# Stockholm Syndrome: Are we being held captive by our ancient interoperability standards?

**Simon G. Skinner**
**Thales UK Ltd.**
**Crawley, W. Sussex, UK**
**simon.skinner@uk.thalesgroup.com**

## ABSTRACT

Expenditure on Modelling and Simulation for training and operations (MSTO) is rapidly growing, with it likely to exceed $26 billion annually in the USA alone by 2028 (Global Data, 2024). There is an urgent need for MSTO to provide operational dominance for the US and its allies for multi-domain operations (MDO) given the rise of international conflicts and peer and near-peer aggressors.

MSTO compatibility between allies relies on common Interoperability standards. These standards that govern how the vast majority of MSTO equipment works together are based on work in the 1980's and 1990's. A time when the training systems that were connected were single service, based on computing platforms a million times inferior to those available today, so limited in performance and costly to maintain. For example, packet-based data broadcasting requires substantial investment in perimeter-based security to ensure that data is kept from adversaries.

Deployed interoperability standards were never originally designed to cope with modern engineering practices; dynamically updated simulations using digital twins, cloud based scalable computation systems, advanced zero-trust security architectures, and the advent of Artificial Intelligence technologies which thrive on vast quantities of data. Nevertheless, dedicated and experienced teams of simulation experts strive to update interoperability standards, based on the old paradigms that still capture attention.

This paper proposes a whole new approach to MSTO around data and artificial intelligence, to ensure our forces are prepared fully for the challenging operational environment, with its mixture of physical, cyber and human/social layers.

The author proposes actionable policy insights that are based on data centricity, answering the current challenges of data silos, computational inefficiencies, limitations in processing large data sets, classification levels and intellectual property sharing concerns. The paper describes a plan for the development of secure architectures with a scalable mediation technique using data meshes, responsible artificial intelligence behaviors and the use of existing government toolkits.

## ABOUT THE AUTHOR

**Simon G. Skinner** is the product policy leader for Thales Training and Simulation. He graduated with an honors degree in Electronic Engineering from the University of Southampton in 1986, is a chartered engineer and fellow of the UK institution of Engineering and Technology. He has worked in the simulation industry for more than 30 years in commercial, technical and managerial roles; this has included leading international interoperability standards development as chair of the Common Image Generator Interface (CIGI) group in the Simulation Interoperability Standards Organization (SISO). He was awarded a commendation for research in driver simulators in 2014 by the UK Ministry of Defence's Chief Scientific Adviser. He is the Vice Chair of the NATO Modelling and Simulation Group (NMSG) which has the delegated authority for setting M&S standards across the NATO alliance, and he also co-chairs a 3-year research task group looking at interoperability standards gaps for digital twins.

# Stockholm Syndrome: Are we being held captive by our ancient interoperability standards?

**Simon G. Skinner**
**Thales UK Ltd.**
**Crawley, W. Sussex, UK**
**simon.skinner@uk.thalesgroup.com**

## INTRODUCTION

The fundamental challenges of the 2025 to 2045 epoch in the global military operating environment require the radical reshaping of our technology solutions, to ensure operational dominance for the USA and its allies. These challenges include:

- The growing capabilities of peer and near peer threats (DOD News, 2020);
- The changing nature of war, characterised by the so-called seventh military revolution (Hoffman, 2017); of salience in this new era are developments in artificial intelligence, especially machine learning and deep-learning AI, combined with unmanned systems.
- The advent of increased complexity in multi-domain operations, leading to the requirement for a Systems of Systems (SoS) approach with consequently increased interoperability requirements (Army Science Board, 2019)
- The need to handle the multiple dimensions of operations; not only in the physical space, but also in cyber and social dimensions
- The apparent stall in human cognitive performance improvements over time, compared to the increased challenges of complexity in equipment and cognitive load (James R. Flynn, 2018).

Modelling and Simulation for training and operations (MSTO) must take account of these challenges in the design and implementation of training systems and other uses of modelling and simulation supporting operations – for example, platform design manufacture and support, operational analysis and decision support.

This paper, combining contributions from US Department of Defense (DOD) publicly available strategy and from international industry, provides a compelling viewpoint to challenge our existing thinking around interoperability paradigms and standards for MSTO. The author aims to challenge existing assumptions around simulation interoperability standards and how to reorganize our approach, especially given the vast improvements in technology over time.

## PERSISTENCE OF INTEROPERABILITY STANDARDS

Interoperability standards can be very persistent and affect the implementation of technologies widely separated in time. An example of this is the railway gauge standard. While the legend that the railway gauge is based on the width of two horses' backsides, which determined the width of Roman chariot wheels and the consequent ruts in roads, is apocryphal and subject to a lot of discussion, there is no doubt that railway gauges in the UK and USA become standardized on the width between rails set by George Stephenson in the UK in the early 1800's. (Gabriel, 2000). The standard gauge apparently limited the size of the Solid Rocket Boosters of the space shuttle as they had to fit into a railway tunnel for their transportation by train from manufacturing plant to the assembly site.

