Cybersecurity and Innovative Technology Journal, Vol.4, No.1, 2026, pp. 63-78
e-ISSN 3025-6682. DOI. 10.52889/citj.v4i1.854

A Comparison of UAF and SysML-Based DODAF Implementations for Cybersecurity Architecture Modeling

Submitted 22 February 2026, Revised 20 March 2026, Accepted 29 March 2026

Christopher Green[1,2*]

[1]Department of System Engineering, Capitol Technology University, Laurel, MD., United States

[2]System Assurance Institute, Greentec EHS, Fredericksburg, VA., United States
Corresponding Email: *cgreen@captechu.edu

Abstract

IoT systems with constrained resources are moving towards energy harvesting to ensure sustainable and autonomous operations in resource-limited environments. Yet, incorporating energy harvesting in such a system involves intricate dependencies between energy production, energy storage capabilities, system operation, security controls, and availability considerations at a mission level. Current practices focus on analyzing the mentioned dependencies for individual components/subsystems without accounting for potential cross-domain effects, thus leaving open room for potential errors in system-level integration. In this paper, we propose an architecture-driven approach for integrating energy harvesting based on the Unified Architecture Framework (UAF). Energy availability is considered from the perspective of a system-level architectural constraint within a framework based on a meta-model, instead of being just a design consideration. Capabilities, operations, resources, security, and standards-related concepts are materialized within a common semantic baseline to enable cross-domain traceability of the dependencies between energy, security, and missions. Variability in the energy produced by the energy harvesters propagates through operations, communications, and security controls up to capabilities realization and availability. This technique takes advantage of the relationships between domains provided by the UAF Domain MetaModel to achieve structured dependency propagation and systematic trade-space analysis between domains. It is clear from the findings that integrating energy and cybersecurity elements into a single architectural framework helps minimize fragmentation in integration, enhances system-level reasoning, and facilitates energy-conscious co-design of operations and security functions.

Keywords: Model-Based Systems Engineering (MBSE), Unified Architecture Framework (UAF), Internet of Things (IoT), Energy Harvesting

INTRODUCTION

Defense systems and critical infrastructures today exist as SoS systems. Characteristics of distributed control and tightly coupled interaction define such an environment. Interconnectivity becomes more extensive in this environment, providing opportunities for cybersecurity threats to propagate in operational, systems, and enterprise domains. Under these circumstances, security risks do not stay confined within their own domain; rather, they propagate and affect other systems, thereby impairing the effectiveness of the missions. This is why cybersecurity needs to be approached from an architectural perspective (Maier, 1998; Boardman & Sauser, 2008; Martin & Brookshier, 2023).

Does your company use DODAF for describing its systems? This framework is used by many companies with the same mindset towards describing their products instead of using them for analysis purposes. Although these artifacts provide detailed information about components and interfaces, do they help you analyze the dependencies in terms of cybersecurity across different domains?

To overcome these weaknesses, the transition towards Model Based Systems Engineering (MBSE), supported by the Department of Defense Digital Engineering Strategy, places the emphasis on model-based approaches rather than documentation-based approaches (INCOSE, 2007; DoD, 2018). In a model-based approach, the architecture can be used as the source of truth for the entire system. This allows engineers to express the relationship, dependency, and behavior of the system within the model itself. This is especially critical when considering cybersecurity because analyzing such systems requires consistent and repeatable threat, vulnerability, and control traceability among different domains (DoD, 2010; Mažeika, 2021).

Based on the improvements achieved by MBSE, the Unified Architecture Framework (UAF) takes the modeling approach one step further by providing a Domain Meta-Model where strategic, operational, service, resource, and security domains can be considered together under one semantics umbrella. Instead of considering architectures from different viewpoints separately, UAF considers relationships among architectural artifacts within the model itself. The relationship within this model makes it possible for cybersecurity to become a part of the architecture, making it easier for engineers to model the security artifact along with other system and mission artifacts (OMG, 2021; Hause, 2019).

However, despite all these advancements, there still exists a lacuna in the field of research because very few researchers have looked at how the architecture of the frameworks themselves impacts the modeling of cybersecurity issues. The main emphasis is usually on using the tools or designing diagrams, but not on looking at the semantics involved and how they impact cybersecurity analysis, especially within SoS (Brooks & Hause, 2022; Eichmann et al., 2019).

