Policies Motivating the Data Mesh

Ms. Erica Dretzka
Office of the DoD Chief Digital and AI Officer
Washington, DC
erica.l.dretzka.civ@mail.mil

Mr. Jordan Gottlieb
Office of the DoD Chief Digital and AI Officer
Washington, DC
jordan.gottlieb.ctr@mail.mil

ABSTRACT

The digital world is grappling with the transition in two vector spaces: 1) centralized to distributed architecture and 2) the continuum between human and machine actors. This evolution requires deliberate action and contextual awareness of the various mission spaces and local restrictions such as access-denied environments, semantic conflicts, Intellectual Property (IP) sensitivities, coalition partnerships, and machine interoperability. Each of these is a different aspect of the uphill battle to establish a data mesh responsible for negotiating across physical, regulatory, ontological, and digital borders.

This paper presents the roles of the many policies and strategies and how the mesh makes their touchpoints possible in order to achieve the socio-technical construct of the mesh. Ultimately it facilitates scalable interoperability among digital twins, machines, and humans. It knits the connective tissue among disparate systems, builds collective interoperability, and retains the privilege of local privacy and autonomy. This combination is critical in training and warfighting scenarios, during which multiple simulators built by various entities must interact and share namespaces with minimal to zero delays.

Extending the data mesh (“mesh”) beyond its heretofore idealistic yet ambiguous description in research, this paper illustrates the viability and interoperability of composable foundational building blocks for any organization’s mesh, proposing a bare minimum of additional mesh components to establish a data-mesh-worthy technical backbone. The paper provocatively challenges any single data mesh instantiation, pushing for the ideal of fully-federated domain independence bridging proprietary instantiations and illustrating seminal proof of concepts being tested in real-world scenarios.

A sophisticated technical and strategic response with a well-formed and flexible implementation plan is necessary when linking IP-sensitive proprietary modules with context-tuned data management practices, compliant with regulations yet differentiated from peers. Adopting agile and continuous learning principles, this paper approaches the reference architecture, reference design, and implementation plan for building a data mesh enabling the modeling and simulation community to make seamless connections both 1) between humans and machines and 2) across technical and regulatory boundaries.

ABOUT THE AUTHORS

Erica Dretzka: Ms. Erica Dretzka is a seasoned data scientist with over 20 years of experience in various industries, including Insurance, Energy, and National Defense. She has established two data science teams inside the Department of Defense (DOD) and led the development of advanced Artificial Intelligence (AI) and Machine Learning (ML) models. She focuses on employing engineering-based methods to design the optimal reference architecture and bridge strategy to support AI and data-backed mission support at the scale and resilience required for DOD.

Jordan Gottlieb Mr. Gottlieb is passionate about applying innovation and collaborative techniques for strategic synergies to unify stakeholders across an enterprise and create a data interoperability model across all of industry. He is currently focused on defining and implementing a true data mesh as well as defining an actualized Zero Trust model that is complimentary to current cybersecurity capabilities. His broad background includes system engineering, program management, strategic planning, business operations, government acquisition, and executive support.

Policies Motivating the Data Mesh

Ms. Erica Dretzka
Office of the DoD Chief Digital and AI Officer
Washington, DC
erica.l.dretzka.civ@mail.mil

Mr. Jordan Gottlieb
Office of the DoD Chief Digital and AI Officer
Washington, DC
jordan.gottlieb.ctr@mail.mil

INTRODUCTION

Machine-Human interoperability is currently possible inside of siloed, purpose-built environments, where unaffiliated entities collaborate for a specific use case. Inside that environment, they share data, AI algorithms, mission sets, and information using specified standards unique to each environment. However, modern operations demand more flexibility, requiring the individual instantiations to speak to each other and enabling the digital, physical, and human worlds to interoperate. Thus, modern operations demand an increasingly sophisticated interoperable environment. We propose a data mesh as the solution.

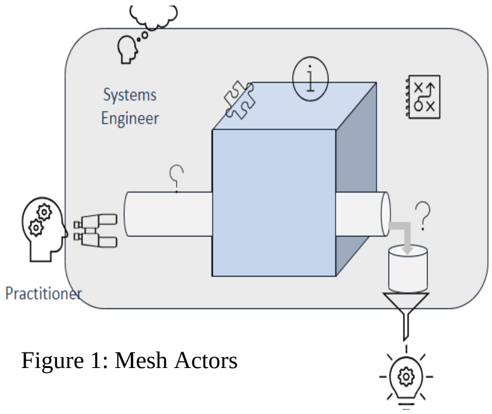


Figure 1: Mesh Actors

This paper acknowledges three major actors in data mesh environments: 1) a policy analyst who creates mesh functions, 2) a practitioner who utilizes the secured, governed, and trusted interoperated environment, and 3) a systems engineer (SE) motivated to develop a transparent, composable system. This trio enables migration away from the inflexible 'standards' that dominate current implementations with governance patterns and processes.

The Data Mesh ("mesh") is the socio-technical infrastructure that enables fluent interoperability through actions such as Modeling and Simulation (M&S) and Digital Engineering (DE) for use cases such as Artificial Intelligence (AI) and Digital Twins (DTs). Current mesh literature focuses on the strategic vision of the mesh without implementation guidance. This paper develops the implementation guidance by contextualizing the fifteen capabilities proposed in a previous paper[1].