Focusing on modelling and simulation (M&S), Figure 1 shows a timeline of M&S technology over the last 40 years. A relevant example from the simulation industry for persistence is the Distributed Interactive Simulation (DIS) standard which is widely used in connecting training simulator systems together, including in Live Virtual Constructive (LVC) applications. The DIS standard derived from previous work on SIMNET sponsored by DARPA and the US Army between 1983 and 1990. (Thorpe, 1995). DIS is an IEEE standard (IEEE 1278) originally promulgated in 1995, with version 7 published in 2015 (IEEE, 2015) and version 8 being approved now. Derived

standards like Compressed-D DIS (C-DIS) are also available to allow transmission of DIS version 7 packets over restricted bandwidth networks. (Simulation Interoperability Standards Organisation (SISO), 2024).

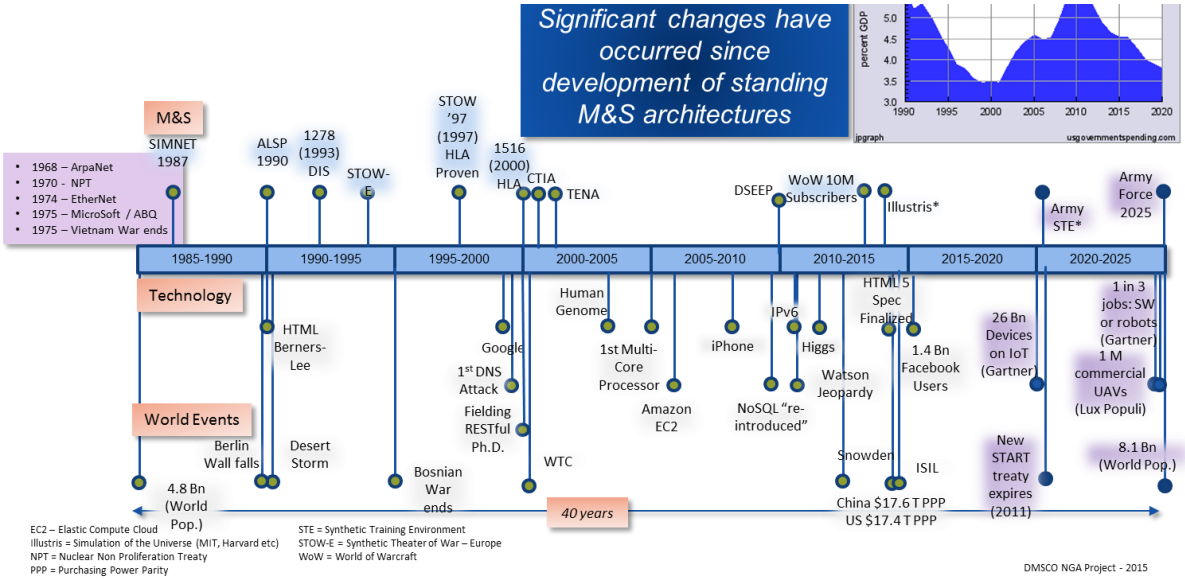


**Figure 1 – Interoperability standards timeline (courtesy Cole Engineering Services Inc.)**

Fundamentally, DIS is a packet-oriented communication protocol using the User Datagram Protocol (UDP) networking standard, to ensure 'wire compatibility' allowing the connection of homogenous or heterogeneous systems to each other using ethernet protocols. A monitor device attached to the network can easily examine the packets passing through it and analyze the data being sent.

In the implementation of a DIS network there is an implied distributed simulation architecture which classically looks like the diagram in Figure 2. This comprises separate computers with separate data, connected by some form of distributed local or wide area network with redundancy incorporated into its structure.

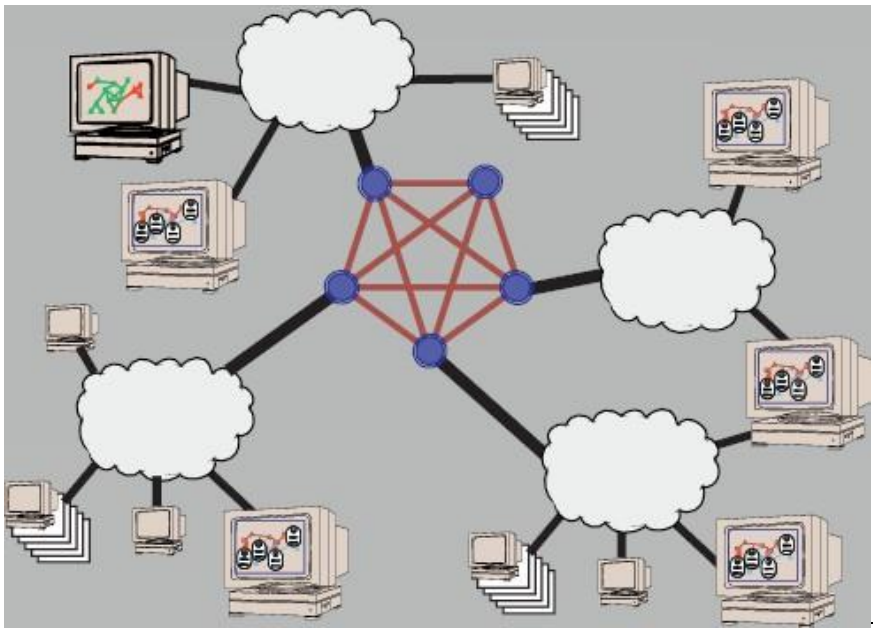

**Figure 2 - Typical DIS architecture implementation (O'Ryan, 1999)**

The diagram reflects the available technology and operating procedures of the time, for instance:

- Use of networks that are separate and generally not connected to the global internet to ensure fast interrupted transmission of data without concern of contention (use of UDP protocols to reduce latency), in 1995 the widely available standard was 10-Base-T providing only a 10Mbit/s capability over twisted pair cables
- Perimeter based security (physical barriers), with either no requirement to encrypt or the use of dedicated expensive hardware technology to encrypt data on the fly.
- Discrete computational nodes with limited performance. In 1995, Windows 95 was released, and typical high end PC hardware had a Pentium™ 90 processor providing about 100 million operations per second with 16 MB RAM and 500MB hard drive storage, generally with primitive 3D graphics performance.

The High Level Architecture (HLA) was designed to remove restrictions that were found in DIS. Introduced in 1996 it has gone through several iterations to the recent introduction of HLA 4 (IEEE, 14 May 2025) IEEE 1516-2025. Nevertheless, many applications of HLA are based on DIS compatibility enabled by the Real-time Platform Reference Federation Object Model (RPR-FOM) which is currently at version 3.

There is no doubt that HLA and DIS have proven their utility and value in distributed simulation applications over the last 30 years, with many dedicated professionals contributing to the development and use of the standards, forming a great community, along with organizations that provide tools either on a paid basis with support, or in some cases with open source repositories to allow academic and other access. The standards have been promulgated through international organizations such as NATO, to be required for simulation systems by those nations that adopt it, for example, STANAG 4603 in respect of HLA (NATO Science and Technology Organisation).

However, just like the example given on train gauges, it cannot be disputed that the foundation of DIS, HLA and their derivative standards are formed on an approach to a distributed simulation architecture which is 30 years old, based on technology that by today's standards, offered very limited computational, networking and storage performance. Some examples of the order of magnitude increase in performance of our typical PC computer, since the approval of the DIS standard in 1995:

- Processor performance: 6 Tera ($10^{12}$) floating point operations per second (TFLOPS) -Intel® Core Ultra 9 288V versus 100 million instructions per second (MIPS) – more than 6000 times increase
- Memory: 64 GB vs 16 MB – more than 4000 times increase
- Network: 10 GBit twisted pair ethernet vs 10MBit – around 100 times increase
- Disk storage: 20 TByte vs. 500 MByte – 40000 times increase

It is true that standards are not easy to develop and maintain, so they tend to persist, and it's easier to update a standard than it is to replace it. This is true within many communities and is not limited to the M&S ecosystem. Such is the weight of previous work developing standards, the legacy of successful implementation, the community of worthy experts, the capability of tools and the infrastructure around existing interoperability standards, it is certainly difficult to propose alternatives. 'Stockholm syndrome' (Namnyak, 2008) provides a colloquial analogy to the difficulty of changing our approach to interoperability standards to meet new challenges and updates in technological capabilities.

## OPERATING CONTEXT CHANGES

In 2025, as previously indicated, the demand for MSTO is growing. While the global market for the training use of simulation is growing year by year, the overall market for modelling and simulation for various operational needs, and the use of digital twins in both civil and military segments and applications is growing much faster – at a compound annual growth rate (CAGR) of more than 30% (Grand View Research, 2025).

There are a huge number of different applications for modelling and simulation and, much like other technological areas, the military share of the market is shrinking compared to commercial applications such as transportation, manufacturing, healthcare and the built environment (Figure 3). Certain applications such as the use of digital twins for Synthetic (or Digital) Test and Evaluation are becoming critically important due to the peer / near peer threat, which means that there is no military testing area on earth that is not being constantly watched by unfriendly sensor systems.

