The Need for Cyber-Physical Digital Twins for Multi-Domain Operational Studies & Analysis

Steven Huang, Douglas Orellana
ManTech International Corporation
Herndon, VA
Steven.Huang@ManTech.com, Douglas.Orellana@ManTech.com

ABSTRACT

ManTech has developed a virtual environment that highlights the value and importance of combining the cyber and space domains to achieve novel and transformational missions. ManTech's capability enables thorough investigation and virtualization of Enterprise architectures necessary to support Multi-Domain Operations (MDO) investigations, studies, and evaluations. MDO is a concept where the joint force can achieve a competitive advantage over a near-peer adversary by presenting multiple complementary threats that each requires a response, thereby exposing adversary vulnerabilities to other threats. The combination of cyber and physical effects in one controlled environment facilitates an increase in tempo for test and evaluations to bring novel solutions to operations faster.

Any enterprise architecture needed for Command and Control (C2) of space-borne and airborne assets has its own unique set of challenges with respect to modeling, timeliness, and robustness. The important addition of the cyber domain to these architectures adds new complexities for consideration. Most architectural approaches build upon software-defined networking and software-defined infrastructure initiatives to emulate, simulate, and stimulate the virtual environment in a hyper-realistic fashion. In addition, there has been an increased focus on improving visualizations within virtual environments, and this paper will highlight some of the obstacles for achieving this when applied to multi-domain operations.

ABOUT THE AUTHORS

Steven Huang has two decades of experience in systems engineering, modeling & simulation, and algorithm development. Steven has worked at ManTech International since 2006 and is currently acting as a Subject Matter Expert within the Intelligence Systems Engineering Technical Focus Area.

Douglas Orellana has over a decade of experience in transformation, systems engineering, and technology integration, and is currently responsible for ManTech's digital transformation of systems engineering and developing the next generation solutions for intelligent systems engineering powered by advanced computing, modeling and simulation, automation, and artificial intelligence.

The Need for Cyber-Physical Digital Twins for Multi-Domain Operational Studies & Analysis

Steven Huang, Douglas Orellana
ManTech International Corporation
Herndon, VA
Steven.Huang@ManTech.com, Douglas.Orellana@ManTech.com

INTRODUCTION

With the maturation of the Internet of Things (IoT), modern systems are more likely to have a multitude of interfaces that continue to grow in scope and scale. These complex systems are more likely to span multiple components that present several issues for system architects and system engineers: cyber components, physical systems, and human actors. (Madni, 2018) Multi-disciplinary approaches can start to overcome these issues due to the benefit and use of multiple and unique perspectives. This type of thought leadership and collaboration is exactly what foreign and domestic military and government institutions discuss in their vision for the future. (Australia, USSF Vision, DHS) This is particularly true for scenarios and concepts that include the space industry. (Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience, 2021)

Space activities and industries are rapidly accelerating, and many countries and cultures recognize that space is essential to a modern way of life. Space solutions deliver critical data, products, and services that drive innovation in the US and around the world. (US Space Priorities Framework) The need and demand for the space-for-ground economy continues to grow, but the space-for-space economy is just getting started. In 2019, the space-for-ground economy had an estimated revenue of $366 billion where goods and services produced in space for use on the ground. Examples include telecommunications, internet infrastructure, earth observation capabilities, etc. With decreased costs for launch and space hardware, this economy will continue to expand past 2040. (Sarang, 2021) Market leaders like Made In Space, Inc and Axiom Space are both moving towards proving that the space-for-space economy is fast approaching. Made In Space, Inc had the opportunity to 3D-print a wrench on-board the International Space Station. Axiom Space is working to become the world's first commercial space station. These market leaders understand the importance of maintaining their lead on the competition by staying focused, having robust approaches for supply chains, and the importance of securing their information technology (IT) networks.

A string of high-profile cyber security incidents in 2021 have clearly highlighted the fact that no person, industry, or government is immune: not users of on-premises hardware nor providers of cloud solutions. Successful companies looking to develop transformational solutions must include interfaces with and impacts of the cyber domain. The concern regarding cyber security goes beyond data breaches, since there is a continued growth of ransomware attacks too. ('We're Losing Control of our Data' as Breaches Reach an All Time High, 2022) With this in mind, a number of companies have started to embark upon the creation of digital twins for IT networks. These have been proven for a range of use cases, but there has been a lack of digital twins that can actively demonstrate how cyber activities impact physical behaviors OR how physical interactions change cyber behaviors. The ability to model and simulate both cyber and physical behaviors in an operationally relevant fashion is critical to support the newest doctrine to emerge from the US Department of Defense (DoD): Multi-Domain Operations (MDO). (Nettis, 2020)