The way ahead must accommodate Cyber-Physical Systems (CPS, also known as Internet of Things [IOT]). CPS introduces the requirement to integrate with the physical world, posing the added challenge of real-time coordination. The mesh makes this possible via its interoperable, flexible, heterogeneous set of components that observe the physical world, generate knowledge from these observations, and create actions back in the physical world. [2]

CPS emerged around 2006, when it was coined by Helen Gill at the National Science Foundation (NSF). It is sometimes confused with "cybersecurity," which concerns the Confidentiality, Integrity, and Availability (CIA) of data and has no intrinsic connection with physical processes. CPS is all about models, focusing on the fundamental intellectual problem of conjoining the engineering traditions of the cyber and the physical worlds[3]. Since Gill's definition, AI has matured the traditional paradigm of a model. Models are, by definition, simplifications of the real thing and in that sense, do not aim to replicate the original system in the same detail as that system [4], by employing sophisticated approaches to increase the fidelity of digital interactions with physical and quasi-physical systems.

The abrupt surge in the adoption of Large Language Models (LLMs) has fueled the awareness of AI in society. This paper contextualizes this AI instantiation and, particularly for military use cases, must make a sustainable association with CPS. It proposes that capabilities, such as access controls, privacy, data, semantic congruence, and asset lineage must be designed as composable elements of the data mesh and provide links to the digital, human, and physical worlds. The ensuing use cases are vast, including training and education, digital twins, Industry 4.0, and Cybersecurity Supply-Chain Risk Management (C-SCRM).

BRIDGING THEOR TO FUNCTIONAL AND TECHNICAL IMPLEMENTATION PLAN

Dehghani's O'Reilly book[5] popularized the mesh, defining it according to Figure 2. This book and its successors continue to establish the theoretical framework but leave readers to intuit the technical implementation. Since widely available authoritative literature dives deep into the four mesh principles, we presume a basic understanding of them and instead address how the mesh enables interoperability among multiple applications. We now propose functional and technical implementation patterns.

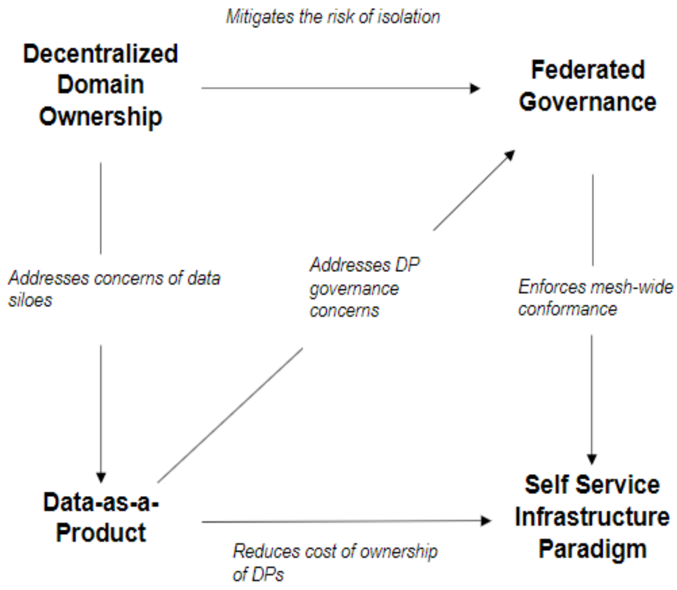

Mitigates the risk of isolation
Decentralized Domain Ownership
Federated Governance
Addresses concerns of data siloes
Addresses DP governance concerns
Enforces mesh-wide conformance
Data-as-a-Product
Self Service Infrastructure Paradigm
Reduces cost of ownership of DPs

Figure 2: Data Mesh Pillars

The mesh calls for connectivity by design, i.e., systems should be able to discover, inherit, evaluate, and share intelligence across different sub-systems or sub-components. We should be able to monitor, analyze, and control at the sub-unit level in real-time ([6] sensors, actuation) and visualize operations not only at the system level but the ecosystem[7]. The latter is perhaps the glue that may accelerate the future progress of digitalization.[7]

Modularizing problems enables composability for each custom use case. For instance, extending the practice of software decomposition analysis to its 'social' side allows policy analysts to employ agile processes when managing future context changes in policy, acquisition guidance, organizational realignments, and emerging mission sets. Similarly, the mesh enables simulation-based training to make all elements of a system, e.g., instructor, trainee, hardware, software, data, and AI, interoperable.

A mesh Implementation Plan (I-Plan) defines how to realize this ill-defined, but acutely needed transparency. We develop breadcrumbs of the mesh characterized by provenance, lineage, privacy, access controls, semantic interoperability, connectivity, and continuous monitoring. The I-Plan must be considered in the light of both data usage and use case maturation. The data transferred through the mesh must be usable for a broad number of use cases, and capable of handling data and information in any format to allow mission set interoperability.

Policy Analyst:
The DoD's Digital Engineering Modeling & Simulation Community of Practice (DEM&S COP) establishes how to perform and maintain Verification, Validation, and Accreditation (VV&A) for models and systems. Less formal methods exist, such as maintaining "change cases", which refine a use case by adding a relationship between the change case and the use cases that are affected by the change.[8] Figure 3 is tailored to military use cases, but generalizable to other use cases.

