‘In Through the Out Door’–
Security and Identity Concerns for Military Digital Twins

Simon G. Skinner BSc. (Hons) CEng FIET
Thales Training & Simulation
Crawley, West Sussex, UK
Simon.Skinner@uk.thalesgroup.com

ABSTRACT

Digital Twins are representations of real world systems with data exchange between the real system and the synthetic digital representation – with uses in manufacturing (Industry 4.0), and for operational use in aerospace and in civil infrastructure and Government contingency planning. There are many military use cases for Digital Twins that include training, but also test and evaluation, concept development and decision support.

Digital Twins are becoming larger and more complex ‘systems of systems’ with emergent properties appearing from interactions of models and data, making them more difficult to analyse and support. Models and data in the Digital Twin are now often using public and open data sources, cloud based storage and computing resources, and Internet of Things (IOT) devices communicating via the internet; with access to the twin using open Application Programming Interfaces (APIs). These all provide opportunities for penetration by unfriendly actors in order to disrupt the twin’s operation or reveal unauthorized intimate detail of the real world system being modelled.

Traditionally, military applications use the ‘System High’ approach where dedicated classified networks are used to protect insecure simulation interface protocols for military operations. This cannot be sustained for most civilian Digital Twins and even in defence applications (e.g. operating across the multinational NATO alliance), there is a need to be able to work in situations where the authenticity of data and models cannot be guaranteed. Some military Digital Twins are also likely to need to rely on unsecured public data sources and networks.

In this paper the author proposes a new approach to security and identity in our modelling and simulation systems using an Information Based Security Architecture / Zero Trust Architecture that should be applied to ensure that Digital Twins will operate safely and securely in both military and civilian contexts.

ABOUT THE AUTHOR

Simon Skinner has nearly 30 years' experience in the training and simulation industry and was for 11 years the CEO of XPI Simulation Ltd. (now a Thales group company). He is the Product Line Manager for Simulation Capabilities for the worldwide Thales Training & Simulation business.

Simon has an honors degree in Electronic Engineering, is a Chartered Engineer recently elected as a Fellow of the UK Institution of Engineering Technology (FIET). As well as being an I/ITSEC subcommittee member, he also serves on the Simulation Interoperability Standards Organization (SISO) Standards Activity Committee (SAC) and is appointed by UK Ministry of Defence (MOD) as a national member of the NATO Modelling and Simulation Group (NMSG).

He is a recipient of the MOD Chief Scientific Adviser’s commendation for research in military driver training, and is the author and presenter of several papers at previous I/ITSEC conferences; including one presented at an I/ITSEC ‘Best papers from around the world’ special session.

'In Through the Out Door'– Security and Identity Concerns for Military Digital Twins

Simon G. Skinner BSc. (Hons) CEng FIET
Thales Training & Simulation
Crawley, W. Sussex, UK
Simon.Skinner@uk.thalesgroup.com

INTRODUCTION

The use of simulation and modelling to characterize activities taking part in the 'real world' is not new; especially in the military and space context where computer simulations have been used for decades for applications including training, analysis and decision support.

However; there is now extreme interest in 'Digital Twins'; the formation of models and simulations that interact with real world entities through the exchange of data. Described in the book 'Mirror Worlds' (Gelernter, 1991), the terminology 'Digital Twin' was described in a NASA technology roadmap report (Piascik & et al., 2010). Applications for Digital Twins have expanded beyond the original niche in space and military operations to include design, production, manufacture (Industry 4.0) and support with end uses in automotive and transport, consumer goods, agriculture, manufacture, energy and utilities which will be much larger than the military sector. The market for Digital Twins is expected to reach $86 billion in 2028 (Grand View Research, 2021).

Security threats and issues around identity including user authentication are problems that are not confined to the military space; commercial organizations are equally at risk to their operational capability due to a wide range of threats, both external and internal.

Over the years various approaches to securing military training simulators have been developed which have satisfied requirements to address security and identity concerns. However, the use of modelling and simulation for purposes other than training is increasing across many nations, with a growth in highly complex and distributed 'system of system' Digital Twins which aim to replicate in a virtual space:

- Complete hierarchies of military systems and platforms, e.g., the US Joint Simulation Environment. (Menke, 2019)
- The whole earth environment, e.g., Destination Earth (DestinE) (European Commission, 2021)

And in the last year, governments around the world have been using a variety of epidemiological models along with data on people and transportation movements and social activities to predict the effect of different controls and restrictions placed on their populations during the COVID-19 pandemic.

These extraordinarily complex systems will source and access sensors, environmental and performance data, models and computing resources from many different places and authors, replicating and reusing existing content which might have a variety of operating and use licenses and conditions as well as differing levels of fidelity, accuracy, and security classification both within and outside secure environments. They will be accessed by many different users for a variety of purposes, storing vast quantities of information including personal data, generating analysis and insights that are highly valuable. The combination of models within the Digital Twin may lead to emergent behaviors and unexplainable outcomes. Outputs from the Digital Twin may change the operation of real systems including military and civil platforms and infrastructure at speeds beyond the capability of human analysis.