The engineer should be aware of the structural distinctions between DODAF and UAF, which would enable him/her to comprehend how the frameworks support modeling for cybersecurity within the SoS environment. The difference in the organization of architectural data affects the way security information is represented within the system of interest in both approaches (INCOSE, 2007; DoD, 2018).

DODAF: A Viewpoint-Centric Framework

DODAF was developed by the Department of Defense for establishing standards in defense architectures, which can be accomplished through three viewpoints—Operational Viewpoints (OV), System Viewpoints (SV), and Capability Viewpoints (CV)—as shown in Figure 1 below. Each viewpoint corresponds to a stakeholder issue. Engineers may rely on SysML to design the viewpoints, making it more systematic compared to conventional

documentation techniques. Unlike other architectures, there is no overlapping between different viewpoints within DODAF.

This structure based on viewpoints presents challenges to the integration of cybersecurity assessments (Mažeika, 2021). While most methods have a meta-model for ensuring coherence between views, DODAF lacks such a tool. Therefore, engineers need to ensure traceability manually or through external mechanisms (DoD, 2010). Figure 2.1 shows the various DODAF views.

From the cybersecurity perspective, this poses a challenge. In order to link a specific weakness to its possible mission impact, engineers would need to manually synthesize information from various architectural artifacts. The framework offers a framework for documenting the system; however, it differs from holistic methods in the sense that it does not impose the connections necessary for cybersecurity analysis (Mažeika, 2021).

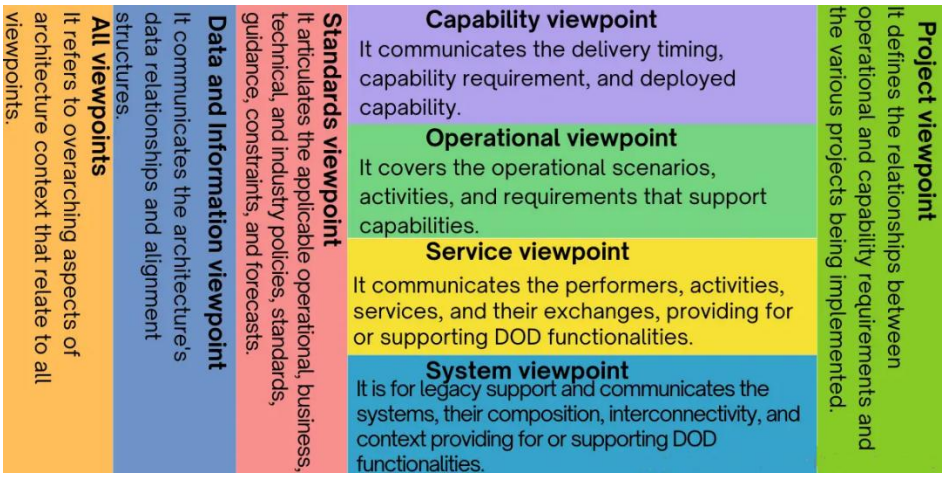

Figure 1. DODAF Views

UAF: A Meta-Model-Governed Architecture

Unified Architecture Framework (UAF) differs from conventional framework architectures by structuring architectural information using a formal Domain Meta-Model (DMM). The domain meta-model describes architectural components and inter-domain associations between strategic, operational, resource, and security aspects of the architecture. Unlike other approaches that divide responsibilities in terms of different viewpoints, UAF integrates relationship information into the architecture. Semantic consistency is ensured throughout the entire meta-model structure, allowing all architectural components to be linked into one unified framework. Consequently, relationships between operational processes, resources, and security mechanisms are defined explicitly in this approach (OMG, 2021; Hause, 2019).

UAF organizes architectural information using a matrix. Columns represent viewpoints; rows capture architectural aspects. Table 1 and Table 2 explain these dimensions. Figure 2 shows the UAF grid as outlined by the OMG standard (OMG, 2021).

Table 1. Column Headings

Viewpoint	Abbreviation	Description
Strategic	St	Capability management process. Describes the capability taxonomy, composition, dependencies, and evolution.
Operational	Op	Describes the requirements, operational behavior, structure, and exchanges required to support (exhibit) capabilities.
Services	Sv	The Service-Oriented View (SOV) is a description of services needed to directly support the operational domain as described in the Operational View.
Personnel	Ps	Shows the taxonomy of types of organizational resources as well as connections, interaction, and growth over time.
Resources	Rs	Captures a solution architecture consisting of resources, e.g., organizational, software, artifacts, capability configurations, and natural resources that implement the operational requirements.
Security	Sc	Defines the hierarchy of security assets and asset owners, security constraints (policies, laws, and guidance), and the locations of these assets (security enclaves).
Projects	Pj	Describes projects and project milestones, how those projects deliver capabilities, the organizations contributing to the projects, and dependencies between projects.
Standards	Sd	A set of rules governing the arrangement, interaction, and interdependence of solution parts or elements.
Actual Resources	Ar	The analysis, e.g., evaluation of different alternatives, what-if analyses, trade-offs, and V&V of the actual resource configurations.