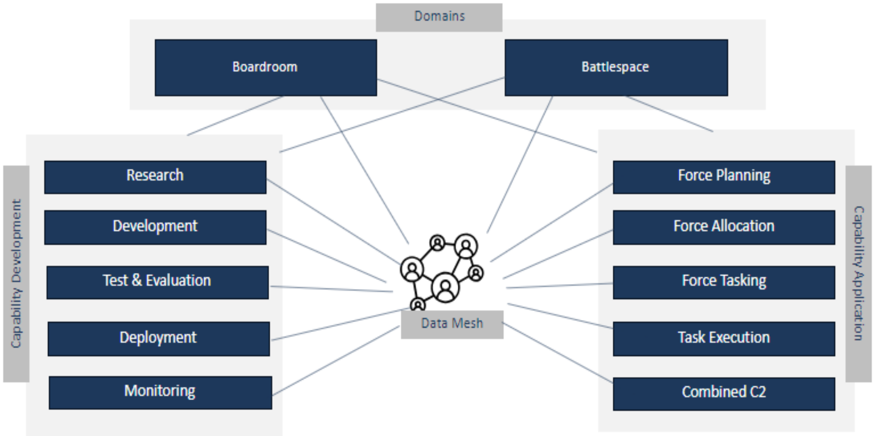


Figure 3: Use Case Network

Notably, each mesh element requires its own policy. For instance, a digital governance capability developed by one nation or entity must be able to cooperate with other nations and entities. This hurdle is one that partner nations in NATO face each day.

Practitioner

The mesh facilitates innumerable use cases. In this discussion we will address AI, Model Based Systems Engineering (MBSE), Digital Engineering (DE), and training operations.

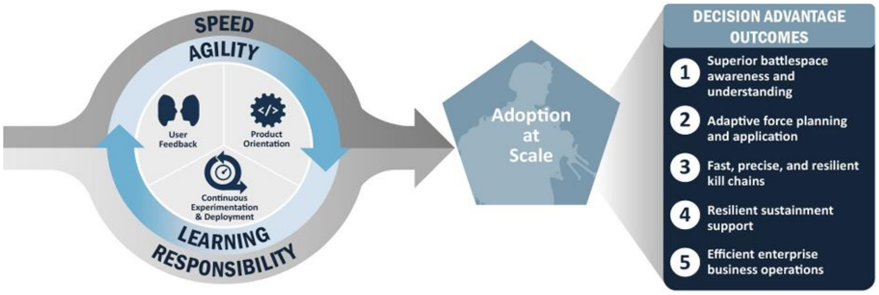

SPEED
AGILITY
User Feedback
Product Orientation
Continuous Experimentation & Deployment
LEARNING
RESPONSIBILITY
Adoption at Scale
DECISION ADVANTAGE OUTCOMES
1 Superior battlespace awareness and understanding
2 Adaptive force planning and application
3 Fast, precise, and resilient kill chains
4 Resilient sustainment support
5 Efficient enterprise business operations

Figure 4: Feedback Loop in the Data, Analytics, and AI Strategy

Artificial Intelligence (AI)

The 2023 DoD Data, Analytics, and Artificial Intelligence Strategy calls for integration of data, analytics, and AI technologies nested within broader U.S. government policy, the network of private sector and academic partners that promote innovation, and a global ecosystem. We need a systematic, agile approach to data, analytics, and AI adoption that is repeatable by all DoD Components. It requires data, analytics, and AI address key operational problems identified in the 2022 National Defense Strategy (NDS). The Department's agile approach to adoption (Figure 4) expects a tight feedback loop between technology developers and users through a continuous cycle of iteration, innovation, and improvement of solutions that enable decision advantage.[9]

Model-Based Systems Engineering (MBSE)

MBSE is a discipline supported by software that provides a digital approach to creating system models and simulating behaviors to understand systems and systems of systems. Those models describe the relationships among key variables within the systems and environmental or operating conditions in which the systems function. It makes complexity more manageable, systems design more scalable through systems-of-systems models, and enables users to weigh trade-offs across many requirements influenced by numerous key design decisions.[10]

Digital Engineering (DE)

The Department of Defense's (DoD) approach to DE is to securely and safely connect people, processes, data, and capabilities across an end-to-end digital enterprise. This enables model use to digitally represent the system of interest (i.e., system of systems, systems, processes, equipment, products, parts). DoD will incorporate technologies such as advanced computing, big data analytics, artificial intelligence, autonomous systems, and robotics.[11] Figure 5 illustrates how an Authoritative Source of Truth acts as a nexus for the diverse space of possible models. This source of truth is essentially a mesh of data sources made interoperable with services that translate data patterns, and negotiate communication methods (e.g., APIs, HPC, cloud compatibility), among other functions.

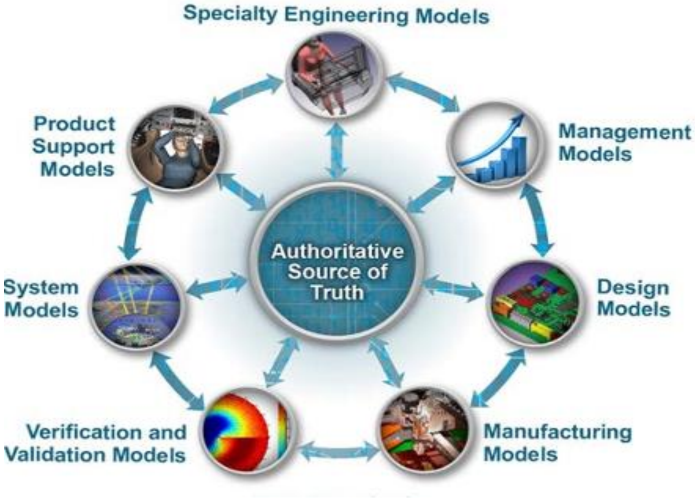

Specialty Engineering Models
Product Support Models
Management Models
System Models
Authoritative Source of Truth
Design Models
Verification and Validation Models
Manufacturing Models

Figure 5: DE's Authoritative Source of Truth

Training Operations

Modern training and education increasingly rely on digital platforms such as Coursera and gameification through simulators. Simulator interoperability is frequently constricted by environment-specific choices, such as data element formats (common ones include Distributed Interactive Simulation [DIS] and High Level Architecture [HLA]), bespoke hardware, scenario design, and how After Action Reports (AAR) capture and feed back into learning records that include Personally Identifiable Information (PII) and Personal Health Information (PHI). Privacy considerations further complicate ability to make these interoperable. The mesh implementation plan presented here proposes capabilities that enable interoperability both at the tactical and strategic level, to include privacy and Intellectual Property (IP) protection.