The use of the phrase 'In through the out Door' in the paper title is to indicate that threats in terms of security, integrity and identity to these systems may not easily be thwarted. Security threats are clearly manifold; including risks of exposing operational capability, intellectual property, and opening attack channels through the virtual systems into the physical system. Massive uncontrolled data sets without specific identity controls make the 'Need to Know' principle hard to enforce. Different approaches to security and identity will need to be carefully considered to improve system resilience in the face of these threats, instead of relying on traditional methods which do not respond quickly enough to changed methods of working and dynamic asymmetric threats. Since the scope of the problem is vast, within this paper the author will not be able to provide a complete solution to the issues raised but will, by indicating the likely effects on government modelling and simulation policy, simulation standards and acquisition processes, stimulate further discussion and solution development.

Terminology and definitions

Throughout this paper the term ‘Digital Twin’ will be used rather than the alternatives that might be found in literature such as ‘data doppelganger’ or ‘virtual twin’.

The Digital Twin Consortium provide a useful glossary of terms in this area. Their definition of a Digital Twin is: ‘*A virtual representation of real-world entities and processes, synchronized at a specified frequency and fidelity.’* (Digital Twin Consortium, 2021)

OVERVIEW OF DIGITAL TWINS

A simplified concept of a Digital Twin is shown in Figure 1. There is a virtual representation of a physical object within some form of computational structure. There is an exchange of data or information from the physical object to the virtual object and vice versa. It is also possible that the virtual object can define the construction of the physical object through a design and manufacturing process.

Bringing the concept into the more familiar space of training and education, as an example, it can be shown that a flight simulator used for rotary wing training is essentially a special case implementation of a Digital Twin (Figure 2). The data from the real helicopter – for example the flight model, information about controls, sensors and communications often forms the Original Equipment Manufacturer (OEM) data pack supplied to the simulator manufacturer. The output from the simulator – a trained pilot - forms part of the overall rotary wing flying system.

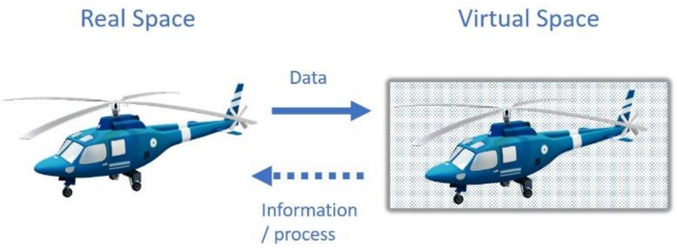

Figure 1 – Digital Twin concept

The flight simulator system can of course be used for other purposes instead of training; for example, for developing alternative concepts of operation, or for improving the way the real helicopter operates; this might be by testing simulated changes to the airframe, sensors, flight computer user interface or many other aspects of the vehicle’s operation.

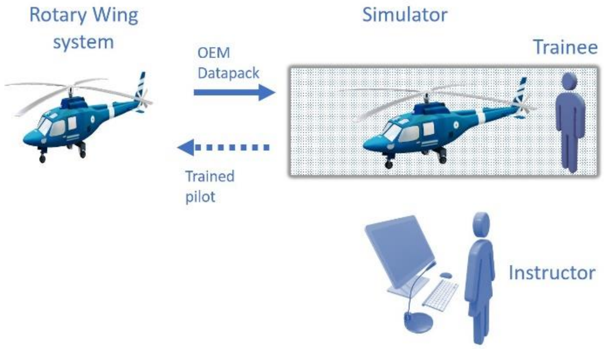

Figure 2 - Rotary Wing training simulator example

Using the OEM data pack within the Digital Twin can help ensure the simulator stays current with the aircraft software, as well as ensuring that responses to unexpected stimuli match the real aircraft.

For experimental or design purposes, the overall simulation may communicate internally with individual simulated components in a ‘system of systems’ approach, or directly with real elements (for example sensors and effectors) in the real platform (Hardware in the Loop or HWIL). These sensors and effectors in their turn will require data - sourced from either the real space or virtual space - for example terrain and atmospheric conditions, electromagnetic spectrum activities, and other actors like platforms and human entities. Essentially this is becoming a fully featured Digital Twin (Figure 3).

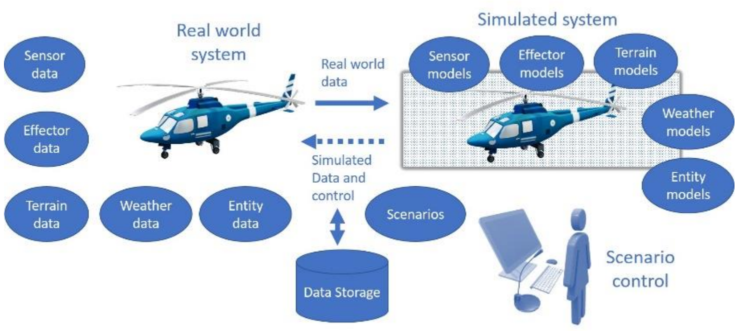

Figure 3 - Experimental simulation system example

Clearly the issue of accuracy and fidelity of the external data being used by the Digital Twin is important to providing useful results. Taking the example of the tactics of a simulated 'red force' actor, if the movements made by the actor are not realistic then any counter activity stimulated in the simulated platform under test won't necessarily provide the right response when the platform is operating in the real world. The incoming data sources will also need to be correlated with each other; there is little point having a high-fidelity synthetic terrain representation if the associated computer generated force ground elements are not correlated with it (commonly known as 'floating tanks' for most readers).

