VOLUME 7 NUMBER 3
DECEMBER 2019

# CSIAC JOURNAL

A Quarterly Publication of the Cyber Security & Information Systems Information Analysis Center

## M&S APPLIED ACROSS BROAD SPECTRUM DEFENSE AND FEDERAL ENDEAVORS

### M&S SPECIAL EDITION

# CSIAC
*Cyber Security & Information Systems Information Analysis Center*

## ABOUT THE CSIAC

**As one of three DoD Information Analysis Centers (IACs), sponsored by the Defense Technical Information Center (DTIC), CSIAC is the Center of Excellence in Cyber Security and Information Systems. CSIAC fulfills the Scientific and Technical Information (STI) needs of the Research and Development (R&D) and acquisition communities. This is accomplished by providing access to the vast knowledge repositories of existing STI as well as conducting novel core analysis tasks (CATs) to address current, customer focused technological shortfalls.**

## OUR MISSION

CSIAC is chartered to leverage the best practices and expertise from government, industry, and academia in order to promote technology domain awareness and solve the most critically challenging scientific and technical (S&T) problems in the following areas:

- Cybersecurity and Information Assurance
- Software Engineering
- Modeling and Simulation
- Knowledge Management/Information Sharing

The primary activities focus on the collection, analysis, synthesis, processing, production and dissemination of Scientific and Technical Information (STI).

## OUR VISION

The goal of CSIAC is to facilitate the advancement of technological innovations and developments. This is achieved by conducting gap analyses and proactively performing research efforts to fill the voids in the knowledge bases that are vital to our nation. CSIAC provides access to a wealth of STI along with expert guidance in order to improve our strategic capabilities.

## WHAT WE OFFER

We provide expert technical advice and assistance to our user community. CSIAC is a competitively procured, single award contract. The CSIAC contract vehicle has Indefinite Delivery/Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements.

Custom solutions are delivered by executing user defined and funded CAT projects.

## CORE SERVICES

- Technical Inquiries: up to 4 hours free
- Extended Inquiries: up to 2 months
- Search and Summary Inquiries
- STI Searches of DTIC and other repositories
- Workshops and Training Classes
- Subject Matter Expert (SME) Registry and Referrals
- Risk Management Framework (RMF) Assessment & Authorization (A&A) Assistance and Training
- Community of Interest (COI) and Practice Support
- Document Hosting and Blog Spaces
- Agile & Responsive Solutions to emerging trends/threats

## PRODUCTS

- State-of-the-Art Reports (SOARs)
- Technical Journals (Quarterly)
- Cybersecurity Digest (Semimonthly)
- RMF A&A Information
- Critical Reviews and Technology Assessments (CR/TAs)
- Analytical Tools and Techniques
- Webinars & Podcasts
- Handbooks and Data Books
- DoD Cybersecurity Policy Chart

## CORE ANALYSIS TASKS (CATS)

- Customer tailored R&D efforts performed to solve specific user defined problems
- Funded Studies - $1M ceiling
- Duration - 12 month maximum
- Lead time - on contract within as few as 6-8 weeks

## CONTACT INFORMATION

266 Genesee Street
Utica, NY 13502

1 (800) 214-7921

info@csiac.org

/DoD_CSIAC

/CSIAC

/CSIAC

# ABOUT THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

## ABOUT THIS PUBLICATION

**The Journal of Cyber Security and Information Systems** is published quarterly by the Cyber Security and Information Systems Information Analysis Center (CSIAC). The CSIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the CSIAC, and shall not be used for advertising or product endorsement purposes.

## ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

***"This article was originally published in the CSIAC Journal of Cyber Security and Information Systems Vol.7, No 3"***

In addition to this print message, we ask that you notify CSIAC regarding any document that references any article appearing in the CSIAC Journal.

Requests for copies of the referenced journal may be submitted to the following address:

**Cyber Security and Information Systems**
266 Genesee Street
Utica, NY 13502

Phone: 800-214-7921
Fax: 315-732-3261
E-mail: info@csiac.org

An archive of past newsletters is available at **https://ww w.csiac.org/journal/.**

*To unsubscribe from CSIAC Journal Mailings please email us at* ***info@csiac.org*** *and request that your address be removed from our distribution mailing database.*

## JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

*M&S Applied Across Broad Spectrum - Defense and Federal endeavors*

# M&S APPLIED ACROSS BROAD SPECTRUM DEFENSE AND FEDERAL ENDEAVORS

By: John Diem

## Welcome to the annual CSIAC edition on Modeling and Simulation.

This year's theme is 'Innovation' – a term that often spurs thoughts of an inspired new gadget or possibly a way of doing something in a different manner. The Merriam-Webster definition simply states that innovation is "the introduction of something new" – that's a pretty broad definition and certainly open to interpretation. A recent podcast panel on the topic provided varied perspectives from the participants, but in the end the group came to the consensus that innovation is "Executing an idea which addresses a specific challenge and achieves value for both the company and the customer." The papers in this year's journal certainly meet that definition – they each highlight excellent examples of meeting a very diverse set of government needs and challenges (the customer) by establishing capabilities via the innovative use of modeling and simulation expertise and tools that provided enduring value to both the innovator and the customer.

Some familiar historical examples that fit this definition of innovation are the installation of a moveable assembly line, a cheap and practical light bulb, and the ubiquitous post-it note. Within the M&S community, we are all aware of a great legacy that includes automated flight trainers, computer based military simulations and wargames, simulation interoperability standards that broke down organizational and distance barriers, and the more recent infusions of Artificial, Augmented, and Virtual Reality that extend the boundaries of our synthetic environments.

We asked this year's contributors to highlight the "so what?" of their innovations that were fueled by modeling and simulation.  During my career, I have seen countless, innovative applications of M&S that have provided excellent training environments for our soldiers, sailors, airmen, and marines.  In many cases those simulations were not the most current or the most technically sophisticated, but innovation – and imagination – resulted in unprecedented operational readiness even during periods of diminished budgets and competing operational demands.  That's a great "so what".

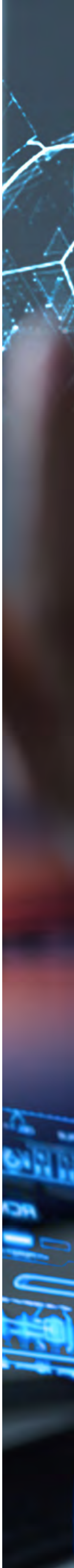
The articles in this year's journal highlight a broad array of modeling and simulation contributions – whether in training, testing, experimentation, research, engineering, or other endeavors:

- Common understanding: Using gaming software to provide a graphical understanding of the concept of operations for unmanned aerial systems [Chell, Hoffenson, Ray, Jones, Blackburn]
- Common data: Establishing common data services to enable joint training objectives via an interoperable synthetic training environment [Dvorak, Hellman, Scrudder, Gupton]
- From paper to data: transition from traditional paper-driven documentation to the use of model-centric requirements and development methods [Kruse, Blackburn]
- Understanding complex problems: The use of a variety of simulations to replicate hybrid networks and understand the effects of cyber and electronic warfare on those networks [Sugrim, Poylisher, Plastine, Newcomb]
- Fostering collaboration: Creation of community-wide collaborative environments via common architectures to support electro-optical and infrared missile system development [Waggoner]
- Modeling and simulation as a "lingua franca": Deploying common modeling tools as freeware to a wide-spread community of government, industry, and academic partners to create an ubiquitous modeling framework [West, Birkmire]

These authors have provided great examples of going well beyond "innovations in modeling and simulation techniques or design" and focus more broadly on "how has modeling and simulation helped you innovate?"  They provide great examples of "innovation, done innovatively" they break down barriers to communication, collaboration and understanding. I believe they will inspire you to join in and innovate.

*Podcast Reference: (https://www.ideatovalue.com/inno/nickskillicorn/2016/03/innovation-15-experts-share-innovation-definition/#ultimatedefinition)*

**MR. JOHN DIEM** was selected to the Senior Executive Service in November 2017 and is the Executive Director of the US Army Operational Test Command (USAOTC), headquartered at Fort Hood, Texas with test directorates at Fort Bliss, TX; Fort Bragg, NC; Fort Hood, TX; Fort Sill, OK; and Fort Huachuca, AZ. A subordinate command to the US Army Test and Evaluation Command (ATEC), the US Army Operational Test Command plans, conducts, and reports the results of rigorous operational tests, assessments and experiments to provide effectiveness, suitability and survivability information for the acquisition and fielding of warfighting systems. Mr. Diem's professional areas of emphasis are modeling and simulation integration and interoperability, mission command systems testing and training, and technology development and acquisition.



3RD BASE
GAME TIME 01:03:02
5 6 7 8 9 R H E
211 680
300 521
PRIMARY TARGET
11 | 55

# OPTIMIZING FOR MISSION SUCCESS USING A STOCHASTIC GAMING SIMULATION

By: Brian Chell, Steven Hoffenson, Douglas Ray, Roger D. Jones, Mark R. Backburn, *Stevens Institute of Technology*

## *THIS ARTICLE DESCRIBES HOW MISSION SCENARIOS CREATED USING GAMING SOFTWARE CAN BE USED AS A GRAPHICAL CONCEPT OF OPERATIONS (CONOPS) AND OPTIMIZED TO ENSURE THE HIGHEST PROBABILITY OF MISSION SUCCESS.*

Traditional optimization methods have not been designed for mission-level problems, where highly uncertain environmental and operational parameters influence mission success, and clear objectives beyond success or failure are not well-defined. This unique class of problems requires new optimization processes. The case study in this article showcases a surveillance mission-level optimization problem with a graphical CONOPS and applies an efficient design space sampling strategy, surrogate modeling, and a value-driven multi-objective formulation to efficiently find an optimal solution. This new approach offers a method for diverse stakeholders to understand, communicate, and optimize system designs for complex and uncertain mission scenarios.

Two of the major ways that engineers use modeling and simulation are to support design decision-making and to provide realistic visual representations of scenarios. When dealing with complex systems, such as aircraft, these activities fall under the umbrella of model-based systems engineering (MBSE), where relevant domain models are connected to form a comprehensive model of the system lifecycle (Ramos, Ferreira, & Barceló, 2012). The overarching goals of MBSE are to enable systems engineering and design through a unified, coherent model, reduce the cost and time devoted to building and testing physical prototypes, and facilitate greater communications among stakeholders. However, there is still a marked disconnect between the subject matter experts who develop domain models and the higher-level decision-makers who perform trade-off analyses and set system requirements and objectives. This article proposes a new mission-level optimization approach to MBSE that integrates design optimization and trade-off analysis tools with a graphical concept of operations (CONOPS) to provide design solutions with the highest probability of mission success. By focusing on mission-level success, rather than system-level performance, and by using gaming technology to provide more realistic visual representations of system scenarios, this new approach brings these stakeholders closer together to support stronger and more mission-focused systems engineering and design.

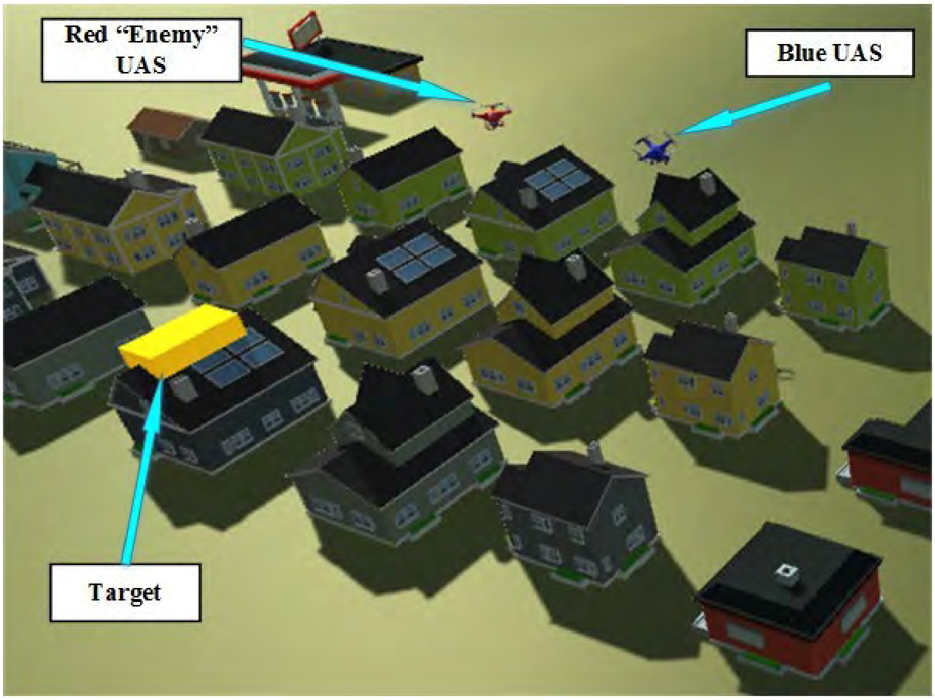


**Figure 1:** *Snapshot of UAS/Counter-UAS Graphical CONOPS*

## MISSION-LEVEL MODELING THROUGH A GRAPHICAL CONOPS

Communicating design trade-off options to decision-makers and other stakeholders in an easily understood manner is important for delivering the best system possible. The concept of operations (CONOPS) document is a common method for systems engineers to present a proposed system design to these stakeholders. However, CONOPS documents can span hundreds of pages of dense text and tables, which limits their value for busy groups of decision-makers. One relatively new approach is to create a graphical CONOPS, where the information contained in a traditional CONOPS document is presented using gaming software that provides a visual simulation of the mission scenario. Presenting system characteristics this way can be a powerful method to simplify the decision-making process (Korfiatis, Cloutier, & Zigh, 2012). A graphical CONOPS is similar to using modeling and simulation to support wargames; however, the scope of the graphical CONOPS is generally more focused than that of a wargame. In a graphical CONOPS, the decisions that influence mission success are made before the simulation starts, and it therefore does not require the strategic layers seen in wargames.

While the stakeholders interact with the gaming software, "under the hood" is a collection of engineering models that control the physics of what is being shown on screen. The stakeholders have a dashboard from which they are able to set mission parameters, including how many actors are involved as well as important design inputs for the systems involved. One key characteristic of mission-level modeling is the need to characterize and represent sources of operational, tactical, and environmental uncertainty.

The example case in this article uses a graphical CONOPS mission simulation built in the Unity game engine. In this simulation, a blue "friendly" unmanned aerial systems (UAS) is searching for a target in a suburban environment, while a red "enemy" UAS maneuvers itself to block the path of the blue UAS. The blue UAS has a limited battery life, which is set by the design inputs and puts an upper bound on the amount of time it can search. If the blue UAS finds the target, the mission is considered a success. However, if the blue UAS crashes due to depleted batteries, the mission is a failure. Figure 1 shows a snapshot of the simulation in progress.

The UAS flight trajectories are determined by a simple dynamics model. For the blue UAS, the destination it is traveling toward is randomly set every few seconds. The red UAS continuously attempts to collide with the blue UAS and knock it off its planned trajectory, while also occluding its camera view. The acceleration toward the destination for each UAS is determined by the distance to the target, where a larger distance requires greater acceleration. Specifically, the rotors apply a force related to a spring constant multiplied by the distance to destination, and this accelerating force is counteracted by a drag force. Collision forces and dynamics are handled by the collision software internal to the Unity software.

While the simulation is running, the blue UAS is constantly traveling around the suburban scene while the red UAS tries to block it. If the blue UAS comes within a threshold distance of the target while maintaining a line of sight to it, then the mission is successful.

This simulation has many inputs that can affect mission success or failure. Each UAS is defined by nine design variables that govern its geometry, power, and acceleration characteristics. Table 1 shows these simulation inputs, along with the upper and lower bounds programmed in the model. Several of these design variables are loosely bounded, and they are allowed to vary by more than an order of magnitude. However, even when the design variables are held to constant values, individual runs of the

**Table 1:** *Design Variables and Domains*

| Design Input | Lower Bound | Upper Bound |
|---|---|---|
| Battery Charge (maH) | 1 | 2000 |
| Battery Voltage (V) | 1 | 15 |
| Battery Specific Energy (MaH V / g) | 1 | 500 |
| Battery Life (min) | 1 | 60 |
| Battery Canister Mass (g) | 30 | 100 |
| Mass UAV Frame (g) | 200 | 1000 |
| Rotot Radius (cm) | 3 | 20 |
| Spring Constant (Nm) | 1 | 3 |
| UAV Volume (cm^3) | 1000 | 500000 |

simulation have highly stochastic outputs. One set of simulations with constant inputs found a range in the time that the blue UAS took to find the target from a low of 1 second to a high of 25 minutes.

The high number of input variables and level of output uncertainty raises a number of unique challenges for optimization. One of these challenges, for this and any scenario with high dimensionality and uncertainty, is that traditional optimization approaches would require many thousands of simulations in order to capture the likelihood of mission success across the design space. Running this many simulations would require a significant amount of time as well as extensive computing resources. Another challenge is that there are currently only two outputs that can be used as optimization objectives: The most important output is a binary parameter representing mission success or failure, and the secondary objective is a continuous parameter representing the time to find the target.

## COMPLEX SYSTEM OPTIMIZATION

A broad range of research has examined challenges related to the optimization of complex systems. Much of this is in the domain of multidisciplinary design optimization (MDO), which includes architectural techniques to manage different disciplinary or subsystem models, as well as algorithms and response surface techniques for optimizing simulation models. MDO techniques enable designers to ensure that subsystem interaction behavior is adequately modeled and that optimization is performed in an accurate and efficient manner (Martins & Lambe, 2013).

When the objective or constraint functions involve simulations, such as a computational fluid dynamics (CFD) model or a graphical CONOPS, a number of approaches are available to facilitate optimization. These methods can be broken down into four categories: random search and metaheuristics, ranking and selection, direct gradient methods, and surrogate model methods (Barton & Meckesheimer, 2006). Often, this choice can be difficult when the simulations include "black boxes," where the underlying functions are unknown and only inputs and outputs can be used for analysis.

Another theme that is common to complex system design problems is the presence of uncertainty, which can be in the variables, parameters, or models themselves. While robust design optimization (RDO) and reliability-based design optimization (RBDO) (Paiva & Crawford, 2010) have been successfully used to optimize designs in situations where the uncertainty is low, such as in component tolerances, their applicability to scenarios with very high levels of uncertainty is limited. Both methods assume that the problems have well-defined constraints and well-known levels of uncertainty that can be analytically modeled. However, when optimizing for mission success, where many sources of extreme epistemic and aleatory uncertainty are present, alternative optimization approaches are needed.

## WHAT IS MISSION-LEVEL OPTIMIZATION?

Mission-level optimization has not been clearly and consistently defined in the literature. In this case, we refer to the optimal design of a system to successfully perform a job that takes place under highly varying external conditions. Crucially, the complexity of the mission scenario can bring about many different outcomes, and the most meaningful way to describe these outcomes is either success or failure. There are likely "intermediate" outputs, often referred to as key performance indicators (KPIs) when discussing system-level optimization, which may or may not be correlated to mission success but on their own do not account for environmental or operational factors.

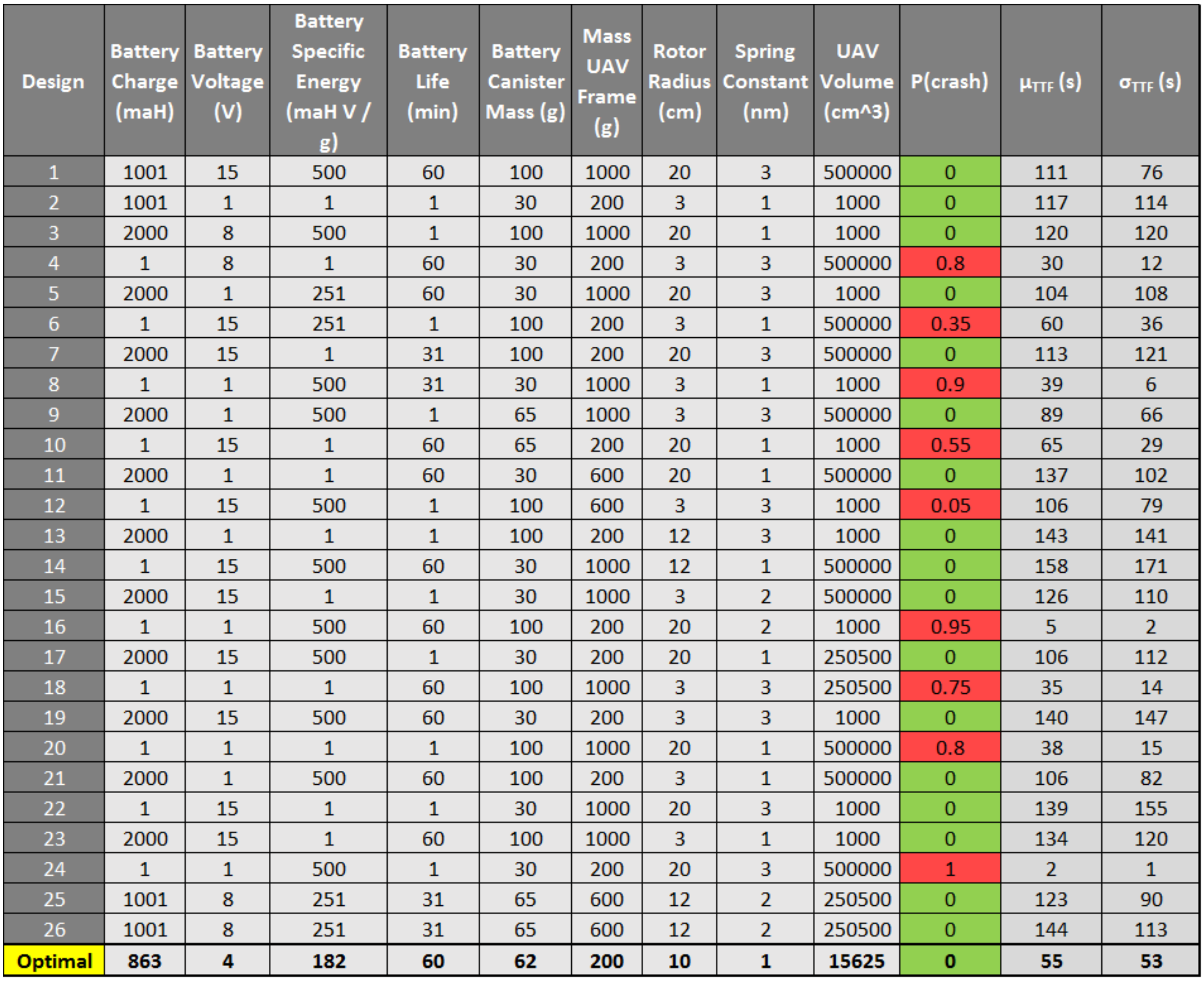
Previous work that discusses mission-level optimization has largely focused on autonomous robot design and aerospace vehicles. Mission-level optimization of autonomous robots seeks the highest possible success/failure ratio when performing tasks such as maneuvering over an obstacle (Tesch, Schneider, & Choset, 2013) or grasping an object (Boularias, Bagnell, & Stentz, 2014). As in the current study, the objective is a binary success or failure output; however, their design variables relate to the robots' behavior rather than the hardware design, and they do not account for high levels of operational or environmental uncertainty. The studies on mission-level optimization of aerospace vehicles typically refer to the tasks their systems perform as missions, using continuous objective functions that can leverage the optimization methods of more general problems (Bérend, Bertrand, & Jolly, 2007; Goulos et al., 2013; Yang, Luo, & Zhang, 2013). The key differences between the previous uses of the term and our definition are the emphases on the binary success/failure output and the presence of high levels of operational and environmental uncertainty.

> "This simulation has many inputs that can affect mission success or failure."

## OPTIMIZING THE MISSION-LEVEL GAMING SIMULATION

In order to simplify analysis, a "headless" version of the graphical CONOPS simulation was developed, in order to suppress the graphical user interface (GUI) and allow automated and accelerated simulation through command line arguments. This was then wrapped in the Phoenix Integration ModelCenterTM MDO software package to perform a diverse set of simulations using a "design of experiments" (DOE) (Myers, Montgomery, Anderson-

**Table 2:** *Simulation Sample Inputs and Outputs, including Definitive Screening Design (DSD) and Optimal Solution*



| Design | Battery Charge (maH) | Battery Voltage (V) | Battery Specific Energy (maH V / g) | Battery Life (min) | Battery Canister Mass (g) | Mass UAV Frame (g) | Rotor Radius (cm) | Spring Constant (nm) | UAV Volume (cm^3) | P(crash) | $\mu_{TTF}$ (s) | $\sigma_{TTF}$ (s) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1001 | 15 | 500 | 60 | 100 | 1000 | 20 | 3 | 500000 | 0 | 111 | 76 |
| 2 | 1001 | 1 | 1 | 1 | 30 | 200 | 3 | 1 | 1000 | 0 | 117 | 114 |
| 3 | 2000 | 8 | 500 | 1 | 100 | 1000 | 20 | 1 | 1000 | 0 | 120 | 120 |
| 4 | 1 | 8 | 1 | 60 | 30 | 200 | 3 | 3 | 500000 | 0.8 | 30 | 12 |
| 5 | 2000 | 1 | 251 | 60 | 30 | 1000 | 20 | 3 | 1000 | 0 | 104 | 108 |
| 6 | 1 | 15 | 251 | 1 | 100 | 200 | 3 | 1 | 500000 | 0.35 | 60 | 36 |
| 7 | 2000 | 15 | 1 | 31 | 100 | 200 | 20 | 3 | 500000 | 0 | 113 | 121 |
| 8 | 1 | 1 | 500 | 31 | 30 | 1000 | 3 | 1 | 1000 | 0.9 | 39 | 6 |
| 9 | 2000 | 1 | 500 | 1 | 65 | 1000 | 3 | 3 | 500000 | 0 | 89 | 66 |
| 10 | 1 | 15 | 1 | 60 | 65 | 200 | 20 | 1 | 1000 | 0.55 | 65 | 29 |
| 11 | 2000 | 1 | 1 | 60 | 30 | 600 | 20 | 1 | 500000 | 0 | 137 | 102 |
| 12 | 1 | 15 | 500 | 1 | 100 | 600 | 3 | 3 | 1000 | 0.05 | 106 | 79 |
| 13 | 2000 | 1 | 1 | 1 | 100 | 200 | 12 | 3 | 1000 | 0 | 143 | 141 |
| 14 | 1 | 15 | 500 | 60 | 30 | 1000 | 12 | 1 | 500000 | 0 | 158 | 171 |
| 15 | 2000 | 15 | 1 | 1 | 30 | 1000 | 3 | 2 | 500000 | 0 | 126 | 110 |
| 16 | 1 | 1 | 500 | 60 | 100 | 200 | 20 | 2 | 1000 | 0.95 | 5 | 2 |
| 17 | 2000 | 15 | 500 | 1 | 30 | 200 | 20 | 1 | 250500 | 0 | 106 | 112 |
| 18 | 1 | 1 | 1 | 60 | 100 | 1000 | 3 | 3 | 250500 | 0.75 | 35 | 14 |
| 19 | 2000 | 15 | 500 | 60 | 30 | 200 | 3 | 3 | 1000 | 0 | 140 | 147 |
| 20 | 1 | 1 | 1 | 1 | 100 | 1000 | 20 | 1 | 500000 | 0.8 | 38 | 15 |
| 21 | 2000 | 1 | 500 | 60 | 100 | 200 | 3 | 1 | 500000 | 0 | 106 | 82 |
| 22 | 1 | 15 | 1 | 1 | 30 | 1000 | 20 | 3 | 1000 | 0 | 139 | 155 |
| 23 | 2000 | 15 | 1 | 60 | 100 | 1000 | 3 | 1 | 1000 | 0 | 134 | 120 |
| 24 | 1 | 1 | 500 | 1 | 30 | 200 | 20 | 3 | 500000 | 1 | 2 | 1 |
| 25 | 1001 | 8 | 251 | 31 | 65 | 600 | 12 | 2 | 250500 | 0 | 123 | 90 |
| 26 | 1001 | 8 | 251 | 31 | 65 | 600 | 12 | 2 | 250500 | 0 | 144 | 113 |
| **Optimal** | **863** | **4** | **182** | **60** | **62** | **200** | **10** | **1** | **15625** | **0** | **55** | **53** |

Cook, 2016), evaluate the results, and perform optimization.

Due to the high stochasticity of the results even when the design variables are held constant, the mission-level objective is to minimize the probability of crash and failure, *P(crash)*, over multiple runs of the simulation. Each set of inputs evaluated was run 20 times in order to characterize the different designs along this objective. In order to efficiently explore the design space, a DOE-based approach was leveraged using a definitive screening design (DSD) (Jones & Nachtsheim, 2011) with JMP 13 Pro Statistical Discovery SoftwareTM. Screening designs are useful for early design phases to quickly identify major trends in how the design variables affect the outputs. The DSD assesses each input at three levels, providing the ability to identify and potentially model curvature in the outputs when compared to a two-level screening design, which can only model linear effects. The DSD required 26 design variants, and with each replicate repeated 20 times, a total of 520 simulations were executed, shown in Table 2. Of the 26 unique design variants evaluated, 18 of them had a 100 percent mission success rate. The UAS designs that experienced failures show a wide range of success rates, with design variant number 24 having zero successful runs.

