointing attack vectors that require further mitigation. Furthermore, if an attack was not identified in this study, it does not necessarily indicate that modular open systems are not susceptible to it. Given the proprietary nature of cyber incidents in both industry and defense, such reports may not be currently available to the public and additional research may be needed. Correlation between real-world cybersecurity incident data specific to systems that have modular and open system characteristics with the attacks identified in this study are also future research avenues that may provide more technical insight of MOSA attack vectors and vulnerabilities.

Of the attacks identified in this study, one challenge is determining the trusted and untrusted boundaries given different supplier security provenances. Based on these challenges, MOSA has the potential to exacerbate supply chain risk and exploring how to mitigate these risks has the potential to highly impact research in this area.

Maintaining the integrity of the system during operation is also critical and was identified as a needed security function in literature. For example, malicious software and hardware logic insertion both during the operation of a system and due to supply chain domain attack vectors, such as manipulation during manufacture or distribution, are top concerns reported in the studies. Because of this, thought needs to be given to other aspects of a system lifecycle as well. For example, establishing a secure framework for hardware and/or software updates in the MOSA construct is important because there is the possibility that module updates introduce lower security postures into a system and can later affect the system's operational phase. Requirements for compliant standard open interfaces are necessary for MOSA to work, however simply because a module is designed with compliant interfaces does not guarantee a synergy of operation once installed in a system. Future work and research on applying a secure framework, such as zero trust as applied to smart grids [40] and to embedded and cyber-physical systems [46], [47], to MOSA cybersecurity has the potential of addressing these security concerns and attack vectors.

REFERENCES

[1] A. Smith, "Text - H.R.6395 - 116th Congress (2019-2020): National defense authorization act for fiscal year 2021," Accessed: May 04, 2021. [Online]. Available: https://www.congress.gov/bill/116th-congress/house-bill/6395/text

[2] P. Zimmerman, "Modularity and open systems: Meaningful distinctions," in *Proc. 18th Annu. NDIA Syst. Eng. Conf.*, 2015.

[3] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015, doi: 10.1016/j.infsof.2015.03.007.

[4] M. Felderer and J. C. Carver, "Guidelines for systematic mapping studies in security engineering," Jan. 2018, Accessed: Jul. 30, 2020. [Online]. Available: http://arxiv.org/abs/1801.06810

[5] B. Kitechenham, "Guidelines for performing systematic literature reviews in software engineering version 2.3," School Comput. Sci. Math., Keele Univ. Dept. Comput. Sci., Univ. Durham, Tech. Rep. EBSE-2007-01, Jul. 2007.

[6] Department of Defense Data Rights Team, "Open System Architecture (OSA) Contract Guidebook for Program Managers v.1.1," Accessed: May 18, 2021. [Online]. Available: https://www.acqnotes.com/Attachments/Open%20System%20Architecture%20(OSA)%20Contract%20Guidebook%20for%20Program%20Managers%20June%2013.pdf?_ga=2.145612658.793279734.1621366196-671456943.1538360305</bib>

[7] P. Zimmerman, M. Ofori, D. Barrett, J. Soler, and A. Harriman, "Considerations and examples of a modular open systems approach in defense systems," *J. Defense Model. Simul.*, vol. 16, no. 4, pp. 373–388, Apr. 2018, doi: 10.1177/1548512917751281.

[8] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[9] G. Bonilla-Ortiz and D. Verma, "The need for a secure modular open systems approach (MOSA): Building the case using systems thinking methodologies," in *Proc. IEEE Syst. Secur. Symp.*, 2020, pp. 1–4, doi: 10.1109/SSS47320.2020.9197726.

[10] R. B. Friend, C. Arroyo, and J. Hansen, "Big missions, small solutions advances and innovation in architecture and technology for small satellites," in *Proc. AIAA SPACE Forum, Amer. Inst. Aeronaut. Astronaut.*, 2016, pp. 1–3, doi: 10.2514/6.2016-5229.

[11] "CAPEC - Common attack pattern enumeration and classification (CAPECTM)," Accessed: May 04, 2021. [Online]. Available: https://capec.mitre.org/</bib>

[12] Joint Task Force Interagency Working *Group*, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, MD, USA, Sep. 2020, doi: 10.6028/NIST.SP.800-53r5.

[13] A. Souag, R. Mazo, C. Salinesi, and I. Comyn-Wattiau, "Reusable knowledge in security requirements engineering: A systematic mapping study," *Requirements Eng.*, vol. 21, no. 2, pp. 251–283, Jun. 2016, doi: 10.1007/s00766-015-0220-8.