A real benefit of implementing Digital Twins is the use of the data gathered through the life cycle of a particular platform or capability from its initial concept through to its eventual disposal – (Concept, Assessment, Demonstration, Manufacture, In-service, Disposal – CADMID), so that it can be used to reduce design issues, so improving reliability, quality and effectiveness and hence reducing lifetime cost (Figure 4). The repositories of information created and linked across time and lifecycle stage are commonly known as a *'Digital Thread'*. The ability to use a Digital Twin in Model Based System Engineering with the data it produces to design and implement a verifiable, reliable, and resilient platform with less time and rework is a key benefit and value of the approach.

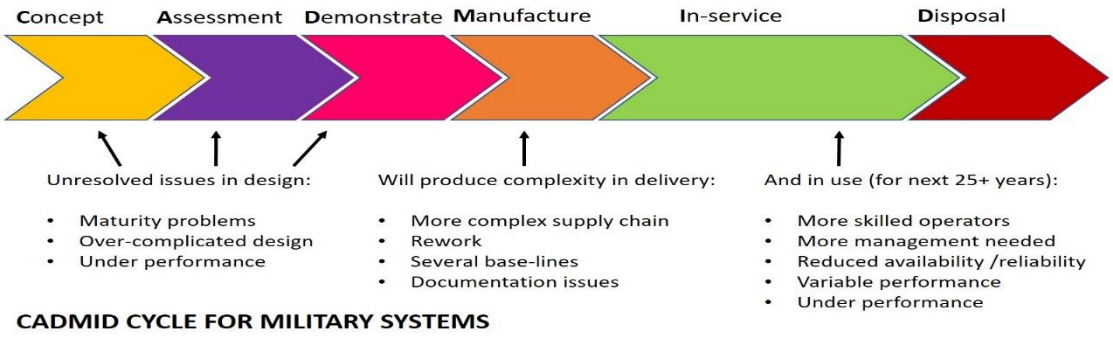

Figure 4 - CADMID life cycle

As a result of generating a digital thread, vast quantities of data will be produced – sometimes referred to as a '*Data Lake'*. In a complex system, some data may be stored in different places and be accessible via cloud storage systems. Some data may be useful, other data might be generated because of a failed test which results in a virtual redesign and is seen as less valuable. However even this data might contain patterns which could indicate trends over time. This approach is sometimes referred to as *'Big Data'* (Figure 5). Algorithms that tag, sort, and manipulate data are vital to finding key trends within complex manufactured systems. Artificial Intelligence Machine Learning techniques are being used to detect these data patterns within Digital Twins. (Liu, Meyendorf, & Mrad, 2018)

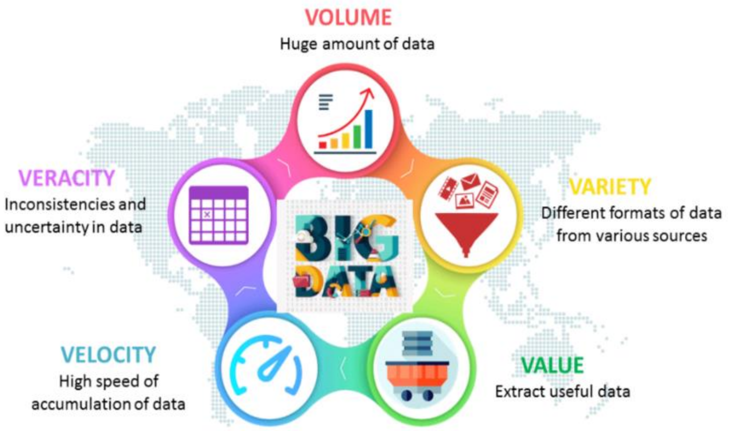
VOLUME
Huge amount of data
VERACITY
Inconsistencies and uncertainty in data
VARIETY
Different formats of data from various sources
BIG DATA
VELOCITY
High speed of accumulation of data
VALUE
Extract useful data

Figure 5 -'Big Data' approach to data management

Key take-away points about Digital Twins

- While simple Digital Twins have some benefit, within the military context, complex 'System of systems' Digital Twins will be required to ensure a platform is tested in all types of conditions. Ever more connected and autonomous systems require a new engineering approach as traditional methods are no longer feasible for coordination, cost, time, safety and security reasons.

- The human component within Digital Twins is often forgotten but is a vital part of most military systems whether as an operator or as part of the complex system 'human within the loop'.