While mission success is the optimization objective in this case, the time to find the target is another important output that can be used to determine the best designs. By minimizing the mean time to find the target, $\mu_{TTF}$, the mission success rate will also, generally, increase. However, this can be complicated by the way that the model accounts for failed runs. For example, many designs with weak batteries actually have a low $\mu_{TTF}$, because the battery life will put an upper limit on the amount of time the UAS takes to find the target regardless of mission success. This means that while these designs have more failures, their successful runs will be completed very quickly; examples include designs 16 and 24 in Table 2. To address this issue, a bi-objective optimization problem can be formulated to minimize both *P(crash)* and $\mu_{TTF}$, which results in a Pareto-optimal set giving decision-makers information about the tradeoffs among the different objectives.

Analyzing the data from the simulation experiment using JMP Pro 13TM and ModelCenter$^{TM}$, a sensitivity

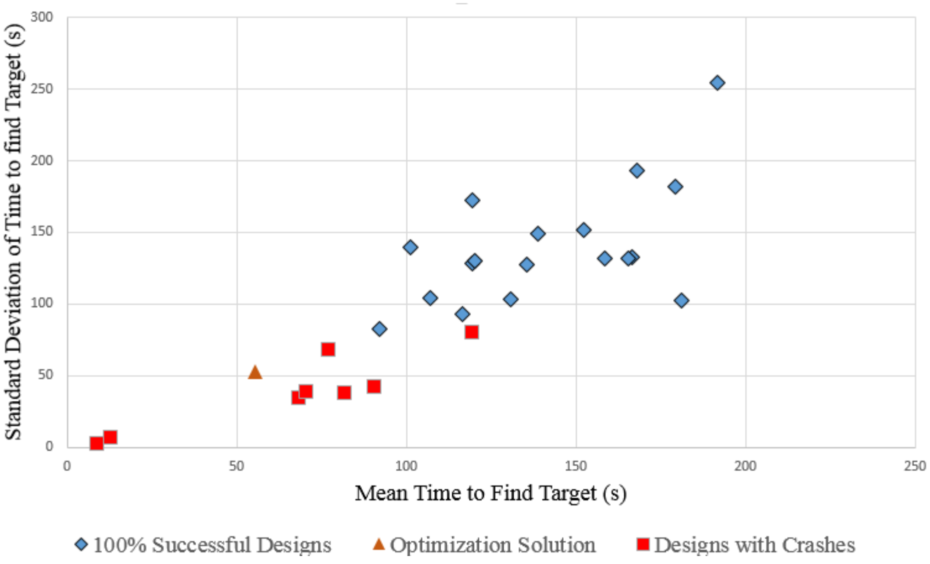


**Figure2:** *Bi-Objective Plot of All Design of Experiments Runs with Optimal Solution*

analysis was performed using only the successful runs to identify and rank model inputs by how much they influence the outputs. The analysis found that, for instance, the battery canister mass had very little effect on any of the outputs and could reasonably be ignored when creating surrogate models for the three objectives. On the contrary, the objectives are highly sensitive to the level of battery charge, which is used in the surrogate models.

For *P(crash)*, a binary logistic regression model, a form of generalized linear models (McCullagh & Nelder, 1989), was trained. Firth penalized likelihood (Firth, 1993) was employed to account for the sparsity of design runs resulting in mixed results (both successes and failures). The surrogates for $\mu_{TTF}$ and $\sigma_{TTF}$ were analyzed using loglinear variance regression models, which capture relationships between the input and output in both the mean and variance effects (Carroll & Ruppert, 1988). These models are then used to create a utility function to find the best design inputs depending on how much stakeholders weigh the three objectives against one another. The weights used for this analysis are 5 for *P(crash)*, 3 for $\mu_{TTF}$, and 1 for $\sigma_{TTF}$.

An optimal solution that maximizes this utility was found with a predicted *P(crash)* of less than 2 percent, $\mu_{TTF}$ of 69.1 seconds, and $\sigma_{TTF}$ of 51.7 seconds. This design, seen at the bottom of Table 2, was then simulated 20 times in order to fully capture its behavior, resulting in an evaluated *P(crash)* of zero, a $\mu_{TTF}$ of 55.4 seconds, and a $\sigma_{TTF}$ of 52.6 seconds. These results both fit the prediction very well and represent a significant upgrade over the other design points with a 100 percent observed success rate, even by using this relatively straightforward and efficient optimization technique. The upgrade in system desirability can be seen in Fig. 2, where the optimization solution is clearly better than any of the other solutions that did not experience crashes in their 20 simulated missions.

> *"Screening designs are useful for early design phases to quickly identify major trends in how the design variables affect the outputs."*

## CONCLUSIONS

Mission-level optimization offers a new approach to designing systems in which the objective is to succeed at particular tasks under highly stochastic operational and environmental conditions. One way to do this that can engage multiple stakeholders is to link graphical CONOPS simulations with design optimization tools. The graphical CONOPS was originally developed to provide decision-makers with a realistic visualization of the system while also showing mission-level outcomes, supporting the vision of MBSE. Design optimization has long been used at the system level to maximize key performance indicators, which generally contribute to mission success but are not always synonymous with these higher-level outcomes. Combining these methods results in an improved approach to design for mission success.

The use case in this article demonstrates how mission-level optimization can be done for a relatively simple surveillance mission, where the optimization challenges are the high levels of uncertainty in environmental and operational parameters and the large number of design variables. Using statistical sampling, modeling, and optimization methods, an optimal system design was identified that had a simulated 100 percent mission success and better KPIs than any of the successful designs from the original sample, showing that mission-level optimization can be efficiently and effectively done with relatively small numbers of simulation executions, even in the presence of extreme variation.

As the systems engineering community advances its MBSE capabilities in linking multi-domain models into comprehensive representations of system behavior, the ability to optimize for success under highly stochastic mission scenarios will become increasingly valuable. Combining graphical CONOPS and state-of the-art statistical and optimization techniques can help bridge the communications and modeling gaps between strategic decision-makers and domain-modeling subject matter experts, while supporting the identification of optimal system designs for mission success.

## REFERENCES

[1] Barton, R. R., & Meckesheimer, M. (2006). Chapter 18 Metamodel-Based Simulation Optimization. ***Handbooks in Operations Research and Management Science***, 13(C), 535–574. https://doi.org/10.1016/S0927-0507(06)13018-2

[2] Bérend, N., Bertrand, S., & Jolly, C. (2007). Optimization method for mission analysis of aeroassisted orbital transfer vehicles. ***Aerospace Science and Technology***, 11(5), 432–441. https://doi.org/10.1016/j.ast.2007.01.007

[3] Boularias, A., Bagnell, J. A., & Stentz, A. (2014). Efficient Optimization for Autonomous Robotic Manipulation of Natural Objects. ***AAAI Conference on Artificial Intelligence***, 2520–2526.

[4] Carroll, R. J., Ruppert, D., Stefanski, L. A., & Crainiceanu, C. M. (2006). ***Measurement error in nonlinear models: a modern perspective***. Chapman and Hall/CRC.

[5] Firth, D. (1993). Biometrika Trust Bias Reduction of Maximum Likelihood Estimates Author ( s ): David Firth Published by : Oxford University Press on behalf of Biometrika Trust Stable URL : http://www.jstor.org/stable/2336755 REFERENCES Linked references are available on ***J. Biometrica Trust***, 80(1), 27–38.

[6] Goulos, I., Hempert, F., Sethi, V., Pachidis, V., d'Ippolito, R., & d'Auria, M. (2013). Rotorcraft Engine Cycle Optimization at Mission Level. ***Journal of Engineering for Gas Turbines and Power***, 135(9), 091202. https://doi.org/10.1115/1.4024870

[7] Jones, B. (2010). mODa 9 – Advances in Model-Oriented Design and Analysis, (October 2010), 0–15. https://doi.org/10.1007/978-3-7908-2410-0

[8] Korfiatis, P., Cloutier, R., & Zigh, T. (2012). Graphical CONOPS Development to Enhance Model- Based Systems Engineering. ***Development***, (June), 18–20. https://doi.org/10.1073/pnas.0709132105

[9] Martins, J. R. R. A., & Lambe, A. B. (2013). Multidisciplinary Design Optimization: A Survey of Architectures. ***AIAA Journal***, 51(9), 2049–2075. https://doi.org/10.2514/1.J051895

[10] Paiva, R. M., & Crawford, C. (2010). A Robust and Reliability Based Design Optimization Framework for Wing Design. ***Aerospace***, 52(April), 2919–2919. https://doi.org/10.2514/1.J052161

[11] Ramos, A. L., Ferreira, J. V., & Barceló, J. (2012). Model-based systems engineering: An emerging approach for modern systems. ***IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews***, 42(1), 101–111. https://doi.org/10.1109/TSMCC.2011.2106495

[12] Tesch, M., Schneider, J., & Choset, H. (2013). Expensive function optimization with stochastic binary outcomes. ***30th International Conference on Machine Learning, ICML 2013, n PART 3***, 2320–2328. Retrieved from https://www.engineeringvillage.com/share/document.url?mid=cpx_52c24f28145700c9863M55a110178163125&database=cpx

[13] Yang, Z., Luo, Y. Z., & Zhang, J. (2013). Two-level optimization approach for Mars orbital long-duration, large non-coplanar rendezvous phasing maneuvers. ***Advances in Space Research***, 52(5), 883–894. https://doi.org/10.1016/j.asr.2013.05.013

## ABOUT THE AUTHORS

**BRIAN CHELL** is a Ph.D. candidate in Systems Engineering in the School of Systems and Enterprises at Stevens Institute of Technology, focusing on multidisciplinary design optimization (MDO). His research interests are in reducing the computing resources required for optimizing complex systems and techniques for applying MDO early in the design lifecycle. Brian received an M.E. in Space Systems Engineering from Stevens Institute of Technology and a B.S. in Aerospace Engineering Sciences from the University of Colorado Boulder.

**STEVEN HOFFENSON** is an Assistant Professor in the School of Systems and Enterprises at Stevens Institute of Technology. His research focuses on design, sustainability, and complexity, and he studies design processes, sustainable design methods, systems modeling, and policy analysis. Dr. Hoffenson holds a B.S. in Mechanical Engineering from the University of Maryland and an M.S.E. and Ph.D. in Mechanical Engineering from the University of Michigan. Prior to joining Stevens, he served as a Congressional Fellow of the American Association for the Advancement of Science (AAAS) in 2014-15.

**DOUGLAS RAY**, PStat, is the Lead Statistician of the Statistical Sciences Group at the US Army CCDC Armaments Center at Picatinny Arsenal, NJ. His work focuses on applying industrial statistics to armament systems across the acquisition life cycle. His work focuses on Design of Experiments, reliability data analysis, machine learning, and uncertainty quantification/probabilistic optimization of computational models and simulations. Mr. Ray leads a team of 12 statisticians and data scientists who collaborate with engineering teams on a spectrum of armament projects and systems. He is currently a Ph.D. candidate in Systems Engineering at Stevens Institute of Technology. Mr. Ray is the Chair-Elect of the ASA's Section on Statistics in Defense and National Security, an ASA Accredited Professional Statistician, a Lean Six Sigma Black Belt, and an ASQ Certified Reliability Engineer. In addition to his 13 years of experience as a DoD Mathematical Statistician he is also a retired combat veteran of the US Army.

**ROGER D. JONES** is a physicist and entrepreneur. He currently is a Research Fellow at the Center for Complex Systems and Enterprises at the Stevens Institute of Technology and a scientist with the X-Center Network.

**MARK R. BLACKBURN, PH.D**. is a Senior Research Scientist with Stevens Institute of Technology and serves on the System Engineering Research Center (SERC) research council. Dr. Blackburn is the Principal Investigator on SERC research tasks for both Naval Air Systems Command NAVAIR and U.S. Army ARDEC on Systems Engineering Transformation through Model-Centric Engineering.

# Discover the value of sharing your DoD-funded research...

Increase peer citations and worldwide dissemination

Advance industry innovation

Inspire increase use of past S&T work

Leverage results of defense-funded research

Ensure long-term availability and preservation of documents

**SUBMIT** your research today!

R&E Gateway *Powered by* DTIC

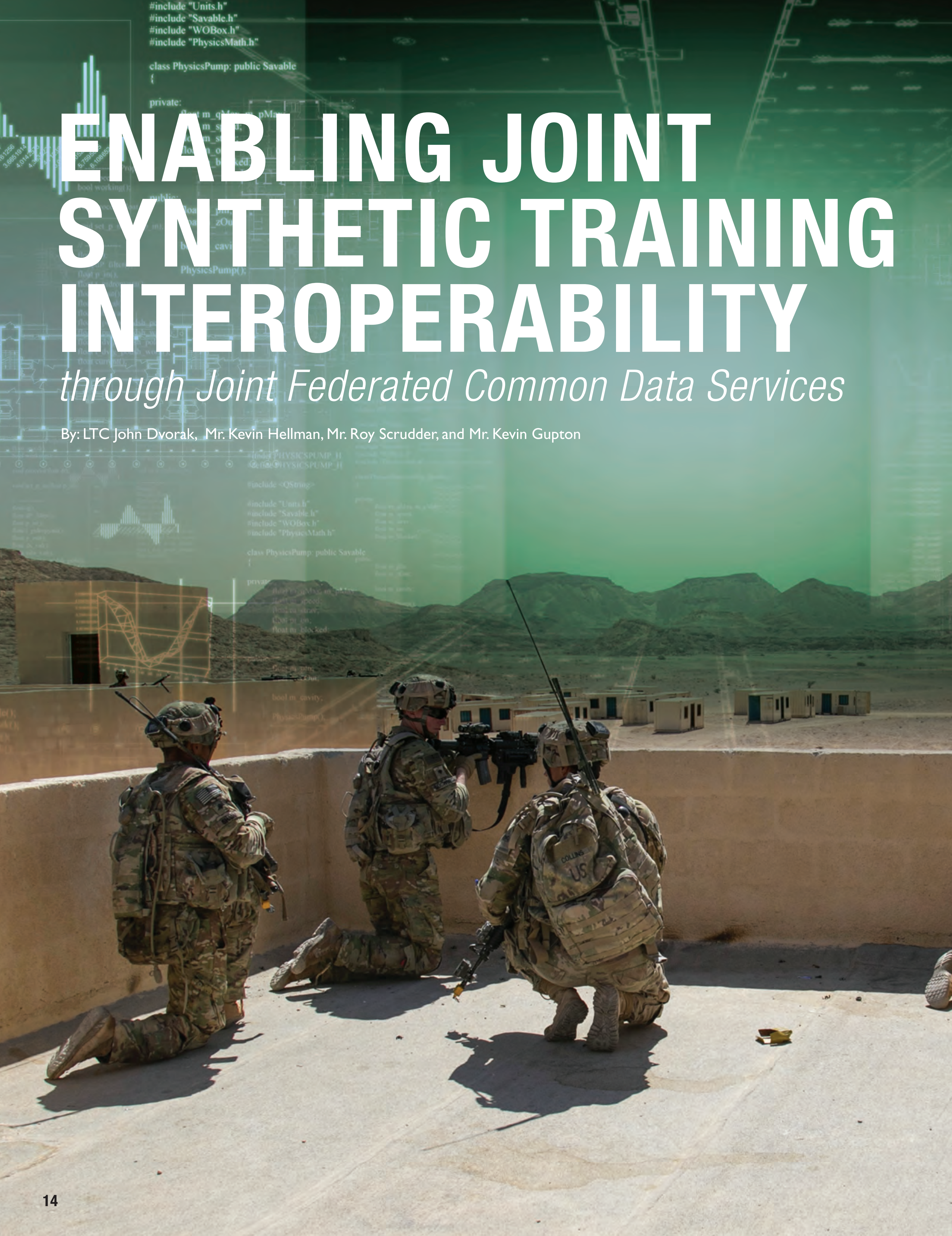
**https://go.usa.gov/xVMjH**

Defense Technical Information Center (DTIC) | Fort Belvoir, VA | https://discover.dtic.mil

# ENABLING JOINT SYNTHETIC TRAINING INTEROPERABILITY

## *through Joint Federated Common Data Services*

By: LTC John Dvorak,  Mr. Kevin Hellman, Mr. Roy Scrudder, and Mr. Kevin Gupton



// ------------ Properties
float speed();
bool working();
void process(float dt);
void set_p_in(float p_in);
// ------------
float q();
float dP_filter();
float p_in();
float t_gidropyata();
float p_out();
float dx_val();
float vibr_val();
float t_pump_podsh_pole();
float t_pump_podsh_work();
float t_dvig_podsh_pole();
float t_dvig_podsh_work();
float current();
void PIDRegulator::valve_3d_open()
void PIDRegulator::valve_3d_close()
void PIDRegulator::valve_3d_stop()
void PIDRegulator::valve_3d_shturval_button_cl
void PIDRegulator::set_broken(bool broken)
Symbols:
- Fluorescent lamps
- Junction box
- Switch Splashproof
- ACCIDENTAL lamp lighting
- lamp emergency lighting
- cabinet powerplant, a distribution
panel lighting

**THE JOINT TRAINING ENTERPRISE (JTE) REQUIRES EFFECTIVE INTEGRATION OF AND TECHNICAL INTEROPERABILITY AMONG DISPARATE SYNTHETIC TRAINING CAPABILITIES FROM ACROSS THE SERVICES TO ENHANCE JOINT OPERATIONAL CAPABILITY AND ACHIEVE JOINT READINESS. OPPORTUNITIES TO ENHANCE JOINT TRAINING INTEROPERABILITY INCREASE WHEN DISPARATE SYNTHETIC TRAINING CAPABILITIES EMPLOY COMMON OR SHARED MODELS AND SIMULATION DATA.**

This idea underpins the development of ***common data services (CDS)***, a coordinated capability designed to rapidly locate, access, transform, transmit, to enhance the JTE's synthetic training capabilities. Overlaying the CDS concept across the JTE creates the framework for ***Joint Federated Common Data Services (JFCDS)***, which enables each Service to develop and maintain its own data service provisioning capability, federated through common technical standards and protocols, which together allow the sharing of authoritative source data among the Services and across the JTE.

This article explores data-related synthetic training interoperability gaps, considers how current capabilities and capabilities in development (partially) address these gaps, and shows how JFCDS effectively leverages the successful attributes of these programs while meeting remaining data-related shortfalls.

While this paper focuses on the needs and solution for joint training, the same needs exist for training within the Services and extend to other application areas for modeling and simulation with the DoD. The modeling and simulation users supporting acquisition, experimentation, and test and evaluation require the same type of CDS solutions to provide current, authoritative, and appropriate data. The ability to locate, obtain, and integrate data from sources across DoD components is critical to enable innovation at the pace necessary to provide agile and adaptive systems for the defense of our nation.

## INTRODUCTION

The Joint Training Enterprise requires a systemic approach to synthetic training capability development and integration that leverages collaboration and cooperation among joint training stakeholders by enhancing, facilitating, and synchronizing information sharing, capability development requirements management, and technical interoperability. A series of documents articulates DoD and Joint strategy, policy, and governance to this end, including DoDD 5000.59, "DOD Modeling and Simulation Management", DoDI 5000.70 "Management of DoD Modeling and Simulation (M&S) Activities," the 2018 Joint Technical Training Interoperability Strategy, and the 2016 Joint Training Technical Interoperability Memorandum For Record. Yet for this approach to succeed, Joint stakeholders must commit to the development and Joint-level integration of their synthetic training capabilities so the Joint Force can truly train as it fights. When disparate synthetic training capabilities employ common or shared models and simulation data, the capacity to integrate these capabilities increases. The Joint Training Enterprise, led by the Joint Staff J7 through its Joint Training Synthetic Environment (JTSE) Work Group (WG), has therefore an interest in developing a framework for the discovery and access to authoritative data sources.

This initiative seeks to provide *common data services*, a coordinated capability to rapidly locate, access, transform, transmit, and distribute authoritative source data. These data types include terrain and geospatial, order of battle, parametric, and operational environment data describing Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT) variables — each correlated into application-usable formats that facilitate interoperability among joint synthetic training capabilities. This article will describe the simulation data-related problems and gaps within the broad portfolio of synthetic joint training enablers and show how the concept of common data services—implemented through the provision of a standardized architecture of authoritative data and transformation as a service in a cloud based, web enabled platform—will facilitate interoperability among these capabilities across the Joint Training Enterprise. Accordingly, this paper proposes a framework for **Joint Federated Common Data Services (JFCDS)** in which each Service develops and maintains its own data service provisioning capability, federated through common technical standards and protocols, which allows the sharing of authoritative source data among the Services. JFCDS leverages individual Service expertise on their respective authoritative data sources and training enabler data needs for the benefit of the whole Joint Training Enterprise. JFCDS further improves synthetic training capability interoperability across Services and therefore enhances the training of joint combined arms operations.

"*Joint training exists to improve joint operational capability and to achieve joint readiness, each integral to the Services' collective capacity to conduct joint combined arms operations.*"

## BACKGROUND

Joint training exists to improve joint operational capability and to achieve joint readiness, each integral to the Services' collective capacity to conduct joint combined arms operations. The conduct of joint training exercises, using distributed simulation-based training enablers, constitutes an integral component of the joint training strategy. These simulation-based training enablers depend upon readily accessible, consistent, up-to-date data in both their development and subsequent employment across the Joint Event Life Cycle (JELC)—this includes event planning, scenario generation, exercise execution, and after action review (which correlates to the Army's Operations Process—Plan, Prepare, Execute, and Assess). Unfortunately, the JELC cycle is often costly in terms of time, manpower, and resources due to the difficulties involved in synchronizing and integrating the current portfolio of joint synthetic training capabilities in service of a common joint training event.

Yet the Services' use of the same authoritative data baseline for their respective synthetic training capabilities (present and future) may significantly reduce joint training interoperability challenges. Additionally, such a data-service foundation would enable data preparation and management throughout the JELC, thereby reducing time, manpower, and resource requirements.

## PROBLEM OVERVIEW AND ROOT CAUSES

With respect to the data required to support the use of Live, Virtual, Constructive, and Gaming (LVC-G) simulations and capabilities in conjunction with mission command/command and control systems (MC/C2), three core problems currently exist. First, the preparation and provisioning of appropriate data for use LVC-G simulation and MC/C2 systems for joint training (and Service-specific training) takes too much time. Using current methods and tools (and in response to often changing exercise design and associated training requirements), data preparation and provisioning can take weeks to months. Second, these data preparation and provisioning processes are labor-intensive (requiring a significant, dedicated staff) and thus are costly. Finally, inconsistencies in data used among LVC-G systems and between LVC-G and MC/C2 systems negatively impact training quality, consistency, and availability.

The above core problems are attributable to a variety of root causes. In some cases, governance bodies have not identified the appropriate sources for data required for joint training. Data sources include both the authoritative sources and the sources for additional data required to provide sufficient level-of-detail (LOD) for applying LVC-G simulation. Additionally, authoritative data sources are often hard to access (security or policy issues), incomplete in content; or include errors, gaps, and out-of-date data. Training and exercise planners cannot consistently and thoroughly discover what data is available from these sources, as well as what data from prior training events is suitable for reuse.

Once data has been identified, automated capabilities are lacking at times to support request and delivery or direct retrieval of the needed information. Complicating the use of data is the fact that there are many formats and standards for simulation data – currently each model and/or simulation has proprietary data formats and standards. Simulation data managers often create and maintain characteristics such as parametric, probability of hit/probability of kill (Ph/Pk), weapons pairing, etc., at the individual simulation level. Some of this variation reflects the current reality that Services have different simulation needs and training requirements that demand varying levels of fidelity and resolution.

*"Training and exercise planners lack automated capabilities to combine and transform data from multiple sources into a form that is appropriate for use in LVC-G and MC/C2 systems."*

Training and exercise planners lack automated capabilities to combine and transform data from multiple sources into a form that is appropriate for use in LVC-G and MC/C2 systems. These features include capabilities to select data subsets, merge data from multiple sources, and transform data both semantically (e.g., enumeration translation) and syntactically (e.g., format translation).

As seen, data challenges encompass issues with "visibility, access, extraction, understandability, trust, interoperability, transformation (including [modification], fusion, integration, enhancement, filtering, and tailoring), and reuse" (PEO-STRI, 2015). The aforementioned issues clarify the problem space and inform (practically and methodically) the requirement for both technical and management solutions that incorporate JFCDS.

## FOUNDATIONAL DATA STRATEGY

The data concerns of the US Government and DoD are far larger than how data supports Joint Training; nevertheless, the US Government's strategy to solve difficult data-related problems will inform this paper's recommended approach. Strategic documents that shape the broad approaches that the Federal Government and DoD employ in their respective enterprise data strategies include the DoD Net-Centric Data Strategy (US Department of Defense, 2003), DoD Net-Centric Services Strategy (US Department of Defense, 2007), and the Federal Cloud Computing Strategy (Kundra, Vivek: US Chief Information Officer, 2011). The Joint Federated Common Data Services framework proposed in this paper seeks to build on these strategies and nest with the goals of the JTSE in order to build a coherent, holistic approach for managing the provision and use of data among emerging synthetic training capabilities.

## VISION STATEMENT

With these core problems, root causes, and governing strategy documents as a point of departure, the authors present the following vision for Joint Federated Common Data Services:

> The Joint Training Enterprise will, in conjunction with Intergovernmental, Multinational, and Commercial partners, develop the technical and procedural infrastructure required to ensure the availability of data and enable its rapid discovery and retrieval; while leveraging common data service principles and standards; and employing Authoritative Data Sources (ADS) in standardized "simulation and application agnostic" exchange formats, to inform the development and use of next-generation, interoperable training capabilities within the Joint Training Synthetic Environment (JTSE), including the Army's Synthetic Training Environment (STE), the Navy Continuous Training Environment (NCTE), the Marine Corps Synthetic Training Environment (MCSTE), the Air Force

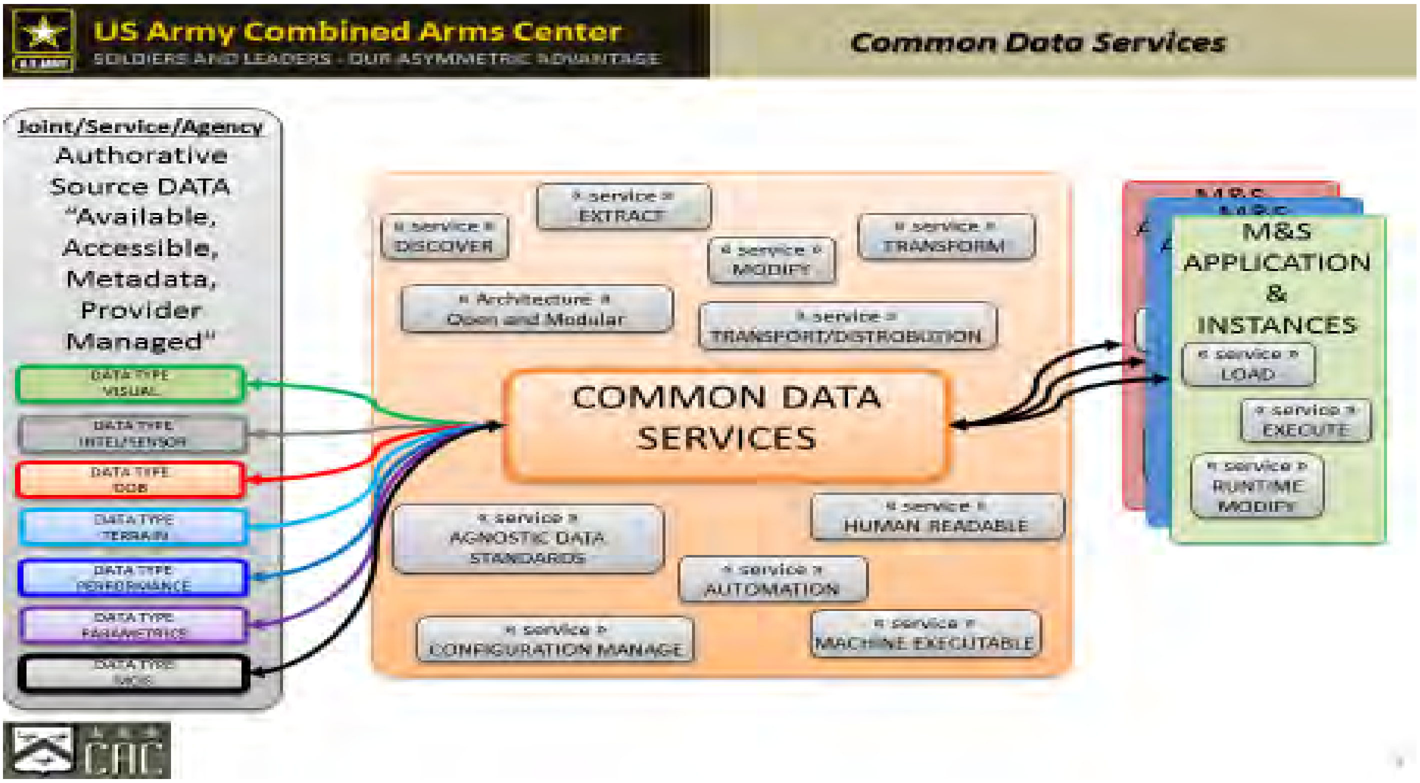

US Army Combined Arms Center
SOLDIERS AND LEADERS - OUR ASYMMETRIC ADVANTAGE
Common Data Services
Joint/Service/Agency
Authorative Source DATA "Available, Accessible, Metadata, Provider Managed"
DATA TYPE VISUAL
DATA TYPE INTEL/SENSOR
DATA TYPE OOB
DATA TYPE TERRAIN
DATA TYPE PERFORMANCE
DATA TYPE PARAMETRICS
DATA TYPE MOE
« service » DISCOVER
« service » EXTRACT
« service » MODIFY
« service » TRANSFORM
« Architecture » Open and Modular
« service » TRANSPORT/DISTROBUTION
COMMON DATA SERVICES
« service » AGNOSTIC DATA STANDARDS
« service » HUMAN READABLE
« service » AUTOMATION
« service » CONFIGURATION MANAGE
« service » MACHINE EXECUTABLE
M&S APPLICATION & INSTANCES
« service » LOAD
« service » EXECUTE
« service » RUNTIME MODIFY
CAC

**Figure 1:** *Common Data Services Concept*

Operational Training Infrastructure (OTI), and other emerging Service synthetic training capabilities.