Table 2. Row Headings

Aspect	Abbreviation	Description
Architecture Management	Am	Identifies the metadata required to develop a suitable architecture that is fit for its purpose.
Traceability	Tr	Describes the mapping between elements in the architecture.
Taxonomy	Tx	Presents all the elements as a standalone structure.
Structure	Sr	Describes the breakdown of structural elements, e.g., logical performers, systems, projects, etc., into their smaller parts.
States	St	Captures state-based behavior of an element.
Sequences	Sq	Expresses a time-ordered examination of the exchanges as a result of a particular scenario.
Roadmap	Rm	Addresses how architectural elements change over time.
Processes	Pr	Captures activity-based behavior and flows.
Parameters	Pm	Shows the measurable properties of something in the physical world and elements and relationships that are involved in defining the environments applicable to

		capability, operational concept, or set of systems.
Motivation	Mv	Captures motivational elements that pertain to enterprise transformation efforts, as well as different types of requirements.
Information	If	Address the information perspective on operational, service, and resource architectures.
Constraints	Ct	Details the measurements that set performance requirements constraining capabilities.
Connectivity	Cn	Describes the connections, relationships, and interactions between the different elements.

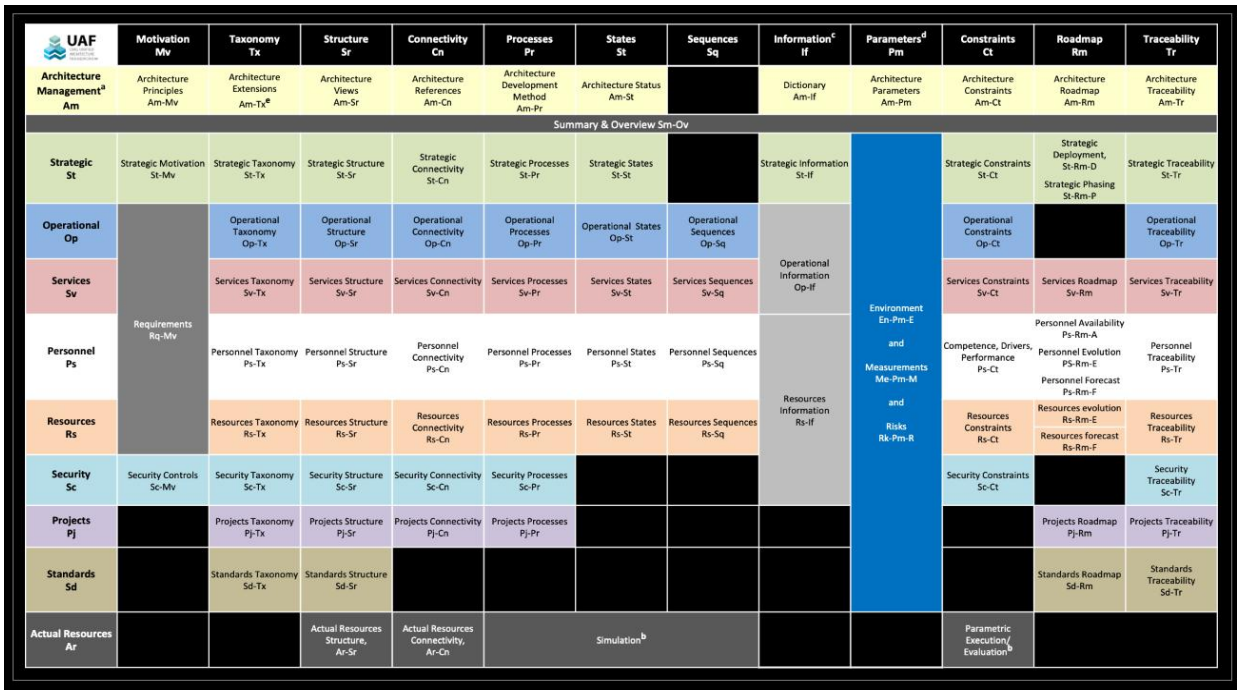

Figure 2. UAF Grid

Unlike many other approaches that view security documentation as a distinct process, UAF provides two capabilities related to cybersecurity modeling. The first one is the Security (Sc) domain within the architecture that encompasses elements such as security assets, security policies, security constraints, and security enclaves along with mission and system elements. Another capability of UAF is the separation of logical domains, such as operational and capability domains, from their physical realization in terms of implementation in the meta-model of the architecture. This allows engineers to connect security threats, vulnerabilities, and security controls to mission and operational processes to which they are associated.