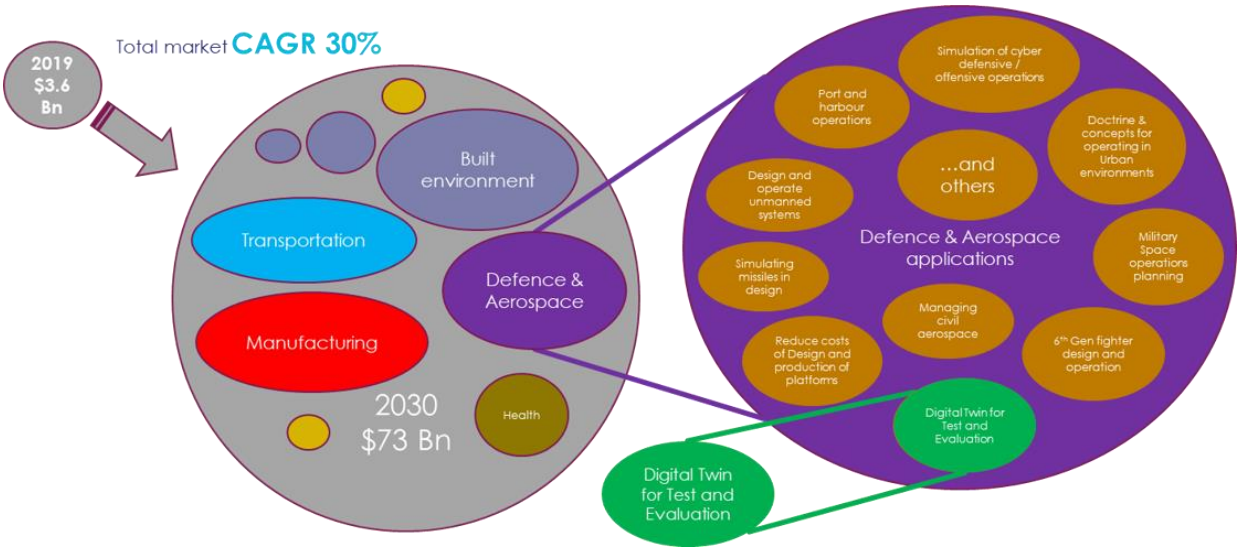


**Figure 3 - M&S and Digital Twin market segmentation and growth**

**Consequences of the new challenges on our MSTO systems**

The growing capabilities of peer and near peer threats mean that our solutions need to be resilient against physical attack and be reconfigurable to overcome degradation; particularly to support operational use cases, ensuring that key data is not lost. The value of the data in our systems means that we should ensure that its integrity is protected by strong encryption and with secured identity of users, to protect against both external and internal attack.

The changing nature of war means that our training systems need to be more mobile; work with operational networks and with limited edge computing, and not just be isolated at a training base, with data available to feed Artificial Intelligence tools (e.g. machine learning) to allow adaptive training to achieve operational dominance. There is a need to quickly bring data from operational lessons and adaptations into our training systems, ensuring they are capable of rapid adaptation. There is also a need to increase the use of digital twins and digital shadows to gather performance data and achieve real time or near real time feedback.

The advent of increased complexity in multi-domain operations leading to the requirement for a Systems of Systems (SoS) approach means that our MSTO interoperability standards need to be wider in scope, handling not just the components of distributed training simulators but in addition all kinds of operational standards, with rapid interchange of data. The exchange of data between different systems via interoperability standards should be more automated, reducing development and deployment time.

The need to handle the multiple dimensions of operations; not only in the physical space, but also in cyber and social dimensions, means that operational data of many different types needs to be analysed quickly and effectively against mission simulations to ensure that there is a complete operational picture which is abstracted and adaptable to inform decisions and reduce the ‘fog of war’.

The apparent stall in human cognitive performance improvements over time requires more effective human / machine teaming, informed by machine analysis of data, to reduce unnecessary cognitive load on human operators to give time for critical decisions to be made correctly.

It is no surprise that all the conclusions for change have a key element in them, *data*. In all our MSTO solutions we therefore need to change and center our approach around data – a *data-centric* approach. Data centric architectures are now actively being pursued across the defense enterprise in the US and in NATO, examples being the Next Generation Command and Control (NGC2) program, (Nesaw, 2024) and the NATO Data Centric Reference Architecture (NCIA, 2025).

## CURRENT ARCHITECTURES, APPROACHES AND ISSUES

Significant work has already been done within the simulator based training ecosystem to improve our approach to training system architecture and implementation, giving just three examples:

- The development of 'Modelling and Simulation as a Service' (MsaaS). (NMSG, 2025), an initiative for development of a service-based approach for M&S being undertaken for well over a decade within NATO.

- An understanding that our approach to security on legacy training devices needs to improve; including reworking of existing simulator software to move away from insecure programming languages like C++ to more memory safe languages like RUST; (Oey Kevin Andrian Santoso, 2023). (Mitchell, 2025)

- New standards to improve the interoperability of training and operational systems such as C2SIM (Command and Control Systems to Simulation Systems Interoperation) (SISO, 2020).

However there are significant issues that must be addressed; one example is the mandatory action for the USA government, including DOD, that data on federal systems must be encrypted and secured while in movement and at rest using Zero Trust Cybersecurity principles (OMB, 2022).

Although work has been done to try and refactor zero trust security paradigms on top of existing interoperability standards and tools (Patric Stout, 2024), in this case HLA, they do not fully address the requirements – for example, in the referenced case, handling the problem of dynamic identity revocation.

The author proposes that a more radical shift is needed in our approach to MSTO architectures, as well as taking advantage of the gradual steps described above.

For example, the reliance of artificial intelligence algorithms on large quantities of data implies that the data should be centralized for access, rather than spread across many different connected systems, typical in our current distributed simulation systems used for training.

Other challenges that need to be addressed for a modern MSTO environment include data silos, computational inefficiencies, limitations in processing large data sets, classification levels and intellectual property sharing concerns. These concerns are not limited to the MSTO environment, and there have been a few government initiatives around more modern architectures and paradigms for defense applications, particularly around the area of data and encouraging data-centricity.

In terms of a solution, the author proposes that adopting a 'data centric' approach may be a productive approach to mitigating the issues identified above, taking guidance from other parts of the defense enterprise.