## CURRENT CAPABILITIES AND CAPABILITIES IN DEVELOPMENT

This section considers the ways data managers in Joint Training and other M&S application areas have positioned past, current, and in-development data management capabilities to meet requirements, while exploring remaining data-related gaps. This analysis seeks to inform design discussions and Joint Title X authorities for validation of emerging data-related capability requirements that the JFCDS is intended to satisfy. Over the last 25 years, data managers in DoD that have sought to address many of the issues outlined in above, via numerous efforts. These efforts focused on one or more of the following activities:

- Discovery of data for use in M&S.
- Transformation of data from its source form and the merging of data to generate data appropriate for use in M&S.
- Access to (or retrieval) of that data.

These activities support three high-order, training simulation use-cases. First, data is need for exercise planning and preparation. Second, software engineers need data to support the engineering the synthetic training capabilities. To reuse of data and support event timelines, commonly a third preemptive activity occurs--the bulk preparation of data to support those first two activities.

These efforts inform both design discussions and Joint Title X authorities for validation of emerging data-related capability requirements that the JFCDS is intended to satisfy. A survey of both current and future capabilities demonstrate how each are positioned to meet data-related requirements while exploring remaining data-related gaps. Programs like the Global Force Management Data Initiative (GFM DI), Defense M&S Catalog, Joint Data Support (JDS), Joint Rapid Scenario Generation (JRSG), Joint Training Data Services (JTDS), Enterprise Data Services (EDS), Data Services Environment (DSE) and Unified Data have made important strides in the provision of a variety of disparate data sources. To varying degrees, they promoted reuse, provided analytical baselines of models and data, and showed that governance was possible through the establishment of standards for databases, scenarios, and terrain. Innovative features such as semantic search and scenario development made finding and using data easier. Additionally, AMSO's Unified Data initiative, in its design to acquire access to authoritative source data, constitutes another important achievement. These programs also demonstrated limitations of keeping source data and model catalogs current, providing data at the required level of accuracy and resolution (i.e., data abstracted at too high of a level), and answering all data questions with only metadata. These limitations continue as manifestations of the core, systemic problems in data provisioning.

## CDS OVERVIEW

Here the authors describe the Common

Data Services concept that we advocate advancing within the Joint Federated Common Data Services framework. The data required by today's M&S systems spans a broad range of uses, type, content, and resolution. Managing this data, and providing timely and effective access to it, requires leveraging and advancing key capabilities and technology areas, including:

- Architecture (systems, reference)
- Standards (data exchange, enumerations, logical data models/ontologies, service interface specifications)
- User interfaces (user applications, widgets)
- Tools (transform, inspect, auto-correct, enhance, integrate/fuse, add value, tailor, auto data creation)
- Data tagging (discovery, structural, and semantic metadata)
- Discovery tools and services
- Automatic service composition and orchestration

A coherent architecture to support the data services' operational activities—from data generation, through data integration, provisioning of data to simulations, and managing the data produced for and/or resulting from M&S executions—is essential. The architecture must rely on the use of standards to reduce integration costs by ensuring interoperability at the technical, semantic, and syntactic levels. The architecture must utilize a services-based approach to the maximum extent possible; we must therefore customize data management capabilities through integrating and orchestrating a set of commonly available services. Reuse or development of appropriate system-level architectures is essential for ensuring different M&S users (and different M&S systems) can access, exchange or retrieve, and understand the data they need. This requirement demands significant use and/or extension of appropriate standards that ensure consistency and cost-savings in handling diverse data. These include standards for accessing, identifying, representing, understanding, and—importantly—transforming data according to established semantic, syntactic, and technical standards that are agnostic to the ingesting simulation or application. Accordingly, data management should be a cooperative, Service effort that leverages open standard formats and machine interfaces, to provide the user required data access at the point of need (PON).

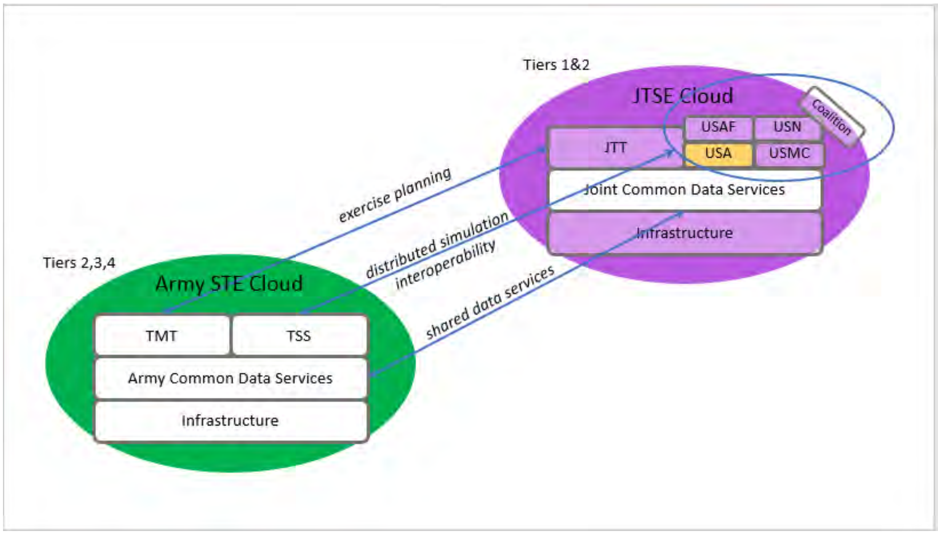


**Figure 2:** *Army Application Services (including Army Common Data Services)*

Identifying the relevant and desired data relies on the use of proper data tagging and discovery techniques. This process, in turn, requires the development of meaningful and standardized tagging techniques and encoding values that can be processed by machines (and not just humans), as well as the engineering and development of methods for automating both the tagging and discovery processes. The development of supporting tools and services that enable automated data tagging and discovery is also essential. Rapid and accurate retrieval of data, using standard discovery and structural metadata, constitutes an existing gap in need of addressing.

## CDS DEVELOPMENT

The development of common data services includes the technical and engineering efforts required for the deployment of the tools and services. These include integration with existing systems and services, understanding and accommodating the capabilities and limitations of existing data warehouses, repositories, and consuming systems. The essential elements in automating data handling processes are tools and services that can operate reliably and with minimum or no human intervention, extract the required information needed by specific consuming applications, present the data in the desired form. These tools and services may perform a variety of tasks including inspection, transformation, auto-correction, enhancement, integration / fusion, value adding, tailoring, auto-generation, identification, and discovering the required data. Common services also require well-designed interfaces and protocols to be intuitive to users. These interfaces and protocols must also be capable of detecting and self-forming to automatically connect the sequences of data operations to produce a chain of processes that meet specific requirements for handling, modifying, or transforming the data.

## JFCDS INTRODUCTION

In light of the aforementioned root causes and core data-related problems; US Government, DoD, and Service data strategy guidance, and the vision for a potential solution that centers on a common data services concept, this paper advocates the development and implementation of the following:

> That each Service and the Joint Staff (and potentially coalition

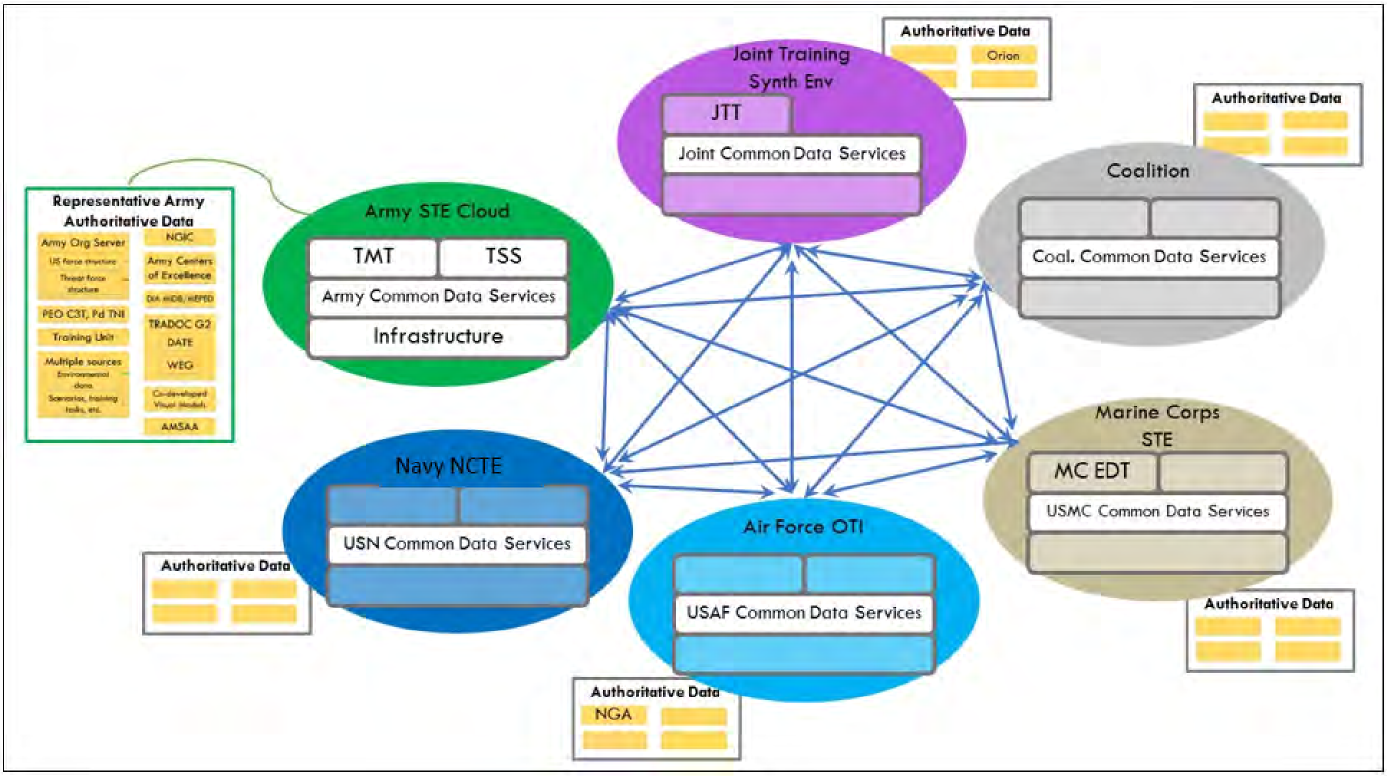


**Figure 3:** *JFCDS Implementation Across The Joint Training Enterprise*

> partners) develop and maintain its own data service provisioning capability, federated through common technical standards and protocols, that enables the sharing among Service (and coalition) partners (through proper channels and at the appropriate classification level) of authoritative, standardized, data in exchange formats that are agnostic to simulation or application.

This approach reflects the reality that there is currently no validated requirement for common data services at the joint level (nor resources specifically aligned against this effort). Therefore, JFCDS will rely on the Services (with support from the Joint Staff) to establish a framework to provision and share their own data services amongst one another. This Service, common data service sharing will function through a mutually agreed upon set of standards, policy, protocols, and data exchange agreements. Critically, this article does not recommend the implementation of a particular CDS data exchange standard, format, or application programming interface (API) that would risk obsolescence. Instead, we propose an ongoing evaluation of open standards favored by commercial and industry leaders that are capable of evolving in a way that is commensurate with rapid technology advancement. This approach ensures that JFCDS remains robust and will not become obsolete even in the face of significant technological advances.

## JFCDS ANALYSIS

The Joint Federated Common Data Services (JFCDS) framework allows for several significant advantages:

- *Flexibility*. This approach allows each Service to develop its own data provisioning capability at its own pace as requirements and resources align. The authors stipulate that each Service will pursue next generation synthetic training capabilities at its own pace based on considerations like validated requirements, available resources, and training strategy. For example, the Army is aggressively addressing its data service requirements in the development of the Synthetic Training Environment's (STE) Training Simulation Software (TSS) and Training Management Tool (TMT). Accordingly, Joint Federated Common Data Services can begin delivering capability in piecemeal, as individual Service data provisioning services come up on line (e.g., Army Common Data Services) and become federated to one another.
- *Data Expertise*. Services are experts on their own data requirements and source needs (e.g., force structure, parametric). Accordingly, each Service is uniquely positioned to identify and access the suites of data needed to support its respective training enablers (and therefore, which data sets to share among fellow Services).
- *Leverage J7 Leadership*. The Joint Staff J7 sponsored Joint Federated Common Data Services WG (as part of the broader Joint Training Synthetic Environment WG) can continually help inform common joint standards for data discovery,

access, extraction, transformation, distribution, and transmission among Services. This enduring WG can inform and influence individual Services as each develops its own respective, capable data-provisioning service to ensure high levels of interoperability and data-sharing capacity among each Service.

## JFCDS APPLICATION CONTEXTS AND FUNCTIONAL OVERVIEW

The Army provides an example of what a Service can do to implement common data services. The Army envisions its next generation Synthetic Training Environment (STE) as a cloud-based distributed system. The STE Cloud is defined as a set of application services, common data services, and supporting infrastructure. Army Application Services include the Training Management Tool (TMT) supporting planning, preparation, execution and assessment activities; and Training Simulation Software (TSS), which supports runtime activities. Army Common Data Services (ACDS) provides a foundation for application services to extract, transform, load, and distribute data from Army authoritative data sources and between STE Cloud instances. Supporting infrastructure is a key enabler for the STE Cloud.

Expanding the approach depicted in the figure above provides the groundwork for our proposal that each Service, Joint, and Coalition partners establish solutions for accessing authoritative data source and managing data needed for engineering of training systems and for conducting training with those systems. As each Service and partner establishes their respective common data service solutions, the Common Data Service Working Group should collaboratively identify the service-interface standards and specifications as well as Service Level Agreements (SLAs) needed to enable a meshed access to each other's authoritative data sources and exercise data—insofar as that information needs to be shared. These interface standards and specifications are critical, as JFCDS must avoid the "n squared" problem of requiring new, additional, tailored gateways to enable data sharing and exchange among each Service's respective synthetic training capability system architectures.

To achieve the necessary data infrastructure, a working group/integrated product team (IPT) (including service, joint, and eventually coalition stakeholders) must select and set service standards for the following:

- discovery (search and subscription)
- retrieval (request-response, publish-subscribe, or other means of delivery)
- access control (user, group, and attribute-level authorization; cross-domain solutions)
- configuration management and version control, and
- collaborative data management (e.g., in support of exercise planning)

> *"The Joint Federated Common Data Services (JFCDS) framework allows for several significant advantages."*

Service and data exchange standards adopted by JFCDS will be consistent with the DoD Standardization Program, relying on open, consensus-based standards where available, and establishing military standards only when appropriate open standards are not yet available.

Services, joint, and coalition partners that employ JFCDS may share force structure, environmental, characteristics/performance, plans/operations, and other types of data in support of exercises, thereby assisting to establish sufficient interoperability among the respective training environments. Moreover, while not all data sources are needed by all stakeholders, common integration standards will ensure that data may be accessed anywhere as a need arises.

## CONCLUSION AND WAY AHEAD

This article documents the collective challenges that Combatant Commands, Services, and Agencies face in the effort to produce common data services that are available to the Joint Training Enterprise for reuse and interoperability--all to support joint readiness and the capability to execute effectively joint combined arms operations. Additionally, challenges remain as joint and Service combat M&S capability developers work to coordinate a synchronized joint training capability development strategy that promotes cooperative and collaborative development, prevents unnecessary redundancy and stove-piping, and identifies standardized technical and procedural approaches. The implementation of Joint Federated Common Data Services represents an important component of the broader joint training capability development strategy as JFCDS will—through the Services and with support from the Joint Staff—establish a framework for the Joint Staff and the Services to provision and share their own data services amongst one another.

Future efforts may include JCIDS-like efforts such as Capabilities Based Assessment (CBA), and defining measures of performance such as reuse, access, and interoperability that ultimately leads to CDS Standardization and JFCDS implementation. Other near term actions include the development of standardized, simulation agnostic data models for terrain, force structure, and entities for Services to employ in joint synthetic training; as well as the arranging of access and retrieval permissions for authoritative data sources from each Service and from the JS J7 that can populate the standard data models under development. Authoritative Data provisioned by Joint

Federated Common Data Services supports the replication of the complex operational environment at a high level of detail across the air, sea, land, space, and cyberspace domains; replicating operational variables and mission variables (PMESSI-PT and METT-TC) and elements of national power (DIME).

While the authors focused on the needs and solution for Joint training in this paper, the commonality of needs, problems, and root causes, and solutions extends far beyond that Joint Training. These are common to training at large, as well as to other activities that employ modeling and simulation with the DoD. The needs and solutions from training most directly relate to those for acquisition, experimentation, and test and evaluation, but also extend to other applications such as strategic analysis. Common, consistent, authoritative data must drive all these activities to support innovation and agility.

## REFERENCES

[1] Defense Modeling & Simulation Coordination Office. (2016, June 10). ***Defense M&S Catalog***. Retrieved from Defense Modeling & Simulation Coordination Office: https://www.msco.mil/DoDTools/DoDEnterpriseManagementTools/MS-Catalog.aspx

[2] Joint Staff J7. (2016, June 03). Joint Training Technical Interoperability Memorandum. Washington, DC.

[3] Joint Staff J7. (2018). Joint Technical Interoperability Strategy. Suffolk, VA: Department of Defense.

[4] Kundra, Vivek: US Chief Information Officer. (2011, February 11). Federal Cloud Computing Strategy. Washington, DC.

[5] Novetta Solutions. (2013, August 2). Department of Defense Data Services Environment Concept of Operations (CONOPS). Reston, Virginia.

[6] PEO-STRI. (2015, August 21). Data Strategy for Army M&S (Initial 4th draft). Orlando, FL.

[7] US Air Force. (2017, September 5). Air Force Operational Training Infrastructure 2035 Flight Plan.

[8] US Department of Defense. (2003, May 9). DoD Net-Centric Data Strategy. Washington, DC. Retrieved from http://www.acqnotes.com/Attachments/DoD%20Net-Centric%20Data%20Strategy.pdf

[9] US Department of Defense. (2007, August 8). Department of Defense Directive (5000.59): DoD Modeling and Simulation (M&S) Management. Washington, DC.

[10] US Department of Defense. (2007, March). Net-Centric Services Strategy: Strategy for a Net-Centric, Service Oriented DoD Enterprise. Washington, DC.

[11] US Department of Defense. (2012, May 10). Department of Defense Instruction (5000.70): Management of DoD Modeling and Simulation (M&S) Activities. Washington, DC.

[12] US Department of Defense. (2014, February 19). Department of Defense Instruction (8206.03): The Global Force Management Data Initiative (GF MDI). Washington, DC.

## ABOUT THE AUTHORS

**LTC JOHN DVORAK** is an FA57 Simulation Operations officer, and serves on the Army Staff in HQDA G-3/5/7. There he programs resources for the Army's synthetic training portfolio and represents Army equities in collaborating with the Joint Staff on joint training synthetic interoperability. He holds a Bachelor of Science degree from the United States Military Academy, and Master's degrees from Kansas State University and the MOVES Institute at the Naval Postgraduate School.

**ROY SCRUDDER** is the Program Manager for the M&S Engineering Group at the Applied Research Laboratories, The University of Texas at Austin (ARL:UT). He has over 30 years' experience in information systems analysis and development, concentrating the last 20 years in information management for M&S. Mr. Scrudder's professional experiences are in the areas of data management and data engineering. Projects with which he has provided metadata expertise include Common Data Services, Enterprise Data Services, Joint Strike Fighter Product Development Metadata Specification, M&S Community of Interest Discovery Metadata Specification, and DoD M&S Resource Repository Board of Directors. Mr. Scrudder holds a Bachelor of Science degree in Applied Mathematics from the University of Tennessee.

**KEVIN GUPTON** is a systems architecture in the M&S Engineering Group at the Applied Research Laboratories, The University of Texas at Austin (ARL:UT). He has over 18 years' experience in enterprise system engineering, data modeling, and knowledge management in the simulation domain. Projects with which he has provided system architecture and data management expertise include Common Data Services, Enterprise Data Services, the US Army Synthetic Training Environment, Integrated LVC Test Environment, and NATO MSG-164 Modeling and Simulation as a Service. Mr. Gupton holds a Bachelor of Science in Mathematics and a Master of Science in Computer Science from Texas A&M University.

**KEVIN HELLMAN** is a Capability Developer for both the Synthetic Training Environment Cross-Functional Team (STE CFT), Integrated Visual Augmented System (IVAS) and former US Cavalry Scout. He has 19 + years' experience in Data Management, Process Management, Data Conversion Services and Data Fusion in both industry and government. He has lead data efforts at the Tactical, Operational and Joint levels for the Army. Mr. Hellman holds a Bachelor's degree, Master's degree and a MBA-Finance.

# VIEW AND VIEWPOINT BASED DIGITAL SIGNOFF

## *using OpenMBEE as an Authoritative Source of Truth*

By: Benjamin Kruse, Mark Blackburn

***FOLLOWING THE DOD'S DIGITAL ENGINEERING (DE) STRATEGY NAVAIR'S SYSTEMS ENGINEERING TRANSFORMATION (SET) FRAMEWORK INVESTIGATES THE MODELING, FEASIBILITY AND COLLABORATION WITH AN AUTHORITATIVE SOURCE OF TRUTH (AST) AS PART OF A DIGITAL ENGINEERING ENVIRONMENT.***

This ongoing research investigates the use of SysML together with OpenMBEE as an AST for a more holistic, model-based systems engineering approach centered on an evolving system model, by means of a conducted pilot study. It uses a developed viewpoint library and modeling methods to progress towards a new operational paradigm between government and industry by eliminating paper artifacts and large-scale design reviews in favor of continuous insight via the digital collaborative environment that supports collaboration between various stakeholders by providing consistent data in the form of model-derived views. An example of a developed modeling method is a digital signoff, used, e.g., to formally approve simulation model results as part of suggested designs, demonstrating feasibility to work within the model-based AST environment.

## INTRODUCTION

To keep pace with the accelerating evolution and adoption of Model-Centric Engineering (MCE) with its enabling technologies, Naval Air Systems Command (NAVAIR) pushes further towards its Systems Engineering Transformation (SET) [1] in the context of the DoD's Digital Engineering (DE) Strategy [2]. DE is defined as an integrated digital approach that uses an authoritative source of system data and models, representing the system of interest as a continuum across disciplines and the system lifecycle. It utilizes MCE as well as Model-Based Systems Engineering (MBSE) and associated enabling technologies. The pilot programs of this initiative are there to identify issues and evaluate tools as well as processes for acquiring more efficient and effective approaches within a digital development environment, e.g., to collaborate among stakeholders while moving the primary means of communication away from documents towards digital models within an Authoritative Source of Truth (AST) to support a more agile and responsive development process with faster and cheaper design iterations [2, 3].

"Based upon Systems Engineering Research Center (SERC) research that includes members from academia, government and industry, the NAVAIR surrogate pilot."

Based upon Systems Engineering Research Center (SERC) research that includes members from academia, government and industry, the NAVAIR surrogate pilot [1] in particular is experimenting with the execution of NAVAIR's SET Framework. This includes model-based collaboration between government and industry using an AST by doing everything in models to demonstrate the art-of-the-possible. The surrogate development process uses a Search and Rescue mission case study, and focuses on an experimental Unmanned Aerial Vehicle (UAV) system called Skyzer, modeled in the OMG's Systems Modeling Language SysML [4].

Being comparable to the single source of truth in MBSE [5], an AST provides consistent data in the necessary format from a potentially distributed set of repositories. These repositories constitute the AST by containing data that represents the system under development. Having a system model in an AST includes interconnected model elements from various sources to enable reasoning about the system. Data can be retrieved as stakeholder-specific views on mission, system, or discipline-specific aspects. Successfully using an AST requires standardized procedures to maintain integrity and quality of its data [2].

The used AST is implemented with the open-source Open Model-Based Engineering Environment (OpenMBEE) [6] developed by NASA/JPL. It aims to enable multi-tool integration across disciplines with its Model Management System (MMS) that stores the model data in an open and accessible way to provide versioning, workflow management and controlled access. Its Model Development Kit (MDK) plugin of the SysML modeling tool Magicdraw enables the model synchronization with MMS and includes the DocGen language [7]. DocGen provides a means for exposing the model content not only as static documents but also in the View Editor, offering light-weight, web-based and live access to the model data in MMS for agile virtual reviews and real-time collaboration. A more in depth overview of OpenMBEE as the AST is given in section 2.

The results of the pilot study presented herein focus on the modeling with a developed viewpoint library in section 3.1 as well as a digital signoff of model elements from linked simulation models in section 3.2, both identified as essential for the conducted collaborative development. The library contains generic viewpoints with their DocGen methods, to quickly create consistent results when exposing various aspects of the UAV mission and system in the View Editor. The signoff mechanism is realized by using a custom stereotype for SysML together with DocGen to enable digital approval of exposed elements in the View Editor while capturing the decision makers and the date and time of decision.

The paper ends with a discussion in section 3.3 and a summary with the planned path forward in section 4. It is concluded that to fully utilized an AST, certain modeling procedures and support are needed, e.g., in the form of the viewpoint library, to allow the here used OpenMBEE to be to be promising AST implementation that enables an improved cooperation and communication also toward stakeholders which are not familiar with SysMIL. Using the View Editor as an interface to the AST data supports moving the primary means of communication away from paper-based documents towards digital models, while including their formal approval through the signoff mechanism.

## OPENMBEE ENVIRONMENT

OpenMBEE [6] is used for the surrogate pilot's digital cooperation environment to support collaboration between various stakeholders by providing consistent data from an AST in the form of model-derived views. The used tools are: Magicdraw and Teamwork Cloud v. 18.5 SP3, MMS v.3.2.2, View Editor v.3.2.1 and MDK v.3.3.6. These tools are only used for demonstration purposes. There is no implied approval or endorsement by the authors, SERC or NAVAIR.

The MMS captures all model elements of the committed SysML models with their complete change history. This

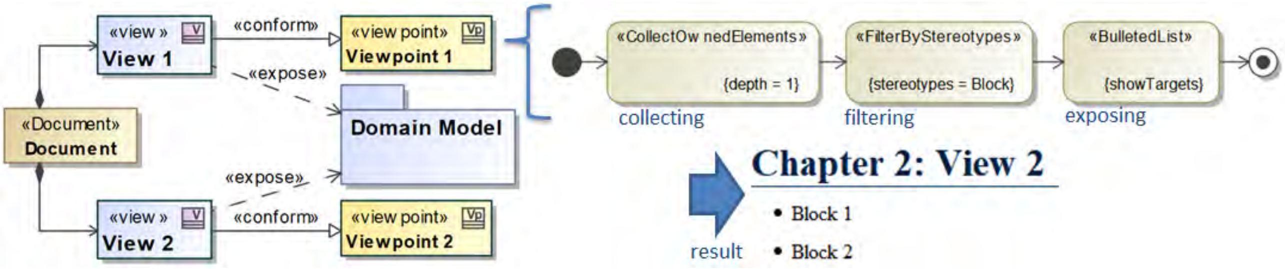


**Figure 1:** *Generic DocGen view hierarchy example (left) with viewpoint behavior (top right) and excerpt of generated document (bottom right) [10]*

includes, the classes, properties, values, instances, relations, and the view instances for the View Editor of a model, but not any diagram layout. MMS stores the data in JavaScript Object Notation (JSON) format and makes it accessible through RESTful web services, to allow a broad range of tools from various disciplines to be able to synchronize with it, as here done through the Magicdraw MDK plugin. Besides this synchronization MDK also includes modeling support in form of the Systems Reasoner and an implementation of the DocGen language [7]. This enables a model-based document creation following ISO-42010 where views are defined as representations of a system from the perspective of a viewpoint [8]. Views are hereby representations of a system from the perspective of a viewpoint. Viewpoints contain the necessary conventions and rules for building a view in order to address stakeholder concerns [4]. This way they do provide a model of the relevant information by focusing on how to use the available information [5].