- More complex Digital Twins will need multiple incoming data sources that will need to be accurate and correlated to provide correct results.

- The amount of data stored during the lifetime of the Digital Twin is large and is varied, storage of this data may be distributed, and some of the data produced might be highly valuable, being used to predict patterns and trends of interest. This value may not be visible at inception but become apparent later in the system lifecycle.

DIGITAL TWIN SECURITY AND IDENTITY CONCERNS

The UK, USA and allied governments within NATO are moving to new concepts of warfare where traditional kinetic activity warfare is replaced by political and cyber activity warfare where allied data and computing assets are regarded as high value targets to be attacked by adversaries of various kinds. (Carter, 2021)

Some security and identity concerns around the growth of Digital Twins are described; within the limited scope of the paper it is not intended to be an exhaustive list:

Public data sources

Some very useful and accurate real time data sources regarding population and traffic movements are aggregated, are publicly available and may be useful within a military use Digital Twin. For example, Automatic Identification System (AIS) and Automatic Dependent Surveillance–Broadcast (ADS–B) provide information on civil maritime and aviation movements. Some data is highly aggregated to produce an effective Digital Twin – for example google maps produces traffic density forecasts on major roads across the globe including a future predictive capability. These data sources being public in nature are also available to adversaries, with data from a fitness app accidentally showing information about allied military capabilities and activity (Guardian Media Group, 2021) and Figure 6.

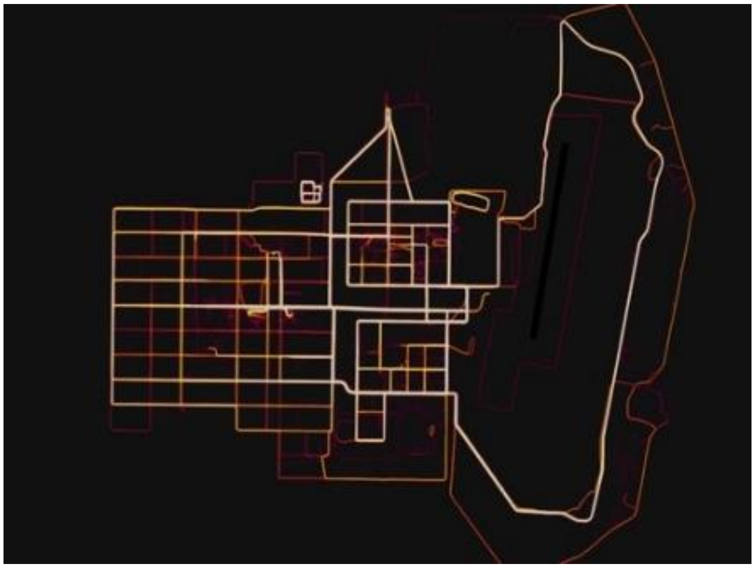

Figure 6 - 'Strava' map of US military facility - Guardian Media Group

Ownership and storage of data

Data that is required for operation may not be easily accessible by the Digital Twin. For example, OEM originated data may be available via a license and can only be accessed remotely with information being stored remotely from the Digital Twin instantiation and passed when required via a data interface. Such data may be subject to payment on a subscription or 'pay-as-you-go' model.

While many military organizations are moving to a model where data is owned by the contracting party with the aim of reducing recurring spend on data and giving more control over it, often the design authority role remains with the OEM with consequent payment for any changes in the data.

In a complex system of systems where multiple Digital Twins are connected, then different OEM data streams may be required leading to issues about competition and selective availability of the data.

Additional issues present due to the inclusion of personal data in Digital Twins; this might relate to the performance (or otherwise) of personnel modelled in the twin or specific information (e.g. medical) that is protected by law and which needs special treatment.

Data Aggregation and analysis

The tendency for the aggregation of data within a complex system of systems Digital Twin provides excellent capability for analysis and insight. Machine learning techniques could find emergent patterns of behavior which would be extremely useful. The corollary is that the aggregation of data is also extremely appealing to an adversary that could conduct similar analysis should they have access to that data.

Geographic proximity threat from Digital Twins

Where Digital Twins are being set up by civilian authorities then these twins can pose a threat to nearby military facilities. An example of this is a coastal municipal authority setting up a Digital Twin to enable unmanned aerial system activities for parcel delivery and model 5G radio access, transport, and marine traffic infrastructure with free and open access to all in order to improve employment and skills in a traditionally deprived area. While there is no physical connection an adversary might use this Digital Twin to attempt to gain information on the nearby naval base.

User access control, model maintenance and reuse

The typical life of a military platform may be greater than the working lifetime of people who support it, and the number of people who have access to an extended Digital Twin may be large. In this context, maintaining the proper controls of access and documentation around the components of the Digital Twin may be challenging – ensuring that the correct people have access, and that knowledge is maintained is a common challenge within most industries but even more so when there is a requirement to keep the Digital Twin current over an extended period of time. Reusing simulations and the associated models will be difficult unless they are well designed and maintained by qualified personnel.