General Robert Brown defined MDO as "a concept that the Joint force can achieve competitive advantage over a near-peer adversary by presenting multiple complementary threats that each requires a response, thereby exposing adversary vulnerabilities to other threats. It is the artful combination of these multiple dilemmas, rather than a clear overmatch in terms of any particular capability, that produces the desired advantage". (US General Brown Multi Domain Operations Warfare, Perception Management, 2019) It is the skillful combination of effects from distinct layers (e.g. air, land, sea, space, cyber) that has created the demand signal to pursue systems like the Advanced Battle Management System (ABMS), Cross Mission Ground and Communications Enterprise (ECX), Project Overmatch, and Project Convergence. (Pope, Birkey)

These pursuits will unveil important considerations for the DoD community, specifically regarding the primary benefits for creating cyber-physical digital twins and the impact upon multi-domain missions. The phrase "cyber-physical" implies a complex system that integrates the cyber world and the dynamic physical world, and the integration of control, communications, and computing delivers real-time sensing and information feedback. The phrase "digital twin" indicates a bi-directional dynamic mapping between a virtual and physical system. Such a system requires high-fidelity virtual models to properly reflect real world behaviors in the virtual environment. When combined the phrase "cyber-physical digital twin" embodies a closed loop system formed between the cyber/digital and physical worlds that incorporates high-fidelity models and control of processes to inform real-time analysis, decision making, and precise execution.

Section 2 of this paper will discuss the typical uses of digital twins, and then Section 3 points out some gaps in digital twins, specifically for multi-domain operations. Section 4 provides some background on virtual environment solutions, before Section 5 highlights some effective visualization tools for visualizing multiple domains. Section 6 then highlights the benefits for combining visualization tools with virtual environments in order to realize the promise of cyber-physical digital twins.

TRADITIONAL USE OF DIGITAL TWINS

Department of Defense Use of Digital Twins

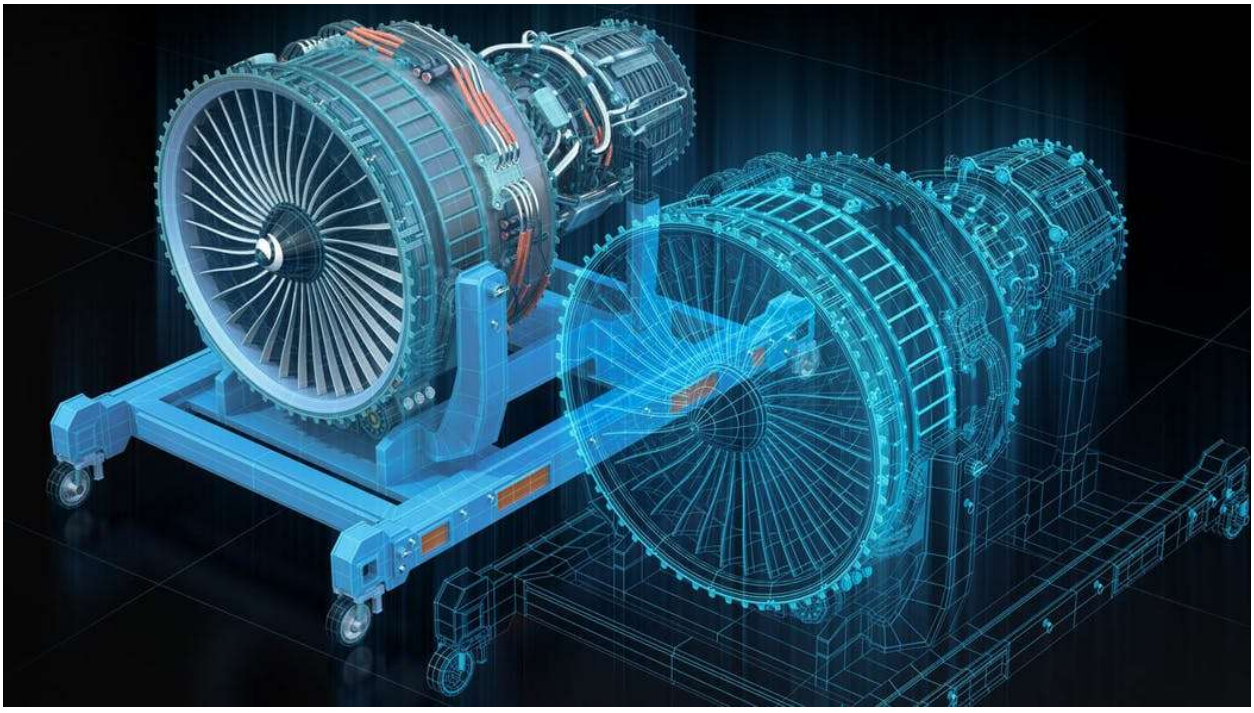

Figure 1: Graphical depiction of how the DoD uses digital twin technology (Air Force Turns to Digital Twin Technology that Uses Virtual Representations of Real Objects for Prototyping, 2021)