Figure 1 shows a generic example of how DocGen is used. On the left there is a view hierarchy with two views representing two sections of a document that expose the same model element while conforming to different viewpoints. This way the two views can address different stakeholder concerns, while working with identical information. The top right of Figure 1 shows a viewpoint method example, using DocGen actions to collect, filter and present the exposed model elements. In addition to such predefined actions it is also possible to use custom user scripts or Object Constraint Language (OCL) [9] constraints for the viewpoint methods. OCL is useful for more specific collect or filter operations, such as looking at tagged values of custom stereotypes. The bottom right of Figure 1 finally shows a possible result of "View 2" with bullet points of SysML block elements, which are owned by the exposed "Domain Model" package.

DocGen offers the capability to automatically generate documents from models, making those models more accessible to stakeholders not familiar with SysML. This applies especially when considering their use in the View Editor, where dynamically editing the document equals editing the model data saved in MMS. Using views, the View Editor offers live, web-based access to the model data outside of its original modeling tool, to support communication with non-modelers. It also enables agile virtual reviews and real-time collaboration, as crucial factors for the requested [3, 5] shift from document-centric to model-based approaches.

> *"DocGen offers the capability to automatically generate documents from models, making those models more accessible to stakeholders not familiar with SysML."*

An excerpt of a document in the View Editor is given in Figure 5 with the response to the surrogate pilot Request For Proposal (RFP). On top it shows a diagram with an instance for the general performance values of the tiltrotor UAV. Below is a table to approve those values in two configurations, with and without editing enabled. The editing capabilities of the View Editor allow a stakeholder with appropriate access rights to edit the exposed SysML model elements such as name, value and documentation. Adding content includes for example the addition of further presentation elements (e.g. text, tables or comments) and the creation of cross-references to all accessible model elements, but almost no creation of new SysML model elements. Instead it is possible to have placeholder elements created in the SysML tool, to be adapted in the View Editor. Since the full editing history of all elements is captured, their history can be shown and compared. This can be used for agile virtual reviews. Besides OpenMBEE's open nature, it is also the View Editor's editing capabilities that sets it apart from alternative solutions. For example, the Cameo Collaborator [11] has recently been released with a version (i.e., 19) with some similar editing capabilities, which only work if the full model is exposed as a document by default.

## APPLICATION AND LESSONS LEARNED

Going towards a demonstration of the feasibility of and collaboration with an AST, certain modeling guidelines and support are developed. An essential part is a viewpoint library that provides support to generate consistent documents from models. Part of the viewpoint library is the implementation of the signoff mechanism model elements. This is shown here by using an example from the surrogate contractor's model-based response to the RFP, approving the suggested initial general performance parameters of the UAV, as determined by multi-physics-based simulation models.

### *Viewpoint Library*

The viewpoint library contains a collection of viewpoints with their respective viewpoint behavior using DocGen, as shown on the top right of Figure 1. A sample collection of the almost 60 generic viewpoints in the library is given in Figure 2. The library contains viewpoints for various types of SysML modeling elements and different levels of details. The legend on the right shows the general type of exposed input elements for which the viewpoints are designed. For example, the "Element Documentation" viewpoint creates a simple paragraph of text from the documentation of the exposed element, while the "Default Viewpoint for a Package" displays diagrams and accompanying tables within automatically created subsections for further nested, i.e. contained, packages. Such viewpoint behavior that calls itself or the behavior of other viewpoints is represented here with dependencies. So is, for example, the behavior of the "State Machine Diagrams" viewpoint called by the behavior of "Behavior Overview" or the "Glossary Recursive," which loops recursively through the exposed nested packages, creating glossary tables for each of them, as long as they contain required SysML term elements. Even without such loops in the viewpoint behavior, it is possible to collect elements with a varying scope. The "ToDo Items" viewpoint creates a table of all ToDo elements directly and indirectly owned by the exposed elements. In contrast the "Generic Table" viewpoint only recreates the exposed element, which must be a table or matrix. Finally, there are the two signoff viewpoints that create signoff tables, either for only its

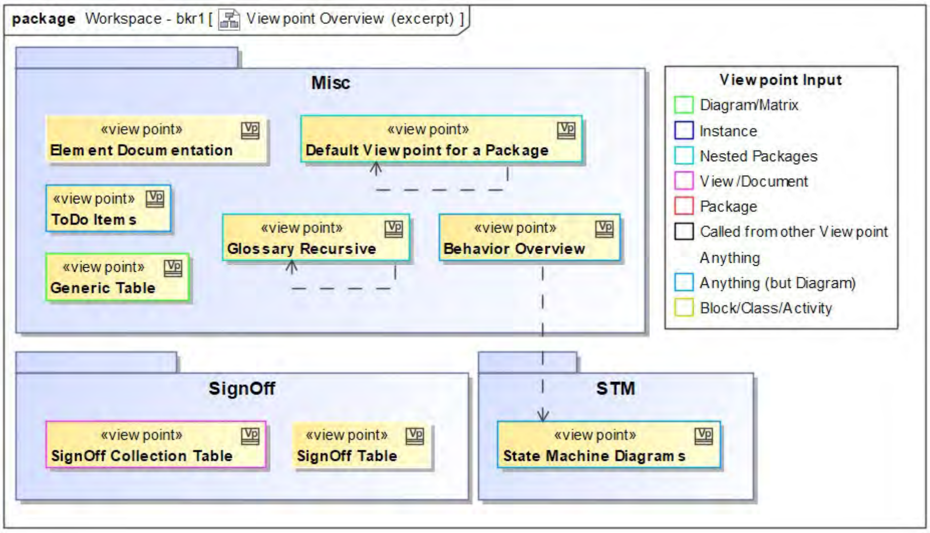
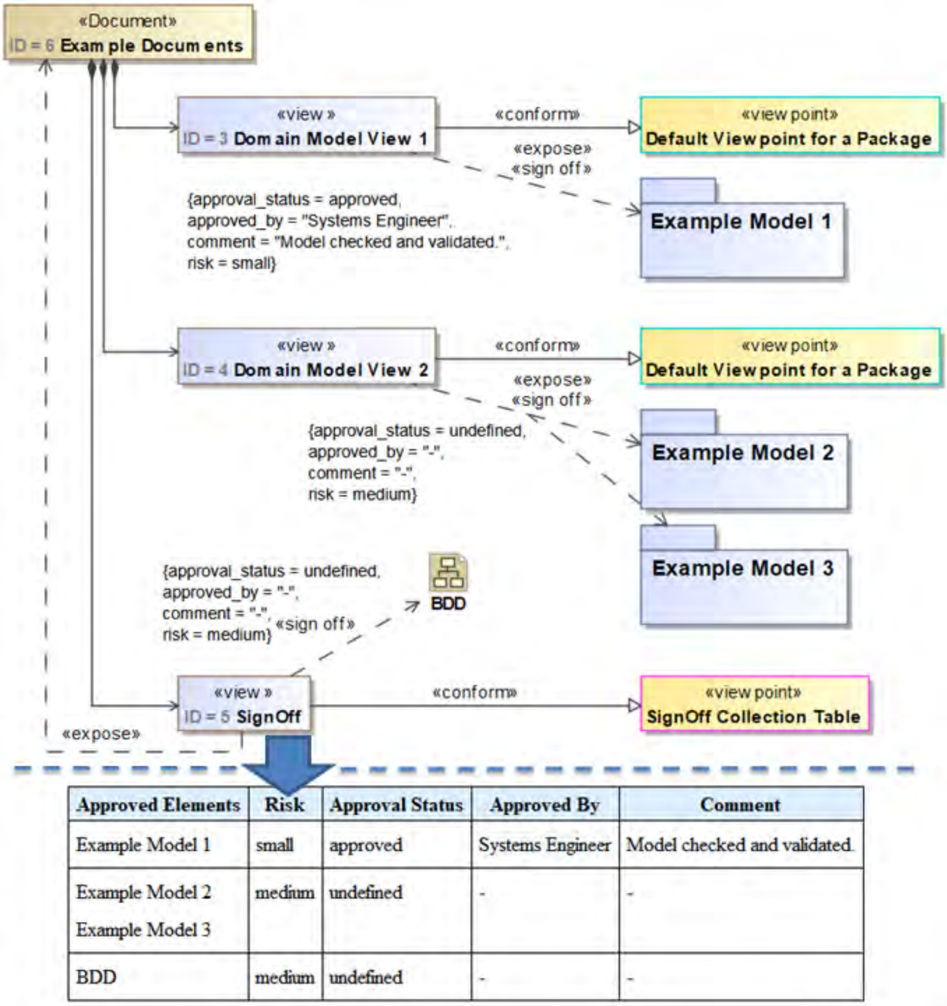

package Workspace - bkr1 [ View point Overview (excerpt) ]
Misc
«view point» Elem ent Docum entation
«view point» Default View point for a Package
«view point» ToDo Item s
«view point» Glos sary Recursive
«view point» Behavior Overview
«view point» Generic Table
SignOff
«view point» SignOff Collection Table
«view point» SignOff Table
STM
«view point» State Machine Diagram s
View point Input
🟩 Diagram/Matrix
🟦 Instance
🟦 Nested Packages
🟪 View /Document
🟥 Package
□ Called from other View point Anything
🟦 Anything (but Diagram)
🟨 Block/Class/Activity

**Figure 2:** *Example collection of viewpoints from developed viewpoint library*


«Document» ID = 6 Exam ple Docum ents
«view » ID = 3 Dom ain Model View 1
«conform»
«view point» Default View point for a Package
«expose» «sign off»
{approval_status = approved, approved_by = "Systems Engineer", comment = "Model checked and validated.", risk = small}
Example Model 1
«view » ID = 4 Dom ain Model View 2
«conform»
«view point» Default View point for a Package
«expose» «sign off»
{approval_status = undefined, approved_by = "-", comment = "-", risk = medium}
Example Model 2
Example Model 3
{approval_status = undefined, approved_by = "-", comment = "-", risk = medium}
«sign off»
BDD
«view » ID = 5 SignOff
«conform»
«view point» SignOff Collection Table
«expose»

| Approved Elements | Risk | Approval Status | Approved By | Comment |
|---|---|---|---|---|
| Example Model 1 | small | approved | Systems Engineer | Model checked and validated. |
| Example Model 2<br>Example Model 3 | medium | undefined | - | - |
| BDD | medium | undefined | - | - |

**Figure 3:** *Generic view hierarchy example, with three signoffs of four elements (top), exposed in the generated table (bottom)*

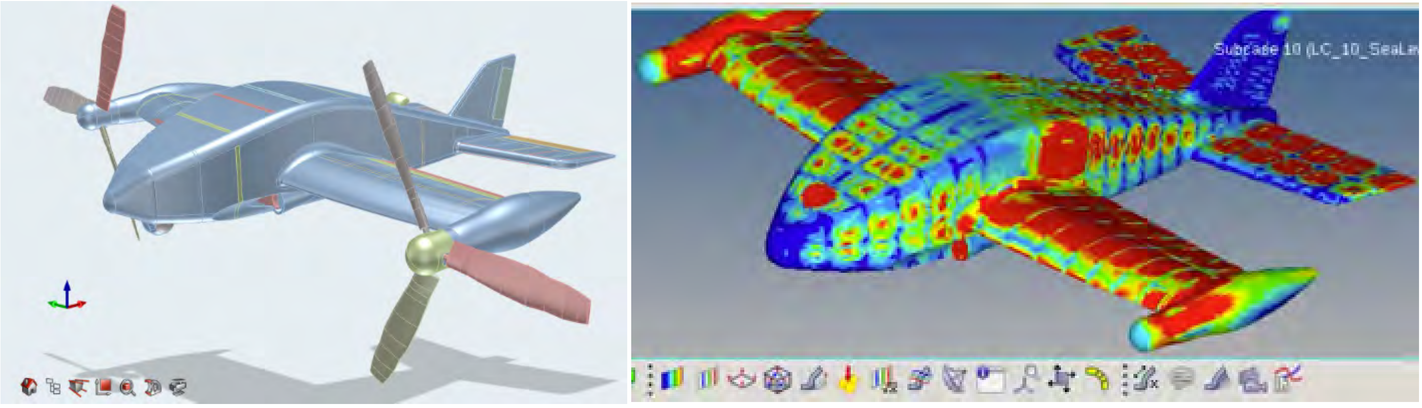


**Figure 4:** *UAV CAD model (left) used for CFD (right) and structural simulations*

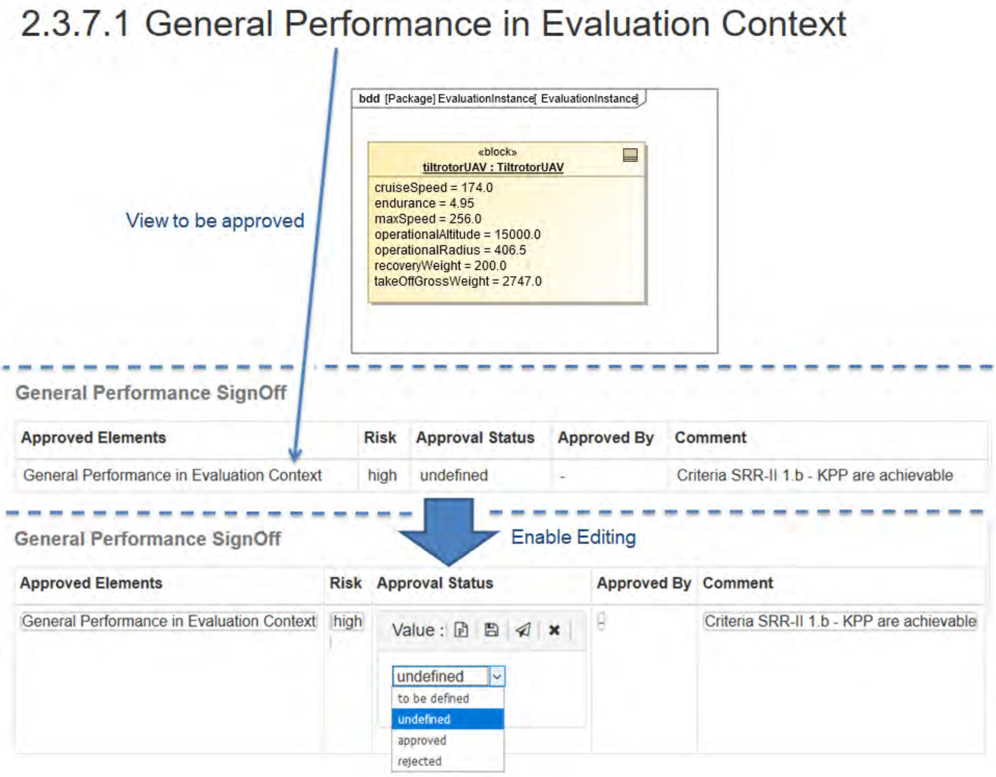
conforming view, as used for Figure 5, or for other documents and views with their sub-views, as shown in Figure 3.

Certain modeling considerations must be made to ensure a working collection of elements through the viewpoints. The types of the exposed model elements must match including their contained elements, as indicated with the legend on Figure 2, where, e.g., SysML term elements must be inside the nested packages of the glossary viewpoint. To notify the modeler if no correct model elements are found, OCL constraints are used in the library viewpoints to generate adequate warning messages, which provide a means for reflecting incompleteness in the model. Model elements that should not be shown may have to be moved, if the viewpoint does not filter them out.

## DIGITAL SIGNOFF

The digital signoff mechanism presented here is used to formally approve SysML model elements, as part of the progression towards a digital development with model-based documents. It captures the signoff status with its properties in the MMS, including when and by whom a change is done. It is realized by using a custom stereotype for SysML together with DocGen to enable a digital signoff in the View Editor. The signoff stereotype extends the dependency and has tagged values for the risk, approval status, approver, and a comment. These properties use enumerations for the different approval status and risk estimates.

A generic example view hierarchy with signoff is given in Figure 3 with the resulting table below. Coming from the views, the signoff dependencies point towards the various model elements to be signed off. The signoff stereotype can also be applied to existing expose relations to directly sign off the exposed model elements. This dual use of the expose relations is used for the first two views of Figure 3, to sign off the exposed packages with their content. In contrast, the "BDD" named diagram on Figure 3 is to be signed off individually, i.e., not as part of an expose dependency. If multiple different elements are to be signed off at once, e.g., "Example Model 2" and "Example Model 3," additional generic dependencies can be added to the signoff relation. This way they can be both signed off at once, as shown in the table below,



2.3.7.1 General Performance in Evaluation Context

bdd [Package] EvaluationInstance[ EvaluationInstance]

«block»
tiltrotorUAV : TiltrotorUAV

cruiseSpeed = 174.0
endurance = 4.95
maxSpeed = 256.0
operationalAltitude = 15000.0
operationalRadius = 406.5
recoveryWeight = 200.0
takeOffGrossWeight = 2747.0

General Performance SignOff

| Approved Elements | Risk | Approval Status | Approved By | Comment |
|---|---|---|---|---|
| General Performance in Evaluation Context | high | undefined | - | Criteria SRR-II 1.b - KPP are achievable |

General Performance SignOff

| Approved Elements | Risk | Approval Status | Approved By | Comment |
|---|---|---|---|---|
| General Performance in Evaluation Context | high | Value :<br>undefined<br>to be defined<br>undefined<br>approved<br>rejected | - | Criteria SRR-II 1.b - KPP are achievable |

**Figure 5:** *RFP response example with excerpt of view to be approved (top) and signoff table with and without enabled editing of the approval status (below)*

which is created by the view exposing the document and using the matching signoff viewpoint from the library.

In the surrogate pilot study the signoff mechanism was used to formally approve performance parameters of the UAV design suggested by industry. The signed off parameters come from multi-physics simulation models, which are accessible through hyperlinks in the View Editor, providing relevant data as part of the AST. There are two virtual collaboration environments used by the surrogate contractor: Altair 365 [12] provides cloud access of simulation scripts and Computer-Aided Design (CAD) models, as seen on the left of Figure 4. Altair Access [13] manages structural Computer-Aided Engineering (CAE) models, Computational Fluid Dynamics (CFD) models, as seen on the right of Figure 4, and their cloud-based execution. From those resources the results are imported as instances into the SysML system model, to be signed off and to be used for the evaluation of the suggested design in respect to the demanded key performance parameters.

This signoff in the RFP response is shown in Figure 5. On top there is a view with the calculated general performance parameters in the evaluation context, which is to be signed off. This is done in the table below by enabling editing, to change the approval status or the risk via a drop down menu and by entering the name of the person responsible and a comment. The shown name of the approved element is hereby a cross reference to it, providing reliable information about what is to be signed off. Instead of having the used decision criteria of the signoff in form of a comment, as shown in Figure 5 with the System Requirement Review (SRR) II Entry Criteria, it is planned to extend the signoff mechanism by adding additional custom properties resulting in an analogue drop down menu as shown for the approval status, if enumerations are used. Having this signoff information not only captured in MMS, but also in the synced SysML model allows metrics to be created, e.g., tracking the signoff status of all rejected or approved elements throughout the model.

## DISCUSSION

Several advantages and disadvantages of the here presented development system with its associated processes are identified in addition to the previous findings as found in [10]. Reusing viewpoints from the library not only supports a quicker creation of view hierarchies, it also results in less required knowledge about DocGen, resulting in more modelers being able to create view hierarchies and expose their models. Another advantage is that documents become more consistent, due to the reuse of standardized viewpoint methods. Additionally, it is possible to reuse existing view hierarchies, e.g., as part of a framework or reference models such as NAVAIR's Acquisition System Reference Model (ASRM) [14]. This offers additional guidance during the system modeling, since the deliverable document is predefined with its document structure together with the required input types from the viewpoints. Reusing library viewpoints requires the library to be used as a project, which is a mechanism to access, use, trace and reference read-only model elements from other models. This mechanism is also important for data security and access, since it impacts user permissions in MMS, dictating what elements in the View Editor can be seen or edited in a document without write access on the exposed model content. As with every model library, it is important to adequately maintain and manage the viewpoint library. Changes to viewpoints in the library should always be made with caution, due to the potentially broad impact across multiple documents. Instead it can be advantageous to create a local copy of a provided viewpoint and adapt that for the particular application.

"Reusing viewpoints from the library not only supports a quicker creation of view hierarchies."

Potential improvements of the library come from the current implementation of the DocGen language. To fix the partially varying representation between the View Editor and the SysML modeling tool or the feature to capture and reuse expressions, e.g., in OCL. Here the viewpoint methods of the library serve instead to capture working expressions and patterns while simultaneously providing additional context. Finally, a DocGen action might be added that filters based on certain properties of elements, including tagged values, analogous to existing capabilities to, e.g., sort by those properties.

In the context of an AST, the viewpoint library provides extensive support to create model-derived documents. Having the capability to quickly and reliably generate and update required online documents from models, supports remote cooperation, faster design iterations and demonstrates the feasibility of the surrogate pilot's [1] model-based AST approach. Users should consider the document generation during modeling, e.g., by properly documenting model elements or reducing the size of diagrams. To make sure that the derived document correctly addresses the stakeholder concerns, it is important to involve subject matter experts when setting up the view hierarchy. This allows them to get the required, relevant and custom-generated information, while only the modelers themselves need to have a broad understanding of the entire model and only few of the modelers require in-depth DocGen knowledge.

In the context of documents derived from an AST, the signoff mechanism serves to capture the formal approval of documents and data as seen in the View Editor, also clarifying which data has authority, e.g. in case of newer data in a model branch versus the approved data in the baseline master branch. This way it is a crucial part of progressing towards a digital development with model-based documents. Additionally, it can be used as a means for tracking model completeness and correctness through metrics in the SysML model.

Current issues with the signoff mechanism exist, such as: limitations to either prevent changes of signed off elements, to automatically revert the approval status or at least to notify when an already approved element changes, e.g., by comparing the respective dates and times stored in the MMS. Hereby it is of importance that not only changes to the single approved model element are considered, e.g. a name change of the view "General Performance in Evaluation Context" in Figure 5, but also of the elements shown in it, e.g., the "EvaluationInstance" diagram. The same applies for owned elements, e.g. of the package "Example Model 1" of Figure 3. Similarly, it would be beneficial to provide an automatic fill-in of the "Approved By" property using the logged-in user information, to ensure correctness and consistency. Solutions for these issues are under investigation, as described in section 4.

With a focus of the surrogate pilot project being the demonstration of the art-of-the-possible of doing everything in models, testing a new operational paradigm between government and industry, a general look at the hereby supported use of a collaborative AST shows its initial potential to capture and provide required multi-discipline data during the development. Yet, even this cooperation encountered initial network and access issues with various parties from government and industry having to work together on the same environment. Related to such cyber-security issues, intellectual property and data rights are identified as important and planned for further investigation. The fact that the open-source OpenMBEE [6] software is used for the AST environment carries further challenges in form of the potential insertion of malicious code. The further use of the AST also requires more adapted processes and guidelines, to not only determine which data has the authority, e.g., supported through the signoff mechanism, but also for its crucial multi-discipline data integration, e.g., improving the linkages to simulation models and their analysis results as non-SysML information.

> *"Related to such cyber-security issues, intellectual property and data rights are identified as important and planned for further investigation."*

## SUMMARY AND FUTURE WORK

Modeling with and for an AST requires new methods and standardized processes, especially when aiming at a fundamental change away from traditional and static paper artifacts towards live, model-derived views that provide continuous insight via a digital collaborative environment. In addition to previous results of the general use of OpenMBEE as a promising AST environment [10], this work focuses on modeling with the developed viewpoint library and the signoff mechanism, which are both crucial for the surrogate pilot's AST-based development process [1]. This provides a means for discipline-specific subject matter experts to interact with and contribute information to the system model that links upward to the mission model, without needing to know how to use a SysML modeling tool.

The viewpoint library supports the modeling of view hierarchies by providing a collection of generic viewpoints. This results in less effort to create such model-based documents, while not requiring modelers with in-depth DocGen knowledge. Reusing identical or standardized viewpoints results in more consistent documents for common model element types. Using model-based documents supports faster design iterations of the surrogate pilot [1], through the synchronization between the document in View Editor and the SysML model. Beyond minor improvements regarding the DocGen implementation mentioned in section 3.3, it is recommended to continue improving the existing viewpoints while sharing and documenting them together with their used expressions. Other suggested work related to the viewpoint library may be a more custom formatting of the document, to seamlessly recreate existing templates.

The signoff mechanism allows to approve or reject any model element or collections thereof in the View Editor or also in the SysML model. Capturing who and when a change to the signoff status is made provides necessary functionality to formally approve versioned digital model information, as shown with the model-based RFP response. This supports the transition from traditional paper-based documents towards model-based and model-derived documents as part of a digital development. Looking at the identified issues in section 3.3, it is important to improve the signoff mechanism by including some kind of change management, e.g., to make sure that there are no seemingly approved elements that did change after they were approved.

This goes together with an improved integration of non-SysML data into the AST, for instance in form of disciplines-specific models and analyses. With data integration being identified as essential for modeling and simulation and the main challenge being data format and semantics [15], there exists ongoing research in form of the Integration and Interoperability

Framework (IoIF) [16], that aims to enable the digital thread. The IoIF is a Semantic Web-enabled framework that aims to enhance tool interoperability together with ontological reasoning, allowing, e.g., to reason about the signoff data in MMS and therefore providing the required functionality. Part of this was recently accomplished together with an ontology-based weight breakdown and will be published soon. It is also planned to continue this research by incorporating CFD simulation data directly from its tool, to have it linked semantically to the SysML data in MMS as the AST. Other future work that involves the continuation of the surrogate pilot as well as IoIF is about a model-centric source selection process that includes traceability between the SysML models and multi-physics simulation models as well as the consideration of distributed data rights. The surrogate pilot study continues additionally with the integration of selected and more detailed development and analyses, as well as the alignment of the surrogate pilot mission and system models with the ASRM framework and its process model to further leverage the research results as relevant and yet unclassified examples for training.

To conclude, this paper presents a developed viewpoint library together with a digital signoff mechanism as part of a UAV surrogate pilot study that investigates and demonstrates the art-of-the-possible of using an AST environment based on OpenMBEE for a more iterative and collaborative development process. The presented modeling support and methods in particular, support moving the primary means of communication away from static paper-based documents towards digital models that provide views for an improved communication also towards non-modelers and discipline-specific subject matter experts. This cooperative modeling research project was developed in cooperation with Altair, NAVAIR and SERC.

## REFERENCES

[1] Blackburn, M., et al.: Transforming Systems Engineering through Model-Centric Engineering*. SERC*, 2019. # SERC-2019-TR-005. https://apps.dtic.mil/dtic/tr/fulltext/u2/1073187.pdf.

[2] Department of Defense: Digital Engineering Strategy*. Office of the Deputy Assistant Secretary of Defense for Systems Engineering*, 2018. www.acq.osd.mil/se.

[3] Beihoff, B., et al.: A World in Motion – Systems Engineering Vision 2025*. INCOSE*, 2014.

[4] OMG: Systems Modeling Language (OMG SysML)*.* Version 1.4, 2015. # formal/2015-06-03.

[5] Madni, A.M. and M. Sievers: Model-based systems engineering: Motivation, current status, and research opportunities. Systems Engineering, 2018. 21(3): p. 172-190.

[6] NASA/JPL: Open Model Based Engineering Environment. [accessed 2019 02 14]; http://www.openmbee.org/.

[7] Delp, C., et al.: Model Based Document and Report Generation for Systems Engineering, in *Aerospace Conference*. 2013, IEEE: Big Sky, MT, USA

[8] ISO/IEC/IEEE: Systems and Software Engineering - Architecture Description*.* 2011. # ISO/IEC/IEEE 42010:2011(E).

[9] OMG: Object Constraint Language*.* Version 2.4, 2014. # formal/2014-02-03.

[10] Kruse, B. and M. Blackburn: Collaborating with OpenMBEE as an Authoritative Source of Truth Environment*. Procedia Computer Science*, 2019. 153(C): p. 277-284.

[11] NoMagic, Inc.: Cameo Collaborator. [accessed 2019 02 14]; https://www.nomagic.com/products/cameo-collaborator-for-alfresco.

[12] Altair Engineering, Inc.: Altair 365. [accessed 2019 07 01]; https://solidthinking.com/product/altair365/.

[13] Altair Engineering, Inc.: Altair Access. [accessed 2019 07 01]; https://www.pbsworks.com/PBSProduct.aspx?n=Altair-Access&c=Overview-and-Capabilities.

[14] Grosklags, P.: Systems Engineering Transformation - Industry Day*.* NAVAIR, California, MD, USA, 2018.

[15] Allen, G.W.: Modeling and Simulation Data Integration – Inviting Complexity*. Journal of Cyber Security and* Information Systems, 2016. 4(2): p. 2-6.

[16] Bone, M., et al.: Toward an Interoperability and Integration Framework to Enable Digital Thread*. Systems*, 2018. 6(4).

## ABOUT THE AUTHOR

**BENJAMIN KRUSE**, Sc.D. is a Research Assistant Professor at Stevens Institute of Technology, working as a SERC researcher on Systems Engineering Transformation through Model-Centric Engineering research tasks, focusing on the use of SysML and OpenMBEE with their view and viewpoint mechanism.

**MARK R. BLACKBURN**, Ph.D. is a Senior Research Scientist with Stevens Institute of Technology and serves on the System Engineering Research Center (SERC) research council. Dr. Blackburn is the Principal Investigator on SERC research tasks for both Naval Air Systems Command NAVAIR and U.S. Army ARDEC on Systems Engineering Transformation through Model-Centric Engineering.