## DOD DATA STRATEGY AND IMPLEMENTATION

The US DOD Chief Data and AI Office (CDAO) has been considering data centricity for some time and has published strategy and implementation guidelines which are described here. These guidelines apply across the whole DOD and so the M&S community is included in their scope and should carefully consider the implications of the strategic direction.

The DOD data strategy (US Department of Defense, 2020) contained key vision and principles for data centricity, it has focused on ensuring the following seven goals (also known as VAULTIS) are achieved:

1. Make Data **Visible** – Consumers can locate the needed data.
2. Make Data **Accessible** – Consumers can retrieve the data.
3. Make Data **Understandable** – Consumers can recognize the content, context, and applicability.
4. Make Data **Linked** – Consumers can exploit data elements through innate relationships.

5. Make Data **Trustworthy** – Consumers can be confident in all aspects of data for decision-making.
6. Make Data **Interoperable** – Consumers have a common representation/ comprehension of data.
7. Make Data **Secure** – Consumer data is protected from unauthorized use/manipulation.

Significant work has been done around data sharing, and the department has determined to follow a *'data mesh'* approach (Dehghani, 2022) rather than a *'data lake'* or *'data warehouse'*. There is a draft Data Mesh Reference Architecture (DMRA) which has been recently published (DOD CDAO, 2024) with 15 suggested baseline capabilities (Table 1):

**Table 1 - Data mesh baseline capabilities**

| Service | Data Mesh Service Title | Service Description |
|---|---|---|
| 1 | UID | Tool to provide an enterprise wide globally exclusive and unique reference identifier to track any object |
| 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 | Federated Data 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 |

In addition, the DMRA describes an operational viewpoint which describes how data and data teams can use the DMRA, including how heterogeneous mission specific data is transformed to answer specific questions (*data domains*). Data product teams then transform data and data assets into *data products*, logical units which contain all components to process and store domain data and make them available to other teams. Figure 4 shows the operational concept description from the DMRA and Figure 5 how it might be implemented in a services context.


**Figure 4 - DMRA operational concept description (DOD CDAO, 2024)**

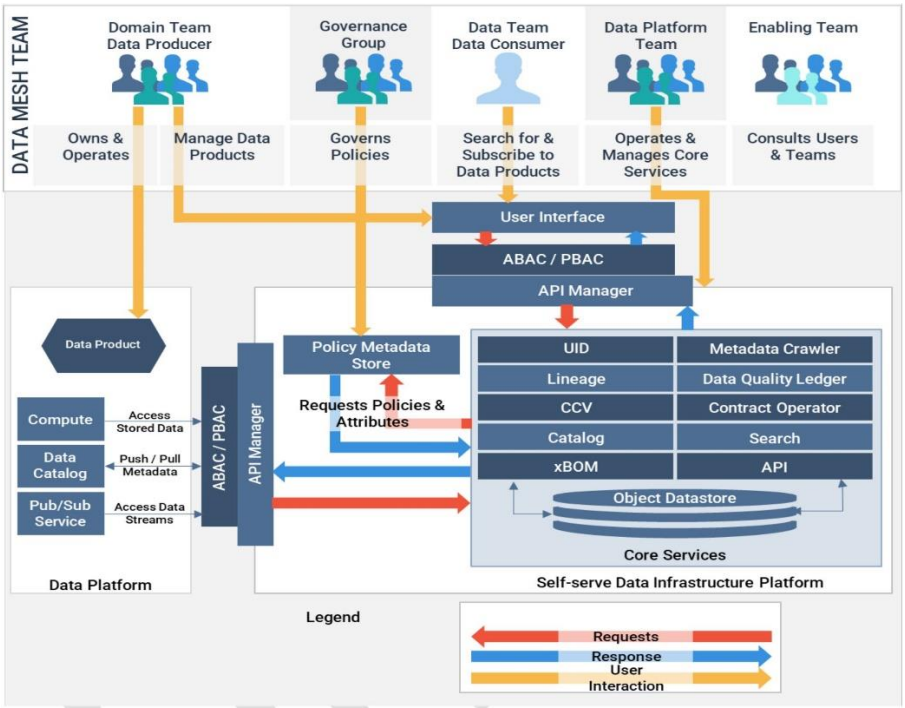


**Figure 5 - DMRA services context description (DOD CDAO, 2024)**

## FROM INTEROPERABILITY-CENTRICITY TO DATA-CENTRICITY

At first glance, concepts like the DMRA look very alien to the way MSTO systems have been constructed over the past 30 years since the early days of SIMNET. (Thorpe, 1995). There are however similarities in approach which show that the MSTO community understands the need to change. Some examples of change are identified here:

- The MSaaS approach promulgated by NATO (NMSG, 2025) – brings in the concept of a service-based architecture implemented with micro-services and containerization. There are established concepts of governance, and the need for catalogs, and repositories of models which are provided to users – essentially coming closer to data products.

- There are signs that industry products and services for MSTO from some vendors are gradually moving to a data centric approach, with an increasing use of artificial intelligence techniques to manage incoming data streams, provide analysis of performance and enable other useful metrics for adaptive learning.