Digital Twins (DTs) and Modeling and Simulation (M&S) are the intersection of AI, MBSE, and DE. Coined by Michael Grieves in 2014, DTs characterize a variety of digital simulation models that run alongside real-time processes that pertain to social and economic systems as well as physical systems[4]. A digital model represents an actual or conceptual system that involves physics, mathematics, or logical expressions. A simulation is a method for implementing a model over time[12]. Users are able to simulate the behavior of a physical or digital system inside of a DT. Together, models and simulations allow users to simulate virtually any process, such as vetting potential system requirements prior to the Request for Proposal release, assessing engineering change orders or program upgrades, and training and education. M&S can assess and optimize resource usage, examine process changes, support supply-chain management routing and inventory quantities, business decisions, etc.[12]

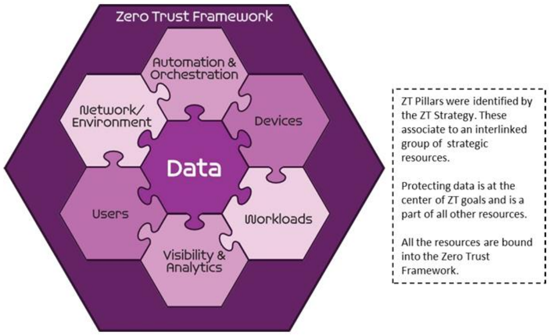
Systems Engineer

A well-designed and well-implemented mesh is positioned to be the scalable, agile, and accessible platform that enables the DEM&S and training industries to overcome challenges, e.g., scalable CPS, privacy and security, change monitoring and performance management, AI integration across the DEM&S lifecycle to alleviate overhead, requirements management across teams, and interoperability among distinct solutions architectures.

The success of the mesh requires implementers to achieve socio-technical and strategic change. Ultimately, governance and policy must be made machine-readable and interpretable by semantic services that translate the meanings of words with minimal human intervention. This is then layered with a flexible yet stable access control framework and encryption fabric for ad hoc access determination.

The Conundrum of Organizational Change, Security, and Privacy

Significant challenges to the mesh include1) organizational change, 2) security implementation, and 3) privacy practices. While many organizations are struggling with these three challenges the authors propose a set of mesh services that accommodate each of these barriers for a complete mesh implementation.



ZT Pillars were identified by the ZT Strategy. These associate to an interlinked group of strategic resources.

Protecting data is at the center of ZT goals and is a part of all other resources.

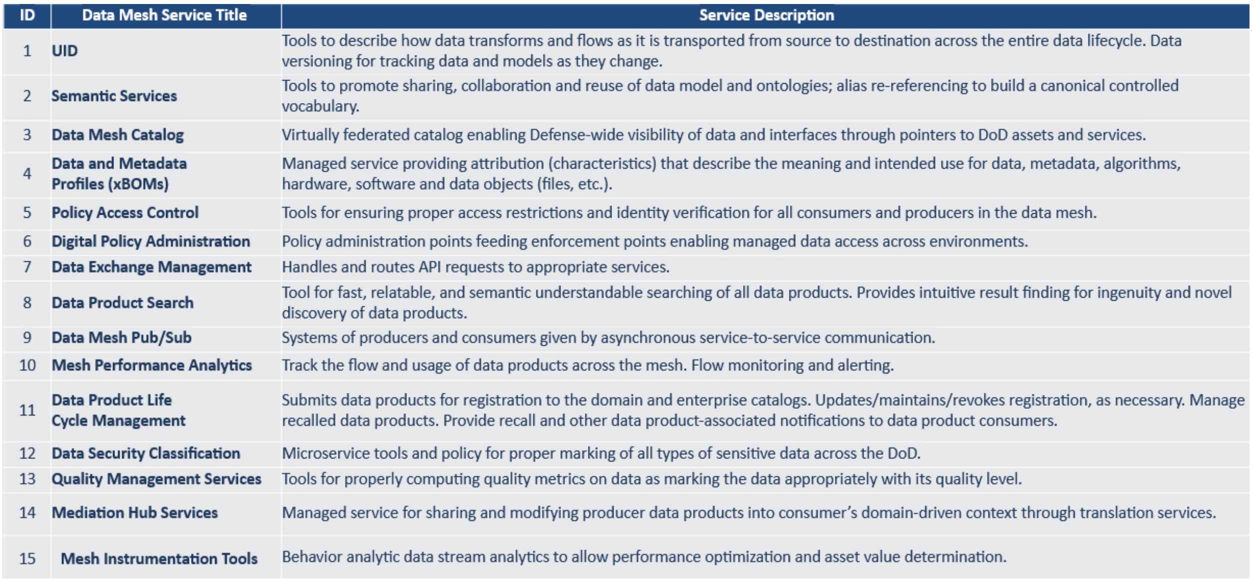
All the resources are bound into the Zero Trust Framework.