Cyber Security & Information Systems
Information Analysis Center

# Need Specialized Technical Support with Easy Contract Terms?

## Core Analysis Task (CAT) Program

*A Pre-Awarded, Pre-Competed Contract Vehicle.*

CSIAC provides Subject Matter Expert (SME) support on an as-needed basis to quickly address technical requirements with minimal contracting effort. CSIAC provides such solutions via the utilization of our Core Analysis Task (CAT) service/capability. CSIAC is a competitively awarded contract with Indefinite Delivery/Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements. Custom solutions are delivered by executing user-defined and funded CAT projects without the need for further competition.

Through the CAT program, CSIAC is a pre-competed contracting vehicle, enabling the DoD and other agencies to obtain technical support for specific projects/programs that fall within one of the CSIAC technology areas. As with any inquiry, the first four hours are free. If the scope requires a CAT, CSIAC will assist with the development of a Performance of Work Statement (PWS) to be approved by the Contracting Officer's Representative (COR).

## Key Advantages of working with CSIAC:

***Expansive Technical Domain***

The CSIAC's broad technical scope provides numerous pre-qualified resources for potential projects, and is especially valuable for today's information system challenges that frequently cross multiple domains.

***Comprehensive STI Repositories***

As a consolidation of three predecessor Information Analysis Centers (IACs), CSIAC has a wealth of expertise, data and information to support the successful completion of CATs.

***Expansive Subject Matter Expert Network***

CSIAC is able to leverage reach-back support from its expansive SME Network, including technical experts from the CSIAC staff, team members, or the greater community, to complete CATs.

***Minimal Start-Work Delay***

Not only does CSIAC provide DoD and other government agencies with a contract vehicle, but as a pre-competed single award CPFF IDIQ, work can begin in just a matter of weeks.

***Apply the Latest Research Findings***

CSIAC draws from the most recent studies performed by agencies across the DoD, leveraging the STI holdings of the Defense Technical Information Center (DTIC). The results of all CSIAC CATs and other DoD-funded efforts are collected and stored in DTIC's STI repository to support future efforts by the CSIAC and others.

## How To Get Started

If you have a need for CSIAC technical support, the first step is to contact us. All Technical Inquiries are free to the customer for up to four hours of service. If the scope of the support is more extensive and requires a CAT, CSIAC will assist with the development and submission of the task description and related contract documents. CATs may be awarded as either Cost Plus Fixed Fee (CPFF) or Firm Fixed Price (FFP) delivery orders.

Inquiries may be submitted by email to **info@csiac.org**,
or by phone at **1-800-214-7921**.

***Please visit our website for more information:***
https://www.csiac.org/services/core-analysis-task-cat-program/

## Who We Are

The Cyber Security Information Systems Information Analysis Center (CSIAC) is the DoD's Center of Excellence in Cyber Security and Information Systems, covering the following technical domains:

- Cybersecurity
- Software Engineering
- Modeling and Simulation
- Knowledge Management/ Information Sharing

CSIAC is chartered to leverage best practices and expertise from government, industry, and academia to solve the most challenging scientific and technical problems. The Center specializes in the collection, analysis, synthesis, and dissemination of Scientific and Technical Information (STI) to produce solutions in support of the defense community.

## Our Team

Quanterion Solutions Incorporated is the prime contractor responsible for operating the CSIAC. In addition to Quanterion, customers also have access to the other members of the CSIAC team which include leading technology corporations as well as prestigious academic institutions that perform cutting edge research activities to expand our knowledge base.

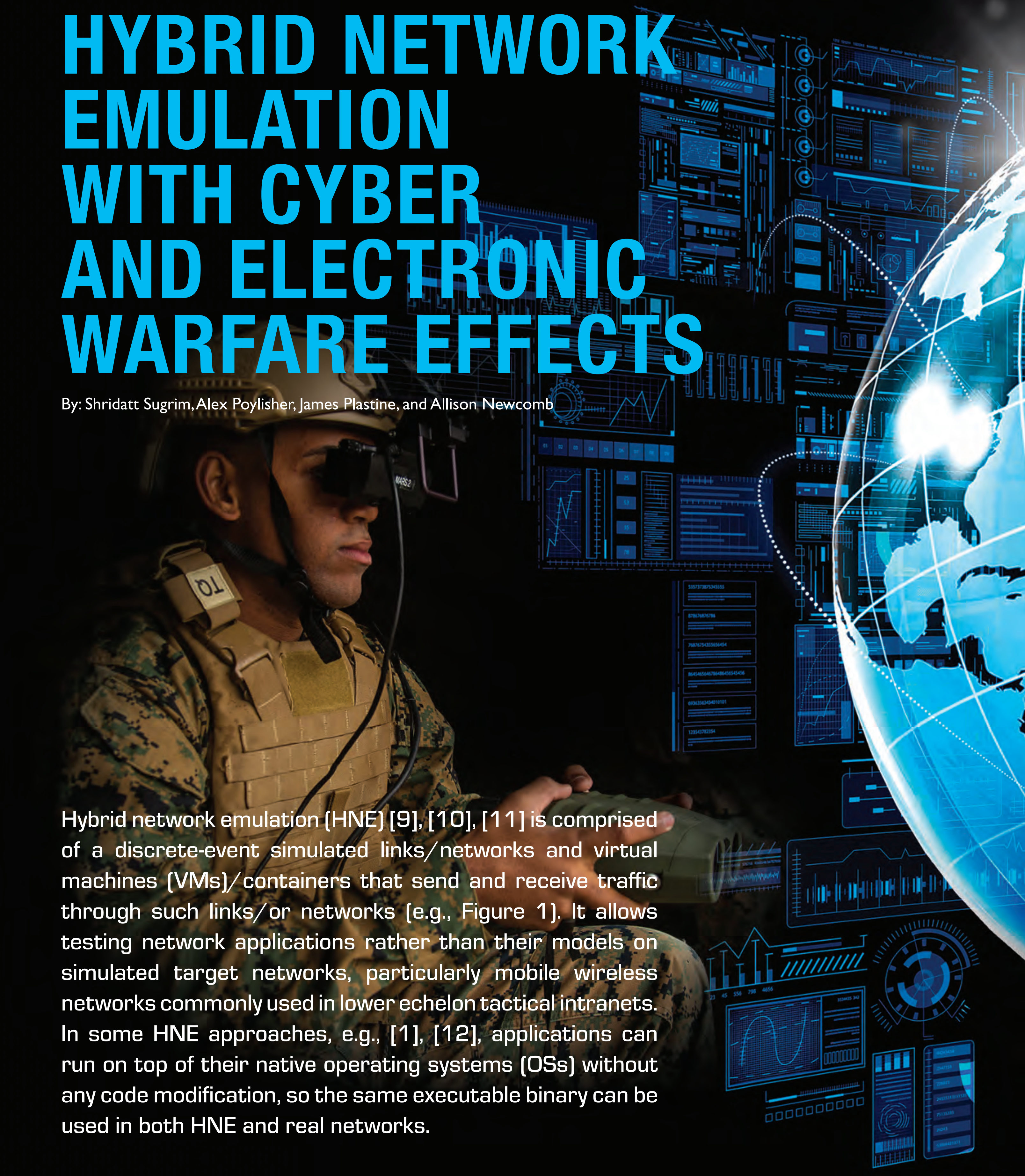
CSIAC
*Cyber Security & Information Systems*
*Information Analysis Center*

266 Genesee Street
Utica, NY 13502

1-800-214-7921
https://www.csiac.org

# HYBRID NETWORK EMULATION WITH CYBER AND ELECTRONIC WARFARE EFFECTS

By: Shridatt Sugrim, Alex Poylisher, James Plastine, and Allison Newcomb



Hybrid network emulation (HNE) [9], [10], [11] is comprised of a discrete-event simulated links/networks and virtual machines (VMs)/containers that send and receive traffic through such links/or networks (e.g., Figure 1). It allows testing network applications rather than their models on simulated target networks, particularly mobile wireless networks commonly used in lower echelon tactical intranets. In some HNE approaches, e.g., [1], [12], applications can run on top of their native operating systems (OSs) without any code modification, so the same executable binary can be used in both HNE and real networks.

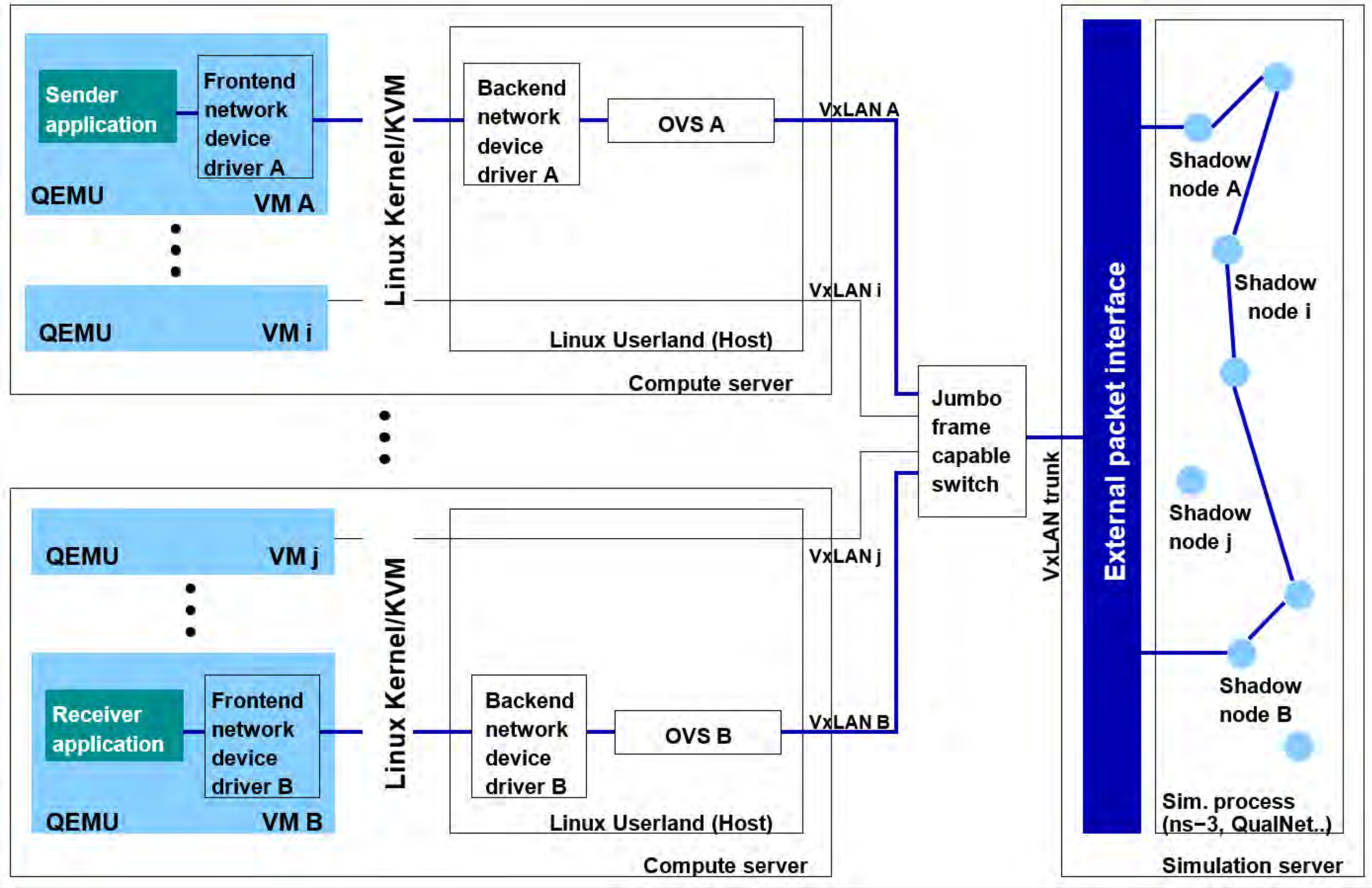


**Figure 1:** *Hybrid network emulation in CyberVAN.*

HNE addresses both feasibility and scalability concerns of testing applications over target networks. With respect to feasibility, as testing requires only the models of network elements, the availability of network element hardware (e.g., expensive tactical radios or next generation waveforms) is not an issue, and simulation enables testing over various network topologies and configurations, with terrain, mobility, and electronic warfare (EW) conditions that would be prohibitively expensive, perhaps even dangerous, to create in field tests. When both an actual implementation and a simulation model are available, HNE allows the use of either or both in the same experiment. When some physical devices are available, they can be plugged into the HNE networks that can be run in real time (typically at Layer 3). HNE also allows, in principle, the mixing and matching of link and device models developed for *multiple* simulators to be used in the same experiment.

With respect to scalability, theoretically the scale of the target network is constrained only by the capabilities of discrete event simulators and hardware resource availability. However, major discrete event network simulators with significant model libraries and active user communities (e.g., [25], [11]) at the time of writing use conservative scheduling and provide limited support for parallel execution (essentially, only for highly medium-independent network partitions connected over wired links). In this commonly used approach, an indivisible spectrum-sharing wireless network is modeled in a single-threaded simulator process, and may execute slower than real time beyond a certain combination of network size, model complexity, and traffic load. If not addressed, this becomes an issue for the VMs/containers, where emulation by default produces the real-time rate of time advancement for the VM OSs ; the ensuing mismatch can easily invalidate the experimental results as protocols and applications are faced with much slower than intended communication links/networks. In this paper[1], we describe our HNE implementation in a Cybersecurity Virtual Assured Testbed (CyberVAN) [1], [2], [3], [4], [6], [7], [8], designed and developed by Perspecta Labs (PL) since 2008 with U.S. Army and OSD funding, and currently used for validating the U.S. Army CCDC Army Research Laboratory's

[1] The work reported in this paper was partially performed in connection with contract number W911NF-14-D-0006 with the U.S. Army Research Laboratory. The views and conclusions contained in this document are those of the authors and should not be interpreted as presenting the official policies or position, either expressed or implied, of the U.S. Army Research Laboratory, or the U.S. Government unless so designated by other authorized documents. Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

(ARL) Cyber Security Collaborative Research Alliance (CRA) [13] research. CyberVAN has also been used internally at Perspecta Labs to support several recent and current DARPA and C5ISR programs, including [19], [20].

CyberVAN enables creation of high-fidelity enterprise and tactical network scenarios by constructing a mix of physical machines/devices, virtual machines, physical networks and simulated networks, with active support for ns-3, QualNet, and EMANE, which automatically makes available  all the models developed for these simulators. CyberVAN provides scenario creation, deployment, and run-time control from GUIs or command line. CyberVAN includes special features for supporting large-scale, high-fidelity network experimentation, in particular addressing the time advancement problem in HNE, and provides utilities that facilitate the experiment process, including mobility generation, visualization and data collection.

Cyber and EW effects in tactical networks present a unique space that is very difficult to model with real networks. The HNE's mix-and-match approach allows CRA researchers to rapidly and cheaply create realistic experiments, where both the software under attack, attacks themselves and defensive mechanisms can be developed and tested with the QoS and security assumptions correct for the tactical universe.

We demonstrate the use of HNE in CyberVAN on a platoon-level tactical internet scenario, developed for the CRA, with a situational awareness application (a) evaluated for basic performance (message delivery ratio, latency), (b) attacked in the cyber domain, including the network control plane (unicast routing) and information plane (location falsification), and (c) attacked in the EW domain with a UAV-mounted jammer. Given the open nature of CRA research, we have used only freely available models, OSs, libraries, and applications in the scenario, but we expect readers familiar with the sensitive tactical technologies used for similar purposes to be able to readily translate the scenario to the tactical reality.

The rest of the paper is structured as follows.  We briefly describe how hybrid network emulation is implemented in CyberVAN. Next, we present the tactical scenario used in all the experiments. Then, we estimate the distortion introduced by HNE into the application performance metrics of importance to the scenario. Lastly, we discuss two cyber attacks and an EW attack.

## HYBRID NETWORK EMULATION IN CYBERVAN

CyberVAN's HNE consists of three seamlessly integrated enabling technologies: software-in-the-loop network simulation, transparent packet forwarding, and host virtualization. Software-in-the-loop (SITL) network simulation allows real network traffic to be forwarded through simulated links, paths or networks, transparent packet forwarding ferries IPv4/IPv6 packets generated in virtual machines and physical devices to and from the network simulator, and host virtualization enables running real applications, libraries, and OSs in virtual machines/containers. As shown in Figure 1, the current implementation uses: (a) custom-built SITL modules (co-simulators) for each supported simulator type, (b) an Open vSwitch (OVS)-based transparent forwarding fabric, with VxLAN Layer 2 tunneling, and (c) QEMU/KVM-based host virtualization.

An IP packet from the sender application on VM A destined to the receiver application on VM B passes through the network device driver and device emulation on VM A, emerges on the virtual interface on the compute server hosting VM A, is encapsulated into a VLAN-tagged frame by the OVS logic, and is sent to a simulation server in a VxLAN tunnel, via a jumbo frame-capable switch (software or hardware). At the simulation server, the packet is extracted from the VLAN-tagged frame, and the VLAN identifier is used to determine the simulated node and network interface on which the packet is injected into the simulated IP stack. Two modes of injection are supported: pre-routing and post-routing. In the former, the packet is subject to the simulated Layer 3 forwarding logic installed in the particular IP stack. In the latter, the simulated Layer 3 forwarding logic is bypassed and the packet is injected straight into the IP interface. Regardless of the injection mode, the simulation logic then determines whether, when and where the packet may emerge from simulation to be delivered to VM B. If the packet emerges, it is again encapsulated into a VLAN-tagged frame and sent towards the compute server hosting VM B. On the compute server, it is de-encapsulated by the OVS logic and injected into the virtual interface corresponding to VM B. It then emerges inside VM B, and is received by the receiver application. The underlying physical network connecting the compute and simulation servers is currently GbE-based.

The post-routing injection mode is useful when Layer 3 decision-making (e.g., forwarding, access control, deep packet inspection) is implemented in real software running inside a VM. While real software can always run in VMs, post-routing injection is not always the best choice as it comes at a price. With pre-routing injection, a packet that traverses multiple simulated links between the sender and the receiver has to be ferried once between the compute server of the sender and the simulator and once between the simulator and the compute server of the receiver. With post-routing injection on every link in the same example, however, the packet will have to be ferried between the simulator and a compute server as many times as there are hops on the path between the sender and receiver nodes. In large scenarios, this can dramatically increase the network load on the transparent forwarding fabric. Pre-/post-routing injection is configurable per network interface.

The HNE packet forwarding story would not be complete without the Address

Resolution Protocol (ARP, for IPv4), Neighbor Discovery (IPv6) and ICMP/ICMP6, which involve interactions of VM-based and simulation-based protocol endpoints. CyberVAN supports seamless interaction of real and simulated implementations of the above protocols, for example, handling of ARP requests from VMs in simulation and ICMP-based traceroute through simulated nodes with pre-routing injection. CyberVAN's HNE also includes support for end device emulation features unrelated to packet forwarding, including National Marine Electronics Association (NMEA)-compliant GPS receiver data, and simulated battery state/consumption.

The simulated/emulated time advancement problem, inherent in HNE, is addressed by driving the emulated clock hardware with the dynamic rate of advancement of the simulator clock, sampled at small real-time intervals [7]. This is a practical solution for most experimental work at or above Layer 3, with the software under test (OSs, libraries, applications) running in VMs/containers. Figure 2 illustrates the concept as currently implemented: the horizontal axis represents the progression of real time, the vertical axis represents the progression of simulation time and VM time.

Simulation time for a scenario is sampled at the simulation server at regular real-time intervals (its advancement is shown in blue); the sampled values are multicast to all QEMU emulators running the VMs in the scenario. Based on the real time passed (as measured by each emulator independently) and simulation time passed since last update, each emulator computes the dilation factor (DF) used to determine the rate of advancement of VM time for the next sampling interval. If the DF is too high or too low based on the actual data, the error is corrected for the next interval. Note that the simulator has been configured not to run faster than real time in this example. The rate of clock advancement is enforced via the QEMU-emulated HPET chip, and the VM OSs are configured to use HPET as the only

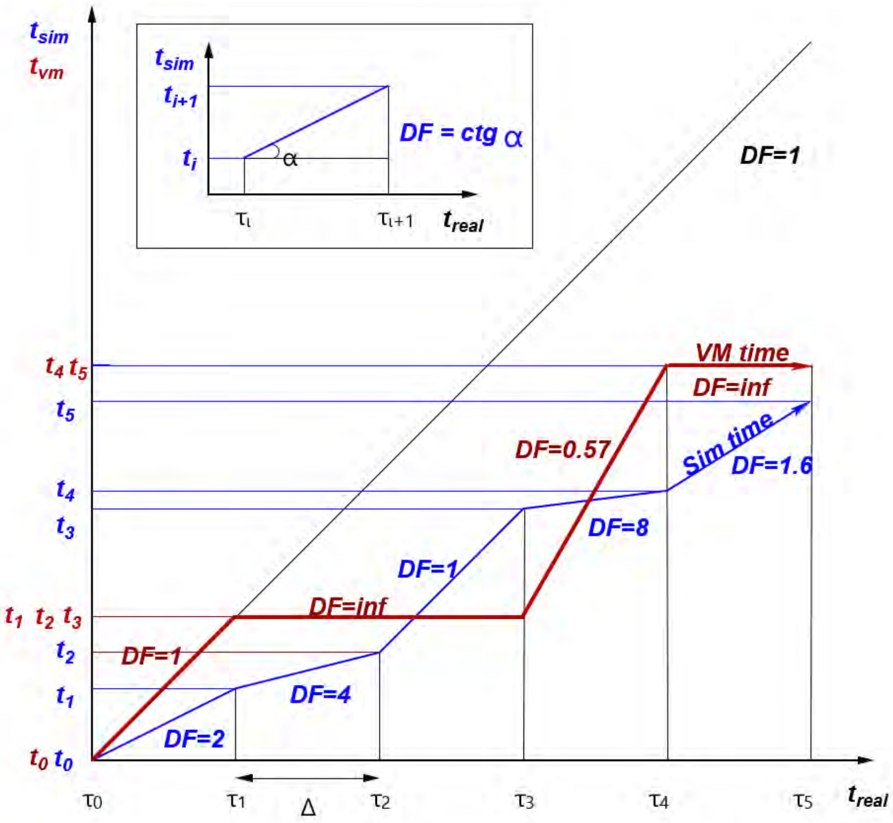
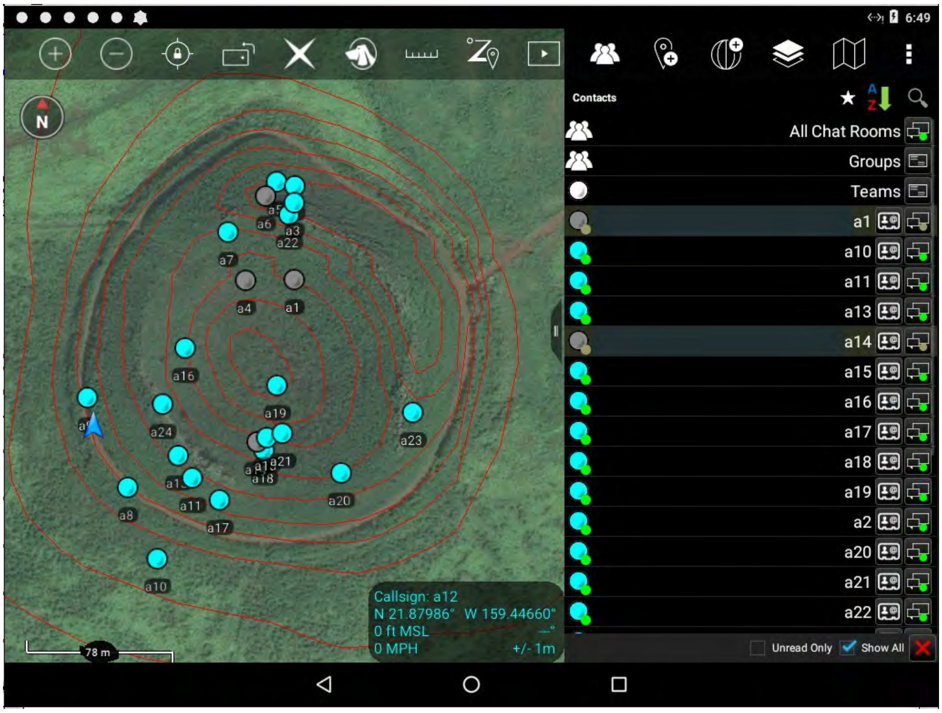


**Figure 2:** *VM time advancement in CyberVAN.*



Contacts

All Chat Rooms
Groups
Teams
a1
a10
a11
a13
a14
a15
a16
a17
a18
a19
a2
a20
a21
a22

Callsign: a12
N 21.87986° W 159.44660°
0 ft MSL
0 MPH +/- 1m

□ Unread Only ☑ Show All

**Figure 3:** *A screen shot of the Android Tactical Assault Kit (ATAK) application.*

clock source. This approach works for all major OSs, including Linux, Windows, Android, OSX, BSDs, and Cisco IOSv.

## AN ARMY-RELEVANT, OPEN SCENARIO: PLATOON-LEVEL SITUATIONAL AWARENESS

In support of Cybersecurity CRA, we have recently developed a platoon-level lower tactical internet scenario that utilizes the civilian version of the Android Tactical Assault Kit (ATAK) [14], an extensible situational awareness (SA) application initially developed by AFRL; the military version of ATAK is in active use in the U.S. Army. Figure 3 shows a screenshot of the main ATAK SA panel with locations of the platoon members on the terrain, and a peer-to-peer messaging panel. Note the GPS data in the lower-right corner of the SA panel. The core ATAK functionality, present in all versions, includes: (a) maintaining blue force SA, (b) posting incident/intelligence reports for the team and higher level commanders, and (c) supporting peer-to-peer and group chat.

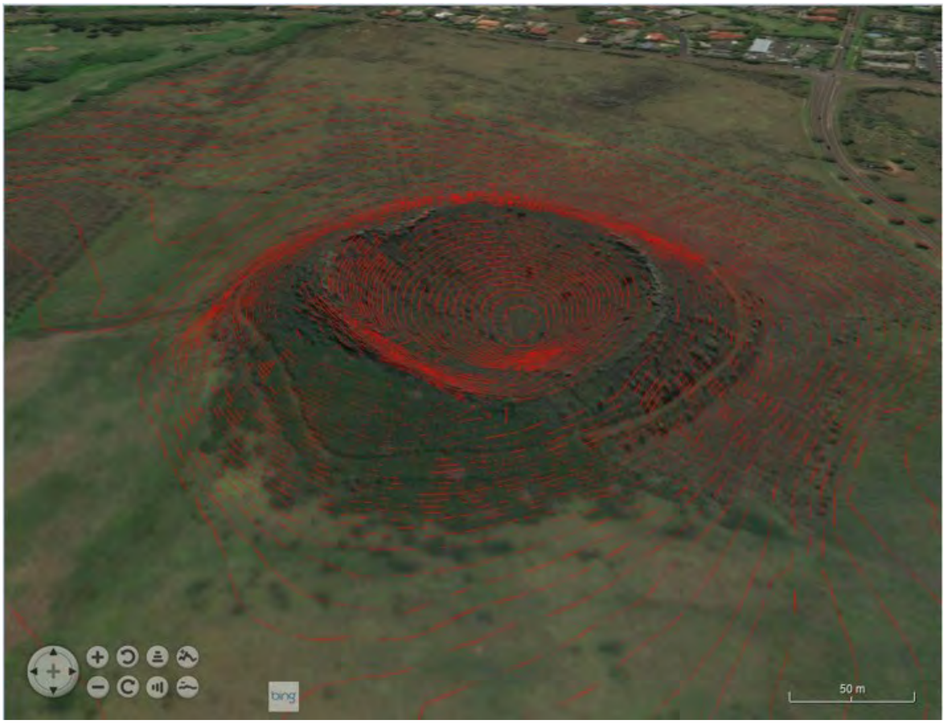


**Figure 4:** *The Puu Wanawana crater area on Kauaiuai, HI with contour lines at 1m altitude increments.*

In support of blue force tracking, the ATAK application is typically configured to send Position Location Information (PLI) reports (either periodically, or on significant movement) to other team members, via UDP and IPv4 multicast. For the remainder of this paper, we will be concerned with this PLI traffic, and have configured ATAK to send the reports every 3 seconds. Our notional mission involves search and recovery of a small object lost in the vicinity of the Puu Wanawana crater in Kauai, Hawaii. This area (Figure 4) is interesting because it involves complicated terrain, with implications for radio propagation, and high-resolution terrain data are openly available for it from USGS.

For this scenario, we use ns-3-simulated 802.11n radios with omnidirectional antennas at the 2.412 GHz frequency, in ad hoc mode, with broadcast/multicast rate fixed at 1Mbps. The transmission power, antenna gain and sensitivity parameters have been adjusted to enable multi-hop topologies on the scenario terrain, within a distance of a few hundred meters. We use a terrain-aware propagation loss model based on a combination of [15] and [16], and a modified reference point group mobility model from [17], extended to allow (a) explicit group membership, (b) using an actual node as a reference point, and (c) terrain-following 3D mobility. In the scenario, 24 nodes move in groups of two across the terrain at low human speeds, with pause times of up to a few minutes. The scenario duration is 20 minutes.