- The increasing application of digital twins, for example in platform development and synthetic test and evaluation, are bringing in new concepts of interoperability into the MSTO environment and interoperability standards from different organisations. There is a growing need for developing simulations for different applications that have a 'single source of truth' approach to models.

Figure 6 shows a typical distributed training simulator application where there is an HLA/DIS interface connecting systems together and some form of cloud-based AI performance analysis. This is an interoperability-centric approach, data is distributed in many places, is most likely duplicated to allow some AI analysis (depending on what data is transmitted), with the data not easily available outside the security perimeter for other users:

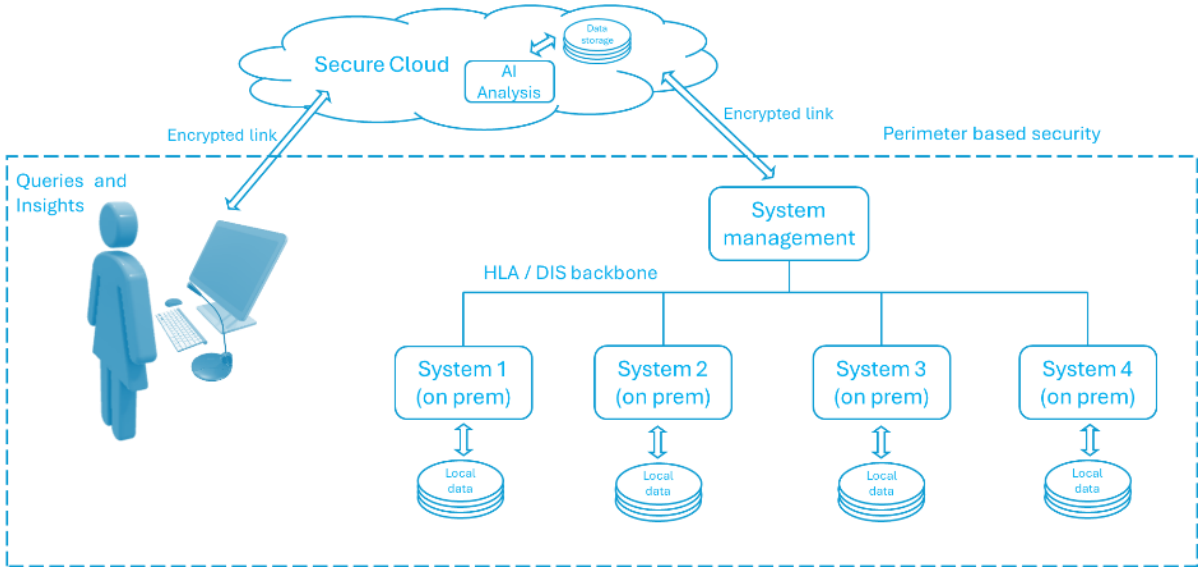


**Figure 6 - Typical training simulator architecture with AI enabled data analysis**

Figure 7 shows how the distributed training simulator might be integrated with a data-centric approach, using the DMRA as an example. The data within the system is available as a Data Product, distributable to everyone who has permission to access it, with central management including security, access control, search and governance of data products and the data infrastructure platform. This would more easily enable the speedy utilization and re-use of data, allowing enterprise access to all the information in the system, not just that which is initially thought to be valuable. With the whole of the system available through the data backbone, reconfiguration of the training simulator with different scenarios and applications would also be more easily possible to handle rapidly changing operational needs.