Architectural Implications for Cybersecurity in SoS Environments

These differences directly impact the manner in which engineers approach cybersecurity concerns in SoS systems. Risk management necessitates that threats can be identified at the lower levels of technical vulnerability and traced all the way through their

effects on the capability for mission execution. The conduct of such an analysis requires engineers to establish consistent relationships at multiple levels (Maier, 1998; Boardman & Sauser, 2008).

In a viewpoint-oriented architecture like DODAF, there is no enforcement of these relationships within the framework. Rather, it is up to the analyst to develop traceability through gathering information from several architectural views. The task demands a degree of manual work and the consistency of artifacts being used. Consequently, the analysis of cybersecurity issues becomes fragmented, particularly in cases where the impact of vulnerability is traced throughout the various domains. The UAF framework follows a different strategy where the above relationships are embedded within a formal domain meta-model. Security is not considered as a distinct layer in the analysis but part of the entire architecture.

Since the architecture itself specifies these relations, it is possible for the analyst to look into how cyber threats spread and influence mission outcome without establishing links between different perspectives. This methodology is consistent with the US Department of Defense's Digital Engineering Strategy that values integrated models over fragmented documents. After all, it is the architecture's design that dictates how well the engineers will incorporate cybersecurity measures, perform cyber threat analysis, and control security. Frameworks that compel analysts to establish the relationship on their own add an extra layer of complexity. On the other hand, frameworks that incorporate such relations into the model create a straightforward route to cyber threat analysis (DoD, 2018; Mažeika, 2021; Martin & Brookshier, 2023).

Related Work on UAF for Cybersecurity and System-of-Systems Architectures

The most recent body of literature explores the application of the Unified Architecture Framework (UAF) in developing SoS environments through engineering practice, especially with regards to cybersecurity. Most studies in this area focus on how the UAF domain meta-model allows for better integration within architectural domains than viewpoint-based methods.

According to Brooks & Hause (2022), engineers should treat cybersecurity not as a collection of disparate technical controls but as an integral component of a system-of-systems. The study illustrates how the UAF security perspectives enable engineers to model cybersecurity assets, threats, and protective mechanisms in an integrated architecture. In turn, this enables analysts to address security issues through the operation, system, and mission domains in one model. In another study, Hause (2025) highlights how architects include

security constructs directly in the enterprise architecture using UAF security perspectives. These perspectives provide the ability for engineers to model cybersecurity objectives, threats, vulnerabilities, and mitigation measures as separate components of the architecture rather than as distinct analysis deliverables. Several researchers investigate the impact of UAF on the modeling of systems-of-systems in a model-driven approach. For example, Eichmann et al. (2019) show how engineers use UAF in the context of a model-based engineering practice consistent with the V-model life cycle.

Furthermore, researchers investigate the role of UAF in facilitating analysis and validation of models. Ding, Wang, and Cao (2020) describe an approach where description logic is used on UAF models to allow engineers to automatically conduct consistency check of the architecture's components. This technique makes possible more robust verification of relationships in the architecture. Later developments of the approach enhance UAF in order to promote reuse and facilitate more sophisticated analysis. For example, Adejokun et al. (2023) introduce reusable libraries, patterns, and profiles within security views of UAF models to implement knowledge transfer in relation to cybersecurity. Feng et al. (2025) illustrate an application of UAF models when engineers create agent-based simulations to allow system behavior, missions effectiveness, and resilience assessments in SoS settings. As seen from this review of the literature, the use of UAF models offers certain structural advantages for modeling cybersecurity issues. It includes the possibility to utilize the domain meta-model in order to represent cybersecurity elements within the architecture and maintain their relationships.