Each node is running ATAK on QEMU-emulated Android/x86 7.1 tablets. Layer 3 forwarding is implemented with ns-3-simulated OLSRv1 and SMF; pre-routing injection is used.

## PERFORMANCE EXPERIMENTS

Two critical metrics for network performance are latency and packet delivery ratio (PDR). To evaluate the differences between the purely simulated and hybrid emulated networks, we analyzed both cases and compared the values of these metrics across 10 runs to ensure that the results are repeatable and not due to random chance.

Both the ATAK application and the ns-3 simulation set the ID field of the IP packets. Thus we can identify the unique send/receive pairs for all nodes. The ATAK application periodically emits PLI information every 3 seconds and the SMF protocol floods these PLI updates across the entire network. Because traffic is being flooded, each PLI that is emitted, will be received in duplicate proportional to the number of 1-hop neighbors at each node.

### *One-way Latency*

Since the nodes are in a mobile ad hoc network, we measured the one-way latency for each pair of nodes across the entire network. Because packets are received in duplicate, we compute the difference between the emission time and the first reception time as the one-way transit time. The network is entirely simulated, thus there is no need to synchronize the endpoints as the flow of time is strictly enforced by the network simulator.

To establish a baseline for comparison we ran a purely simulated version of the scenario described in section III. To replicate the traffic pattern of the actual application we used the OnOff traffic generator to generate UDP packets of the right size, destined for the same multicast group and port, every 3 s, with small, normally distributed jitter.

In Figure 5 we show 10 cumulative distribution functions (CDF) for the one way latency. The median transit time was 0.0029 seconds across all 10 runs. The variation in the CDFs between runs is very small compared to the transit time across the network.

To compare we also preformed 10 runs where traffic was generated from the ATAK applications, and injected directly into the simulated network.

The behavior of the network was consistent across all 10 runs as there is very little variation between the CDFs shown in Figure 6.

We plot the averaged CDF across all 10 runs for both cases to verify that the distributions are the same in both cases. Figure 7 demonstrates that there is hardly any impact on the in simulation network latency when traffic is generated from the applications running on VMs in hybrid-emulation.

### *Packet Delivery Ratio (PDR)*

The packet delivery ratio is computed as the ratio of received packets to sent packets. Using the IP address and IP ID fields of the packet header, we identify the unique send and receive pairs. Similar to the latency measurement we count only a single reception of the packet to avoid over counting due to duplication. Figure 8 shows the CDF of the PDR for the simulation baseline. Because of the reliable flooding of the SMF protocol, the PDR is very high 0.9974.

In the case of hybrid emulation (Figure 9), there is again very little impact on the delivery rate. The CDFs for both cases are very tightly clustered demonstrating that the experimental results are very repeatable. The usage of hybrid emulation does not introduce any variability to the distributions.

Looking again at the averaged CDFs side by side (Figure 10) we can see that the CDFs are not significantly different in any meaningful way.

### *Transparent Forwarding Transit Time*

Because the forwarding fabric used to move packets between the VMs and the simulator is a high speed wired Ethernet network, packet loss between the VMs and simulator is extremely rare (unmeasurable). Therefore the only potential impact might be on the transit time of a packet.

We have already measured the transit time through simulation (in section IV-A) and determined it to be approximately 0.003 s. This transit time reflects the network models delay profile based on channel conditions and mobility patterns. To measure the complete path, we need

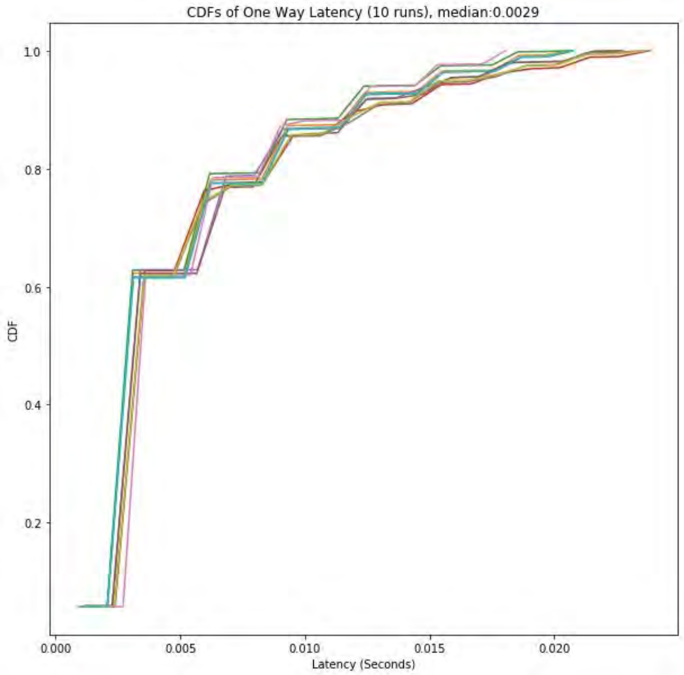


**Figure 5:** *The reference implementation of the mobile network in ns-3 establish the baseline for comparison. In the purely simulated case the median one-way latency between all pairs for nodes in the mobile ad hoc network was 0.0029 seconds across 10 runs.*

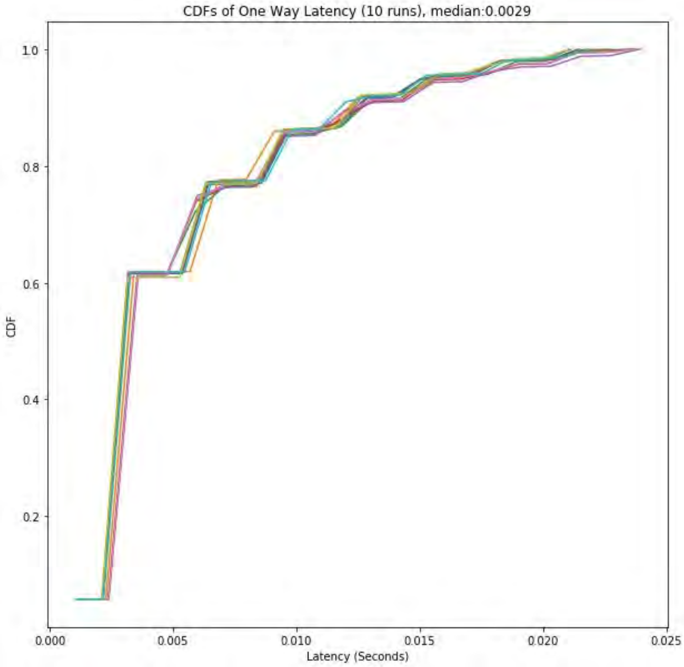


**Figure 6:** *When using hybrid emulation, the traffic is generated in virtual machines using real applications. This traffic is then injected into the simulated network. This injection has no detectable impact on the one-way latency within the simulated network as the median in the case of hybrid emulation was also 0.0029.*

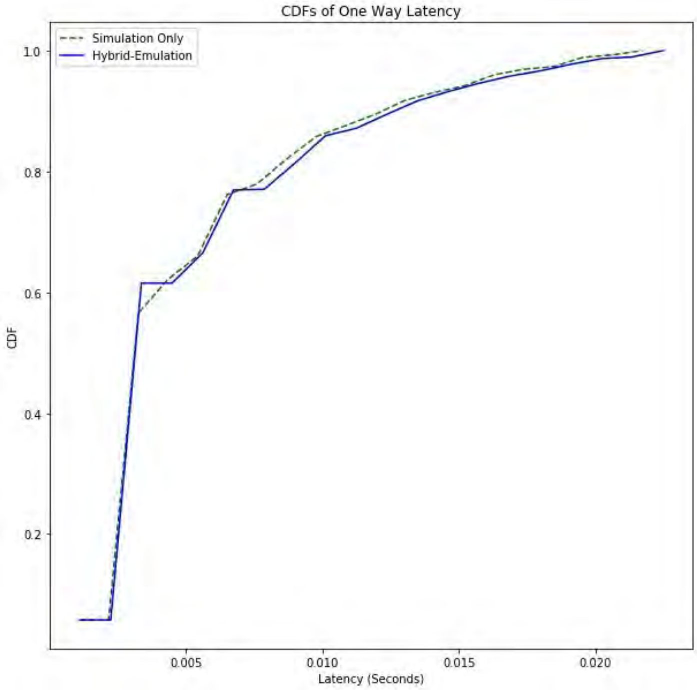


**Figure 7:** *When the averages across 10 runs are plotted together, we note that there is no discernible difference between simulation and hybrid-emulation one-way latency CDFs.*

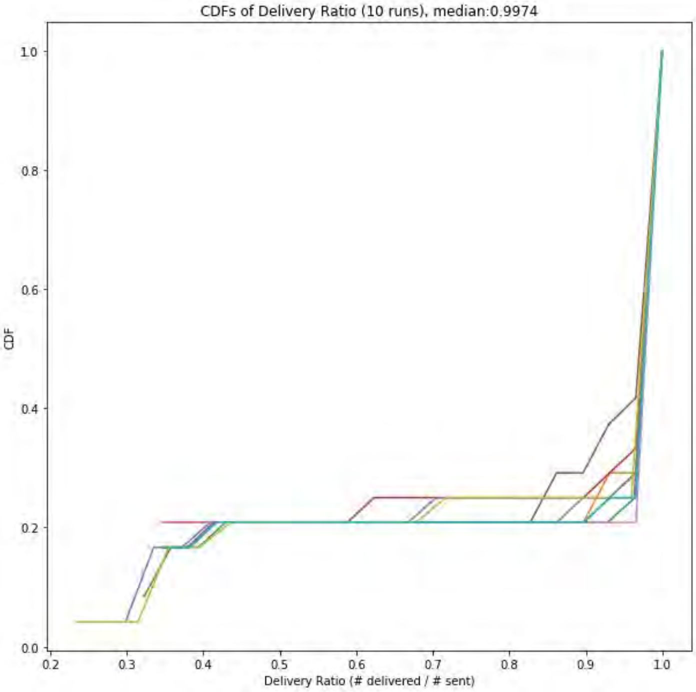


**Figure 8:** *Because each packet is reliably flooded across the entire ad hoc network, packet delivery rates are very high. The median delivery rate for the purely simulated case is 0.9974.*

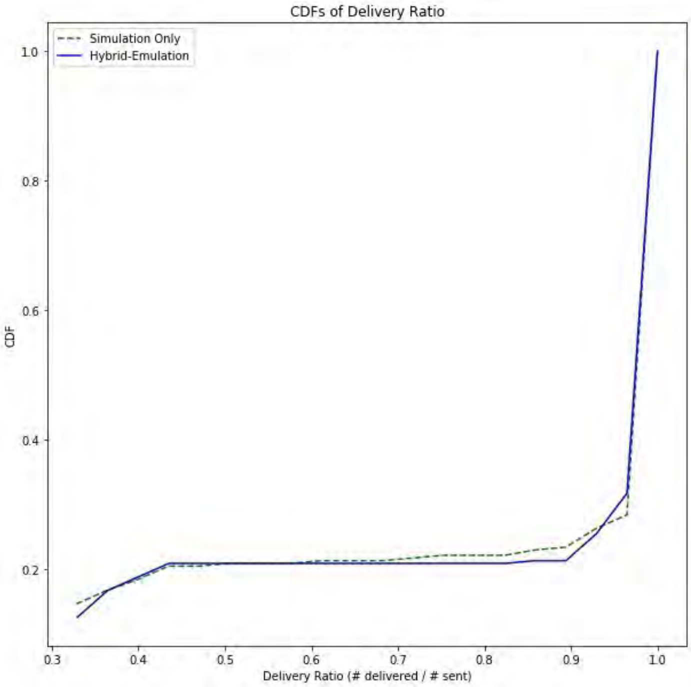


**Figure 9:** *A direct comparison of the delivery rates between the simulated and hybrid emulated traffic shows very little difference in the CDFs.*

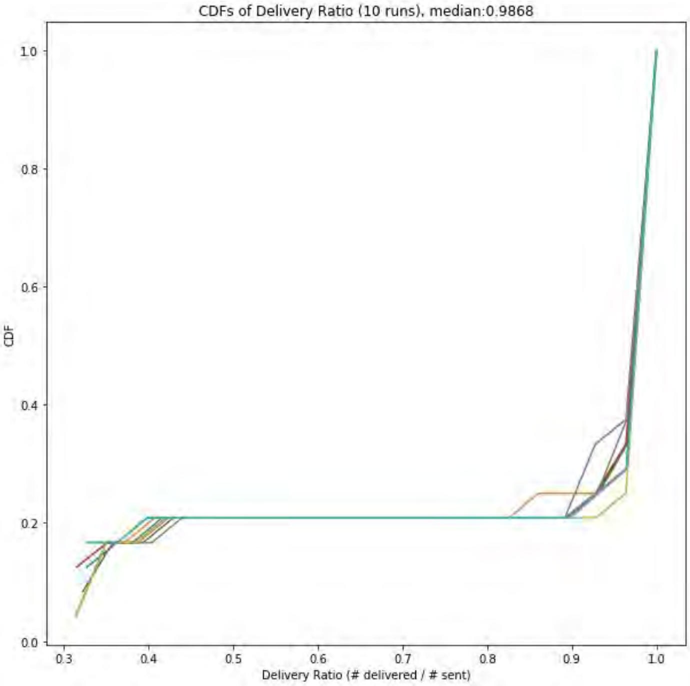


**Figure 10:** *The injection of actual application traffic in hybrid emulation does not have a significant impact on the delivery rate. The median delivery rate in this case was 0.9868.*

to account for the transit time between the VMs and the network simulator in both directions. In Figures 11 and 12 we show the CDFs form the transit times to and from the network simulator. In both cases the median transit time is approximately 0.0001 seconds, an order of magnitude smaller than the delays introduced by the simulated network conditions. While there is some variation between runs (due to existing network loads on the shared network forwarding fabric), even the worst case delay is 0.0006 seconds which is well below the delay introduced by the network simulation.

## CYBER EXPERIMENTS

In this section, we describe two cyber attacks on the search and recovery mission, and their implementations in CyberVAN.

### *Black hole attack on Layer 3 unicast forwarding*

Layer 3 unicast forwarding with Optimized Link State Routing Protocol (OLSR) can be implemented with either pre-routing or post-routing packet injection, as there exist both an Android based implementation (Naval Research Laboratory OLSRv2/NHDP) [21][22]) and an OLSRv1 [23] simulation model (in ns-3). For this example, we chose to implement it in the VMs, with post-routing injection. The VMs are configured with static ARP entries for all the nodes in the platoon, so packets can be injected without ARP requests. Also, for ease of presentation, we consider a single stationary snapshot of the dynamic topology created by the mobility model. The OLSRv2/NHDP-created topology before the black hole attack is shown in Figure 13.

The black hole attack consists of two distinct parts. The first part (”attraction”) is executed in the OLSRv2/NHDP control plane, by falsely claiming non-existing one-hop neighbors in the HELLO and TC messages. As the OLSRv2/NHDP protocols are built on implicit trust, actual neighbors and non-neighbors accept such claims at face value. Our attack is relatively stealthy as it only claims up to a configurable number of false neighbors at and beyond two hops in the actual topology. It is also adaptive as the set of falsely claimed one-hop neighbors is re-evaluated periodically to match topology changes. The effect of the attraction part of the black hole attack executed on node 22 is shown in Figure 14. The rest of the network, after the short time that it takes to propagate fake link information, considers node 22 as having 10 extra links, shown in red. As a result, OLSRv2 routes, based on the shortest path computation, will force a considerable amount of traffic (e.g., from node 11 to node 23) to go through node 22. At this point, the attacker at node 22 can drop all (black hole) or some (grey hole) traffic that has been forced through it; this is the second (“data plane”) part of the black hole attack. The attack has been implemented as a direct modification of the NRL OLSRv2/NHDP source code, but could equally well be implemented in a packet mangling process external to the OLSRv2/NHDP daemon. It has been used in the evaluation of defensive technologies for link state routing protocols developed on [24].

### *Location-falsifying attack*

In the Location-falsifying attack, the goal is to poison the network by flooding false PLI information. Under nominal conditions, each PLI message is flooded to the rest of the network (as depicted in

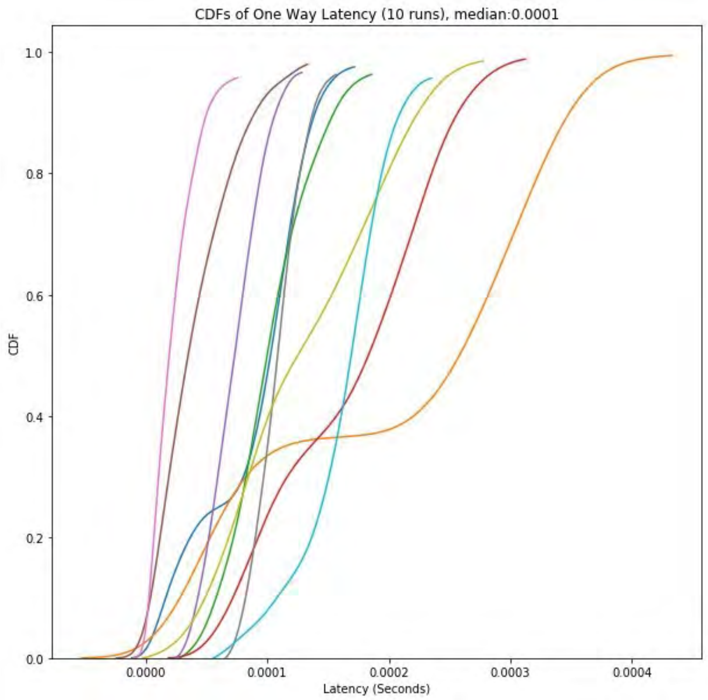


**Figure 11:** *The median transit time to the VM from the network simulator was also 0.0001 seconds.*

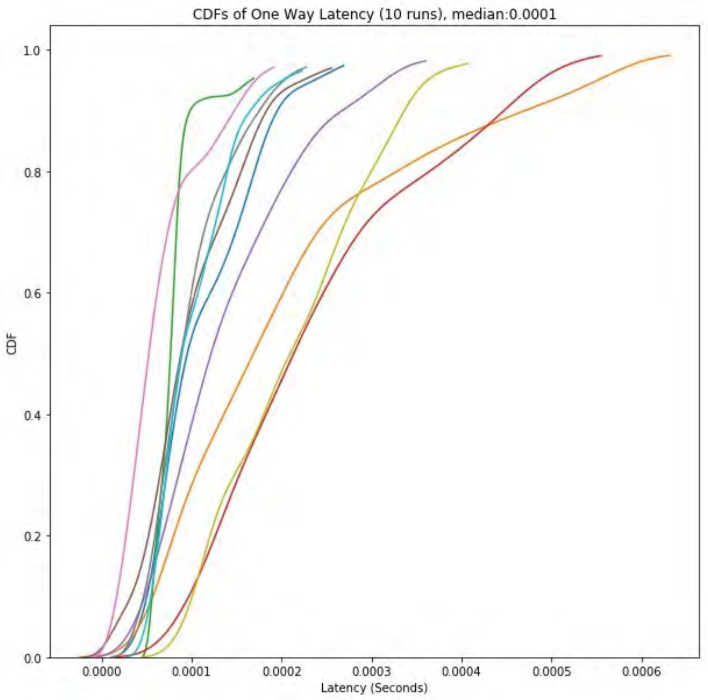


**Figure 12:** *The median transit time to the network simulator from the VM was 0.0001 seconds.*

Figure 15). This will occur even if a node is isolated from the rest of the network, as long as there is a one hop neighbor within range that can forward packets on behalf of the sender (e.g. A13 forward for A18). In the most naive case the attacker can simply pick a victim and blindly modify the packet body of the PLI update message with a random location. In the absence of message signatures, these spoofed updates will cause the victim's position marker to jump around the map as the client receive both the real and fake PLI information. This approach, however, is easily detectable both in the client (seeing the victim's position indicator jump around) and in the network (seeing duplicate packets with differing information).

A stealthier attacker may use the topology of the formed network to their advantage and carefully choose the modified position to be within a reasonable distance of the network. They can determine when a node is isolated by examining the routes and positions of a node. In the case of A18, the attacker would note that their position is physically far from the rest of the network and that they have no routes to other nodes via A18. If the attacker floods false information into the network at this point, the rest of the network will only get the falsified packets. In Figure 16, Node A13 is in such a position and delivers altered PLI updates on behalf of A18.

In the CyberVAN testbed, the ATAK application gets its GPS information from the network simulator (via the Android OS location service) and then uses these GPS coordinates to form its PLI message. We tested this attack by modifying the SMF client within the VM to alter the PLI packet bodies when the network conditions are appropriate for a stealthy attack.

## ELECTRONIC WARFARE EXPERIMENT

In this experiment, we demonstrate a simple but effective jammer deployed by a passing adversarial UAV on its reconnaissance mission. The UAV's flight path, at a constant altitude of 500m, is shown in Figure 17. The jammer has a period of $\frac{1}{60}$ $\frac{1}{60}$ seconds and a duty cycle of 0.75.

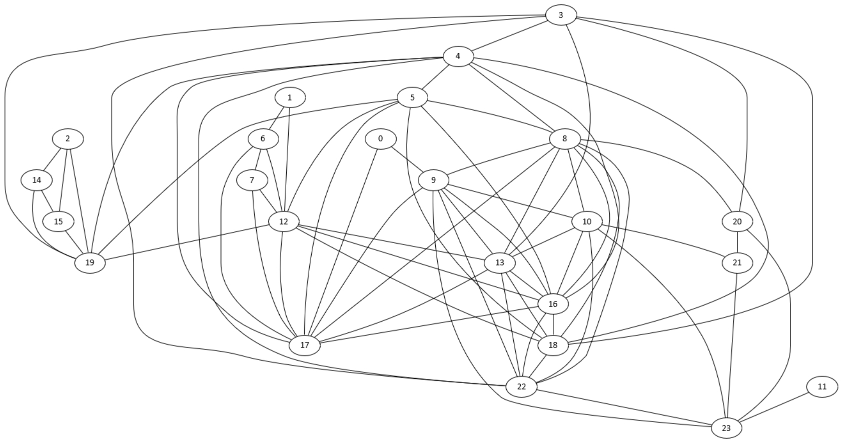


**Figure 13:** *Network topology before the black hole attack.*

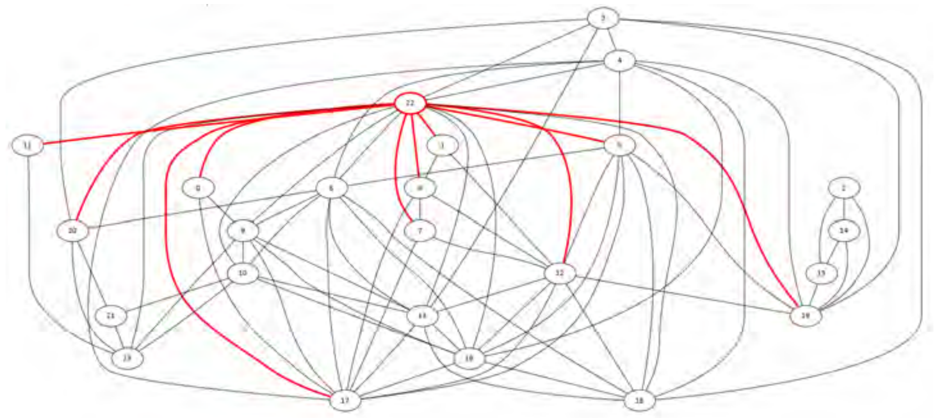


**Figure 14:** *Network topology during the black hole attack.*

The jammer is implemented with the microwave oven model available in the ns-3 Spectrum module and described in [18]. The jammer injects interference in free space, on all frequencies between 2.4 and 2.499 GHz, and kills a number of multicast PLI reports that have no redundancy in the 802.11 MAC layer. The jammer was operational for the entire 20 minutes of the scenario duration.

While the illustrated jammer is deliberately chosen to be as simple as possible, a sophisticated jammer modeling framework is under development for ns-3 [5].

The effect of the jammer's operation is shown in Figure 18 and Figure 19.

## CONCLUSION

In this paper we presented CyberVAN, a hybrid network emulation testbed. CyberVAN uses network simulation and VMs running unmodified software to model a network at varying levels of fidelity. We described several aspects of the testbed that allow a user to tune the fidelity of the model for use cases ranging from network performance modeling to assessment of cyber threats in representative network topologies.

We have demonstrated that the CyberVAN HNE introduces minimal distortion to network performance measurements, for experiments with emulated components at Layer 3 and above. We have also demonstrated

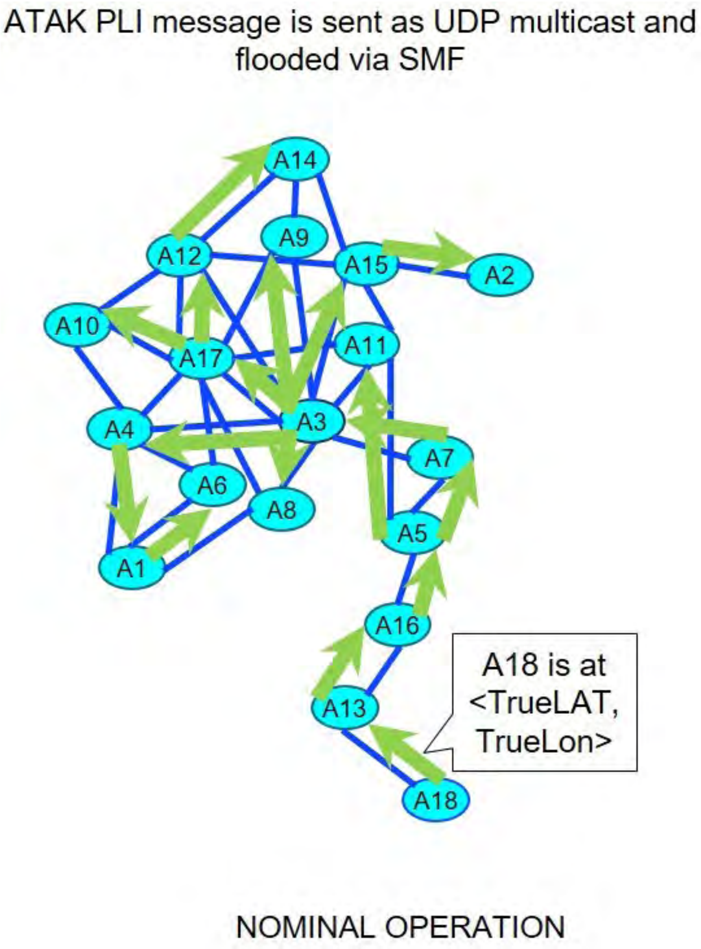

ATAK PLI message is sent as UDP multicast and flooded via SMF
A14
A9
A12
A15
A2
A10
A17
A11
A4
A3
A7
A6
A8
A5
A1
A16
A13
A18
A18 is at <TrueLAT, TrueLon>
NOMINAL OPERATION

**Figure 15:** *Under nominal conditions each unaltered PLI message is reliably flooded through the network via the SMF protocol even if the source is isolated.*

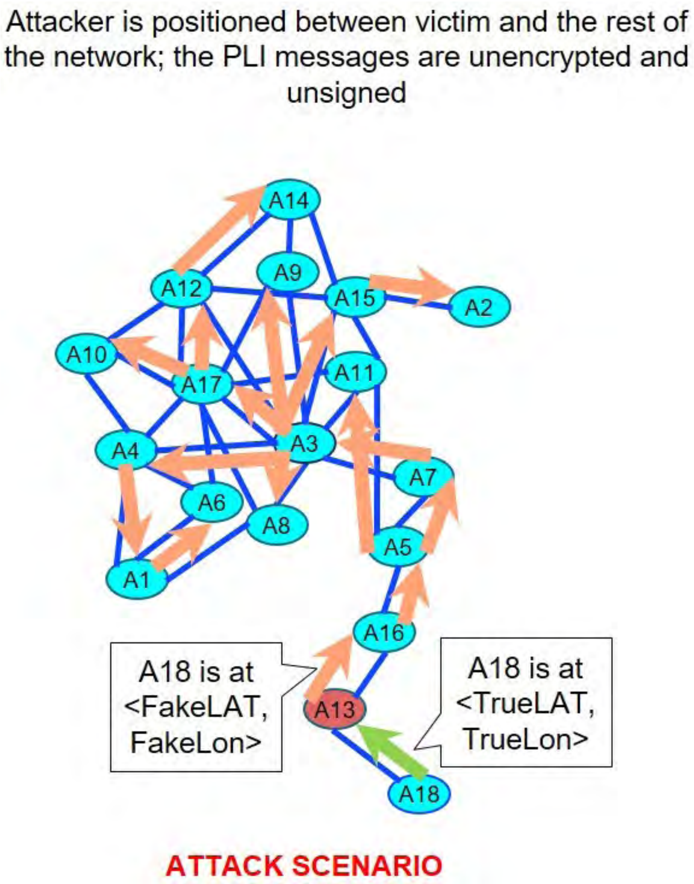

Attacker is positioned between victim and the rest of the network; the PLI messages are unencrypted and unsigned
A14
A9
A12
A15
A2
A10
A17
A11
A4
A3
A7
A6
A8
A5
A1
A16
A13
A18
A18 is at <FakeLAT, FakeLon>
A18 is at <TrueLAT, TrueLon>
ATTACK SCENARIO

**Figure 16:** *When the correct conditions for attack are identified false PLI information is flooded through the network. Recipients of these updates are misinformed about the victim's position. The condition for the attack to be effective that is shown in this diagram is that the target of the attack can only reach the rest of the network by forwarding through the attacker.*

CyberVAN's ability to model tactical networks, including replicating effects of terrain, mobility and EW. We showed the evaluation of cyber effects in these difficult to reproduce settings. The usage of real applications and OSs as part of the model enables testing of cyber effects which would be difficult in a purely simulated setting. CyberVAN enables repeatable testing in a virtual environment that is easy to manipulate and instrument. This can reduce the cost of testing and reasoning about cyber and EW effects in the networks of interest.