Financial management

A Digital Twin only creates value through its use. Costs are incurred in sourcing data to it and for the concentration of compute and data storage use to make it work. Data results including analysis will be a source of income and value. Thus it is necessary to meter and account for this usage which will generally accrue in small amounts and be charged on an accrued basis in an automated fashion. Apart from the issues around securing payments, detailed analysis of charge logs and invoices may provide an adversary information about the activity of the Digital Twin; for example if there was information included about the geographical location of data access.

Interoperability standard insecurity

As simulations contained within Digital Twins connect to each other to communicate data it is natural to use existing simulation interoperability standards like Distributed Interactive Simulation (DIS) - IEEE 1278.1-2012 and Higher Level Architecture (HLA) - IEEE 1516-2010 to form the interconnection. Unfortunately, both of these protocols rely on the bearer networks to be secure and they have very little control over ensuring the identity of participants and to prevent ‘man in the middle’ attacks where data might be accessed by an intruder on the same network; although HLA is slightly more secure than DIS. DIS packet analyzers are readily available. Historically the DIS protocol was produced at a time (1995) when compute power was one ten-thousandth the performance available on today’s mobile phones, 100Mbit Ethernet was just being introduced and low latency was preferred over encryption and identity certification; the protocol has not been updated to account for technology improvements; and indeed is being extended to provide wireless communication between live and constructive assets in test and evaluation simulations (SISO Inc., 2021)

Model fidelity and sourcing

The increase in the availability and utility of open source software libraries has led to their inclusion in more and more models. There is a danger that untested or unverified libraries of software may be incorporated into models that inadvertently get used in system of system Digital Twins or in the source data these systems rely on. These models may contain accidental errors and unexpected behaviors, but additionally there may be specific weaknesses which an adversary may use to disrupt a Digital Twin, corrupt its operation or to extract useful data.

POTENTIAL SOLUTIONS

‘System High’

In this situation, the Digital Twin’s entire network, physical assets and all the users on it will be operating at a predetermined security level which is decided by the security level of the most highly classified asset. Also known as a Perimeter-Based Architected Network (PBAN), generally all compute resources and data storage will be located on the same network and protected by the security protocols associated with that network. Access to the network and export of data are strictly controlled.

Advantages of this approach are:

- Any insecurity in simulation protocols does not cause a problem as the network itself is secure from penetration and access from unauthorized parties
- Data generated by the system is protected as it is stored securely and accessed on protected computer systems
- Physical military assets are protected from external access through the Digital Twin’s network
- Users of the Digital Twin are authorized and monitored

Figure 7 shows the PBAN approach in action in the aviation based Digital Twin example.

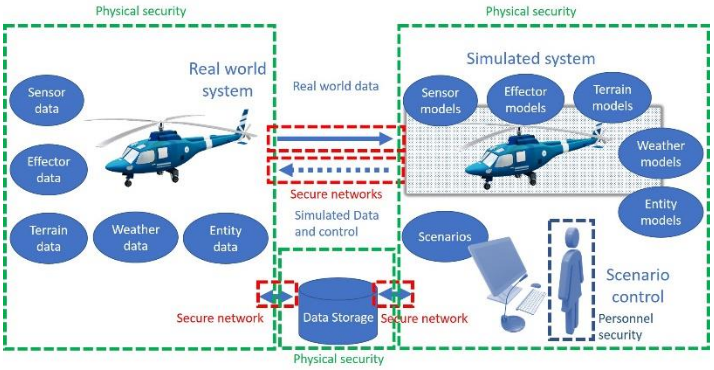

Figure 7 - Perimeter Based Architected Network example

The problems of this approach on a Digital Twin operating with classified models are well known and include the following:

Increased expense

The network must be physically protected, isolated from other networks, and formally accredited and people and computing systems accessing the network must be authorized and monitored. Any data leaving the network (and most likely data entering the network) must be checked; in some cases manually. This adds expense to the operation of the Digital Twin.

Specific investment needed for the engineering and support of the Digital Twin and associated tools is likely to be expensive as it cannot achieve the economies of scale that commercial activities can obtain.

Reduced flexibility and composability

New paradigms of connectivity, Internet of Things (IOT) devices, trusted interoperable communities, the pace of the evolving cyber threat (and therefore the need to adapt to combat) are imperatives that require rapid change. In a PBAN system any changes to the configuration of the Digital Twin would need to be approved, for example through Configuration Control Boards (CCB); this takes time – especially in a classified environment, and reduces the flexibility of the system to adapt to configuration changes; these are likely to be frequent in any non-trivial application meaning that a ‘System High’ approach will be extremely inefficient.

Limited expertise and tools
The pool of expert staff able to operate and develop the Digital Twin is reduced as these staff members must be cleared and authorized. This limitation also applies to tools where it would be necessary to assess each tool in use, with commercial off the shelf items or models generated in certain countries subject to severe limitations in use.