METHOD

This paper presented a structured comparative analysis of the cybersecurity modeling capabilities of SysML-based implementations of the Department of Defense Architecture Framework (DODAF) and the Unified Architecture Framework (UAF). The methodology focuses on the inherent architectural semantics and structural enforcement mechanisms of each framework rather than on the performance of specific modeling tools or software implementations. The analysis draws on the formal specifications of DODAF and the UAF Domain Meta-Model, as well as representative modeling practices described in the literature.

This paper evaluates the two frameworks across four key dimensions of cybersecurity modeling (INCOSE, 2007; Mažeika, D. 2021):

1. Threat and Vulnerability Representation – how the architecture instantiates and links threat actors, vulnerabilities, and attack surfaces within the model.

2. Risk Propagation Modeling – the framework's ability to represent how cyber incidents cascade across interconnected architectural domains.

3. Security Control Integration – how the architecture represents security controls and integrates them with system resources, services, and operational activities.

4. Mission-Level Risk and Traceability – the framework's ability to trace cybersecurity risks from technical vulnerabilities to mission-level consequences.

For each dimension, the analysis examines three primary characteristics of the architectural framework:

1. The degree to which the framework's meta-model enforces relationships among architectural elements
2. The mechanisms available for establishing cross-domain traceability
3. The framework's ability to represent cybersecurity constructs directly within the architectural model

By comparing these characteristics, the paper evaluates how effectively each framework supports architecture-driven cybersecurity analysis in system-of-systems environments (Mažeika, 2021; Brooks & Hause, 2023).

RESULTS AND DISCUSSION

Cybersecurity Modeling Requirements in Digital Engineering

In a paradigm of digital engineering, it is essential for the architecture framework to consider cybersecurity as an intrinsic domain rather than an independent compliance document through model-based analysis. This demands an architecture that will act as the authoritative source for any security aspect in the organization. In order to make this happen, a framework should meet the following fundamental criteria (DoD, 2018; Mažeika, 2021).

1. Integrated Threats and Vulnerabilities Modeling: It is essential for the architecture to support a method for integrating the depiction of threats, vulnerabilities, and attack surfaces as elements of the model. Importantly, the connection between these components and their impact on particular operations, system assets, and information flows should be clear, enabling the identification of attack vectors within the model (Brooks & Hause, 2022; Hause, 2025; Mažeika, 2021).

2. Mission-Impact and Risk Propagation Modeling: The formal definition of dependencies between system components, services, and functions in the semantic structure of the proposed framework would allow one to identify such dependencies and analyze their propagation in case of localized cyber threat. Such risk propagation modeling will allow us to identify

impacts of risk in terms of mission degradation and loss, rather than only technical damage (Boardman & Sauser, 2008; Brooks & Hause, 2022; Eichmann et al., 2019; Maier, 1998).

3. Integration of Security Controls within Architectures: The use of security controls like encryption, access control policies, and surveillance systems should be depicted as components of the architecture itself instead of generic needs. It entails establishing the connection between security measures and the weaknesses they address and the resources they guard. Such integration also facilitates systematic cost-benefit analysis, which will help assess the influence of diverse security options on overall system efficiency, cost, and effectiveness (Adejokun et al., 2023; Hause, 2025; NIST, 2020).

4. Embedded Compliance and Assurance: The system must be able to trace back from the compliance framework, such as NIST SP 800-53 and ISO 27001, to the actual control implementations within the architecture. It would make compliance not only an audit but also something that can be proven and verified throughout time. This feature is a cornerstone of developing security assurance cases based on the architecture, where all security claims are supported by actual evidence (Mažeika, 2021; NIST, 2020; ISO, 2013).

5. Automation and Monitoring Support: Ideally, the architecture should support automation and continuous monitoring capabilities. The model must provide tools to query it to detect any unaddressed risks, gaps in traceability, or mismatches in security measures. This approach will help move from periodic security evaluations to an environment of real-time risk awareness that dynamically adjusts with changes in the architectural design (DoD, 2018; Ding et al., 2020; Feng et al., 2025).

This section evaluates the SysML-based DODAF and the Unified Architecture Framework (UAF) against the previously defined cybersecurity modeling requirements. The analysis shows that while both support model-based representation, their underlying architectural philosophies lead to significant differences in their ability to integrate cybersecurity.

Comparative Cybersecurity Modeling Analysis

In this part, SysML implementation of both Department of Defense Architecture Framework (DODAF) and the Unified Architecture Framework (UAF) is evaluated with respect to the cyber security modeling requirements mentioned before. While the two frameworks provide for model-based systems engineering, they differ in terms of structure in that DODAF defines viewpoints to structure the architecture, which deal with different stakeholder concerns, while the UAF uses formally defined domain meta-model to structure the architecture.