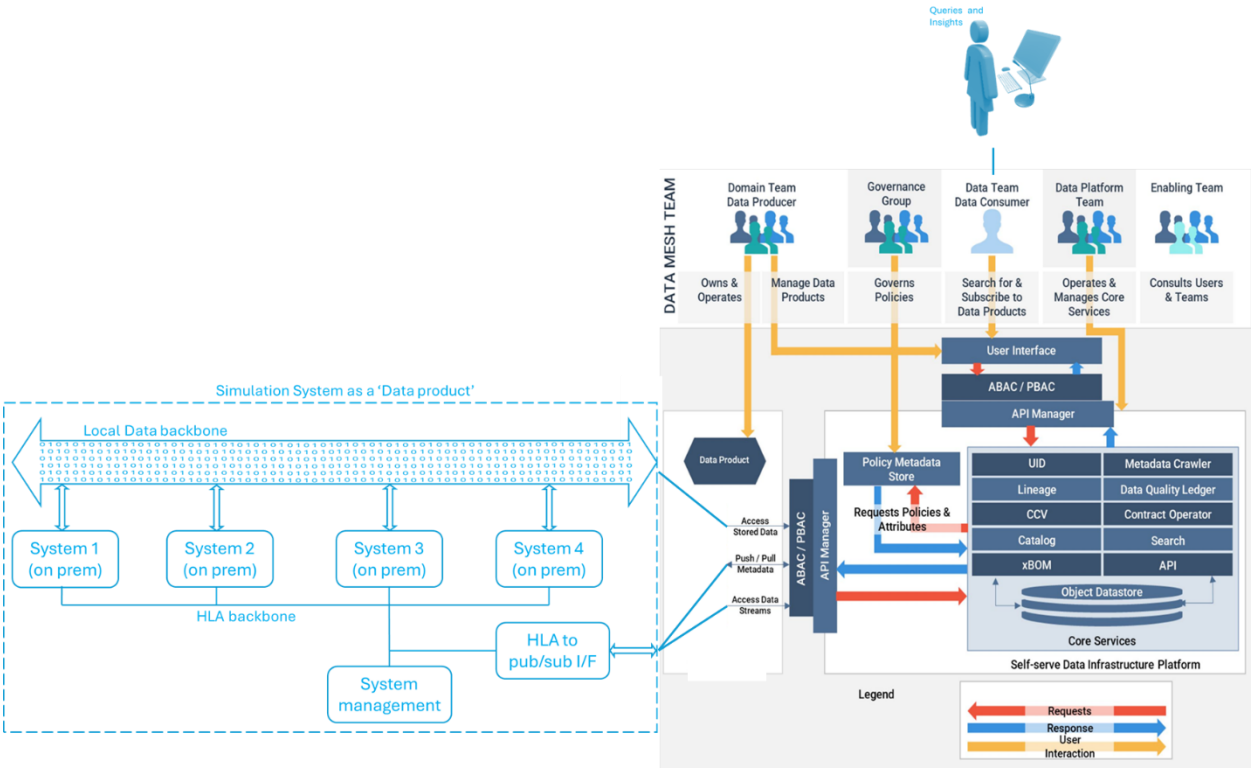


**Figure 7 - Previous training simulator system example reconfigured as a 'Data Product'**

In this scenario, there is still a specific place for legacy interoperability standards, in this case forming a publish/subscribe interface between the simulator and the Data Infrastructure platform API manager.

## RECOMMENDATIONS FOR CHANGE

The advent of data-centricity into MSTO could be revolutionary in its extent. The longevity of typical training simulator systems means that a wholesale change in approach is unlikely to happen quickly, and any change could be costly in terms of finance and resources. Therefore, recommendations in terms of changes in policy and standards must take these constraints into account, ensuring an initial experimental and graduated approach. While the scope of this paper does not allow too much detail, some recommendations are provided, split into three parts: policy, standards, and management of acquisition.

### Policy recommendations

1. Conduct in-depth experimentation to show that a typical training simulator system can be integrated into a system based on the DMRA. This experimentation should include small and large companies, academic institutions and other stakeholders in the training simulation community and operational simulation community.
2. Consider working with allies (for example within NATO or bilaterally) to ensure that there is commonality in approach around data-centricity, even if implementation differs.

### Standards recommendations

1. Work with existing standards organisations and stakeholders to ensure a wide survey of existing M&S standards is undertaken to determine their continued viability within a data-centric ecosystem.
2. Determine existing and new standards that should be promulgated in implementing the DMRA, and other alternative architectures, with suitable experimentation to ensure the standards are robust and can gain both domestic and international acceptance by allies (for example using NATO research task group activities).

**Management of Acquisition**

1. Establish a catalogue of existing systems to be migrated along with a roadmap, prioritising around the expected benefits to the war-fighter from migration.
2. New and replacement MSTO systems should be organised around a data-centric approach, ideally conforming with the concepts of the DMRA, but retaining suppliers' ability to retain the capacity to innovate and develop systems around the DMRA paradigms.
3. Critical legacy MSTO systems should be migrated to a data-centric approach over time depending on requirements and budgets.
4. Take account that less critical MSTO systems will achieve a partial or zero compatibility, due to the cost of transition.

## CONCLUSIONS

There is an urgent need to move from an interoperability-centric to a data-centric approach for MSTO systems to gain the full benefit of advances in security and identity, artificial intelligence, data and information management and advances in computing, storage and communication technologies that were only a dream 30 years ago.

Data centricity will be a revolutionary change from our current methods of managing distributed simulation and will require a break with long-held paradigms and interoperability standards which could hold us back from the comprehensive changes needed.

Given the change in approach is significant, and likely to lead to benefits across the international M&S community and not just for US DOD, the author recommends that collaborative research and experimentation within the NATO modelling and simulation group and within existing standards organizations like SISO, would ensure that the benefits of a data-centric approach to M&S could be obtained by allied nations, and would also ensure buy-in from industry suppliers and other partners.

The expert international community and stakeholders – government, industry and academia - who develop, manage and support the current approach of interoperability standards for MSTO have dedicated huge efforts over the last 30 years since the introduction of DIS to support the warfighter. They will need to be supported through the transition and have great capability to support new ways of working, not least because existing interoperability standards will need to be maintained and updated to support the DOD mandated data enterprise models, as well as ensure support for legacy systems persists for the next couple of decades.

## ACKNOWLEDGEMENTS

The author would like to acknowledge the ideas, assistance and support of Erica Dretzka of the US DOD Chief Digital and AI Office (CDAO) in the preparation of this paper.

## REFERENCES

Army Science Board. (2019). *Multi Domain Operations.* Washington, DC: Office of the Deputy Under Secretary of the Army.

Dehghani, Z. (2022). *Data Mesh - Delivering Data-Driven Value at Scale.* O'Reilly Media, Inc.