Data analysis
The analysis of large quantities of data will require algorithms that run locally within the secure space. Artificial Intelligence Machine learning systems rely on learning using large data sets and powerful computing resources which may not be available in a system with specifically limited resources, and potentially may have issues in terms of performance and reliability if data is unreliable or unduly filtered before ingestion, or if the system has been compromised through a back door. (Figure 8).

Figure 8 - 1983 vintage fictional Digital Twin system (WOPR) – 'Wargames' © United Artists

Sharing and collective activities
Where a Digital Twin is being used in distributed multinational or collective events, it can only be used at the lowest level of classification of any of the players; making it difficult to use for 'real world' applications and thus limited in terms of its utility.

Unscalable and impracticable
While 'System High may work for well bounded activities, plans to scale up to form Digital Twins of a national or multinational collective military force, or to provide a Digital Twin of an entire continent do not look achievable without vast investment of resources and time.

Geographic proximity threat
Military systems that are classified may still be threatened by a civilian operated or unsecured Digital Twin that overlaps geographically or which accesses data and aggregates this to provide an indication of military intent.

'Multi-Level Security'

Multi-level security, where a Digital Twin or simulation operates with some aspects at one classification, and other aspects at a higher or lower level has often been promulgated as a solution for operating distributed simulation across different classification levels and across computing clouds (including public clouds) but there are implementation difficulties in practical terms (Watson, 2012), and many of the problems listed above are the same.

In addition, problems such as multiple copies of models operating at different fidelities and classifications causing 'fair fight' issues are recognized in these types of systems.

A DIFFERENT APPROACH

There is a newer and different approach to enable a secure Digital Twin architecture that provides high assurance security, known as Information Based Security Architecture (IBSA) (Sirius / CSIIS, 2021), or 'Zero Trust Architecture' (ZTA) (National Institute of Standards and Technology, 2020). With an IBSA/ZTA approach, all information and all transactions of that information are secured rather than the networks or architectures they reside in.

An IBSA/ZTA is designed and deployed with adherence to the following zero trust basic tenets:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.

4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioural and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

While not completely risk free this approach has the following advantages over conventional methods:

- There is no assumption that assets must be based locally, they can be local or in the cloud.
- The protection of assets through encryption is the same wherever they are located.
- Access to any object is only granted based on enterprise policy and requestor's identity.
- The network can dynamically react to threats whether internal or external.
- Applications can run in a sandbox fully protected from other applications on the same host enabling virtualization and access from mixed mode hosts.

There are several ways in which an IBSA/ ZTA can be deployed. Figure 9 shows a typical approach applied to the aviation Digital Twin example. In this case there is a Policy Decision Point (PDP) which communicates with several policy enforcement points within the Digital Twin architecture which manage access and encryption. The PDP can take real time input from sources like threat intelligence and security event logs to change behavior rapidly in the event of perceived issues and also to ensure a coherent approach across the enterprise in terms of access to individuals. All data is encrypted at rest and in transit which means that unsecured networks and cloud storage / computing resources can be used.

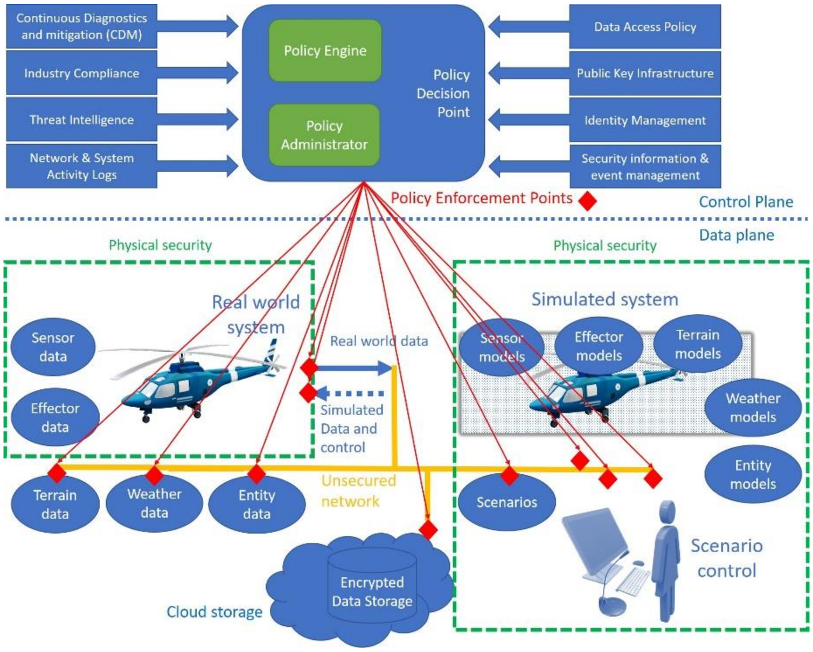

Figure 9 - ZTA implementation of aviation Digital Twin

The IBSA / ZTA approach with its ability to unlock scalable and remote computing and data storage resources has the potential to avoid most of the issues of the 'system high' approach for Digital Twins. Even in the Geographic Proximity Effect case, as all traffic is encrypted independent of network topology, there is the potential to route data in multiple ways to reduce the impact and detectability of the interaction of the Digital Twin with physical assets and data sources.