Current literature on model-based cybersecurity and systems of systems focuses on the need to capture cross-domain dependencies in architectural models (Brooks & Hause, 2022; Eichmann et al., 2019). A framework that captures semantic connections between operational, systems, and mission components offers more powerful means for cybersecurity than a framework where such components are treated as loosely coupled entities.

Threat and Vulnerability Representation

In general, threats and vulnerabilities tend to be represented in DODAF models that use SysML in particular architectural views, like system or operational views. Using SysML diagrams makes it possible for engineers to model behaviors, resources, and relationships, however, SysML does not make any relationship mandatory between security elements and mission constructs. In other words, analysts need to draw relationships by themselves in order to connect technical vulnerabilities with operational tasks or missions.

By utilizing UAF, the architect will be able to model threats, vulnerabilities, and security constraints as architectural components that belong to the security Sc domain of the architecture. Since UAF domain meta-modeling dictates relationships between architectural components across domains, it is possible to relate the security concepts with activities, services, and resources in the architecture (Martin & Brookshier, 2023).

Previous studies have identified the significance of such capabilities. In their article, Brooks & Hause (2022) emphasize the need for engineers to represent cybersecurity infrastructures as architectures that involve a system of systems with threats, assets, and security controls cutting across both enterprise and operational perspectives. Likewise, Hause (2025) notes that UAF security views provide engineers with the opportunity to describe threats, risks, and risk mitigation measures in the architecture model without having to consider security analysis as a separate exercise.

Risk Propagation and Mission Impact Analysis

Cybersecurity analysis in complex systems requires engineers to model how localized technical failures propagate through interconnected system components and ultimately affect mission capabilities. In SysML-based DODAF architectures, analysts must infer these relationships by synthesizing information across multiple viewpoints. Activity diagrams, sequence diagrams, and resource interaction models can illustrate dependencies, but the framework does not provide a formally enforced mechanism to traverse those dependencies across architectural domains.

UAF provides stronger support for this analysis because its meta-model explicitly defines relationships between operational activities, services, and the resources that

implement them. Analysts can therefore trace dependency chains directly through the architecture model. When a system resource becomes compromised, analysts can follow those relationships to determine which operational activities depend on that resource and which mission capabilities may degrade as a result.

Research on UAF-based system-of-systems modeling supports this interpretation. Eichmann, Melzer, and God (2019) show that UAF-based development methods provide stronger traceability across lifecycle stages and architectural layers than traditional system-centric modeling approaches. Because the meta-model explicitly defines these relationships, analysts can examine cascading effects across operational and technical domains.

Security Control Representation

Engineers often represent security controls in SysML-based DODAF models as system components, functions, or requirements within system views. These representations capture the presence of security mechanisms. Still, analysts usually maintain the relationship between a control and the vulnerability it mitigates through external artifacts such as risk registers, control matrices, or compliance documentation. This separation limits the ability to evaluate security architectures directly from the model. Without explicit architectural relationships between vulnerabilities, controls, and protected assets, analysts must rely on external documentation to determine the effectiveness and coverage of implemented security mechanisms. UAF addresses this limitation by allowing architects to represent security controls as architectural elements within the Security domain and to link those controls directly to the resources, services, and operational activities they protect. These relationships integrate security controls into the architecture's dependency structure (Hause, 2025; Mažeika, 2021).

Recent research that extends UAF security views supports this integrated approach. Adejokun et al. (2023) propose augmenting UAF security views with reusable architectural libraries and patterns to support cybersecurity modeling across projects. By embedding these reusable constructs within the architecture, engineers can improve modeling consistency and reduce the effort required to represent security mechanisms across large system-of-systems environments.

Mission-Level Risk Assessment and Traceability

The process of analyzing cybersecurity at the mission level involves identifying cyber vulnerabilities and following their influence throughout the system architecture to assess whether the vulnerability will have an impact on the operational effectiveness of the mission.

When conducting cybersecurity analysis using DODAF architectures, the analysis is done through inference.

While SysML helps with the structural integrity of such models, traceability cannot be ensured automatically by the modeling framework. The analysts have to manage such relations through their own practices within the modeling process and other outside processes of governance. The UAF approach offers a much more structured way to analyze risk at the level of missions by linking the strategic, operational, service, and resource domains. A straight line of causality can be drawn between a threat agent, a vulnerable resource, its associated operational processes, and finally, the impacted mission capability.