Across the Department of Defense (DoD), a number of organizations have embarked on creating, curating, and maintaining digital twins. Most of these efforts typically define a digital twin as the concept of using a virtual representation of a real object. These "twinning" efforts can be as simple as a single piece of hardware to as extensive as an entire command and control architecture for space operations. (Air Force Turns, Waterman, Erwin) The utility of a digital twin, however, is far reaching. Some support trade study investigations for exploration of concepts of operation, others support the rollout of new software or hardware upgrades to understand their mission utility.

Manufacturing Use of Digital Twins

For manufacturing, digital twins have a broader definition and scope than that currently used by the DoD. In addition to using the virtual environment to model a process, system, service, or product, manufacturing digital twins use virtual and augmented reality for 3D graphics and data modelling. Moreover, in order to keep the digital replica synchronized with its physical counterpart, manufacturing digital twins maintain a network connection (real-time or near-real-time) between the two. (Downey, 2022) In an effort to improve manufacturing efficiencies, manufacturer digital twins are also used for process improvement that spans design, development, manufacturing, and production phases. Emerging applications also include quality management, supply chain management, predictive maintenance, and customer experience analysis. (Crawford, 2021) Manufacturers are realizing the benefit for using digital twins as a means to improve their asset lifecycle management. This use case allows repair technicians to make use of augmented reality by overlaying virtual engineering models on top of the physical equipment they are servicing. This approach provides the most accurate and current information in procedures and performance specifications that directly impacts the timeliness and efficiency of servicing efforts. (Slansky, 2022)

GAPS IN DIGITAL TWINS FOR MULTI-DOMAIN OPERATIONS

The combination of experience and insights from manufacturing digital twins coupled with DoD Multi-Domain Operational concepts is where DoD and industry partners are gradually heading, but there are difficulties in realizing an effective implementation. The first notable gap is how to achieve near-real-time connectivity to systems or devices that may be at multiple classification levels. This may be achievable during design and development when they are at a commensurate classification level or common network, but when capabilities transition to an operational environment, they typically operate on different networks which makes connectivity more challenging. For some systems, this could be further compounded with export control laws and limitations to sharing with international partners. The other challenge affecting this gap is the information content that needs to be shared between the cyber and physical twins. Typical security operations often allow 1-way traffic (from low-side to high-side) where integration and analysis can occur on a network appropriate for higher classifications, but the same security posture allows minimal if any traffic out. This inability to share updates and status from the virtual environment with its physical counterpart diminishes the potential value of the digital twin. There are approaches to establishing trusted processes for cross-domain security, but these are not in widespread use, and this will be critical for systems supporting Joint All-Domain Command and Control (JADC2) efforts. (Kamis, 2021)

The second notable gap in digital twins for multi-domain operations is the need to incorporate cyber resiliency approaches. Network security scans are common for standard network components and operating systems, but the same cannot be said for systems or platforms running real-time operating systems (like VxWorks or RTEMS). Typically, DoD customers establish standards for recommended security technical implementation guides (STIGs), but these do not encompass real-time operating systems. (SRG / STIG Library Compilations, 2022) An additional obstacle with the cyber domain is how to incorporate cyber stimulation and analytic insights into a virtual environment specifically for digital twins. Cyber security standards are not widely known for non-network hardware or software products, so this will need to be an area for continued industry involvement to define cyber physical digital twins needed for multi-domain operational studies and analysis.

VIRTUAL ENVIRONMENT SOLUTIONS

Software Defined Networking

Software Defined Networking (SDN) technology has been described as an approach to dynamically and efficiently configure networks that is cost-effective and adaptable to a variety of situations. This approach decouples the network control and forwarding functions, which in-turn enables the network layer to be directly programmable, and the underlying hardware layer can also be abstracted. (Software-Defined Networking - Definition, 2021)

In early developments, OpenFlow was the standard protocol used to communicate with network layer elements, but since 2012 several other (proprietary) systems have emerged to accomplish the same function. In all cases, the protocol used in SDN technology solutions allows them to be programmed directly, agile, and managed centrally (open networking). Several companies offer mature SDN solutions these days including Cisco; Cradlepoint; Dell; IBM; Junos; Masergy; Nuage; Riverbed; and Pica8. (BasuMallick, 2021)

