An Open Standards Data Model and Taxonomy to Enable Digital Twins for Defense

Patrick I. Buckley, PhD

Integration Innovation, Inc. (i3)

Huntsville, AL

patrick.buckley@i3-corps.com

Robert A. Proctor, Jr.

Real-Time Innovations, Inc. (RTI)

Sunnyvale, CA

robert.proctor@rti.com

ABSTRACT

The term "digital twin" (DT) has become ubiquitous across various industries, including defense. So much so that DoDI 5000.97 prescribes a digital engineering framework to include the creation of a "computerized representation… that serves as the real-time digital counterpart of a physical object or process." The Instruction states there can be multiple twins of a physical system, but each should be "based on authoritative sources of information and have clearly defined uses and scopes." While these definitions are helpful to understand the potential context of and usages for a DT, it falls short of prescribing a common data architecture to ensure consistency and utility of the data generated or consumed by the twin itself.

Much of the discussion around DTs within the defense community has stopped short of defining an open standard to enable a common data storage construct wherein all data produced or consumed by a DT must conform to a specific standard. Instead, discussions have favored allowing original equipment manufacturers to define how data is transferred, stored, or processed. Choosing between a closed vs. open standard approach is currently the focal point of the DT discussion in the defense industry.

This paper proposes a common taxonomy to define the terms, roles, and responsibilities for an open standard based approach to data production, management, consumption, and analysis. Additionally, this paper proposes a connectivity framework based on the Object Management Group Data Distribution Service (DDS) standard. The Unified Data Reference Architecture currently in draft is used to define an open standard for DTs to enable a convergence between modeling and simulation, test, and engineering. By leveraging DDS, the proposed open standard for DTs can ensure interoperability, scalability, and security across defense applications.

ABOUT THE AUTHORS

Patrick I. Buckley, PhD is a Senior Technologist at Integration Innovation, Inc. (i3). Dr. Buckley serves as the Technical Lead for PEO Missiles and Space PM IFRCO's Architecture Team overseeing the development enterprise system of systems architectures and the federation of system-level models into objective architectures for acquisition, test, and simulation activities. Dr. Buckley also provides technical mentorship at i3 empowering team members to achieve their career goals. He received his BS from the University of Missouri and his MS and PhD from the University of Alabama in Huntsville. Dr. Buckley's current research interests include digital twins, digital thread, full digital lifecycle, and integration of complex systems.

Robert A. Proctor, Jr. is a Staff Field Application Engineer for Real-Time Innovations. He has over 28 years of experience in A&D Embedded Software as a Software Engineer and Field Applications Engineer. Prior to his time as a Field Application Engineer, he developed and implemented real time embedded software at major Aerospace and Defense corporations. His roles have included developing software and system designs, mission-management, and display processing systems. Rob received his BS from Embry-Riddle Aeronautical University in Aerospace Studies and his MS from the University of South Florida in Engineering Management.

An Open Standards Data Model and Taxonomy to Enable Digital Twins for Defense

Patrick I. Buckley, PhD

Integration Innovation, Inc. (i3)

Huntsville, AL

patrick.buckley@i3-corps.com

Robert A. Proctor, Jr.

Real-Time Innovations, Inc. (RTI)

Sunnyvale, CA

robert.proctor@rti.com

INTRODUCTION

The concept of digital twins (DTs) has rapidly gained traction across various industries, revolutionizing the way organizations perceive and interact with physical assets and processes (Chinesta, el. al, 2018; Kenett & Bortman, 2021; Singh, et. al, 2023). From manufacturing to healthcare, DTs have emerged as powerful tools for enhancing efficiency, optimizing performance, and enabling predictive maintenance. Nowhere is the potential of DTs more pronounced than in the defense sector, where the ability to simulate, analyze, and predict the behavior of complex systems throughout the entire program lifecycle is of paramount importance.

At the forefront of this paradigm shift is the Digital Twin Consortium (DTC), a collaborative effort managed by the Object Management Group (OMG) and aimed at defining and advancing the understanding of DTs across industries (Mullen & Olcot, 2020). Through its seminal works, the DTC has laid the groundwork for a standardized approach to DT implementation, encompassing conceptual models, interoperability frameworks, and architectural guidelines (Budiardjo & Migliori, 2021).

As the defense industry increasingly embraces digital engineering and simulation technologies, the relevance of DTs cannot be overstated. Department of Defense Instruction 5000.97 (DoDI 5000.97, 2023) underscores the importance of DTs as real-time counterparts of physical systems, emphasizing the need for standardized approaches to their creation, management, and utilization.