[14] J. Backer, S. S. Ali, K. Rosenfeld, D. Hély, O. Sinanoglu, and R. Karri, "A secure design-for-test infrastructure for lifetime security of SoCs," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2015, pp. 37–40, doi: 10.1109/ISCAS.2015.7168564.

[15] J. P. Lobo, P. Charchalakis, and E. Stipidis, "Safety and security aware framework for the development of feedback control systems," in *Proc. 10th IET System Saf. Cyber-Secur. Conf.*, 2015, pp. 1–5, doi: 10.1049/cp.2015.0280.
[16] S. Norton and H. I. Akram, "Designing safe and secure autopilots for the urban environment," in *Proc. Int. Conf. System Saf. Cyber-Secur.*, 2016, pp. 1–6, doi: 10.1049/cp.2016.0849.
[17] D. Tychalas and M. Maniatakos, "Open platform systems under scrutiny: A cybersecurity analysis of the device tree," in *Proc. IEEE 25th Int. Conf. Electron., Circuits Syst.*, 2018, pp. 477–480, doi: 10.1109/ICECS.2018.8618042.
[18] A. Uncu, S. Üzümcü, and A. A. Mert, "Cyber security concerns regarding federated, Partly IMA and full IMA implementations," in *Proc. IEEE/AIAA 38th Digit. Avionics Syst. Conf.*, 2019, pp. 1–5, doi: 10.1109/DASC43569.2019.9081614.
[19] Z. Jakovljevic, V. Lesi, and M. Pajic, "Attacks on distributed sequential control in manufacturing automation," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 775–786, Feb. 2021, doi: 10.1109/TII.2020.2987629.
[20] A. Hamed, M. W. El-Kharashi, A. Salem, and M. Safar, "A multicycle pipelined GCM-based AUTOSAR Communication ASIP," *IEEE Access*, vol. 10, pp. 46312–46329, 2022, doi: 10.1109/ACCESS.2022.3171051.
[21] C. Burgos-Mellado et al., "Cyber-Attacks in modular multilevel converters," *IEEE Trans. Power Electron.*, vol. 37, no. 7, pp. 8488–8501, Jul. 2022, doi: 10.1109/TPEL.2022.3147466.
[22] S. Rivera and R. State, "Securing robots: An integrated approach for security challenges and monitoring for the robotic operating system (ROS)," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage.*, 2021, pp. 754–759.
[23] C. T. Shen et al., "Security threat analysis and treatment strategy for ORAN," in *Proc. IEEE 24th Int. Conf. Adv. Commun. Technol.*, 2022, pp. 417–422, doi: 10.23919/ICACT53585.2022.9728862.
[24] H. Asgari, S. Haines, and A. Waller, "Security risk assessment and risk treatment for integrated modular communication," in *Proc. 11th Int. Conf. Availability, Rel. Secur.*, 2016, pp. 503–509, doi: 10.1109/ARES.2016.6.
[25] A. Pereira-Vale, G. Márquez, H. Astudillo, and E. B. Fernandez, "Security mechanisms used in microservices-based systems: A systematic mapping," in *Proc. XLV Latin Amer. Comput. Conf.*, 2019, pp. 01–10, doi: 10.1109/CLEI47609.2019.235060.
[26] B. Dieber and B. Breiling, "Security considerations in modular mobile manipulation," in *Proc. IEEE 3rd Int. Conf. Robotic Comput.*, 2019, pp. 70–77, doi: 10.1109/IRC.2019.00019.
[27] B. Vogel, M. Kajtazi, J. Bugeja, and R. Varshney, "Openness and security thinking characteristics for IoT Ecosystems," *Information*, vol. 11, no. 12, Dec. 2020, Art. no. 564, doi: 10.3390/info11120564.
[28] R. Kour, A. Thaduri, and R. Karim, "Railway defender kill chain to predict and detect cyber-attacks," *J. Cyber Secur. Mobility*, vol. 9, pp. 47–90, Jan. 2020, doi: 10.13052/jcsm2245-1439.912.
[29] K. Littlejohn, V. Rajabian-Schwart, N. Kovach, and C. P. Satterthwaite, "Mission systems open architecture science and technology (MOAST) program," in *Proc. SPIE, Int. Soc. Opt. Photon.*, 2017, Art. no. 1020504, doi: 10.1117/12.2265843.
[30] S. M. Reese and W. Y. Chang, "Joint communications architecture for unmanned systems (JCAUS)," in *Proc. SPIE, Int. Soc.Opt. Photon.*, 2017, Art. no. 101950P, doi: 10.1117/12.2264478.
[31] G. C. Sargent, C. Collier, and I. Lipkin, "Designing the next generation of sensor systems using the SOSA standard," in *Proc. SPIE Int. Soc. Opt. Photon.*, 2019, Art. no. 110150I, doi: 10.1117/12.2520077.