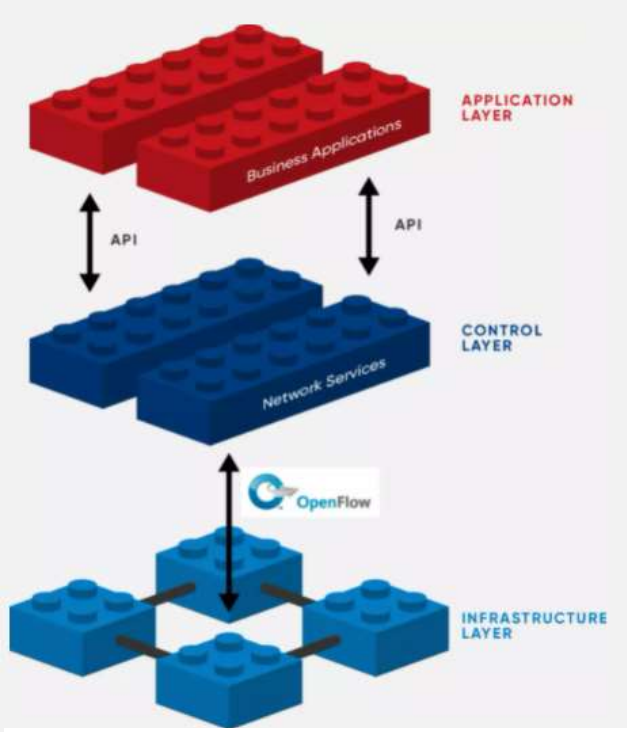

Figure 2: Visual depiction of building blocks for SDNs (Software-Defined Networking - Definition, 2021)

Since SDNs decouple the software from the underlying hardware, this allows network administrators to program and control the entire network through a single pane of glass. This design also allows data to move between distributed locations, which makes an SDN a natural fit as a cloud application. This ease of data movement also facilitates moving workloads around a virtual network which further demonstrates its benefit over traditional networking: the ability to execute all the management (control, configuration settings, provision of resources, increased capacity) from a centralized user interface, while never requiring the introduction of new hardware to the architecture. (What is Software-Defined Networking (SDN)?, 2021)

Software Defined Infrastructure (SDI)

A Software Defined Infrastructure combines SDN with software defined compute and software defined storage capabilities. This triple combination could be considered a virtualized information technology (IT) facility where

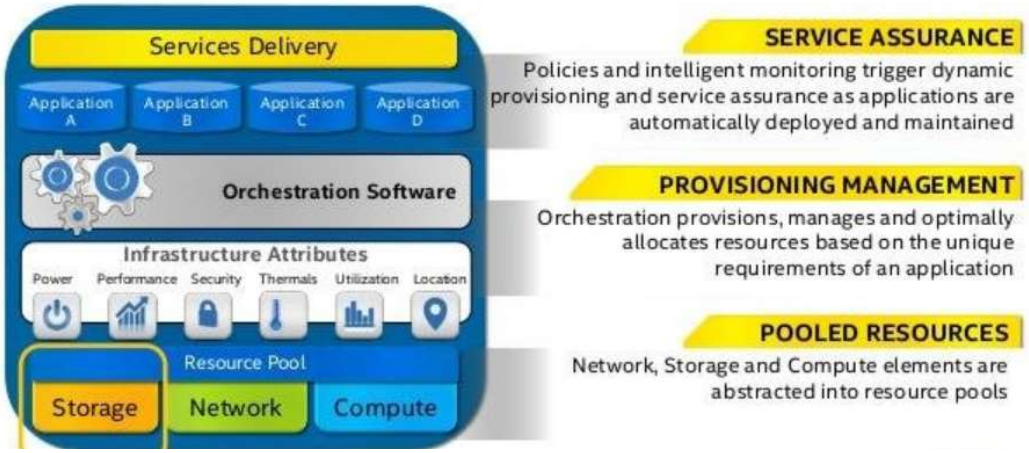

Figure 3: Graphical depiction of SDI (Software Defined Infrastructure / SDI, 2019)

infrastructure elements, processing and security are virtualized and delivered as a service. (Software-Defined Infrastructure, 2021) SDIs consists of fully virtualized compute, networking, and storage resources that can be controlled and managed as if they were software. In this way, one can implement policy-based infrastructure provisioning and enable automation for a wide range of functions. Similar to SDNs, configuration and management of resources can be accomplished via centralized dashboards. Unlike SDNs, SDIs can more easily make full use of hybrid cloud capabilities, and virtualized architectures can be configured on commoditized hardware. (Software-Defined Infrastructure, 2022)