These relationships have also been shown to provide for advanced analysis capabilities. According to Feng et al. (2025), engineers can leverage these UAF architecture modeling capabilities to build a simulation environment for system-of-systems analysis. This analysis capability makes it possible to move away from static security analysis and towards the analysis of dynamic effects of any cyber incidents on system operations. All in all, this implies that the UAF domain meta-model has more structure for supporting cybersecurity analysis aligned with missions. Security analysis is not conducted in isolation but in conjunction with architecture analysis using the UAF approach.

The analysis of the relationship between DODAF based on SysML and the UAF shows that there is a much wider trend of evolution in architecture development practice – moving from document-centric product representation to architecture modeling governed by semantics. Even though the use of SysML helps achieve more structural consistency in implementing DODAF, the framework is still inherently based on viewpoints. It allows architects to model cybersecurity concepts like threats, vulnerabilities, and security controls in separate architectural views. However, relationships between these concepts and other entities at the operation and mission levels cannot be structurally governed by the framework itself.

In contemporary research concerning enterprise architecture modeling and engineering environments for systems-of-systems, this shift towards semantically-driven architectures becomes apparent. There is growing agreement within the community that architectures enforcing relationships across domains will facilitate better analysis compared to architectures based on document-oriented viewpoints (Brooks & Hause, 2022; Eichmann et al., 2019). Within such an environment, the engineer must model the dependencies between operations, technologies, and mission capabilities to understand their propagation in the event of any disruption.

The UAF approach adopts an alternative architectural paradigm by establishing the Domain Meta-Model, which manages the relations between strategic, operational, service, resource, and security domains. Moreover, it guarantees that architecture elements stay interconnected within a consistent semantic network. Under this framework, engineers have the flexibility to incorporate cybersecurity components into the architecture rather than viewing them as independent documents. As noted in prior literature, security viewpoints in the UAF framework enable architects to describe threats, vulnerabilities, risks, and mitigation strategies as native elements of the model associated with the operational and resource domains impacted (Hause, 2025; Brooks & Hause, 2023). However, the need for such an approach is increasingly pertinent to the current SoS environment, where the system is composed of integrated subcomponents, distributed control mechanisms, and emergent properties that facilitate the spread of localized incidents beyond their operational boundaries. While a viewpoint-based architecture provides the means to characterize the constituent components of an SoS, it fails to establish the dependency chains necessary for analyzing the cascading effects on the system. Research on UAF-based system-of-systems development supports this interpretation and demonstrates that meta-model-governed architectures improve traceability and lifecycle integration across architectural layers (Eichmann et al., 2019).

The structural differences between the two approaches also have an impact on how the architects define and analyze their security measures. In most conventional architectures, the engineers define their security controls as system functions or components but keep the connection between the threat and counter-measure in external documents for managing risks. The UAF approach is capable of solving this issue through defining the security controls in the Security viewpoint of the architecture in relation to their associated resources and services. The use of patterns and libraries for UAF security viewpoints recently studied by Adejokun et al. (2023) facilitates this process even more.

Moreover, the use of the UAF meta-model facilitates more sophisticated types of architectural assessments. Recent research suggests that system-of-systems behavior can be evaluated through simulation, using the UAF models, and automated reasoning (Ding et al., 2020; Feng et al., 2025). This allows for a transition from assessing system performance in terms of static document analysis towards assessing the effects of cybersecurity events on such performance and resilience to those events. Nonetheless, the adoption of the framework governed by meta-models presents difficulties for the organization.

While there has been some study done on UAF for enterprise architecture and systems-of-systems modeling, there is relatively little information available regarding how the design

of an architectural framework affects cybersecurity modeling approaches. It has been determined that frameworks controlled through a specific architectural meta-modeling approach offer greater structural advantages for conducting cybersecurity analyses in highly complex systems-of-systems scenarios. These results confirm the general finding that the semantics of the architectural framework have a direct effect on the level of cybersecurity understanding achieved from the model itself. As defense and critical infrastructure systems become more complex and interdependent, architectural frameworks that incorporate cybersecurity into their fundamental structure offer a better starting point for designing mission-aligned systems.