DOD CDAO. (2024, 03). Data Mesh Reference Architecture version 2.6. Washington, DC, USA. Retrieved from https://media.defense.gov/2024/Mar/15/2003414274/-1/-1/1/dmra_paper.PDF

DOD News. (2020, 03 10). *Near-Peer Threats at Highest Point Since Cold War, DOD Official Says*. Retrieved from Defense.gov: https://www.defense.gov/News/News-Stories/Article/Article/2107397/near-peer-threats-at-highest-point-since-cold-war-dod-official-says/

Gabriel, D. G. (2000). *"Railroad Gauge"*. Retrieved from Discover Live Steam: https://discoverlivesteam.com/magazineold/34/34.html

Global Data. (2024, 02 28). *US military simulation spending to exceed $26 billion annually up to 2028.* Retrieved from Globaldata.com: https://www.globaldata.com/media/aerospace-defense-security/us-military-simulation-spending-to-exceed-26-billion-annually-forecasts-globaldata/

Grand View Research. (2025, 05 29). *Digital Twin Market Size And Share, Industry Report, 2030*. Retrieved from Grand View Research: https://www.grandviewresearch.com/industry-analysis/digital-twin-market

Hoffman, F. G. (2017). Will War's Nature Change in the Seventh Military Revolution? *The US Army War College Quarterly: Parameters no. 4*, 19-31.

IEEE. (14 May 2025). "IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)--Framework and Rules". *IEEE Std 1516-2025 (Revision of IEEE Std 1516-2010)*, 1-40.

IEEE. (2015, 11 6). IEEE Standard for Distributed Interactive Simulation (DIS) -- Communication Services and Profiles. *IEEE Std 1278.2-2015 (Revision of IEEE Std 1278.2-1995)* . IEEE.

James R. Flynn, M. S. (2018). IQ decline and Piaget: Does the rot start at the top?,. *Intelligence, Volume 66*, Pages 112-121.

Mitchell, J. (2025). Simulator of Theseus. *I/ITSEC conference* (p. Paper 25218). Orlando, Florida: National Training and Simulation Association.

Namnyak, M. &. (2008, 02). 'Stockholm syndrome': Psychiatric diagnosis or urban myth?'. *Acta Psychiatrica Scandinavica*, pp. 1-8.

NATO Science and Technology Organisation. (n.d.). *STANAG 4603 (HLA).* Retrieved from Higher Level Architecture (HLA) standarisation: https://www.sto.nato.int/publications/STO Technical Reports/RTO-MSG-033/$MSG-033-ES.pdf

NCIA. (2025, 05 30). *Data Centric Reference Architecture for the Alliance*. Retrieved from NATO Digital Staff: https://nhqc3s.hq.nato.int/apps/DCRA_Report/index.html

Nesaw, S. (2024, 12 23). *Fusing Intel and EW Data into the Army's Data Centric NGC2 Architecture*. Retrieved from Army.mil: https://www.army.mil/article/282276/fusing_intel_and_ew_data_into_the_armys_data_centric_ngc2_architecture

NMSG. (2025, 08 29). *Allied Framework for Modelling and Simulation as a Service (MSaaS)*. Retrieved from NATO M&S as a Service: https://www.sto.nato.int/the-collaborative-programme-of-work-cpow/modeling-and-simulation/nato-modelling-simulation-group/nato-ms-research-development/nato-ms-as-a-service/

Oey Kevin Andrian Santoso, C. K. (2023). Rust's Memory Safety Model: An Evaluation of Its Effectiveness in Preventing Common Vulnerabilities. *Procedia Computer Science, Volume 227,* (pp. 119-127). Elsevier.

OMB. (2022, 01 26). *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.* Retrieved from whitehouse.gov: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

O'Ryan, C. &. (1999). Applying a scalable CORBA event service to large-scale distributed interactive simulations. *Proceedings. Fifth International Workshop on Object-Oriented Real-Time Dependable Systems,* (pp. 67 - 74). Monterey, CA: IEEE.

Patric Stout, T. v. (2024). Zero Trust security in cloud-based simulation. *I/ITSEC conference* (p. Paper 24189). Orlando, FL: NTSA.

Simulation Interoperability Standards Organisation (SISO). (2024, 1 11). *SISO-STD-023-2024 Standard for Compressed-Distributed Interactive Simulation (C-DIS).* Retrieved from Simulation Interoperability Standards Organisation (SISO) - Standards Products : https://www.sisostandards.org/resource/resmgr/standards_products/siso-std-023-2024-c-dis.pdf

SISO. (2020, 04 25). *SISO-STD-019-2020: Standard for Command and Control Systems - Simulation Systems Interoperation.* Retrieved from Standards Products: https://www.sisostandards.org/resource/resmgr/standards_products/siso-std-020-2020_lox-c2sim.pdf

Thorpe, D. C. (1995). "SIMNET: the advent of simulator networking". *Proceedings of the IEEE, vol. 83, no. 8*, 1114-1123.

US Department of Defense. (2020, 10 08). *DOD Issues New Data Strategy*. Retrieved from defense.gov: https://www.defense.gov/News/Releases/Release/Article/2376629/dod-issues-new-data-strategy/