Figure 6: Zero Trust Framework[13]

One of the innovative techniques coupled with controlled vocabulary is the use of dynamically constructed Bills of Materials (xBOMs) for characterizing data objects that exist within the mesh. The BOMs are envisioned to be dynamically composable and easily accommodate characterizations for security control data and privacy concerns. Using automated logic engines these xBOM characterizations can be used to implement a fully computable Zero Trust (ZT) practices (Figure 6).

EXECUTION

The core outcome is to use the discipline of modularization to tie policy and strategy with implementation. We propose that the orchestration of the fifteen capabilities described in Figure 7 is the foundational modular components of a mesh. More detail is provided in the Data Mesh Reference Architecture paper.[1]



ID	Data Mesh Service Title	Service Description
1	UID	Tools to describe how data transforms and flows as it is transported from source to destination across the entire data lifecycle. Data versioning for tracking data and models as they change.
2	Semantic Services	Tools to promote sharing, collaboration and reuse of data model and ontologies; alias re-referencing to build a canonical controlled vocabulary.
3	Data Mesh Catalog	Virtually federated catalog enabling Defense-wide visibility of data and interfaces through pointers to DoD assets and services.
4	Data and Metadata Profiles (xBOMs)	Managed service providing attribution (characteristics) that describe the meaning and intended use for data, metadata, algorithms, hardware, software and data objects (files, etc.).
5	Policy Access Control	Tools for ensuring proper access restrictions and identity verification for all consumers and producers in the data mesh.
6	Digital Policy Administration	Policy administration points feeding enforcement points enabling managed data access across environments.
7	Data Exchange Management	Handles and routes API requests to appropriate services.
8	Data Product Search	Tool for fast, relatable, and semantic understandable searching of all data products. Provides intuitive result finding for ingenuity and novel discovery of data products.
9	Data Mesh Pub/Sub	Systems of producers and consumers given by asynchronous service-to-service communication.
10	Mesh Performance Analytics	Track the flow and usage of data products across the mesh. Flow monitoring and alerting.
11	Data Product Life Cycle Management	Submits data products for registration to the domain and enterprise catalogs. Updates/maintains/revokes registration, as necessary. Manage recalled data products. Provide recall and other data product-associated notifications to data product consumers.
12	Data Security Classification	Microservice tools and policy for proper marking of all types of sensitive data across the DoD.
13	Quality Management Services	Tools for properly computing quality metrics on data as marking the data appropriately with its quality level.
14	Mediation Hub Services	Managed service for sharing and modifying producer data products into consumer's domain-driven context through translation services.
15	Mesh Instrumentation Tools	Behavior analytic data stream analytics to allow performance optimization and asset value determination.

Figure 7: Fifteen proposed capabilities of a decomposable mesh

Figure 8 proposes that the data mesh negotiates the socio-technical dependencies between the DoD's Mission Engineering and DevSecOps strategies. It illustrates the connection points of two major DoD policies, the CIO's DevSecOps Strategy ("DevSecOps") and Research and Engineering's Mission Engineering Strategy ("Context Mesh") with the Data Mesh Reference Architecture (DMRA), identified here as the "Data Mesh".

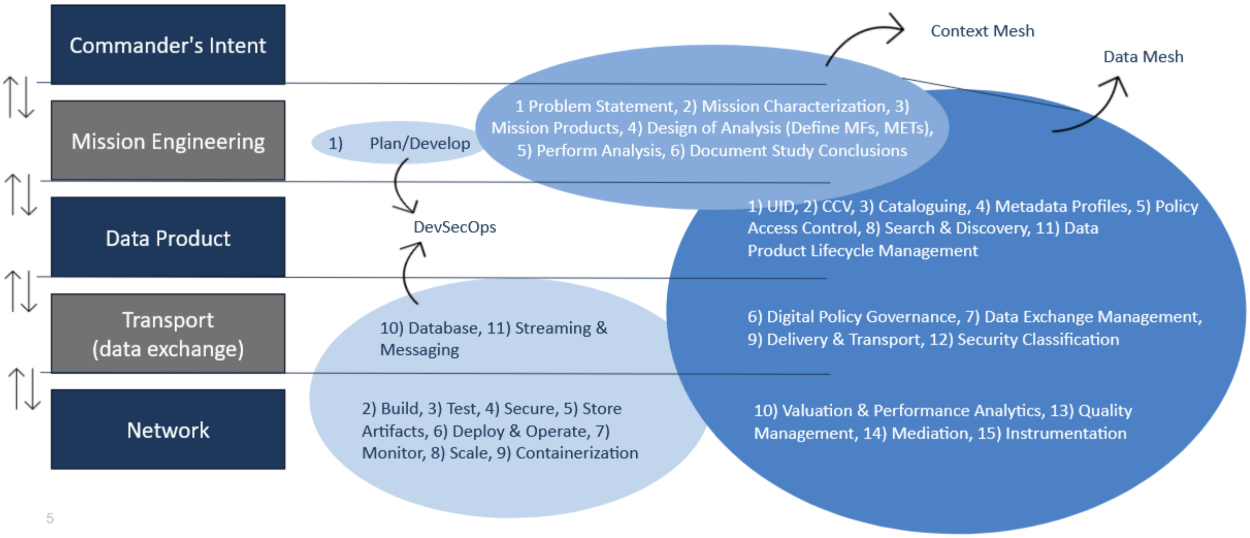
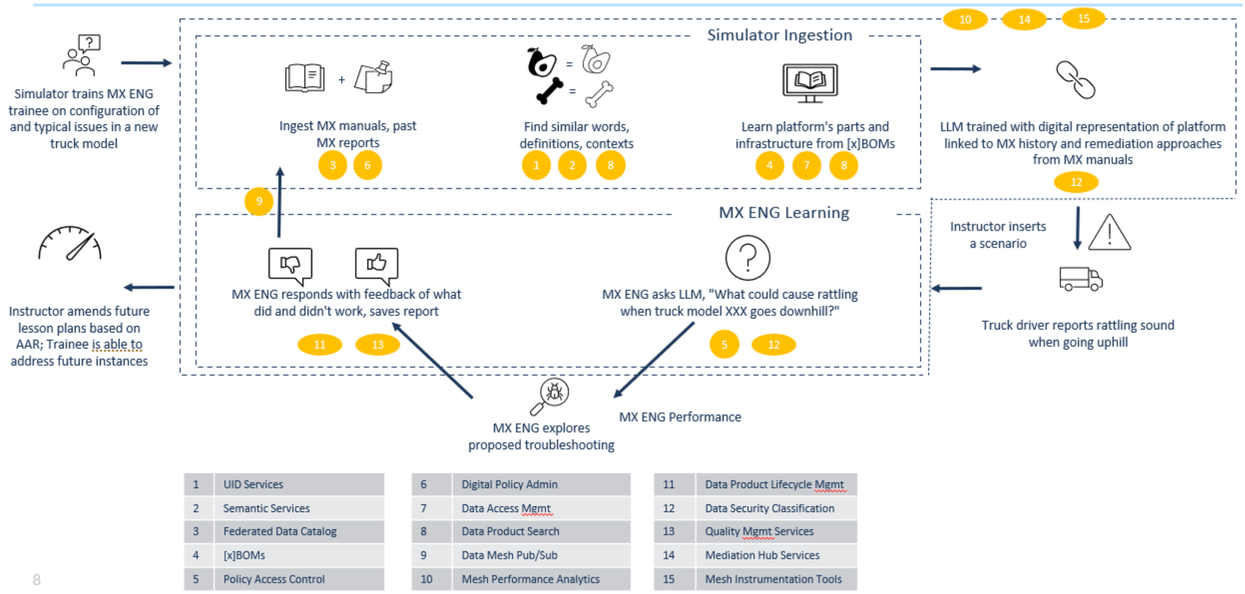