[32] G. Pearson, R. Smith, H. Tripp, and O. Worthington, "A systems approach to achieving the benefits of open and modular systems," in *Proc. SPIE Int. Soc. Opt. Photon.*, 2015, Art. no. 94790A, doi: 10.1117/12.2176564.
[33] A. Pierce, J. Schanck, A. Groeger, R. Salih, and M. R. Clark, "Chaos engineering experiments in middleware systems using targeted network degradation and automatic fault injection," in *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2021*, R. Suresh, Ed., Bellingham, WA, USA: SPIE, pp. 24–36, Apr. 2021, doi: 10.1117/12.2584986.
[34] A. Pierce, A. Alten, and M. Clark, "Protecting publish/subscribe interactions via TLS and a system-wide certificate validation engine," in *Unmanned Systems Technology XXII*, C. M. Shoemaker, P. L. Muench, and H. G. Nguyen, Eds., Bellingham, WA, USA: SPIE, pp. 108–114, Apr. 2020, doi: 10.1117/12.2555930.
[35] J. Williams et al., "Secure Internet of Things architecture (SIoTA) on the battlefield," in *Disruptive Technologies in Information Sciences VI*, M. Blowers, R. D. Hall, and V. R. Dasari, Eds., Orlando, FL, USA: SPIE, pp. 122–127, May 2022, doi: 10.1117/12.2622823.
[36] N. Kovach, B. Natarian, and K. Littlejohn, "The rise of open architectures in the U.S. Department of Defense," in *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2021*, R. Suresh, Ed., Bellingham, WA, USA: SPIE, pp. 12–23, Apr. 2021, doi: 10.1117/12.2589701.
[37] D. P. Zegzhda, M. A. Poltavtseva, and D. S. Lavrova, "Systematization and security assessment of cyber-physical systems," *Aut. Control Comp. Sci.*, vol. 51, no. 8, pp. 835–843, Dec. 2017, doi: 10.3103/S0146411617080272.
[38] P. Kieseberg and E. Weippl, "Security challenges in cyber-physical production systems," in *Software Quality: Methods and Tools for Better Software and Systems*. Cham, Switzerland: Springer, Jan. 2018, pp. 3–16, doi: 10.1007/978-3-319-71440-0_1.
[39] M. Ehrlich et al., "Alignment of safety and security risk assessments for modular production systems," *Elektrotech. Inftech.*, vol. 138, no. 7, pp. 454–461, Nov. 2021, doi: 10.1007/s00502-021-00927-9.
[40] G. P. Sellitto, H. Aranha, M. Masi, and T. Pavleska, "Enabling a zero trust architecture in smart grids through a digital twin," in *Proc. Dependable Comput. - EDCC Workshops*, 2021, vol. 1462, pp. 73–81, doi: 10.1007/978-3-030-86507-8_7.
[41] T. Gaska, C. Watkin, and Y. Chen, "Integrated modular avionics - past, present, and future," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 30, no. 9, pp. 12–23, Sep. 2015, doi: 10.1109/MAES.2015.150014.
[42] Q. Feng, R. Kazman, Y. Cai, R. Mo, and L. Xiao, "Towards an architecture-centric approach to security analysis," in *Proc. 13th Work. IEEE/IFIP Conf. Softw. Archit.*, 2016, pp. 221–230, doi: 10.1109/WICSA.2016.41.
[43] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, "A map of threats to validity of systematic literature reviews in software engineering," in *Proc. 23rd Asia-Pacific Softw. Eng. Conf.*, 2016, pp. 153–160, doi: 10.1109/APSEC.2016.031.
[44] D. I. K. Sjøberg and G. R. Bergersen, "Construct validity in software engineering," *IEEE Trans. Softw. Eng.*, vol. 49, no. 3, pp. 1374–1396, Mar. 2023, doi: 10.1109/TSE.2022.3176725.
[45] A. Ampatzoglou, S. Bibi, P. Avgeriou, M. Verbeek, and A. Chatzigeorgiou, "Identifying, categorizing and mitigating threats to validity in software engineering secondary studies," *Inf. Softw. Technol.*, vol. 106, pp. 201–230, Feb. 2019, doi: 10.1016/j.infsof.2018.10.006.
[46] M. Vai et al., "Security-as-a-service for embedded systems," in *Proc. IEEE Mil. Commun. Conf.*, 2023, pp. 691–695, doi: 10.1109/MILCOM58377.2023.10356297.
[47] S. Hasan, I. Amundson, and D. Hardin, "Zero trust architecture patterns for cyber-physical systems," in *Proc. AeroTech*, 2023, Art. no. 2023–2001–1001, doi: 10.4271/2023-01-1001.