Another advantage of the ZTA approach is the congruence with the Modeling and Simulation as a Service (MSaaS) paradigm. Many organizations are considering the deployment of MSaaS into Modeling and Simulation (M&S) applications including the deployment of Digital Twins but one of the implementation issues identified with it is the issue of cybersecurity due to the distributed nature of the services which it employs (Skinner, Stuart, Ford, & LLoyd, 2018) . ZTA offers the opportunity to secure MSaaS applications for both military and civil Digital Twins.

STEPS TO MIGRATION

The NIST special publication (National Institute of Standards and Technology, 2020) identifies that use of a ZTA approach is consistent with the Risk Management Framework (RMF) required to be applied for all M&S solutions delivered to the US government and includes a step-by-step guide to migration (Figure 10).

From an M&S viewpoint some of the steps match existing roadmap steps to implement MSaaS; including:

- Forming a set of registries and data repositories that can be shared and managed
- Validation and verification of models and data that we wish to reuse

Other steps that need to be considered include:

- Modifying our existing simulation protocols to allow IBSA/ZTA activity (encryption, identification and use of policy enforcement points). This may be easier for interoperability protocols such as HLA rather than DIS.
- Identifying actors within the Digital Twin (e.g. people, platforms, models, analysis and execution tools)
- Actively managing the compositions of models, simulations and associated scenarios
- Ensuring composition and orchestration tools comply with IBSA/ZTA principles
- Ensuring active and dynamic management of the compute and network infrastructure of the Digital Twin from initiation to shutdown

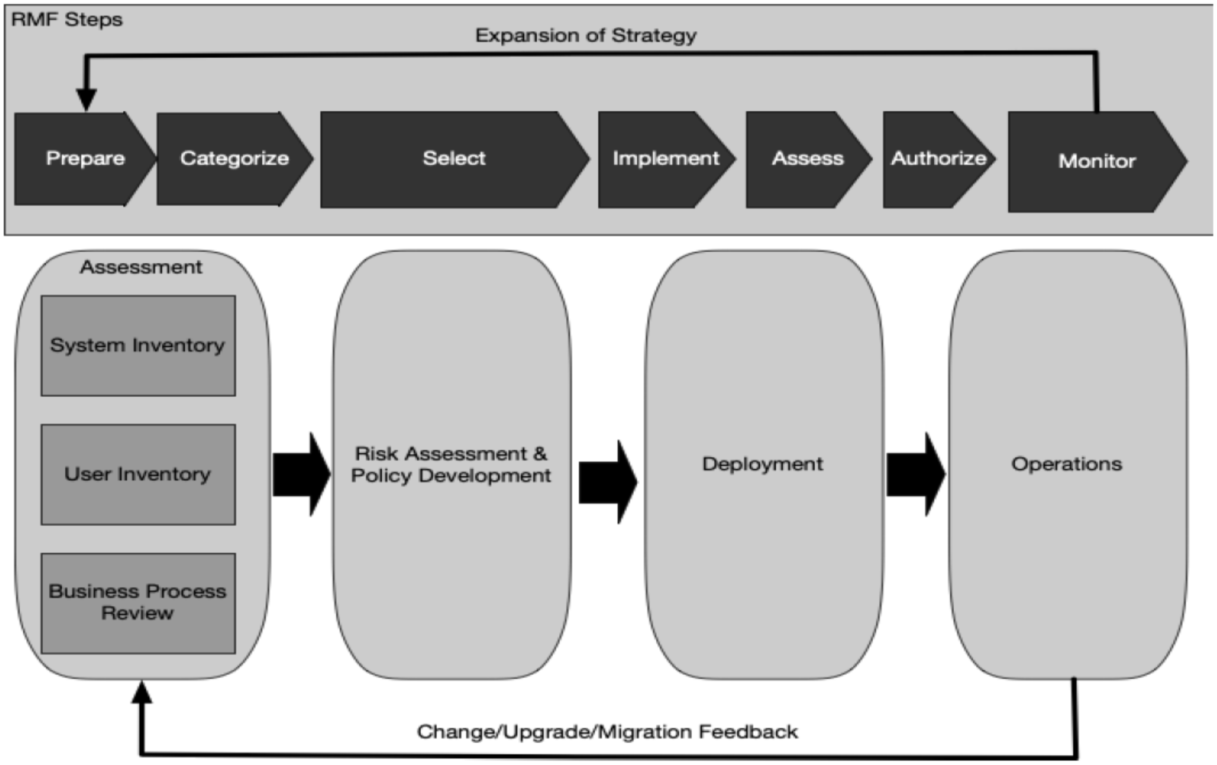

Figure 10 - ZTA deployment as part of the RMF process ((National Institute of Standards and Technology, 2020)

CONCLUSIONS

This paper has shown that concerns around issues of security and identity, common to all military M&S systems are magnified when the complexity and scale of Digital Twins is included. Large scale Digital Twins are likely to form attractive targets to adversaries who will try and disrupt and destroy them by going 'In through the Out Door'.