Commander's Intent
Mission Engineering
Data Product
Transport (data exchange)
Network
Context Mesh
Data Mesh
1) Plan/Develop
1 Problem Statement, 2) Mission Characterization, 3) Mission Products, 4) Design of Analysis (Define MFs, METs), 5) Perform Analysis, 6) Document Study Conclusions
DevSecOps
1) UID, 2) CCV, 3) Cataloguing, 4) Metadata Profiles, 5) Policy Access Control, 8) Search & Discovery, 11) Data Product Lifecycle Management
10) Database, 11) Streaming & Messaging
6) Digital Policy Governance, 7) Data Exchange Management, 9) Delivery & Transport, 12) Security Classification
2) Build, 3) Test, 4) Secure, 5) Store Artifacts, 6) Deploy & Operate, 7) Monitor, 8) Scale, 9) Containerization
10) Valuation & Performance Analytics, 13) Quality Management, 14) Mediation, 15) Instrumentation
5

Figure 8: Interaction of the Socio-Technical Mesh with Other Strategies

The following walkthrough evokes the use of a data mesh in a notional training scenario, in which a maintenance engineer (MX ENG) is learning the configuration of a new truck and how to troubleshoot it. The yellow circles present where each proposed data mesh component is utilized.

First, the simulator ingests all maintenance manuals and past issue reports. Noting that MX ENGs typically use shorthand and slang due to time restrictions and local colloquialisms, it looks for semantic similarity with the CCV service. Next, it applies the previous two steps to xBOMs in order to develop a digital twin (DT) of the truck platform's parts. The DT now injects AI via a Large Language Model (LLM), enabling the instructor and trainee to interact in local language with the DT, allowing, for instance, the trainee to orient to the truck's motor, chassis, and electronics.

Now that the trainee has access to the setup, the instructor injects a scenario that the truck driver reports a loud rattling sound every time the truck is on an incline. The MX ENG, potentially already skilled in this problem set from other vehicles, combines their native knowledge base with what the simulator already knows by querying it to understand whether there are any anomalies possible with this new vehicle. They go to the truck to test different solutions. Finally, the MX ENG returns to the LLM to explain in their native shorthand and slang, what they tried and what worked.


Simulator trains MX ENG trainee on configuration of and typical issues in a new truck model
Simulator Ingestion
Ingest MX manuals, past MX reports
3
6
Find similar words, definitions, contexts
1
2
8
Learn platform's parts and infrastructure from [x]BOMs
4
7
8
10
14
15
LLM trained with digital representation of platform linked to MX history and remediation approaches from MX manuals
12
9
MX ENG Learning
Instructor inserts a scenario
MX ENG responds with feedback of what did and didn't work, saves report
11
13
MX ENG asks LLM, "What could cause rattling when truck model XXX goes downhill?"
5
12
Truck driver reports rattling sound when going uphill
Instructor amends future lesson plans based on AAR; Trainee is able to address future instances
MX ENG explores proposed troubleshooting
MX ENG Performance
8

1	UID Services	6	Digital Policy Admin	11	Data Product Lifecycle Mgmt
2	Semantic Services	7	Data Access Mgmt	12	Data Security Classification
3	Federated Data Catalog	8	Data Product Search	13	Quality Mgmt Services
4	[x]BOMs	9	Data Mesh Pub/Sub	14	Mediation Hub Services
5	Policy Access Control	10	Mesh Performance Analytics	15	Mesh Instrumentation Tools

Figure 9: Notional Data Mesh Use Case Applied to a Simulation-Based Training Scenario

First, this notional scenario demonstrates how data and AI make physical and human systems, i.e., CPS and Industry 5.0, possible. Second, each yellow circle indicates how the mesh components (Figure 7) can be implemented to make the theoretic mesh a reality. Third, it provides a realistic example of how the mesh ties policies, initiatives, disciplines, and strategies together, such as those listed in the Practitioner section above (AI, MBSE, DE, and Training Operations) as well as those in Figure 8.