The OMG DTC is a collaboration between industry, academia, and defense with the purpose of driving awareness, adoption, interoperability, and development of DT technologies.

This paper seeks to explore the evolving landscape of DTs within the defense sector, drawing inspiration from the foundational work of the DTC. By leveraging insights from the Consortium's publications, particularly the Digital Twin System Interoperability Framework (DTSIF, Budiardjo & Migliori 2021), and by drawing upon DoD frameworks such as the Unified Data Reference Architecture (UDRA; US DoD, 2024) and standards such as the OMG Data Distribution Service (DDS), we can establish a common foundation for DTs that transcends disciplinary boundaries and fosters collaboration and innovation. This framework will encompass taxonomy definitions, data-centric approaches, and connectivity frameworks, all aimed at fostering interoperability, scalability, and security in DT ecosystems. This paper aims to propose a comprehensive taxonomy/ontology framework for DTs in defense applications. This paper will also propose several use cases for such a framework to further foster the eight data principles outlined in the DoD Data Strategy (AD1112684, US DoD, 2020).

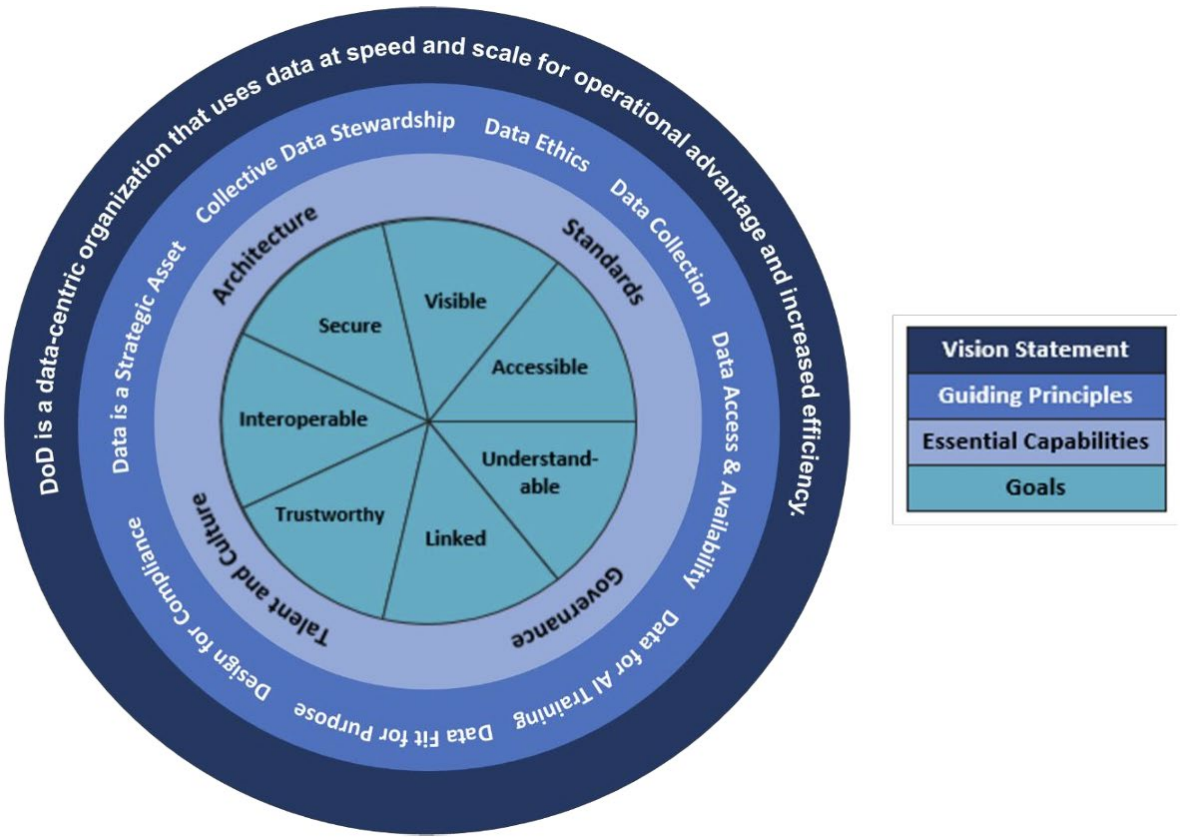


Figure 1: DoD Data Framework from DoD AD1112684

Definition of a System

The International Council on Systems Engineering (INCOSE) defines a system as "an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not" (INCOSE Systems Engineering Body of Knowledge v5.10, 2024). By this definition a system can be products, services, or processes composed of one or many parts. For example, software, firmware, hardware, and/or simulation elements can make up a physical system and any entities external to the system of interest are considered users or input sources. This definition is important to understand as the DTs become more ubiquitous, because all of the above system types could be part of a DT as a system of systems. The data framework ensures the system of systems is interoperable, accessible, and understandable to ensure the needs of all stakeholders are met.

History of Digital Twins

The genesis of DTs can be traced back to the convergence of various disciplines, each contributing its unique perspective to the concept's evolution (Grieves, 2018). At the forefront of this convergence was the emergence of virtual modeling, simulation, and data analytics, laying the foundation for the digital representations of physical entities we now recognize as DTs.

As DTs gained prominence across industries, different organizations and communities began to articulate their own interpretations of the concept, leading to a divergence in definitions and approaches. The DTC, for instance, defines a DT as a dynamic software model that uses data from the physical world to enable understanding, learning, and reasoning. This definition emphasizes the dynamic nature of DTs and their ability to evolve over time.

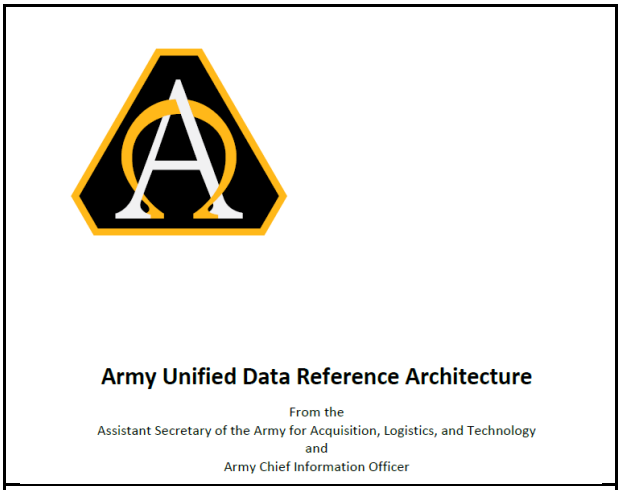