While the CyberVAN TimeSync solution enables theoretically unlimited scenario scalability with limited resources, it is impractical beyond a certain degree of slowdown, which may be possible when modeling large enterprise/tactical networks at full fidelity. We are

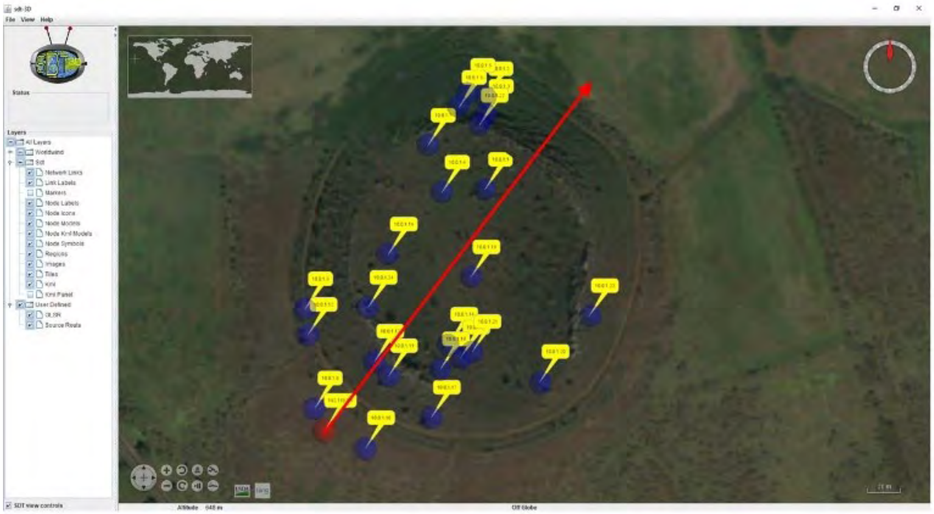


**Figure 17:** *The adversarial UAV's flight path over the mission area.*

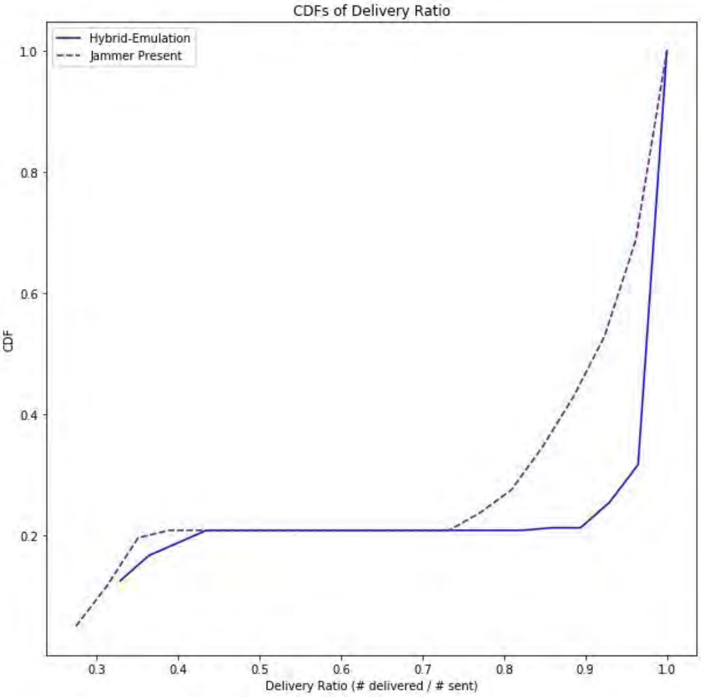


**Figure 18:** *The jammer's effect on the PLI report PDR.*

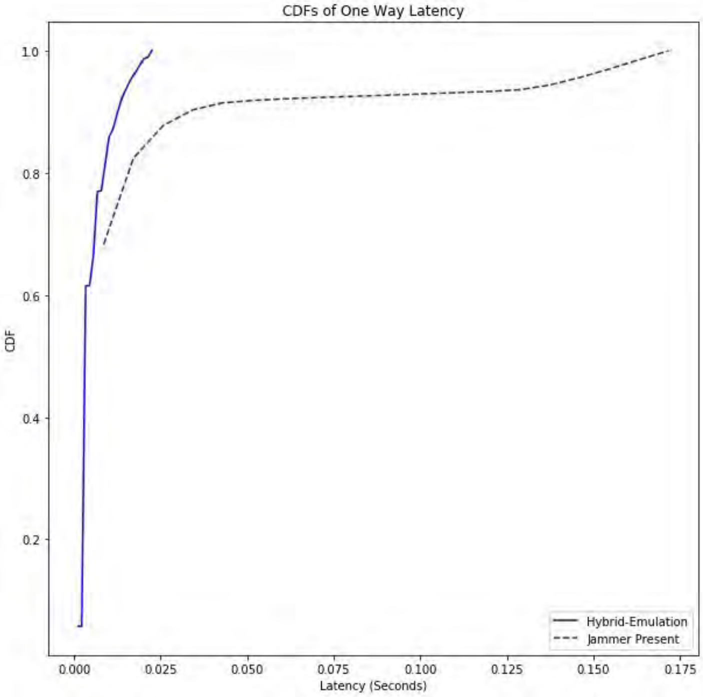


**Figure 19:** *The jammer's effect on the PLI report latency. The jammer does introduce some delays, however the median is unchanged since most of the effect of the jammer is to create packet loss.*

currently investigating multiple HNE solutions to increase scenario scalability in addition to TimeSync, including (a) multi-threaded discrete event simulation with optimistic scheduling and reversible events, (b) distributed simulation, (c) modeling wired links with CyberVAN switching infrastructure (as opposed to network simulators), and combinations of the above.

While running real OSs and applications allows testing against a vast number of possible real cyber attacks, the current CyberVAN environment may be unsuitable for exploits that rely on some specific hardware features, exact instruction timings and precise configurations of real devices. When required, such needs can be addressed with the CyberVAN hardware-in-the-loop (HITL) capability, with the caveat that a scenario with real hardware requires execution in real time.

Hybrid network emulation has been our chosen modeling approach for over a decade because of its ability to balance fidelity and scale, and take advantage of existing models. We encourage the readers to apply the approach to their problems. CyberVAN software is Government Off-The-Shelf (GOTS) and available upon request from Perspecta Labs.

## REFERENCES

**[1]** R. Chadha, T. Bowen, C.J. Chiang, Y.M. Gottlieb, A. Poylisher, A. Sapello, C. Serban, S. Sugrim, G. Walther, L. Marvel, A, Newcomb, and J. Santos, CyberVAN: A Cyber Security Virtual Assured Network Testbed, IEEE MILCOM 2016.

**[2]** A. Poylisher, C. Serban, J. Lee, T. Lu, C. J. Chiang, "Virtual Ad hoc Network Testbeds for high fidelity testing of tactical network applications", IEEE MILCOM, 2009.

**[3]** A.Poylisher, T.Lu, C.Serban, J.Lee, R. Chadha, C JasonChiang, "Realistic modeling of tactical networks with multi-level security in VAN testbeds", Proceedingsof IEEE MILCOM 2010

**[4]** A. Poylisher, C. Serban, J. Lee, T. Lu, R. Chadha, C.-Y. J. Chiang, "A Virtual Ad Hoc Network Testbed", International Journal on Communication Networks and Distributed Systems, 2009.

**[5]** ns-3 Wireless Jamming Model, https://www.nsnam.org/wiki/Wireless jamming model, retrieved on 07/19/19.

**[6]** C. Serban, A. Poylisher, A. Sapello, Y. Gottlieb, C. J. Chiang, R. Chadha, "Testing android devices for tactical networks: A hybrid emulation testbed approach", IEEE MILCOM 2015.

**[7]** F. Sultan, A. Poylisher, C. Serban, C. J. Chiang, R. Chadha, "TimeSync: Enabling Scalable, High-Fidelity Hybrid Network Emulation", the 15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM), Cyprus, 2012.

**[8]** C. Serban, A. Poylisher and C.-Y. J. Chiang, "A Virtual Ad hoc Network Testbed for Network-Aware Applications", Proceedings of12th IEEE/IFIP Network Operations and Management Symposium (NOMS 2010).

**[9]** T. H. J. Ahrenholz, C. Danilov and J. Kim, "CORE: A real-time networkemulator," in Proc. of MILCOM, 2008.

**[10]** U.S. Naval Research Laboratory, "Extendable Mobile Ad hoc NetworkEmulator," 2012. [Online]. Available: http://cs.itd.nrl.navy.mil/work/emane/index.php

[11] Scalable Network Technologies, QualNet, 2019. [Online]. Available:http://www.scalable-networks.com/products/developer.php

[12] S. Wang and Y. Huang, "NCTUns Distributed Network Emulator",Internet Journal, vol. 4, no. 2, pp. 61–94, 2012.

[13] http://www.arl.army.mil/www/default.cfm?page=1417, retrieved on 4/19/16.

[14] Android Tactical Assault Kit (ATAK), 2019. [Online]. Available: https://takmaps.com.

[15] International Telecommunication Union, "Recommendation ITU-R P.525-3. Calculation of free-space attenuation", 2016.

[16] International Telecommunication Union, "Recommendation Rec. ITU-R P.526-8. Propagation by diffraction", 2003.

[17] N. Aschenbruck, R. Ernst, E. Gerhards-Padilla, and M. Schwamborn. 2010. BonnMotion: a mobility scenario generation and analysis tool. In Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques (SIMUTools '10). ICSTBrussels, Belgium.

[18] T. M. Taher, M. J. Misurac, J. L. LoCicero, and D. R. Ucci, "Microwave Oven Signal Modeling", in Proc. of IEEE WCNC, 2008.

[19] DARPA Dispersed Computing (DCOMP) program. 2019. [Online]. Available: https://www.darpa.mil/program/dispersed-computing.

[20] DARPA Secure Handhelds on Assured Resilient networks at the tactical Edge (SHARE) program, 2019. [Online]. Available: https://www.darpa.mil/program/secure-handhelds-on-assured-resilient-networks-at-the-tactical-edge.

[21] RFC 7181. "The Optimized Link State Routing Protocol Version 2", 2014. [Online]. Available: https://tools.ietf.org/html /rfc7181.

[22] RFC 6130. "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", 2011. [Online]. Available: https://tools.ietf.org/ html /rfc6130.

[23] RFC 3626. "Optimized Link State Routing Protocol (OLSR)", 2003. [Online]. Available: https://tools.ietf.org/ html / rfc3626.

[24] DARPA Wireless Network Defense program. 2018. [Online]. Available: https://www.darpa.mil/program/wireless-network-defense.

[25] ns-3, a discrete event simulator for internet systens, 2019. [Online]. Available: https://www.nsnam.org.

## ABOUT THE AUTHORS

**SHRIDATT SUGRIM** is a member of the Machine Learning and Data Analytics Research team at Perspecta Labs for the last 4 years. Prior to that , he was a member of technical staff at WINLAB, Rutgers University for 11 years. His areas of research include networking (from radios to applications), Cyber Security, machine learning/ AI, and probability models. He is currently a PhD candidate in the ECE department of Rutgers University.

**ALEX POYLISHER** has been doing applied computer science at Perspecta Labs (formerly Bellcore/Telcordia/Applied Communication Sciences/Vencore Labs) for over 20 years, working on diverse problems in performance, modeling/simulation/virtualization, and security of distributed systems and protocols, particularly in wireless networks, on multiple U.S. Government and commercial research programs. He is currently the PI of the Perspecta Labs/UPenn/Princeton team on the DARPA Dispersed Computing program.

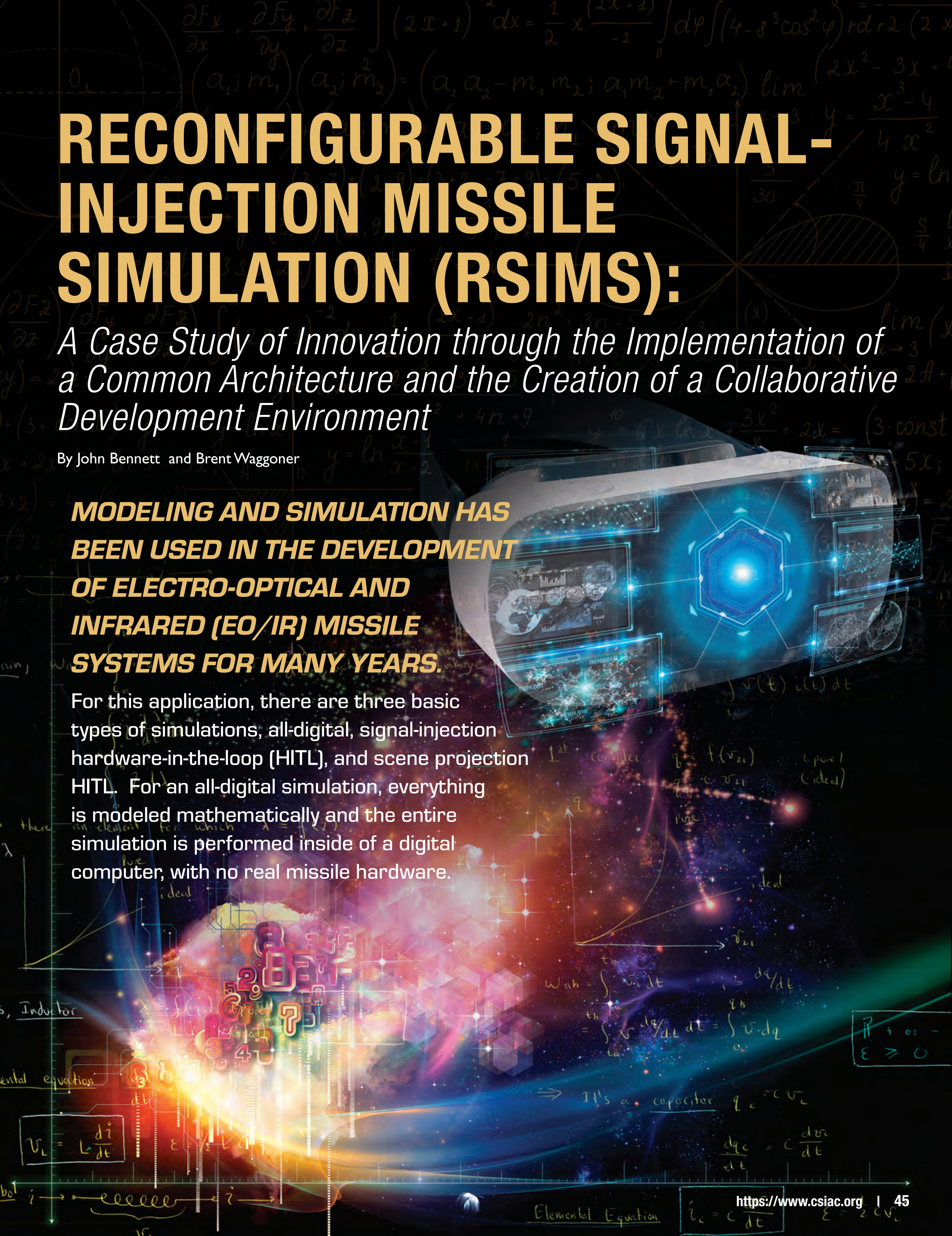
**JAMES PLASTINE** has over a decade of experience in the Information Technology (IT) field. He has filled roles including but not limited to Cyber Security Analyst/Engineer providing support to various US Army Research and Development efforts, Systems/ Network Administrator, Helpdesk Support, Project Lead, and Instructor. Most recently he has been focused on researching the security aspects of container technology, software defined networking, and network simulation/testbed systems and their potential application to military information systems/networks as a Cyber Security Engineer with KDM Security Solutions.

**DR. ALLISON NEWCOMB** earned her D.Sc. in Information Technology from Towson University, Towson, MD in 2016, where she researched computational intelligence approaches for improving cybersecurity postures of military enterprise and tactical networks. She is a member of AUSA, ACM, IEEE and ISC2, and holds the Certified Information Systems Security Professional (CISSP) and Certification and Accreditation Professional (CAP) certifications. Dr. Newcomb serves as a computer scientist at the CCDC Army Research Laboratory's Network Science Division and is a team lead in the Network Security Branch.

# RECONFIGURABLE SIGNAL-INJECTION MISSILE SIMULATION (RSIMS):

## *A Case Study of Innovation through the Implementation of a Common Architecture and the Creation of a Collaborative Development Environment*

By John Bennett and Brent Waggoner



***MODELING AND SIMULATION HAS BEEN USED IN THE DEVELOPMENT OF ELECTRO-OPTICAL AND INFRARED (EO/IR) MISSILE SYSTEMS FOR MANY YEARS.***

For this application, there are three basic types of simulations, all-digital, signal-injection hardware-in-the-loop (HITL), and scene projection HITL. For an all-digital simulation, everything is modeled mathematically and the entire simulation is performed inside of a digital computer, with no real missile hardware.

For scene projection HITL, the missile seeker (including optics and detector/gyroscope) is mounted on a 3 or 5 axis flight motion table (See Figure 1). An EO/IR scene projector is used to present a simulated scene to the missile. This must be done in real-time so that the missile is essentially inside of a virtual-reality type environment with its angular orientations, angular velocities, and angular accelerations provided by the flight motion table. Signal-injection HITL is a blend between an all-digital simulation and a full scene projection HITL simulation. In a signal-injection simulation, the real missile guidance and tracking electronics are used but the mechanical components (such as optics, detectors, and gyroscopes) are not. The detector signal is generated digitally by the computer and output as an electronic signal that is injected into the missile seeker electronics. Any other sensor signals must also be synthetically generated and injected into the seeker.

In human terms, the differences between scene projection HITL and signal-injection HITL can be illustrated by the difference between virtual reality (VR) achieved with VR goggles (scene projection) versus a form of VR where a signal is injected directly to the optic nerve (signal-injection), bypassing your eyes.

In this article, we will describe a DoD community that was formed to jointly develop a signal-injection type HITL simulation architecture called Reconfigurable Signal-Injection Missile Simulation (RSIMS). RSIMS was developed to be very generic so that it can be used for many other applications outside of signal-injection missile seeker HITL simulation.

## RSIMS BASIC DESIGN

At its core, RSIMS is a computer architecture for real-time processing that allows the developer to break a problem into sub-system models, implement these models as individual threads that each run on a single core of a multi-core Linux personal computer (PC), while providing many utilities for timing control and both analog and digital input/output (I/O).

The RSIMS philosophy and design goals are:

- Maximize the use of commercial-off-the-shelf (COTS) hardware (PCs) with custom software
- Make RSIMS a common simulation architecture between many laboratories/facilities to allow sharing of subsystem models (e.g. gyro, flight motion, sensor/scene, I/O, etc.) and promote joint development
- Open source, where the code is freely shared between participants
- Easy integration of Matlab/Simulink® models
- Minimize cost

One of the keys to successful real-time operation of an RSIMS simulator is the ability to shield the required number of cores from interference from the operating system (OS) or system interrupts so that they can be totally dedicated to real-time processing. If this is not done, interrupts generated by the OS will cause latencies that prevent real-time operation. RSIMS has two options for this service, one is a commercial real-time version Linux, and the other is a real-time modification to an open-source version of Linux. This is a good example of the RSIMS collaborative development environment, since the second option was developed by one of the RSIMS partners and provided to the community.

Individual simulation threads can be generated from hand-written C++ code, or from a Simulink® model that has been auto-coded using the Mathworks Simulink Coder™. Giving the simulation developer the option to mix threads from hand-written C++ and Simulink® is very powerful. This allows the developer to choose the best format for development of each subsystem model. For example, in the current missile seeker application of RSIMS, simulation timing control, I/O, and object spatial position threads are all hand-written C++ code, while the gyroscope models and missile flight simulation subsystems are both Simulink®.

Users can easily spawn RSIMS threads to the PC processor cores for all the simulation subsystems. Once the simulation is running, the threads communicate with each other using the PC system memory. Controls have been developed to make sure that system memory values aren't accessed while

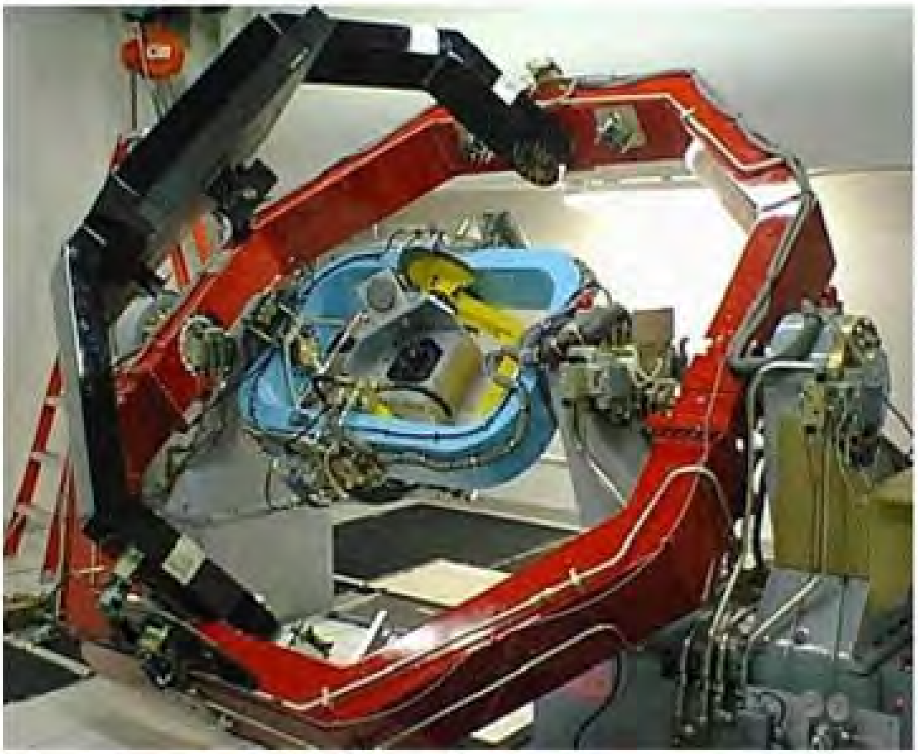


**Figure 1:** *Five-Axis Flight Motion Table used in Scene Projection HITL*

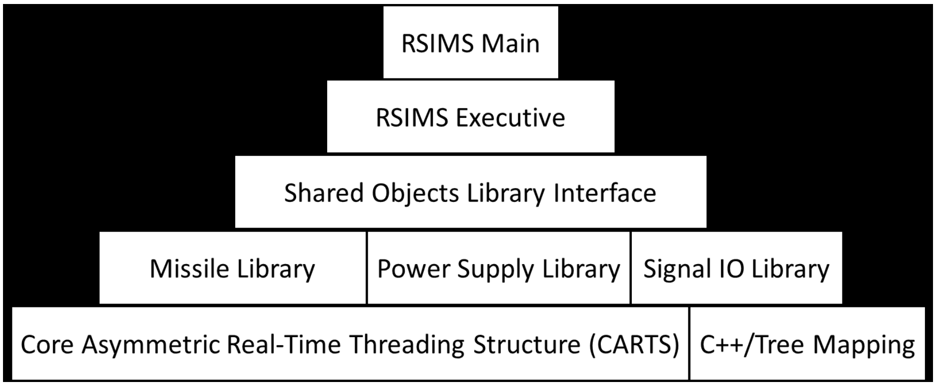


**Figure 2:** *RSIMS Modular System Design*

ARMAMENT RESEARCH, DEVELOPMENT & ENGINEERING CENTER
PICATINNY, NJ
Dynamic Infrared Missile Evaluation
AFRL/RW
NICEL
DEFENSE INTELLIGENCE AGENCY
UNITED STATES OF AMERICA
MECS
ARL / SLAD
THREAT SIGNAL PROCESSOR-IN-THE-LOOP SIMULATION
T-SPIL
GWEF
LISTEN · INFORM · ATTACK · PROTECT
I2WD
RDECOM CERDEC
kinetics
STAY AHEAD OF THE THREAT
BOEING
dstl
DEFENCE R&D DÉFENSE
Canada
DST GROUP

**Figure 3:** *RSIMS Collaborative Development Community*

another thread is updating them. Figure 2 shows the basic RSIMS modular system design. The core of RSIMS is the Core Asymmetric Real-Time Threading Structure (CARTS), which is not tied to any specific application.

RSIMS works well for signal-injection HITL missile simulations, but its flexible design makes it ideal for any real-time application with I/O.

## CREATING A COLLABORATIVE COMMUNITY

Before the RSIMS community was formed, each Department of Defense (DoD) laboratory and each DoD contractor that did signal-injection HITL missile simulation used their own in-house developed architectures. This made the sharing of subsystem models, or other forms of joint-development and collaboration very difficult. This also meant that each facility was expending a large amount of resources to maintain and upgrade their individual architectures.

This changed in 2003 with the formation of the RSIMS development community. After hearing about the idea to develop a common HITL architecture, most of the DoD labs and contractors doing signal-injection simulation joined the group. Other labs that didn't immediately adopt RSIMS still participate in the RSIMS community because of the great collaboration opportunities. Membership in the RSIMS community is open to any DoD activity or DoD contractor. In addition, since RSIMS is Government-owned, there is no charge for the software. All users are encouraged to participate in the RSIMS community and share the code improvements they develop. This will help achieve the benefits of the common architecture and collaborative development environment.

An RSIMS configuration control board (CCB) is currently being formed from the DoD members of the RSIMS community. Users are free to make any changes to the RSIMS code they wish, but the CCB will control which changes will become part of the standard RSIMS distribution.

In addition to the U.S. partners, RSIMS has recently been distributed to three of our close international allies, Australia, Canada, and the United Kingdom. This distribution was done through the appropriate international agreements. Both Canada and the United Kingdom participated in the last RSIMS development community meeting. Including our international partners is a natural extension of the RSIMS open-source and joint development philosophy. More RSIMS users mean more improvements and enhancements to be shared with the community. Figure 3 shows the three groups that make up the RSIMS community, U.S. DoD, U.S. contractors, and national labs from our close foreign allies.

## SIGNAL-INJECTION MISSILE HITL SIMULATION APPLICATION

The specifics of the RSIMS signal-injection missile seeker HITL simulation include EO/IR scene generation using the DoD owned Fast Line-of-sight Imagery for Targets and Exhaust Signatures (FLITES) software. FLITES is managed by the Air Force Research Laboratory (AFRL) and is being used by most DoD EO/IR missile simulation facilities. FLITES also has a large DoD user/developer group, which is closely linked to the RSIMS community. In the past, we have held joint meetings between the RSIMS community and the FLITES User's Group.