CONCLUSION

In this research work, the DODAF and UAF architectures have been analyzed using SysML for their implementation and comparison to study their applicability in cybersecurity architecture modeling in system of systems contexts. Four major criteria were considered: threats and vulnerabilities, risk propagation, security control, and mission traceability. It is found that the structure of the architecture framework plays a vital role in enabling architecture-based cybersecurity analysis.

The use of SysML for DODAF architecture modeling offers a means by which to structure architectural information and enhance the rigors of document-based processes. Nonetheless, the process involves organizing the architectural assets based on the viewpoint perspective. Therefore, an analyst is tasked with the responsibility of combining information from different perspectives in order to relate technological weaknesses to business capabilities.

The limitations are overcome by UAF by using a formal Domain Meta-model which specifies relations between the strategic domain, operational domain, service domain, resource domain, and security domain in the architecture. The benefit of this approach is that it helps in representing security threats, weaknesses, and controls as architectural elements that can be correlated with operational actions and mission capabilities. Through such correlations, the analysis of cyber risk propagation across the architecture and its impact on mission effectiveness becomes possible.

Contribution to the field of systems engineering is made by analyzing SysML-based DODAFs and UAFs in terms of cybersecurity architecture. Particularly, the difference in semantic properties of these frameworks results in various ways of modeling threats, risk propagation, incorporation of security controls, and tracing mission levels in systems-of-systems architecture.

REFERENCES

Adejokun, A. P., Hause, M., Brooks, M., & Huang, L. (2023). Preserving and sharing knowledge: Extending the UAF security views with libraries, patterns, and profiles. INCOSE International Symposium.

Boardman, J., & Sauser, B. (2008). System of Systems Engineering: Innovations for the 21st Century. CRC Press.

Brooks, M., & Hause, M. (2022). Making the Puzzle Pieces Fit: Utilizing UAF To Model A Cybersecurity System of Systems. INCOSE International Symposium.

Brooks, M., & Hause, M. (2023). Model-Based Cyber Security at the Enterprise and Systems Level. INCOSE International Symposium.

Department of Defense (DOD). (2010). Department of Defense Architecture Framework (DoDAF) version 2.02. U.S. Department of Defense.

Department of Defense. (2018). DoD Digital Engineering Strategy. U.S. Department of Defense. https://www.acq.osd.mil/asda/dse/docs/DOD-Digital-Engineering-Strategy.pdf

Ding, Q., Wang, Y., & Cao, G. (2020). UAF Model Verification Method Based on Description Logic. IOP Conference Series: Materials Science and Engineering, 768(7), 072006.

Eichmann, O. C., Melzer, S., & God, R. (2019). Model-Based Development of a System-Of-Systems Using Unified Architecture Framework (UAF): A Case Paper. In 2019, the IEEE International Symposium on Systems Engineering (ISSE). IEEE.

Feng, Y., Ge, P., Shao, Y., Zou, Q., & Liu, Y. (2025). UAF-based Integration of Design And Simulation Model for System-Of-Systems. Journal of Systems Engineering and Electronics, 36(1), 108–126.

Hause, M. (2019). What Is UAF, And Why Do I Care? Object Management Group.

Hause, M. (2025). Using The Security Views In UAF. Object Management Group.

Hause, M., & Kihlström, H. (2021). Preserving and Sharing Knowledge: Extending The UAF Security Views with Libraries, Patterns, And Profiles. INCOSE International Symposium.

International Council on Systems Engineering (INCOSE). (2007). Systems Engineering Vision 2020. INCOSE.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013: Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO.

Lee, E. A. (2008). Cyber-Physical Systems: Design challenges. In Proceedings of the 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC) (pp. 363–369). IEEE. https://doi.org/10.1109/ISORC.2008.25

Maier, M. W. (1998). Architecting Principles for Systems-of-Systems. Systems Engineering, 1(4), 267–284. https://doi.org/10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D

Martin, J.N. & Brookshier, D. (2023). Linking UAF and SysML Models: Achieving Alignment Between Enterprise and System Architectures. INCOSE International Symposium, 33: 1132–1155. https://doi.org/10.1002/iis2.13074

Mažeika, D. (2021). Integrating Security Into Model-Based Systems Engineering Environments. Systems Engineering, 24(5), 375–389.

National Institute of Standards and Technology. (2020). Security And Privacy Controls For Information Systems And Organizations (NIST SP 800-53 Rev. 5). U.S. Department of Commerce.

Object Management Group. (2021). Unified Architecture Framework (UAF) version 1.2 (ISO/IEC 19540). OMG.