PRACTICAL APPLICATIONS

The mesh encourages each organization and mission to find its entry point. An operational unit may dictate needs such as Radio Frequency (RF) communications. An AI engineering team may require an AI provider to ascertain the responsible use of data and algorithms. A headquarters user may need to verify the quality of data presented in a dashboard. Below are a few more examples:

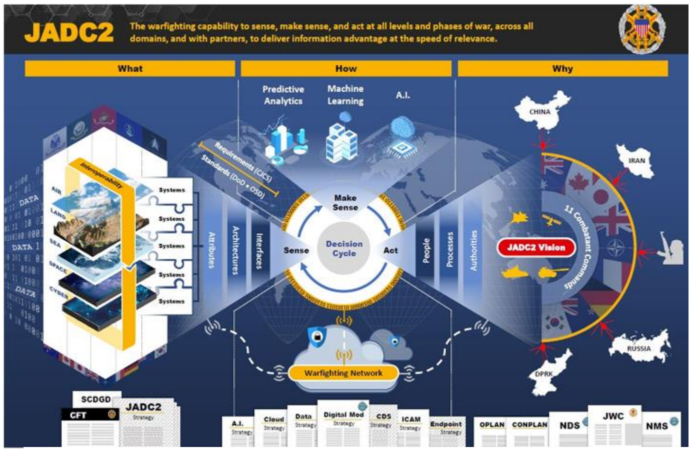


Figure 10: C-JADC2 LOEs [14]

Combined Joint All Domain Command and Control (C-JADC2)

C-JADC2 transcends any single capability, platform, or system; it provides an opportunity to accelerate the implementation of needed technological advancement and doctrinal change in the way the Joint Force conducts C2, enabling the Joint Force to use increasing volumes of data, employ automation and AI, rely upon a secure and resilient infrastructure, and act inside an adversary's decision cycle. It relies on “sense”, “make sense”, and “act”, adding five enduring lines of effort (LOEs) to organize and guide actions to deliver materiel and non-materiel JADC2 capabilities. The LOEs include: (1) Establish the JADC2 Data Enterprise; (2)

Establish the JADC2 Human Enterprise; (3) Establish the JADC2 Technical Enterprise; and (4) Modernize Mission Partner Information Sharing. (Figure 10)

The C-JADC2 strategy presents six guiding principles to promote coherence of effort across the Department in delivering materiel and non-materiel JADC2 improvements: (1) Information Sharing capability improvements are designed and scaled at the enterprise level; (2) Joint Force C2 improvements employ layered security features; (3) JADC2 data fabric consists of efficient, evolvable, and broadly applicable common data standards and architectures; (4) Joint Force C2 must be resilient in degraded and contested electromagnetic environments; (5) Department development and implementation processes must be unified to deliver more effective cross-domain capability options; and, (6) Department development and implementation processes must execute at faster speeds. [14]

M&S and Education

Figure 10: C-JADC2 Lines of Effort (LOEs)[14]

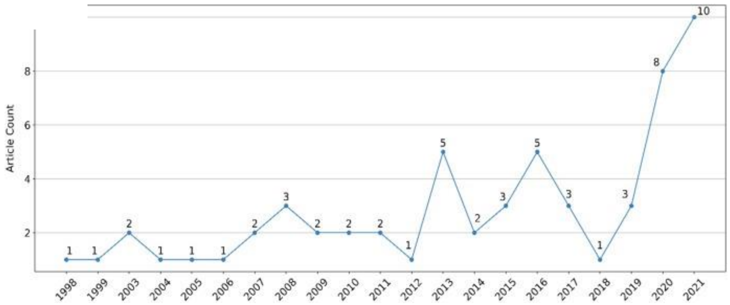


Figure 11: Trends in Simulation-Based learning with AI Applications

Simulation-based learning is defined as an active and immersive experience in a virtual learning environment that re-creates a realistic and authentic real-life event or a set of learning situations to solve a problem. Simulation-based learning offers a cost-effective authentic learning experience that facilitates deeper learning, inquiry, and problem-solving[15]. Methods include virtual reality, augmented reality, mixed reality, virtual lab, serious games, or computer-based simulation systems. A 2021 study estimated the trends in simulation-based learning with AI applications according to Figure 11[15]. It is important to note that this study was conducted prior to ChatGPT's avalanche of a launch in April 2023.

Artificial Intelligence

AI's spectacular adaptability to seemingly innumerable use cases has recently been fueled by Large Language Models (LLMs). The mesh digitizes all assets, converting their cyber, physical, or human realities into data. This non-trivial digitalization extends decades of best practices of Bills of Materials (BOMs) developed by the software and hardware industries to all asset classes. Expanding to new assets requires practitioners to develop digitally intelligible and machine-consumable patterns that may be safely shared with partners. Therein lies the need for the mesh's capabilities, a decomposable stack of services providing semantically coherent security and privacy.

These applications are a small subset of the innumerable use cases for mesh enablement.