Multiple SDI options exist that are being marketed to analyze and improve the cybersecurity needs of government and commercial customers. Some additional features of interest to financial and government customers is the support of configuration rollback and cloning, specifically to help investigate cyber risk and courses of action during automated, scripted, or human actor generated adversarial cyber actions. Similar to the growth of SDI and SDN commercial options, the proliferation of cyber range options span a number of US government, laboratory, and commercial efforts. Some examples include DoD's National Cyber Range; the Joint Chiefs of Staff J7 operates the Joint Information Operations Range (JIOR); Pacific Northwest National Laboratory's (PNNL) Aircraft Cyber Evaluation; Keysight's Breaking Point software; Scalable Networks' EXata Cyber product; IBM Security Command Center Mobile; Raytheon's Cyber Operations, Development and Evaluation (CODE) Center; etc. Due to their flexibility, cyber ranges come in a variety of shapes and sizes, but each fundamentally allows customers to tailor compute, storage, and configuration settings to meet many use cases including cyber testing, operator training, war game exercises, risk assessments, development scripts, Tactics, Techniques, and Procedures (TTPs) development, and more.

SIMULATION VISUALIZATION TOOLS

A number of high-quality, mature visualization tools exist on the market. The principal ones most papers, industry partners, and developers make use of that allow one to model and visualize platforms and behaviors for two or more domains (air, land, sea, space, cyber) are Analytical Graphics Incorporated (AGI), An Ansys Company's Systems Toolkit (STK) and US government-owned Advanced Framework for Simulation, Integration, and Modeling (AFSIM). The former product started out as Satellite Toolkit, but expanded to support the movement, behaviors, and interactions

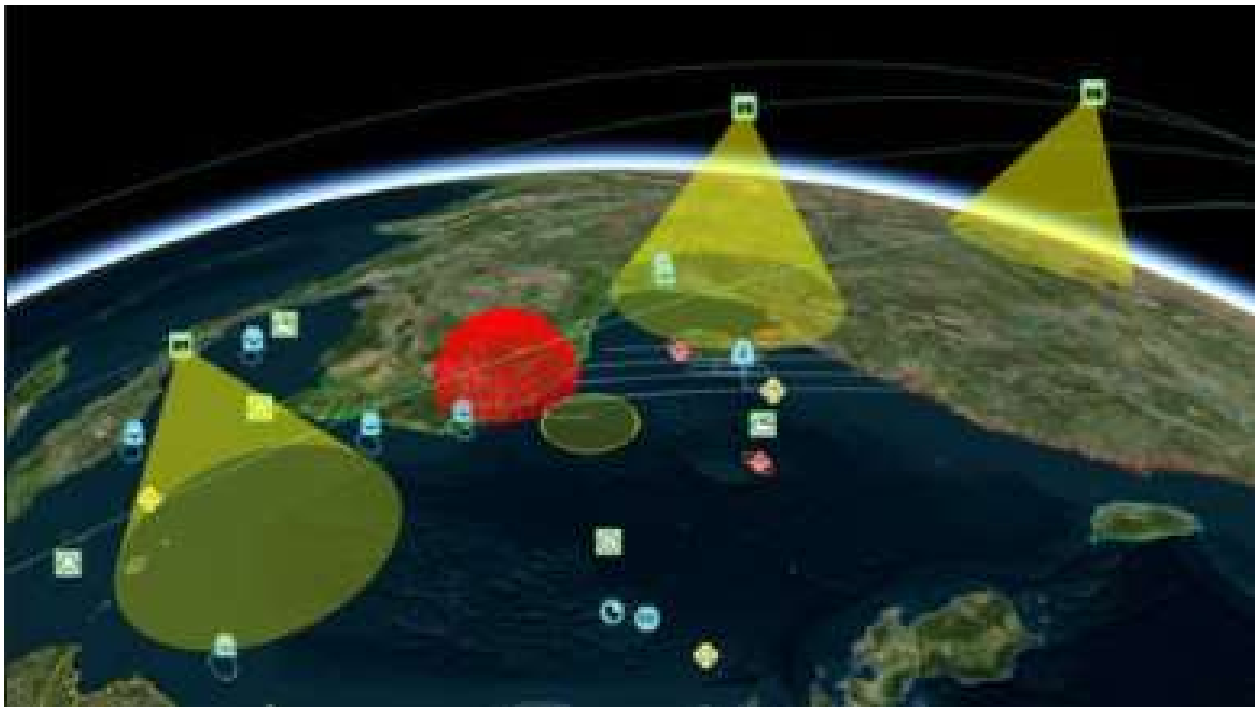

Figure 4: Exemplar AGI screenshot depicting how different domains can impact mission success (Missions: Find the AGI Software That Fits Your Objectives, 2022)

of other physical platforms in their respective environments. AGI has several webinars discussing how their products support the visualization of digital twins and their actions across the product lifecycle. (Missions: Find the AGI Software That Fits Your Objectives, 2022)