In contrast, game engine developers and the Virtual Reality Augmented Reality Association (VRARA) offer a slightly different perspective, defining DTs as virtual representations of physical components or entire systems. This definition highlights the immersive and interactive aspects of DTs, particularly in the context of virtual reality environments.

Meanwhile, Gartner, a leading research and advisory firm, provides yet another interpretation, describing DTs as software models that represent physical objects, processes, or systems. This definition underscores the analytical capabilities of DTs, particularly their role in enabling real-time insights and predictive analytics.

While these divergent definitions reflect the rich tapestry of perspectives surrounding DTs, they also highlight the need for a common standard to reconcile disparate interpretations and ensure interoperability, data transparency, and consistency. By drawing upon frameworks such as the UDRA and OMG DDS, we can establish a common foundation for DTs that transcends disciplinary boundaries and fosters collaboration and innovation.

Digital Engineering Enablement of Digital Twins

Digital engineering frameworks have emerged as indispensable tools for designing, simulating, and optimizing complex systems, providing a seamless transition from conceptualization to realization. At the heart of this paradigm shift lies the concept of DTs, which serve as dynamic, real-time counterparts to physical entities, enabling holistic understanding and predictive analysis, and based on DoDI 5000.97 data transparency and availability is paramount.



The UDRA provides a framework by which to align Army data architectures for the purpose of interoperability and data-driven decision making.

The DTC's DTSIF plays a pivotal role in this ecosystem, providing guidelines and best practices for ensuring interoperability and compatibility across diverse DT implementations. By standardizing interfaces, data formats, and communication protocols, this framework facilitates integration and collaboration, empowering organizations to harness the full potential of DTs across the product lifecycle.

In the context of defense applications, digital engineering frameworks enable the creation of comprehensive DTs capturing the intricacies of complex systems, from individual components to entire platforms and systems of systems. By leveraging advanced modeling and simulation techniques, defense organizations can explore various scenarios, assess performance under different conditions, and optimize resource allocation, ultimately enhancing mission readiness, deployment flexibility, and operational effectiveness. Furthermore, digital engineering frameworks lay the groundwork for digital thread and digital thread integration, facilitating the flow of information across disparate systems and stakeholders. This integration enables a holistic view of the product lifecycle, from concept to disposal, fostering collaboration and informed decision-making at every stage.