Information Based Security Architecture / Zero Trust Architecture approach offers a potential solution to the issues and has the advantage of also being aligned to the increasingly popular MSaaS paradigm to designing and running modelling and simulation applications on a cloud computing enterprise architecture.

However this is a radical change to the traditional operating model in the simulation and training world where a 'System High' / Perimeter Based Architecture Network has been the way sensitive data and applications have been protected for decades.

Radical changes to the way things are done in our existing M&S applications will be needed:

- Our existing reflexive 'System High' approach to M&S with its existing policies and procedures will need to be reviewed. Experimentation should be undertaken to resolve how things will work technically and how accreditation and other policies and procedures should change to provide both effective security and identity control and flexibility to change through the lifetime of a platform.

- Acquisition management models will need to take into account subscription based access to data and modelling services. The move to Government ownership of data does not solve all IP issues and how support is provided.

- Every M&S resource that we currently own (models, simulations, scenarios, other data, and computational resources) will be implicitly untrusted unless properly validated and verified.

- System architecture design will need to take into account that encryption will be applied both to static data and data that is being moved.

- Making our Digital Twins effective will likely mean gathering data from external sources that may be commercial, less trusted or based on IOT sources, using dynamic cloud based computational resources and data storage. This will require a change in thinking of our existing M&S architectural designs to a more service based MSaaS structure.

- Our existing simulation interoperability protocols will need to be compatible with Policy Enforcement Points and the 'zero trust' concept instead of the current 'everyone is trusted' approach.

- Use of the MSaaS paradigm will need to be coupled with effective registry and repository services along with rapid composition tools to allow flexible & modular digital twins to be created, both for the short and long term.

Properly secured military Digital Twins offer many benefits to save money, improve capability and operational effectiveness for the remainder of the century. This will require behavior and cultural changes to traditional ways of operation within the military M&S environment. If we do nothing then they will be of much greater benefit to our adversaries.

REFERENCES

Carter, N. (2021, June 14). *UK MOD Speeches*. Retrieved from UK Government: https://www.gov.uk/government/speeches/chief-of-the-defence-staff-general-sir-nick-carter-launches-the-integrated-operating-concept

Digital Twin Consortium. (2021, June 11). *Glossary*. Retrieved from Digital Twin Consortium: https://www.digitaltwinconsortium.org/glossary/index.htm#digital-twin

European Commission. (2021, June 11). *Destination Earth*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/destination-earth

Gelernter, D. H. (1991). *Mirror Worlds: or the Day Software Puts the Universe in a Shoebox-How It Will Happen and What It Will Mean.* Oxford: Oxford University Press.

Grand View Research. (2021). *Digital Twin Market Size, Share & Trends Analysis Report By End-use (Automotive & Transport, Retail & Consumer Goods, Agriculture, Manufacturing, Energy & Utilities), By Region, And Segment Forecasts, 2021 - 2028.* San Francisco, USA: Grand View Research Inc.

Guardian Media Group. (2021, June 14). *Fitness tracking app Strava gives away location of secret US army bases*. Retrieved from Guardian newspaper: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Liu, Z., Meyendorf, N., & Mrad, N. (2018). "The role of data fusion in predictive maintenance using digital twin". *AIP Conference Proceedings 1949* (p. 020023). AIP Publishing.

Menke, T. (2019). "Joint Simulation Environment for United States Air Force Test Support". *STO-MP-MSG171* (pp. 17-1 to 17-14). Paris, France: NATO Science and Technology Organisation.

National Institute of Standards and Technology. (2020). *Zero Trust Architecture.* Gaithersburg, MD: NIST Special Publication 800-207.

Piascik, R., & et al. (2010). *Technology Area 12: Materials, Structures, Mechanical Systems, and Manufacturing Road Map.* NASA Office of Chief Scientist.

Sirius / CSIIS. (2021, June 14). *Information Based Security*. Retrieved from IAAC Poster 2014 artwork: https://www.nexor.com/wp-content/uploads/2016/12/IAAC-Poster-2014-artwork.pdf

SISO Inc. (2021, June 14). *Compressed-Distributed Interactive Simulation (C-DIS) PDG*. Retrieved from Simulation Interoperability Standards Organization: https://www.sisostds.org/StandardsActivities/DevelopmentGroups/C-DISPDG.aspx

Skinner, S., Stuart, L., Ford, K., & LLoyd, J. (2018). ‘Mind the Gap’ – Avoiding Pitfalls in Taking the MSaaS Concept from Research into Everyday Use. *NATO modelling and simulation group 2018* (pp. 15-1 to 15-13). Ottawa: NATO Science and Technology Organisation.

Watson, P. (2012). A multi-level security model for partitioning workflows over federated clouds. *Journal of Cloud Computing: Advances, Systems and Applications 1*, 15.