As a modeling and simulation framework, AFSIM's intended use is for "engineering, engagement, and mission-level analytic simulations to meet the needs of the operations and analysis community". (Cross Domain Analysis & Simulation, 2021) The purpose of this flexible framework is to streamline integration of external models to represent advanced technologies in multi-domain and multi-fidelity scenarios. The framework allows its users to scale the scenario to the appropriate simulation level to best study the item of interest; hence as the solution matures, the framework can also mature to gain varied and different insights for the system and how it pursues its mission objectives.

BENEFITS FOR USING VISUALIZATION TOOLS WITH VIRTUAL ENVIRONMENTS

Visualization as a means to improve and clarify communications continues to play a significant role in a variety of engineering disciplines. Mechanical engineers used Computer Aided Design (CAD) software initially to create electronic files for print to benefit machining and manufacturing operations. The pre-work necessary to establish standards resulted in improved design quality, engineer productivity, and simplified documentation, all while saving time and energy. (Benefits of 3D CAD Modeling, 2021) The additional value of visualization came as a side-benefit as CAD software packages improved to support measurements and engineering calculations. In a similar way, system engineers (SEs) are working to define or refine standards for modeling tools needed for multi-domain mission-level modeling and simulation. With model-based system engineering (MBSE) approaches, there has been lots of work performed on defining standards (e.g. system modeling language or SysML) that allows improved communication and information sharing across engineering disciplines. This has started a transformation within the SE discipline to make consistent and broader use of models to share and communicate better, while simultaneously reaping the benefits of automation and analytics, similar to how CAD transformed mechanical engineering. (Naval Air Warfare Center Aircraft Division (NAWCAD), 2018)

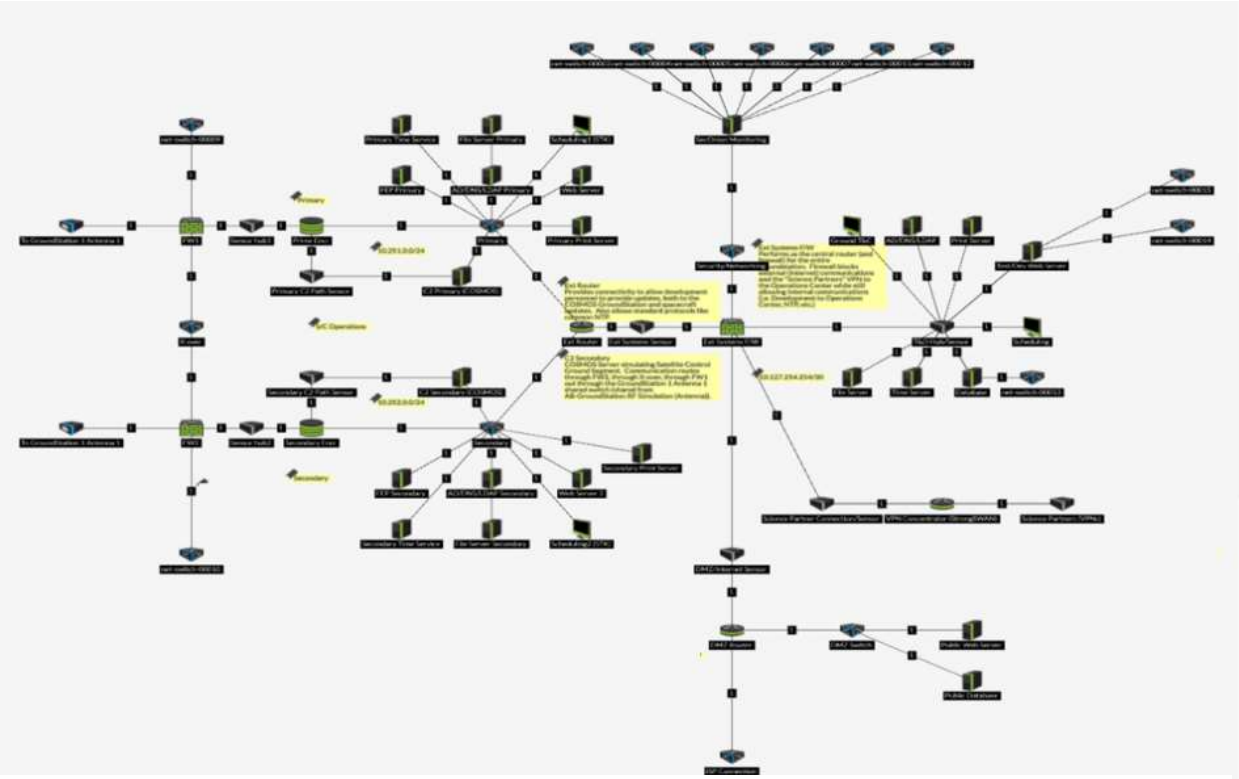

Figure 5: Network topology example from ManTech's Space Range, a cyber-physical virtual environment