As defense organizations continue to embrace digital engineering principles, the role of DTs will only grow in significance. By leveraging the DTSIF and other industry standards, defense organizations can establish a common foundation for DT development and deployment, ensuring interoperability, scalability, and security across diverse applications and domains.

Summary of DoDI 5000.97

Department of Defense Instruction 5000.97 (DoDI 5000.97) serves as a guiding framework for digital engineering and DT implementation within the defense sector. In light of the discussions surrounding DTs in the previous sections, DoDI 5000.97 underscores the importance of standardization, interoperability, and consistency in DT development and deployment. Key tenants of DoDI 5000.97 include:

- Recognition of DTs as real-time digital counterparts of physical objects or processes, echoing the foundational principles discussed in the DTSIF.
- Emphasis on the need for multiple DTs to be based on authoritative sources of information and have clearly defined uses and scopes, aligning with the proposed taxonomy and data-centric view outlined earlier and expanded upon below.

- Acknowledgment of the challenges posed by divergent definitions and approaches to DTs, underscoring the importance of establishing common terms, standards, and frameworks to ensure consistency and utility.

In essence, DoDI 5000.97 provides a strategic roadmap for DT implementation within the defense sector, emphasizing the importance of aligning with industry standards and best practices. By adhering to the principles outlined in DoDI 5000.97 and leveraging insights from the DTC and other relevant stakeholders, organizations can navigate the complexities of DT acquisition, development, and deployment, ultimately enhancing mission success and operational effectiveness.

A PROPOSED TAXONOMY FOR DIGITAL TWINS IN DEFENSE

For the purposes of this paper, taxonomy is a systematic, hierarchical definition framework for the purpose of classification. Taxometric categorization allows for the grouping of complex systems or ideas through a series of different subclassifications to improve definition and thus understanding. Figure 2 depicts the proposed categories and subclassifications for consideration in the definition of a DT.

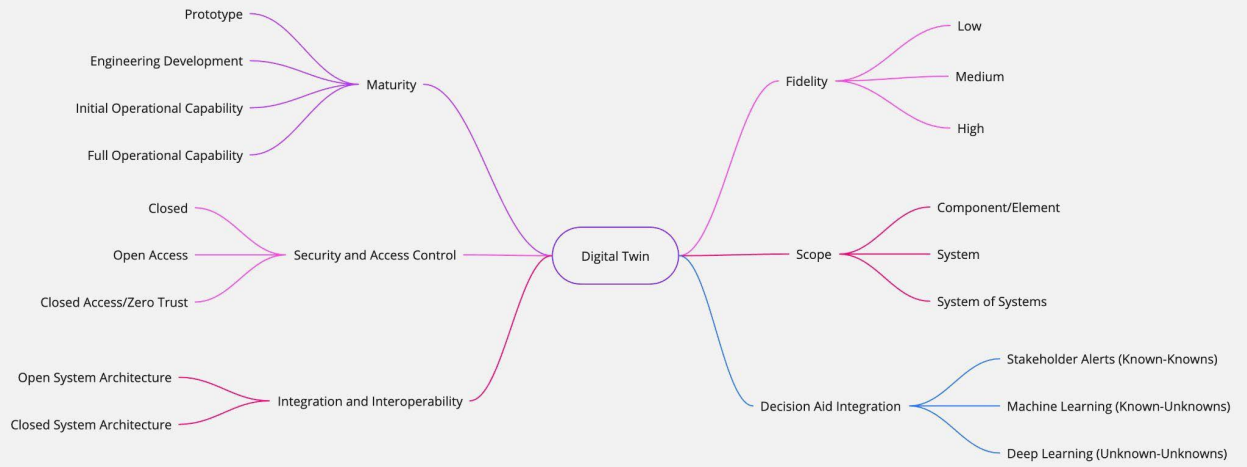


Figure 2. Digital Twin Taxonomy Map

Maturity

DoDI 5000.01 and DoDI 5000.02 define the US DoD Adaptive Acquisition Processes. These instructions form the foundation for all major acquisition programs and specify the key milestones an acquisition undergoes leading to fielding and sustainment. Additionally, DoD provides additional guidance to enable the rapid development and rapid deployment of prototype systems through Middle Tier Acquisition as part of the Adaptive Acquisition Framework. In conjunction with the phases and milestones of defense acquisition, the Digital Twin Taxonomy (DTT) breaks the maturity of a DT into the following subclassifications:

- **Prototype**: System elements are not fully defined and allow developers to analyze alternatives to the design prior to full implementation. The Prototype DT provides a test bed to drive technology roadmaps, future improvements, and long-term test strategies for Fully Operational Capability. Prototype DTs enable early feedback during implementation to ensure the final product meets stakeholder needs. Prototype DTs should not be used to evaluate the performance of the Full Operational Capability but will continue to mature as the parent system matures and verification and validation (V&V) data becomes available.
- **Engineering Development**: System elements are maturing and test data collected by the Prototype DT are providing feedback into the parent system and the DT itself. Engineering Development DTs can begin to assess the system's performance, develop acquisition and fielding strategies, and validate reliability and maintenance of the final product.
- **Initial Operational Capability (IOC)**: System elements are near completion to begin providing critical decision data to the stakeholders. The physical components are production-ready and user's manuals are recorded and validated for training purposes. System performance assessments are further validated to fully assess performance within the operational context.

- **Full Operational Capability (FOC)**: The system is finalized for fielding, sustaining, and informing stakeholders of future developments. An FOC DT precisely and accurately represents the fielded system to the fullest extent and serves as an asset for the remainder of the program's lifecycle.

Fidelity

Automatically developing the most appropriate DT model and its fidelity for a given task remains a challenge. Fidelity is a measure of how accurately a simulation represents the cyber physical system. It categorizes how well the simulation responds to external stimuli and how closely it mirrors the response of the system it's simulating. As the DT matures in lifecycle phase so should the fidelity of the DT itself. For the DTT, fidelity closely corresponds with the phases as outlined above and is subdivided into the following categories:

- **Low Fidelity**: In the Prototype phase the DT is categorized as low fidelity as the elements making up the DT are not anchored by data collected within an operationally relevant context. Low fidelity DTs can provide context to decision makers as they consider alternative solutions and develop technology roadmaps for long-term planning. As mentioned previously, DTs categorized as low fidelity should not be used to assess or predict the overall performance of the DT in its final phase. However, low fidelity DTs will provide the groundwork as it matures.
- **Medium Fidelity**: In the Engineering Development phase, the DT is categorized as medium fidelity and begins to integrate elements validated by test data. Where applicable visualizations are higher resolution to better align with their physical counterparts. Data interfaces move from the conceptual and logical levels to the physical level and provide collection and analysis points for further validation.
- **High Fidelity**: In the Initial and Full Operational phases, the DT is categorized as high fidelity through a process of accreditation. The accuracy and precision of the DT is highly time dependent and necessitates real-time communications between all elements of the DT. Therefore, a DT is only considered high fidelity if the physical, virtual, and simulation components are reliably communicating and providing information at the speed of relevance for the stakeholders.

Scope

The Scope of the DT describes the complexity of the system in question. A DT could exist for a singular component of a system, an entire system, or a system of systems. This decision is driven by many factors, including availability of data needed to build the DT, scalability of the DT, or cost or schedule constraints. The DTT subdivides scope into the following categories:

- **Component**: It may be desirable to produce a DT of a singular component of an overall system due to several factors, including criticality, novelty, and/or overall system complexity. If a component is deemed critical to the operation of a system or system of systems, it may be advantageous to create a DT of the individual component to ensure any failures or abnormalities are addressed with immediacy. If a component is reusable to multiple solutions, developing a twin of the component will help expedite improvements to the component and maximize reuse across a wider enterprise. If a system is too complex for a high-fidelity DT, stakeholders may decide to produce DTs of only certain components to reduce cost and time to market.
- **System**: Following the fielding of a system, the DT of the system provides real-time feedback to decision makers and enables rapid deployment of critical fixes as well as allows for near immediate improvements in training and maintenance operations as the fielded system completes its operational lifecycle.
- **System of Systems**: This scope subcategory is truly the penultimate example of a DT and is the primary driver for the DTT. The DT of a system of systems requires a scalable, secure data centric approach as outlined by the DoDI 5000.97 along with a common set of terms and definitions to ensure the system components culminate in an integrated system of systems.