FUTURE DIRECTIONS AND RESEARCH

Government, industry, and academia are iterating on the appropriate design for a data mesh. Multiple reference architectures have been published to develop baseline, high-level understanding of how to responsible design the mesh. Developed independently and following different enterprise architecture standards, their designs are remarkably interoperable. It is highly likely that each entity will discover that their distinct mission set and socio-technical infrastructure demands unique elements. Importantly, these different configurations are able to achieve interoperability among themselves as long as they agree to each adopt a highly decomposable, Zero-Trust enabled architecture. This critical point is the enabler for the organizational change that accompanies the 'socio' side of 'socio-technology', engendering both trust and technical interoperability.

This paper proposes the following implementation plan: Phase 1 is to develop the reference designs. These will provide direction for the subsequent Phase 2, to develop prototypes of the components. As with any deployment, these prototypes must be vetted, tested, and validated that they perform the required services sufficiently and safely.

These upcoming phases encourage all parties who plan to participate in the mesh to stay abreast of the design and stay involved as it matures. This way, each party will understand how to interoperate with the end product while also being given the chance to provide feedback.

CONCLUSION

Ultimately, everyone benefits from the mesh, and it's up to the 'socio' side of 'socio-technology' to make it viable. All indicators point to a future requiring a data mesh characterized by NSF's CPS in order to achieve seamless interoperability among AI, simulation, digital engineering, and training. This can be achieved by stipulating interoperability as a minimally acceptable outcome in the requirements of each individual micro-fabric.

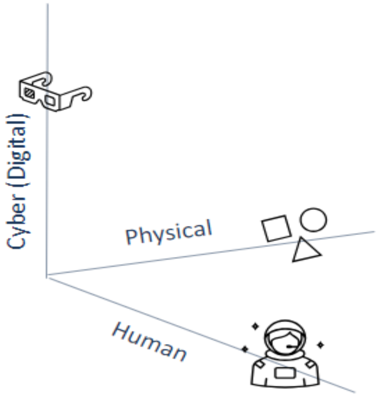


Figure 11: Cyber-Physical-Human Axes

Reimagined as an X-Y-Z axis in Figure 11, NSF correctly defined the X-Y axes of the Cyber-Physical systems and it intuited the need for the Z axis, the Human. We seek to characterize the last of these as the momentum to enable full interoperability from a policy perspective, a practitioner perspective, and a systems engineering perspective. Every organization has use cases requiring interdependence across the three axes. DoD has termed this 'boardroom to battlefield' and DHS sometimes refers to it as 'boardroom to border'. The data mesh develops the digital mechanisms across technology, AI, engineering, and digital policy to make this continuum possible.

One of the goals of the mesh is to interoperate across all three axes seamlessly, to accommodate battlefield to boardroom. One of those combinations is machine-to-machine (M2M), which requires that the two entities can speak fluently with each other, regardless of local context. Combined Joint All Domain Command and Control (C-JADC2) is likely the penultimate AI application for the defense industry. C-JADC2 increases the complexity of the mesh itself by levying an additional requirement, that these mesh capabilities are available at all entry points, including access-restricted edge operations, which may be totally disconnected at points in time. Furthermore, it broaches practically every conceivable use cases, from training to operations, analytics in dashboards and using AI,

A responsibly constructed mesh provides the necessary resources to digitally manage information. The comprehensive solution is a constellation of technology, cognitive processes, and information blending ultimately increasing our ability to synthesize the best outcome. This includes techniques, such as semantic interoperability to improve understanding, Data Product Teams to package content for mission needs, digital policy administration to optimize enablement of access, protection and information flow, and all of the other features of a complete mesh.

ACKNOWLEDGEMENTS

The writing team for this paper would like to acknowledge the work being done by different participants in the DoD CIO working groups around [x]BOMS, UIDs, Canonically Controlled Vocabularies, cybersecurity and Zero Trust, and different instantiations of the data mesh. Each group contributes a distinct perspective to the data mesh, strengthening its design to support all applications, including training and education, in the future.

REFERENCES

[1] Data Mesh Reference Architecture (Mar, 2024). https://media.defense.gov/2024/Mar/15/2003414274/-1/-1/1/dmra_paper.PDF
[2] Cyber-Physical Systems (Aug, 2016). https://www.nist.gov/itl/ssd/cyber-physical-systems
[3] Lee, E.A. (2015) The Past, Present and Future of CPS. Sensors 15 4837-4869 http://www.mdpi.com/1424-8220/15/3/4837
[4] Batty, Michael (2018). *Digital Twins*. Environment and Planning B: Urban Analytics and City Science, Vol. 45, pg 817–820.
[5] Dehghani, Zhamak (2022). Data Mesh: Delivering Data-Driven Value at Scale.
[6] https://issuu.com/opensystemsmedia/docs/eai_rg21_e-mag_final
[7] Datta, Shoumen. "Emergence of Digital Twins. Is this the march of reason?"
[8] Ecklund, Earl; Delcambre, Lois; Freiling, Michael (1996). "Change Cases: Use Cases that Identify Future Requirements"
[9] Department of Defense (2023). Data, Analytics, and Artificial Intelligence Adoption Strategy.
[10] Halpern, Pattanayak. June 2023. Innovation Insight: Model-Based Systems Engineering Is Fundamental to Digital Engineering. Gartner Research.
[11] Department of Defense OUSD(R&E), 2018. Digital Engineering Strategy.
[12] https://www.cto.mil/sea/dems/
[13] July 2022. Department of Defense (DoD) Zero Trust Reference Architecture, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf
[14] SUMMARY OF Tl-IE _ JOINT ALL-DOMAIN COMMAND & CONTROL (_JADC2) STRATEGY