Visualization and metrics of performance for multi-domain scenarios have to be tied to the domains being analyzed or used. As such, STK and AFSIM are quite appropriate for the standard domains that they have been built for: air, sea, land, and space, but cyber metrics and visuals are different. Other entities have realized this as well, and the US Defense Advanced Research Projects Agency (DARPA) has started to invest in a new capability that specifically includes cyber and electromagnetic spectrum capabilities in a multi-domain, mission-level model and simulation effort called SAFE-SiM (Secure Advanced Framework for Simulation and Modeling).

Visualization capabilities play a more crucial role in virtual environments because this often becomes the primary means by which users interact with and control the virtual environment. In addition, visualization of behaviors and actions within the virtual environment must accurately represent how those would transpire in the physical world. Behaviors and actions that are not feasible would be non-sensical and cause potential customers to not trust the results being provided by the virtual environment. In the network diagram below from ManTech's Space Range running within ACRE, each virtual node represents a physical system running a specific operating system. This network topology includes a primary operational string, a secondary operational string, a test and development enclave, and a VPN connection to a remote user network.

The hypervisor interface allows users and administrators interact with each virtual node directly, change its configuration, and the run studies and assessments for how those changes improve or detract from the architecture's performance. The evaluation of network performance or cyber vulnerabilities lend themselves well to dashboards or risk assessments via tables. The details and factors behind such reports illustrate the root cause or indication signs that one could use to predict problems or cyber intrusions. Naturally, all of this data is resident in the virtual environment, so why couldn't this data be exposed for additional metrics, assessments, or graphical indicators? In the virtual environment, this would be trivial to do so, but how would an evaluator tie the cause of the problem or disruption to a physical world action? To do this accurately, the virtual node has to be fully and completely representative of its physical counterpart. To accomplish this, one has a limited set of choices: 1) to create a detailed virtual model of the physical item; 2) to replace the virtual model with hardware-in-the-loop (HITL) with the actual hardware; or 3) to create a digital twin using a data connection between the virtual object and its physical counterpart.

The creation of a detailed virtual model frequently takes a significant amount of time to ensure that the fidelity of the behavior of the model accurately represents the known and unknown failure states of the physical hardware. This approach can be adjusted, however, so that the virtual model only captures the relevant behavior for the most common failure modes, which can greatly reduce the time needed to create an "accurate" model, because it is only accurate for a given set of assumptions. The second option ensures that the virtual environment behavior is truly identical to the physical counterpart, because hosting of HITL allows them to be identical (within manufacturing tolerances). In many situations, however, this is cost prohibitive. So, a similar but reduced cost option is to use an engineering model of the real hardware as the HITL entity, but this is only sufficient (like the virtual model) where the engineering hardware replicates the actual hardware behavior for a limited set of conditions. The third, and most cost-effective option, is to pursue a network connection between the virtual and physical systems so that they can each share status and health information. In this sense, they are truly digital twins of one another because they will both receive the same signals so that their states remain synchronized as a result of their network connection.

CONCLUSIONS

This paper has highlighted the importance of cyber-physical digital twins for multi-domain operational studies and analysis efforts. The maturation of computational technologies and data visualization software are rapidly improving so that the promise of a cyber-physical digital twin is achievable. The manufacturing industry has demonstrated some valuable insights that the DoD can inherit and build upon to advance digital twinning efforts. There is still work to be done to capture insights and capabilities of cyber resiliency that many digital twins or cyber-physical systems lack, but there is on-going work at ManTech International and other companies that illustrate potential paths forward. Successful use of digital twins will soon serve as a cornerstone for programs desiring authoritative sources of truth.