GISELLE BONILLA-ORTIZ received the B.S. degree in computer engineering from the University of Puerto Rico, Mayagüez, Puerto Rico, in 2007, and the M.S. degree in systems engineering from Johns Hopkins University, Baltimore, MD, USA, in 2011. She is currently working toward the Ph.D. degree in systems engineering with the Stevens Institute of Technology, Hoboken, NJ, USA.

She is currently a Senior Principal Systems Engineer who specializes in systems security with Raytheon, an RTX Business, Tucson, AZ, USA. She has more than 16 years of experience in software and systems engineering, cryptographic key management applications, and secure processing solutions architecture.

Ms. Bonilla-Ortiz is a Systems Engineering Research Center Doctoral Fellow.

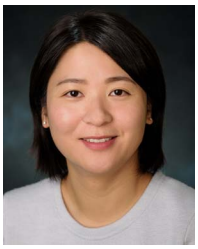
DINESH VERMA received the M.S. and Ph.D. degrees in industrial and systems engineering from Virginia Tech, Blacksburg, VA, USA, in 1991 and 1994, respectively, the Honorary Master of Engineering degree (Honoris Causa) in engineering from the Stevens Institute of Technology, Hoboken, NJ, USA, in 2008, and the Honorary Doctorate degree (Honoris Causa) in engineering from Linnaeus University, Vaxjo, Sweden, in 2007.

During 2007–2016, he was the Founding Dean with the School of Systems and Enterprises, Stevens Institute of Technology. He is currently the Executive Director of the Systems Engineering Research Center, the U.S. Department of Defense sponsored University Affiliated Research Centerfocused on systems engineering research, along with the Acquisition Innovation Research Center. During his 20 years with Stevens, he has successfully proposed research and academic programs exceeding $200M in value.

JAMES N. HEAD received the B.S. degree in astronomy and physics/mathematics from Texas Christian University, Fort Worth, TX, USA, in 1990, and the Ph.D. degree in planetary sciences from the University of Arizona, Tucson, AZ, USA, in 1999.

He is an Engineering Fellow with Raytheon, an RTX Business, Tucson. He has 24 years' experience as a theoretical physicist, inventing and developing new technologies in missile guidance, navigation, and fusing systems and robotic spacecraft. He develops new capabilities in space environment modeling with multiple patents, trade secrets, and publications to his credit. He is a TOGAF and Raytheon Certified Architect, where he spearheaded adoption of modular open systems in Raytheon's missile division.

Dr. Head was an AAAS Science and Technology Policy Fellow in the U.S. State Department, where he helped develop the nation's system of systems space weather observation requirements.



LU XIAO received the Ph.D. degree in computer science from Drexel University, Philadelphia, PA, USA, in 2016.

She is currently an Assistant Professor with the School of Systems and Enterprises, Stevens Institute of Technology, Hoboken, NJ, USA. Her research interests include software architecture, software evolution and maintenance. In particular, she is interested in modeling and analyzing software architecture and its evolution for addressing quality problems, such as maintenance quality and performance.

KODUVAYUR (SUBA) SUBBALAKSHMI received the B.Sc degree in physics from University of Madras, in 1990, the M.Eng degree in electrical communication engineering from Indian Institute of Science, in 1994, and the Ph.D degree in engineering science from Simon Fraser University, in 2000. She is a Professor with the Department of ECE, Stevens Institute of Technology, Hoboken, NJ, USA. Her current research interests include artificial intelligence and machine learning with an emphasis on explainable AI, mental health, cyber safety/security, and cognitive radio networking.

Dr. Subbalakshmi was Associate Editor for several journals. She is currently an Associate Editor for IEEE TRANSACTIONS ON ARTIFICIAL INTELLIGENCE and IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS. She was a Founding Associate Editor of IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. She is the Founding Chair of the Special Interest Group on Security, IEEE COMSOC's Technical Committee on Cognitive Networks. She is a Fellow of the National Academy of Inventors, a Jefferson Science Fellow, and a Member of the National Academy of Science Engineering and Medicines' Intelligence Science and Technology Experts Group. She was the recipient of the New Jersey Inventors Hall of Fame, Innovator Award. Her research is supported by NSF, NIJ, AFRL, US ISSO, CCDC, and other DoD agencies as well as industry.