Security and Access Control

Data security and access control addresses five of the seven goals outlined in the AD1112684; secure, interoperable, visible, linked, and accessible (see Figure 1). The DoD and the National Institute of Standards and Technology (NIST) have many regulations and guidelines to reduce system vulnerabilities and potential attack vectors. As systems become more integrated and data centric, these controls become more critical to protect our systems from attacks while making critical decision data visible and available to those with access. The DT should be designed with security and access control in mind at all levels regardless of scope because neglecting to do so could incur cost and schedule risk through the full lifecycle. The DTT subdivides security and access control into the following categories:

- **Closed Network**: Building a network ontology based on a closed network reduces the potential for attack vectors and ensures data access is closely controlled and monitored. However, the accessibility,

interoperability, and visibility of the DT is greatly reduced and could impact its utility to a larger enterprise. Starting with a closed network approach will limit future improvements and could prove costly in the long term.

- **Open Access**: An open access approach assumes all users of the DT are by default trustworthy and have full access to all components at all times. Open access methodologies may be appropriate for systems deemed non-essential; however, if the open access system integrates with another type of system cross-domain or data diode solutions may be required to fully realize an integrated DT of a system of systems.
- **Zero-Trust**: By contrast, a zero-trust approach assumes all users of the DT are by default not trustworthy. In a zero-trust framework, access denial is set by default and access approval is by permission only. A zero-trust approach to DTs assumes the owning agency has a trusted agent responsible for providing the appropriate, predetermined level of access throughout the entire lifecycle of the DT. This approach likely requires the definition and allocation of additional roles within the managing organization as well as infrastructure to constantly monitor and adjudicate network activities.

Integration and Interoperability

A Modular Open System Approach (MOSA) is an integrated strategy to ensure architectures are open, scalable, and modular by design (see 10 U.S.C. 144 and 10 U.S.C. 4401). In the DoD MOSA is an acquisition and design strategy focused on open standards supporting loosely coupled, cohesive structures, including interfaces and data architectures. However, several considerations for the DT need to be made before fully adopting a modular approach. The DTT subdivides integration and interoperability into the following subcategories:

- **Open System Architecture**: The DoD mandate for MOSA requires consideration of modularity and openness. The DoD MOSA Framework (2020) outlines several engineering considerations, including interface design, use of open standards, and clearly defined data governance and policies. An open architecture DT enables integration with other open architecture systems through non-proprietary, standards-based messaging protocols and data architectures, such as the UDRA.
- **Closed System Architecture**: When developing a DT for internal use only may require a closed system approach in design. If legacy non-MOSA systems are part of the larger design, a closed approach may be required to provide the data required for stakeholders. Also, if sensitive information is part of the DT, using closed interfaces will impose access restrictions naturally. However, use of proprietary or closed protocols and standards greatly limits the DT's ability to integrate with other DTs, reduces reusability and data availability, and results in increased lifecycle costs as proprietary interfaces require bespoke solutions to provide decision makers with the data they need.

Decision Aid Integration

McKee (2023) defines an architectural framework for the purposes of guiding executive-level decision makers in how they plan their technology roadmaps to build DT capabilities. Under consideration are the role of data including management and governance practices, the role of predictive modeling through machine learning, the need for integration and interoperability across the enterprise, and the role of information technologies (IT) and operational technologies (OT) in the design, development, and deployment of DTs. One additional consideration should be the purpose for the DT in the first place. With any decision-making process, one must begin with the question, "What am I attempting to answer/accomplish with this solution?" The answer to this question will drive the level at which decision aids are integrated into the DT. At the core of any DT is the linkage between the real-world system and the virtual system to provide continual feedback to stakeholders, and if the desire is for the DT to support decision making, some level of learning will need to be incorporated. The DTT subdivides decision aid integration into the following categories:

- **Stakeholder Alerts**: As the DT is designed, engineers capture failure modes and maintenance metrics and track those metrics throughout implementation, V&V, and fielding. DTs allow these known-knowns to be tracked and communicated to stakeholders at all levels. Depending on its use and the nature of the alert, engineers should consider human factors to ensure the alerts are clear and concise while not being overwhelming. Engagements with these stakeholders early and often ensures the DT meets their needs and provides alerts in the manner they require (e.g., dashboards, extended reality (XR), mobile alerts).
- **Machine Learning**: With data centricity in mind, the DT should have the capability to host machine learning algorithms to capture system performance and address known-unknowns as the system reaches FOC. Machine learning allows the DT to assess anomalies against nominal function and begin tailoring alerts reducing risk and providing longevity and trust to the DT.