REFERENCES

Australian Army. (2016). *Evolving an Intellectual Edge: Professional Military Education for the Australian Army*. https://cove.army.gov.au/sites/default/files/10-12/11/Evolving-an-Intellectual-Edge-Professional-Military-Education-for-the-Australian-Army.pdf

BasuMallick, Chiradeep. (2022, February 10). *Top 10 Software-Defined Networking (SDN) Solutions in 2022*. Toolbox Tech. https://www.toolbox.com/tech/networking/articles/best-sdn-solutions/

Benefits of 3D CAD Modeling. (2021, August 13). Indovance. Retrieved from https://www.indovance.com/knowledge-center/benefits-of-3d-cad-modeling-in-mechanical-design/

Birkey, Douglas. (2021, May). Command and Control Imperatives for the 21st Century: The Next Areas of Growth for ABMS and JADC2. *Mitchell Institute for Aerospace Studies*, vol 27, 1-30. https://mitchellaerospacepower.org/wp-content/uploads/2021/06/C2ISR_Policy_Paper_27-final.pdf

Crawford, M. (2021, March 17). 7 Digital Twin Applications for Manufacturing. *The American Society of Mechanical Engineers*. https://www.asme.org/topics-resources/content/7-digital-twin-applications-for-manufacturing

Cross Domain Analysis & Simulation. (2021, December 1). Infoscitex. Retrieved from https://www.infoscitex.com/technology-solutions/cross-domain-analysis-and-simulation/

DoD Cyber Exchange. (n.d.). *SRG / STIG Library Compilations*. https://public.cyber.mil/stigs/compilations/

Downey, John. (n.d.). What is Digital Twin Technology and How It Benefits Manufacturing in the Industry 4.0 Era? *SL Controls*. https://slcontrols.com/en/what-is-digital-twin-technology-and-how-can-it-benefit-manufacturing/

Erwin, Sandra. (2021, June 21). Space Force, DoD agencies planning multi-orbit sensor network to track hypersonic missiles. *Space News*. https://spacenews.com/space-force-dod-agencies-planning-multi-orbit-sensor-network-to-track-hypersonic-missiles/

Kamis, George. (2021, August 31). How to Make the Joint All Domain Command and Control Actionable for Defense. *FedTechMagazine*. https://fedtechmagazine.com/article/2021/08/how-make-joint-all-domain-command-and-control-actionable-defense

Love, Jacob. (2019, March 3). *US General Brown Multi-Domain Operations Warfare, Perception Management* [Video file]. YouTube. https://www.youtube.com/watch?v=_fSsccWxrds

Madni, A. M. (2018). *Transdisciplinary Systems Engineering: Exploiting Convergence in a Hyper-Connected World*. Springer.

Militaryaerospace.com. (2021, April 6). *Air Force Designs Rely on Virtual Digital Twin Technology*. https://www.militaryaerospace.com/computers/article/14200706/digital-twin-virtual-prototype

Missions. (n.d.). agi. Retrieved January 26, 2022 from https://www.agi.com/missions

Murray, Allison. (2022, January 25). 'We're Losing Control of our Data' as Breaches Reach an All Time High. *Zdnet*. https://www.zdnet.com/

Naval Air Warfare Center Aircraft Division (NAWCAD). (2018, January 30). *Systems Engineering Transformation* [Video file]. YouTube. https://www.youtube.com/watch?v=171blNCgpCo

Nettis, Maj Kimber. (2020, March 16). Multi-Domain Operations: Bridging the Gaps for Dominance. *Air University*. https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2109784/multi-domain-operations-bridging-the-gaps-for-dominance/

Pope, Charles. (2021, May 21). *With its Promise and Performance Confirmed, ABMS Moves to a New Phase*. Secretary of the Air Force Public Affairs.

Sarang, Mehak & Weinzierl, Matt. (2021, February 12). *The Commercial Space Age Is Here: Private Space Travel Is Just The Beginning*. Harvard Business Review. https://hbr.org/2021/02/the-commercial-space-age-is-here

Slansky, Dick. (n.d.). *The Digital Twin Drives Smart Manufacturing*. ARC Advisory Group. https://www.arcweb.com/industry-best-practices/digital-twin-drives-smart-manufacturing

Software-Defined Infrastructure. (n.d.). suse. Retrieved December 15, 2021 from https://www.suse.com/suse-defines/definition/software-defined-infrastructure/

Software-Defined Infrastructure. (2022, January 4). Hewlitt Packard Enterprise. Retrieved from https://www.hpe.com/us/en/what-is/software-defined-infrastructure.html

Software-Defined Networking. (n.d.). vmware. Retrieved December 18, 2021 from https://www.vmware.com/topics/glossary/content/software-defined-networking.html

Software-Defined Networking - Definition. (n.d.). opennetworking. Retrieved December 19, 2021 from https://opennetworking.org/sdn-definition/

Space Force CTIO. (2021, May 6). *U.S. Space Force Vision for a Digital Service*. Raymond, Gen. John.

U.S. Department of Homeland Security. (2021, March 31). *Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience*. https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience

Waterman, Shaun. (2021, March 26). Air Force Goes All in on Digital Twinning – for Bombs as well as Planes. *Air Fore Magazine*. https://www.airforcemag.com