- **Deep Learning**: Deep learning techniques such as neural networks allows the DT to apply training algorithms to begin assessing how stakeholders are using the DT and begin assessing off-nominal behaviors to capture unknown-unknowns. Deep learning algorithms assess data at all nodes of the DT and provide critical feedback to stakeholders after the DT is fielded. This provides critical maintenance and sustainment data back to stakeholders for assessment of future performance improvements and upgrades and allows the DT to grow with the environment in which it is fielded.

DOD DIGITAL TWINS REQUIRE DATA-CENTRIC DATA MODELS

In the rapidly evolving landscape of defense technologies, especially around AI/ML iterations with regards to unmanned and autonomous vehicles, a data-centric approach is paramount for achieving agility, interoperability, and resilience across diverse operational environments. This section delves into the key components of adopting a data-centric view for DTs within the defense sector, focusing on developing the data model, ownership of the data model, and application of the data model.

Developing the Data Model

The development of a robust data model is foundational to any DT implementation within the defense sector, and at the core of any DT data model is a foundation for capturing, storing, and analyzing pertinent information about physical assets and processes. Aligned with the Department of Defense's mandate for data-centricity outlined in the DoD Data Strategy, the data model must adhere to standardized frameworks and protocols to ensure consistency, interoperability, and reusability.

The OMG DDS emerges as a leading open international standard for enabling data-centricity within defense systems. Widely embraced in Modular Open Systems Approach (MOSA) standards such as the Future Airborne Capability Environment (FACE) and the Sensor Open Systems Architecture (SOSA), DDS offers a scalable platform for real-time data sharing and communication. By leveraging OMG DDS, defense organizations can establish a common data architecture that facilitates seamless integration and interoperability across disparate systems and platforms. Moreover, OMG DDS enables the development of modular and reusable data models that can be owned and managed by the government, mitigating the risks of vendor lock-in and proprietary dependencies.

Ownership of the Data Model

One of the key challenges in DT implementation within the defense sector is ensuring clear ownership and governance of the data model. In contrast to proprietary approaches that often lead to data silos and fragmentation, a data-centric view promotes the centralization and standardization of data models, enabling greater transparency, accountability, and collaboration.

By adopting open standards such as OMG DDS and combining them with mandates such as the UDRA via the principles of DoDI 5000.97, defense organizations can assert greater control over the ownership and management of DT data models. This not only ensures sovereignty and security but also fosters innovation and interoperability by enabling data sharing and collaboration across service branches and international partners.

DDS from OMG is a standardized middleware protocol and Application Programming Interface (API) enables systems to communicate and share data across a distributed, scalable architecture while reducing latency and increasing reliability.

Application of the Data Model

The application of DT data models extends beyond individual platforms or systems, encompassing a wide range of tri-service and multi-lateral distributed multi-domain operations for simulation and training. Through the adoption of standardized data models and interoperable communication protocols, defense organizations can leverage DTs to enhance mission planning, decision-making, and training exercises in dynamic and complex operational environments.

Furthermore, the application of DT data models facilitates the development of digital threads that span the entire product lifecycle, from concept to disposal. This holistic approach enables seamless data exchange and integration

across diverse stakeholders, ensuring continuity and traceability throughout the lifecycle of defense systems and platforms.

Embracing a data-centric view for DTs within the defense sector holds immense potential for enhancing operational effectiveness, collaboration, and innovation. By leveraging open standards such as OMG DDS and adhering to the principles of data-centricity outlined in the DoD Data Strategy, defense organizations can unlock new opportunities for mission success in an increasingly data-driven world.

Adoption of a Black-Box Model to Enable a Standards-Based Approach

In pursuit of fostering interoperability and standardization within the defense sector, adopting a black-box model is paramount. This section explores the rationale behind embracing this model and its pivotal role in enabling a standards-based approach to DT implementation. At the core of a standards-based approach lies OMG DDS, a proven and widely adopted framework for enabling real-time data sharing and communication. By leveraging OMG DDS, defense organizations can establish a robust connectivity framework that transcends proprietary boundaries and promotes interoperability across diverse systems and platforms. Furthermore, the Unified Data Reference Architecture (UDRA) serves as a cornerstone for achieving the goals outlined in the DoD Data Strategy and **VAULTIS** (Visible, Accessible, Understandable, Linked, Trustworthy, Integrated, and Secure). UDRA provides a comprehensive framework for defining data models, schemas, and ontologies, ensuring consistency, scalability, and security across defense applications.

UDRA, Achieving the DoD Data Strategy VAULTIS Requirements

Incorporating UDRA Use Cases from Appendices C & D (UDRA, 2024), defense organizations can align their DT implementations with the overarching objectives of the DoD Data Strategy and VAULTIS. By leveraging UDRA's modular and extensible architecture, defense organizations can achieve greater flexibility and agility in adapting to evolving mission requirements and information security challenges. Moreover, UDRA enables the seamless integration of DT data models with existing defense systems and platforms, facilitating the development of digital threads that span the entire product lifecycle. This integration fosters collaboration and information sharing across disparate stakeholders, driving innovation and enhancing operational effectiveness.

OMG DDS QoS Enables All Quality Metrics and Enables Secure Transport Natively

The inherent quality of service (QoS) capabilities of OMG DDS further enhances the security and reliability of DT communication and data exchange. By leveraging DDS QoS, defense organizations can enforce stringent quality metrics, such as reliability, availability, and timeliness, to ensure mission-critical data is delivered accurately and in a timely manner. Furthermore, DDS QoS enables secure transport natively, mitigating the risks associated with data breaches and cyber threats. By incorporating DDS QoS into their DT implementations, defense organizations can bolster data security and integrity, safeguarding sensitive information and enhancing overall mission assurance.

CONCLUSION

This paper proposes a detailed DT taxonomy for defense applications along with a proposed black-box data model as a cornerstone for enabling a standards-based approach to DT implementation. The DTT provides the foundation setting terms and expectations to ensure stakeholders looking to develop the technology for their application are clearly defining what they require, ultimately reducing cost and expediting fielding. The adoption of a black-box model, centered around OMG DDS and UDRA, enables a governed approach to DT implementation owned by the defense stakeholder and not the equipment manufacturer. This allows for reuse and ensures the DTs support the data-centric vision outlined by the DoD. By leveraging these frameworks and incorporating UDRA Use Cases, defense organizations can achieve greater interoperability, scalability, and security, ultimately enhancing mission success and operational effectiveness.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the contributions of our I/ITSEC birddog, Scott Schutzmeister, Research Staff Member, Institute for Defense Analyses, Project Support to Digital Engineering, Modeling and Simulation (DEM&S), OUSD (R&E), Systems Engineering and Architectures for his contributions to this paper.

REFERENCES

Budiardjo, Anto & Migliori, Doug (2021). Digital Twin System Interoperability Framework [White Paper], Digital Twin Consortium.

Chinesta, Francisco, Cueto, Elías, Abisset-Chavanne, Emmanuelle, Duval, Jean, & el Khaldi, Fouad. (2018). Virtual, Digital and Hybrid Twins: A New Paradigm in Data-Based Engineering and Engineered Data. Archives of Computational Methods in Engineering. 27.

Kenett, R. S., & Bortman, J. (2021). The Digital Twin in Industry 4.0: A wide-angle perspective. *Quality and Reliability Engineering International*, *38*(3), 1357–1366.

Grieves, Michael (2018). The Evolution of the Digital Twin. *IM+io Best and Next Practices*, 66–69.

Mckee, David (2023). Platform Stack Architectural Framework: An Introductory Guide [White Paper]. Digital Twin Consortium.

Mullen, Casey, Olcott, Sean, & Isaacs, Dan (2020), A Digital Twin Is…, BrightTalk. https://www.brighttalk.com/webcast/18347/458528

SEBoK Editorial Board. 2024. The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.10, N. Hutchison (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology. Accessed 19 June 2024. www.sebokwiki.org.

Singh, Maulshree & Fuenmayor, Evert & Hinchy, Eoin & Qiao, Yuansong & Murray, Niall & Devine, Declan. (2021). Digital Twin: Origin to Future. Applied System Innovation. 4. 36.

United States Department of Defense (2020). DoD Data Strategy. Unleashing Data to Advance the National Defense Strategy (AD1112684). Assistance Secretary of Defense.

United States Department of Defense (2020). Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs. Office of the Under Secretary of Defense for Research and Engineering.

United States Department of Defense (2023). Digital Engineering (DoDI 5000.97). Office of the Under Secretary of Defense for Research and Engineering.

United States Department of Defense (2024). Army Unified Data Reference Architecture v1.0. Assistant Secretary of the Army for Acquisition, Logistics, and Technology.