The most difficult part of RSIMS development for signal-injection HITL

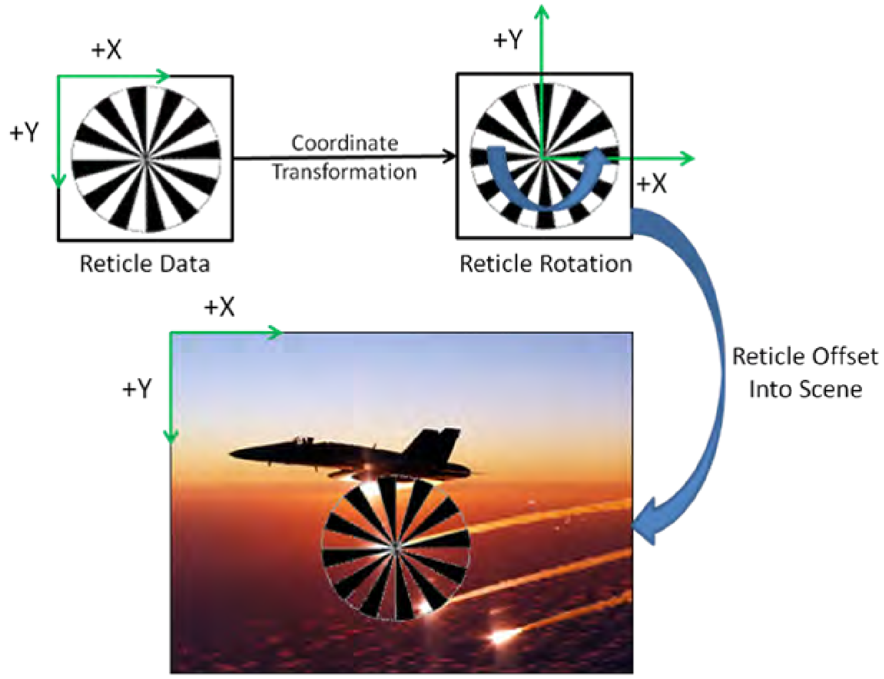


**Figure 4:** *Reticle Processor*

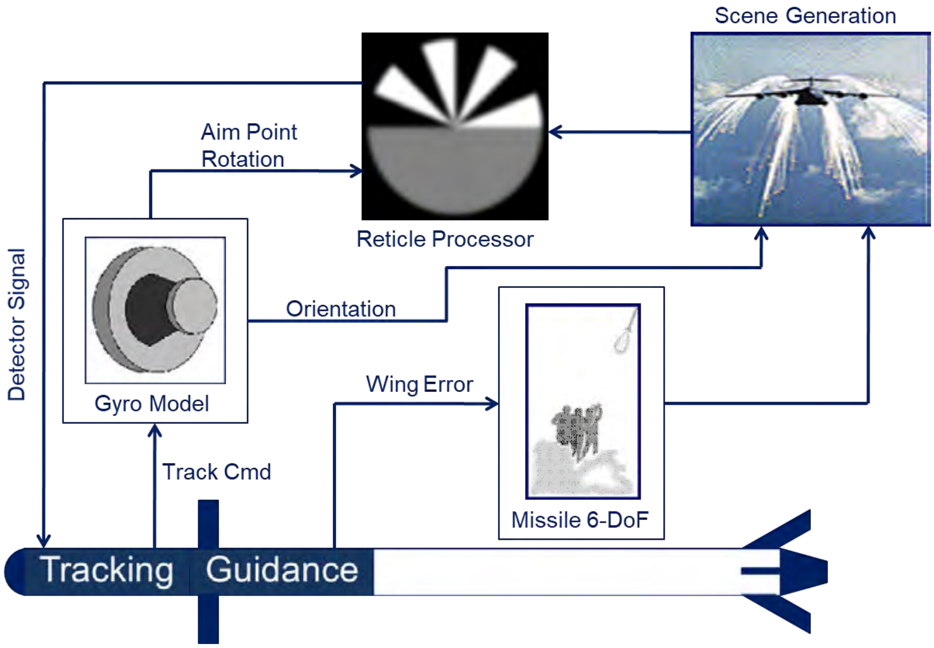


**Figure 5:** *RSIMS Block Diagram*

missile simulators was the reticle processor. Most non-imaging EO/IR missile seekers use a single detector sensor where the EO/IR scene is modulated by a reticle mask to allow tracking of individual sources. This process must be simulated digitally to create the detector signal for injection into the seeker guidance and tracking electronics. This involves spatially aligning the detector sensor reticle mask at the correct position on the EO/IR scene with the correct angular orientation. A multiply-accumulate function is used to determine how much EO/IR energy from the scene is transmitted through the reticle mask at each simulation time step. The detector signal is formed from this operation and output through a digital-to-analog converter for injection into the missile seeker electronics. This process must be done at very high rates to insure proper duplication of the analog detector signal. It is very challenging to complete this process and output the information within the required time step, which is typically between 10 and 50 microseconds, depending on the missile system under test. Figure 4 illustrates the operation of a reticle processor.

In its original design, RSIMS used a COTS PC based field programmable gate array (FPGA) device for reticle processing. However, the latest version of RSIMS performs this operation on the PC COTS graphics processor unit (GPU) which is also where the EO/IR scene is generated by FLITES. This is a superior design, since it does not require each scene to be moved (e.g. to the FPGA) before reticle processing can begin.

Figure 5 shows a basic block diagram of an RSIMS HITL missile simulation. Figure 6 shows how each of these processes is used to generate a threat that operates on one core of a multi-processor PC.

Many RSIMS users perform infrared countermeasure (IRCM) effectiveness analysis. Expendable IRCM models are being developed for FLITES. Additionally, directed energy/laser-based countermeasure modules are currently being developed for RSIMS by two of the partner labs.

The RSIMS I/O interface is designed to be easily adapted for use with any I/O hardware. This gives users the maximum amount of flexibility in choosing the right I/O hardware for their application. Currently, RSIMS has been used with several COTS I/O boards and one Navy designed board provided by one of our partners, the Naval Air Warfare Center at China Lake CA.

Another RSIMS partner, the Air Force Research Laboratory (AFRL) Dynamic Infrared Missile Evaluation (DIME) Laboratory is the developer of the all-digital simulation MOdeling System for the Advanced Investigation of Countermeasures (MOSAIC). MOSAIC has a very nice graphical user interface (GUI) and is used by many of the RSIMS partners in addition to their HITL simulators. The DIME Lab is currently integrating RSIMS and MOSAIC so that the MOSAIC GUI can be used to do simulation runs with both the native MOSAIC all-digital models, and RSIMS HITL simulators. This will give users the ability to use a single GUI to set up simulation runs for a study using a suite of both all-digital missile models and HITL simulators.

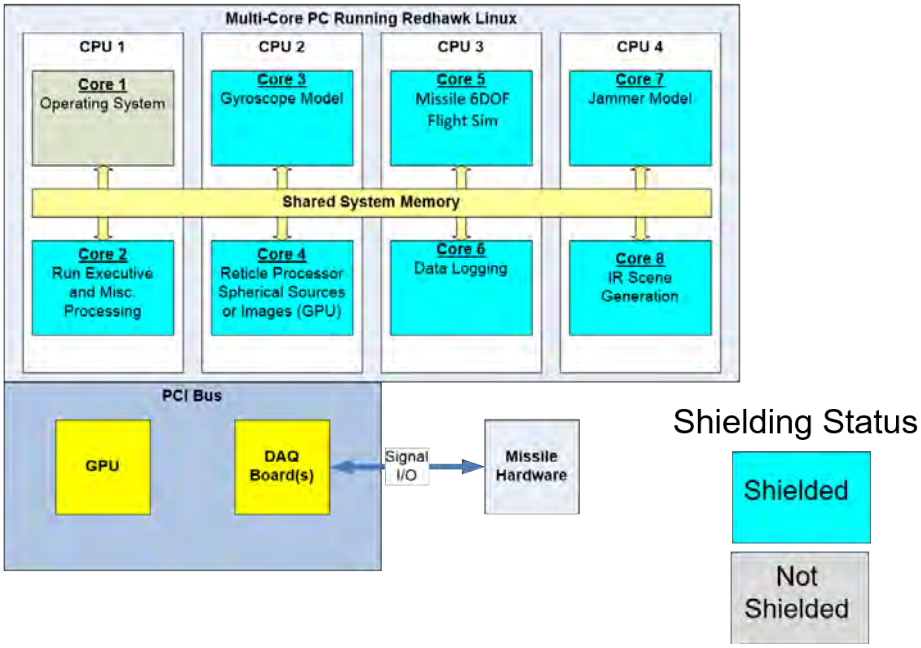


**Figure 6:** *RSIMS Threads on Processor Cores*

## OTHER APPLICATIONS

As mentioned above, the actual RSIMS code is very flexible and could easily be used for many other applications besides signal-injection HITL missile simulators. As an example, the AFRL DIME Lab has already used RSIMS as the architecture for a developmental missile seeker. In this application, RSIMS is the architecture for the missile itself, instead of the overall simulation, as in the more traditional RSIMS applications. This has created a very powerful tool. Since RSIMS is very tightly integrated with Matlab® and Simulink®, the tracking algorithms for this missile can be developed in Simulink® and auto-coded with the Simulink Coder™ to run as real-time threads inside the missile processor. This allows users to very easily and quickly change and update the system's tracking algorithms to optimize its performance. Copies of this system are in use at several DoD and international facilities.

The foundational real-time threading functionality from RSIMS could easily be used for many other real-time applications like industrial process control, or time-critical flight systems for aircraft and unmanned aerial vehicles (UAVs).

## SUMMARY

Developing a common simulation architecture among different labs can be very challenging, especially when each lab has invested heavily in their existing architectures. One of the things that made RSIMS attractive to several of our partners was that it offered features that they didn't currently have in any of their home-grown systems (FLITES scenes, etc.). This, plus the benefits of collaborative development and the ability to easily share models between labs has contributed to the success of our RSIMS community. There are currently 5-6 DoD or DoD contractor facilities actively building or using RSIMS simulators, as well as 2-3 international partners.

RSIMS is a very flexible and capable DoD-owned architecture that is available for use. We hope that there will be many more applications of this technology. Interested parties may contact the authors for more information.

## ABOUT THE AUTHORS

**JOHN BENNETT** holds a B.A. in Mathematics and Computer Science from DePauw University (1986, minoring in Physics), and a M.A. in Mathematics from Indiana University (1988). John began his career at NSWC Crane developing RF expendable countermeasure models. He then transitioned to IR expendable countermeasure modeling and simulation. He developed the Flare Aerodynamic Modeling Environment (FLAME), a fully physics-based expendable countermeasure fly out model, which continues to be used across the DoD. He also developed a tool for archiving and processing IR expendable radiant intensity data that is also currently used in many locations across the DoD. More recently, John worked to develop RSIMS, which is the subject of this paper. He has worked at NSWC Crane for 30 years. John is currently the Software Design Subject Matter Expert for the IR/RF Systems Technologies Division.

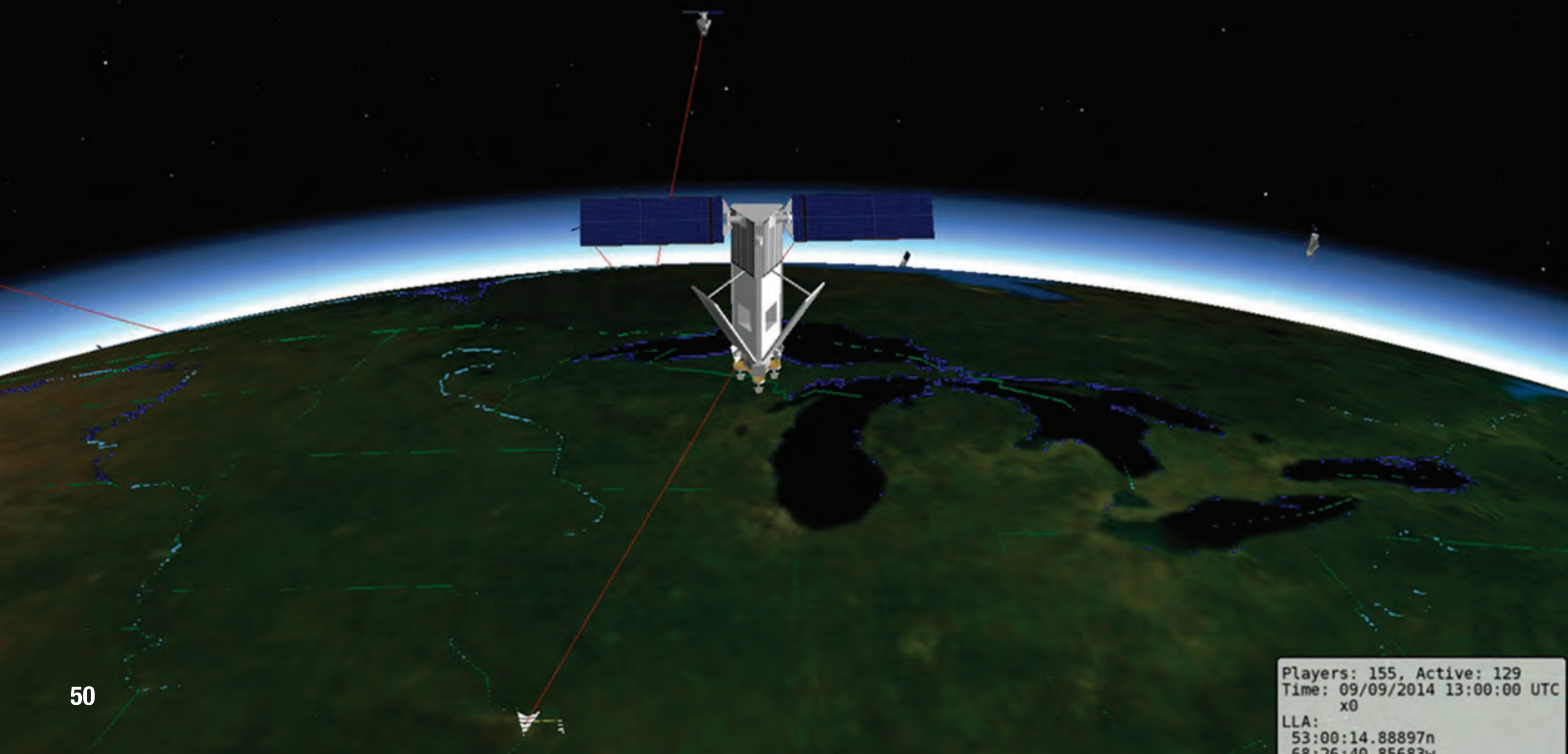
**BRENT WAGGONER** holds a B.S. in Aeronautical and Astronautical Engineering from Purdue University (1987), and a M.S. in Electrical Engineering from Rose-Hulman Institute of Technology (2003). Brent began his career at NSWC Crane doing modeling and simulation (M&S) for several different missile systems. He then transitioned to M&S for aircraft IR countermeasure development, where he has worked for the past 25 years. Brent is the lead engineer for the Navy Infrared Countermeasures Effectiveness Laboratory (NICEL). He has worked at NSWC Crane for 34 years. Brent is currently the Chief Engineer for Modeling and Simulation for the IR/RF Systems Technologies Division.

# AFSIM:

## THE AIR FORCE RESEARCH LABORATORY'S APPROACH TO MAKING M&S UBIQUITOUS IN THE WEAPON SYSTEM CONCEPT DEVELOPMENT PROCESS

By: Colonel Timothy D. West and Mr. Brian Birkmire

*THIS ARTICLE DESCRIBES THE WORK UNDERTAKEN BY THE AIR FORCE RESEARCH LABORATORY (AFRL) TO MAKE ITS ADVANCED FRAMEWORK FOR SIMULATION, INTEGRATION AND MODELING (AFSIM) – AN ADVANCED OBJECT-ORIENTED MODELING AND SIMULATION (M&S) FRAMEWORK FOR PERFORMING ENGINEERING, ENGAGEMENT, AND MISSION LEVEL MILITARY SIMULATIONS INCLUDING ANALYTIC WARGAMES – AS UBIQUITOUS AS MATLAB BY MAKING IT USEFUL, AVAILABLE, AFFORDABLE, AND USER FRIENDLY.*



```
Players: 155, Active: 129
Time: 09/09/2014 13:00:00 UTC
        x0
LLA:
 53:00:14.88897n
 68:26:40.85683w
```

The idea behind AFSIM is a common modeling framework, using common models in a common environment with a common threat laydown. To encourage buy-in across government and industry, AFRL not only built a robust product but also made the software, source code, and training available to approved users free of charge. To date, AFRL has licensed AFSIM to over 275 government, industry, and academic organizations, and provided training to over 1200 users. AFRL's overall approach to software development, distribution, support, and governance could serve as a model for encouraging widespread adoption of future freeware software products.

## INTRODUCTION

Arguably, one indication that a bourgeoning technical concept or capability is on the precipice of widespread usage and acceptance is when it enters the United States (US) Congressional record. For Digital Twin, the notion of building realistic digital models of real-world systems, that moment has arrived. The House Armed Services Committee's Subcommittee on Tactical Air and Land Forces recently drafted language for the Fiscal Year 2020 National Defense Authorization Bill directing the US Secretary of Defense to provide a briefing to the Committee explaining "how the F-35 program is implementing the use of digital twinning technology across the F-35 system enterprise" [1].

In order to mainstream the effective "digital twinning" of F-35 and other weapon systems, the US Department of Defense (DoD) must have a modeling framework that is effective, available, affordable, and relatively easy to use. DoD must also have a culture that is accepting of the results produced by these digital models. The Air Force Research Laboratory (AFRL) is making clear headway on both fronts with its Advanced Framework for Simulation, Integration and Modeling (AFSIM), a C++ based modular object-oriented, multi-domain, multi-resolution modeling and simulation (M&S) framework for military simulations focused on analysis, experimentation and wargaming. The AFSIM community already encompasses over 1200 trained users across 275 organizations, including all branches of the US military; other US Government agencies; industry; academia; and our five closest allies. This broad-based community is already widely using AFSIM to assess and compare various weapon system concepts, refine operational employment tactics for the most promising concepts, and ultimately to inform the weapon system investment decisions within AFRL and across the DoD. This paper describes the steps AFRL is taking and the progress achieved in making AFSIM as ubiquitous in the defense M&S community as MATLAB is in the academic community.

## AFSIM 101

In its present form, AFSIM represents a government/industry investment in excess of $50M. Between 2003 and 2013, Boeing invested approximately $35M of Independent Research & Development (IR&D) funding into what it called the Analytic Framework for Network-Enabled Systems (AFNES) that Boeing designed to simulate threat integrated air defense systems (IADS). Frustrated with the proprietary, inflexible M&S tools available to the Government at the time, AFRL conducted a head-to-head showdown of available tools in 2011, selecting AFNES as the framework of choice for its trade-space analysis and technology maturation M&S work. In 2013, Boeing transferred AFNES to AFRL with unlimited rights, which AFRL subsequently rebranded as AFSIM. [2]

Note that the "AF" in the AFSIM name does not stand for Air Force. This reflects AFRL's belief that AFSIM should not be just an internal Air Force tool, but rather a common framework used broadly across the entire defense M&S community. This naming choice also signifies that AFSIM is more than just a framework for simulating aircraft. It was designed to be a multi-domain platform, meaning it can model land-, sea-, air-, and space-based platforms, enabling modelers to include submarines, naval vessels, tanks, airplanes, helicopters, satellites, and even cyber agents in the same simulation, if needed.

From its earliest conception, AFSIM was also envisioned to be an open system, utilizing "plug and play" modules to overcome expansion and compatibility constraints of earlier frameworks. This modular approach allows the modeler, rather than the AFSIM programmer, to determine the appropriate level of fidelity (i.e., the degree to which the underlying physics are simulated) for the models used in the simulation. Likewise, users can adjust the fidelity of each platform to meet their specific simulation needs. The fidelity of an airplane model, for instance, could vary between a point in space moving along a predefined vector to a full six degree of freedom model that changes speed, direction, altitude, etc. based on the displacement of the virtual cockpit controls. The modular approach also enables the reuse and/or modification of existing models of various platforms without changing the core AFSIM code.

AFSIM's modular structure enables AFRL to distribute the code at two security classification levels, which users can adapt to meet their specific security requirements by adding additional software modules. AFRL offers both an unclassified and classified (US Secret) variant of the code. The primary difference between the two available variants is simply the number, type, and fidelity of included models. To receive the classified variant of the software, contractors must also provide a current, certified DD Form 254 Contract Security Classification Specification. The classified version also comes standard with National Air and Space Intelligence Center (NASIC) approved models of many threat systems, and a National Geospatial-Intelligence Agency (NGA) Digital Terrain Elevation Data (DTED) model. End users may then add their own modules to incorporate models of other platforms of interest for their specialized use. The overall classification of a given instantiation of AFSIM is then driven not only by the initial variant of the software, but also by the classification of modules added to that instantiation. Because of their inherent military utility, both variants are subject to International Traffic in Arms Regulations (ITAR) restrictions, meaning individuals and organizations can be fined or prosecuted for unauthorized release or export of the software. Because of these restrictions, academic institutions must have an approved ITAR-compliant environment before AFRL can release AFSIM to them. Despite this restriction, the pool of academic users is growing. Georgia Tech, Purdue, Ohio State, University of Central Florida, University of Alabama in Huntsville, and the University of Illinois – Champaign Urbana are already part of the AFSIM family.

*"AFSIM spans a broad spectrum of military simulations, to include the engineering, engagement, mission, and 'campaign-lite campaign-lite' level via analytic wargaming and experimentation."*

**Table 1:** *Levels of Wargaming Simulations*

| Simulation Level | Complexity Scale | Time Scale |
|---|---|---|
| Campaign | Many v. Many | Days |
| Mission | Several v. Several | Hours |
| Engagement | One v. One | Minutes |
| Engineering | Subsystem Interaction | Seconds |

AFSIM spans a broad spectrum of military simulations, to include the engineering, engagement, mission, and 'campaign-lite' level via analytic wargaming and experimentation. As Table 1 depicts, the **Engineering level** consists of short-duration subsystem interaction with other subsystems. One example of this could be a radio frequency (RF) transmitter interacting with a receiver to identify subsystem level capabilities and limitations. The **Engagement level** consists of "mano a mano" combat, that is, a brief exchange between two entities, or *platforms*, in the AFSIM vernacular. For instance, a missile exchange between a *Blue* (Friend) and *Red* (Foe) aircraft would constitute an engagement level simulation. The next level of complexity would be the **Mission level**, simulating, for example, a series of combat exchanges between multiple *Red* and *Blue* aircraft over the duration of a single sortie or mission, nominally a few hours. These simulations can contain up to thousands of entities. **Campaign level** engagements extend this even further, potentially including all the *Red* and *Blue* platforms in a given area over an extended period, i.e., days or even months. The focus for AFSIM development has been primarily at the engagement and mission level, with recent development expanding AFSIM's to include "campaign-lite" capabilities via analytic wargaming. Other M&S tools are leveraged when needing to more fully explore engineering or full campaign modeling, such as the Synthetic Theater Operations Research Model (STORM) used by the Air Force Studies, Analyses and Assessments Office (AF/A9). AFSIM enables its user to scale the scenario to the appropriate simulation level to best study the item(s) of interest. Each subsequent level logically builds on the lower levels to create a more intricate simulation in order to identify system-of-systems emergent properties that may not be apparent in simpler simulations. For instance, the combat effects of depleting munitions and fuel reserves may be unnoticeable at the Engagement or Mission level, but a total game-changer in the Campaign level simulation. The limiting factor in the size and complexity of an AFSIM simulation is the storage, memory, and computing power of the host platform – and the associated wall clock time required to run the simulation. AFSIM allows users to set the desired balance between processing time and output fidelity by adjusting the various parameters and behaviors associated with platform.

To achieve the degree of flexibility in platform type, fidelity, simulation type described above, AFSIM uses four architectural elements (Attributes, Elements, Components, and Links) to describe each platform in the simulation, as Figure 1 depicts. **Attributes** include standard data as platform name, type, and affiliation. This sub-element can be expanded to include mission-unique information such as radar, optical, and infrared signature data to determine an aircraft's vulnerability to detection by enemy sensors. The **Information** element encompasses data resident on the platform, along with details on how these data are perceived by the humans that receive them. For an aircraft, this would include the sort of data that would be displayed to the pilot (i.e., altitude, speed, heading, radar indications, etc.), along with the myriad raw data driving these displays. The **Components** element consists of various models that directly

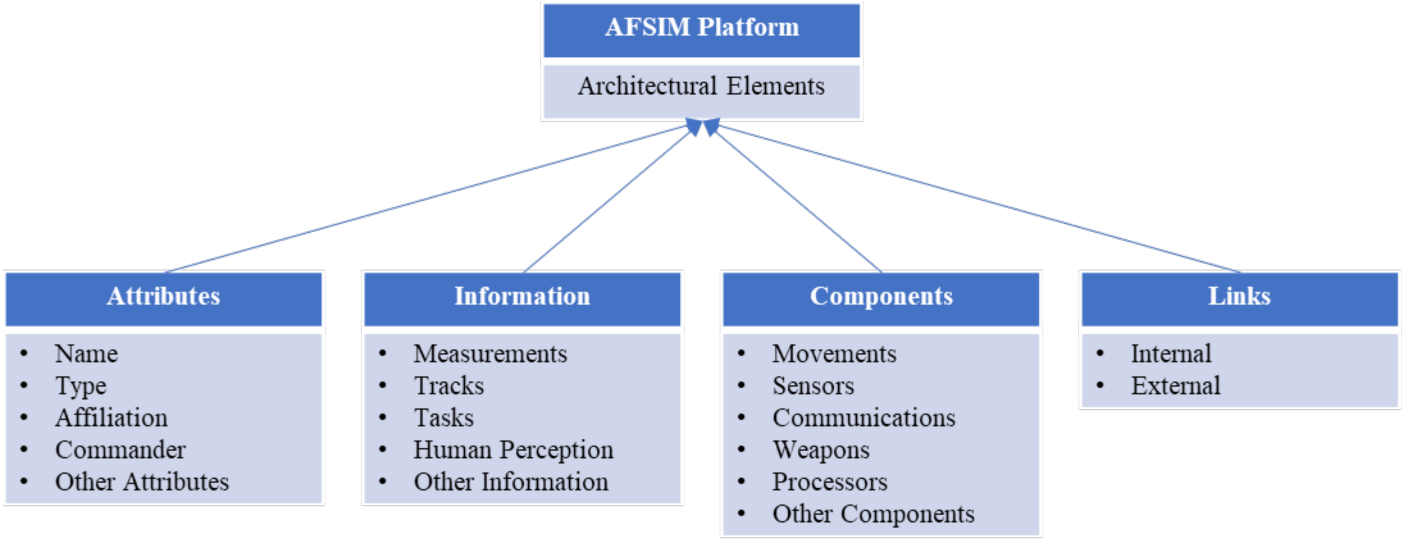


**Figure 1:** *AFSIM Architectural Elements*

control how the platform behaves. These models describe how the platform moves through space-time, senses the surrounding environment, processes the information it collects, communicates with other platforms, and employs its arsenal of kinetic and non-kinetic weapons against adversary platforms, and conducts various other tasks. Finally, the **Links** element coordinates the data exchanges between various subsystems on the platform, as well as communications with other platforms.

Another notable AFSIM is its support of both virtual and constructive simulations. In a constructive simulation, simulated operators control simulated systems – such as a military battle where the red and blue players are all computer controlled. In a virtual simulation, you have real operators controlling simulated systems – such as a pilot flying a flight simulator. AFSIM can be used constructively to conduct large trade space exploration of military capabilities, potentially involving tens of thousands of unique test points executing in a non-real-time manner. The results of such constructive sim activities can then be utilized to define and conduct a virtual simulation that runs in real-time to investigate a narrower trade space (informed by the constructive simulation) for a more focused assessment with operational pilot participation. This allows the same underlying simulation models to be utilized in both the constructive simulation and the virtual simulation, providing more consistent modeling and analysis across both environments. In addition, AFSIM can also be linked into other simulations or other simulators/emulators to provide a true Live-Virtual-Constructive (LVC) simulation capability. Using Distributed Interactive Simulation (DIS) or other supported communication protocols, AFSIM can interact with other simulations or live experiments in order to provide additional entities (both virtual and constructive), system and sub-system models, threat systems or potentially other simulated capabilities. This allows AFSIM to augment and/or complement a larger simulation or experimentation environment with additional capabilities, as needed to best achieve any given test and analysis objectives.

Leveraging its *Warlock* graphical user interface (GUI), AFSIM likewise allows "operator in the loop" execution to facilitate analytic wargaming. Specifically, *Warlock* enables operators to trigger various scenario events, control individual platforms, and even experience the mission from inside the platform – much like *Flight Simulator*. *Warlock* also facilitates the creation of "cells" of operators, e.g., a *Blue Cell* of friendly platform operators and a *Red Cell* of adversary platform operators, each of which only have access to virtual information collected by that cell's platform. In other words, the *Red Cell* and the *Blue Cell* each have imperfect information about the other. AFSIM can add further realism to the wargame by degrading the flow of information between members of the same cell. *Warlock* also supports the creation of a *White Cell* – the referees – that have perfect information about all platforms, which they leverage to control the flow of the overall wargame.

Before any type of AFSIM simulation can be executed, however, the user must define the various platform and component models and then craft the wargame scenario. To facilitate this process, AFRL distributes *Wizard*, AFSIM's Integrated Development Environment (IDE), as a supporting tool (like *Warlock)*. Much like a modern software development IDE, *Wizard* serves as a single application to edit scenario files; write AFSIM script; graphically manipulate scenario laydowns; run software executable (i.e. run the scenario in AFSIM); and view the resulting output or error messages. It also highlights file syntax, flags unknown commands, and provides context-sensitive documentation. *Wizard* even comes with an auto-completion feature and a script debugger to minimize the time required to develop and debug models and scenarios.

## THE ROAD TO UBIQUITY

Recognizing that widespread adoption is more probable leveraging incentives rather than mandates, AFRL has taken several steps to grow the AFSIM following. First, AFRL decided it would give away the product to both Government and industry partners. Intra-government sharing could easily be accomplished under Memoranda of Understanding (MoU). However, sharing software with industry partners initially proved tricky, as existing contract mechanisms only allowed the sharing of government property and information with industry partners as part of a larger contract. The F-22 aircraft program could loan Lockheed-Martin the software as part of the larger F-22 contract, but the ruleset associated with government furnished property meant the software could only be used for M&S work within the scope of the F-22 contract, and the software must be returned to the government at the conclusion of that contract. To overcome this obstacle, AFRL created a new type of contractual agreement, an Information Transfer Agreement (ITA), that gives industry partners full access to the software, without constraining its use to a single program [3], [4].

*"AFRL created a new type of contractual agreement, an Information Transfer Agreement (ITA), that gives industry partners full access to the software, without constraining its use to a single program."*

AFRL also chose to provide free training at its Dayton, Ohio, headquarters. AFRL currently offers two courses: one for general users and one for code developers. The user course is offered monthly while the developer course is offered every other month. The only costs to attendees are travel-related expenses. This combination of free software and free training makes AFSIM very attractive to organizations who might otherwise be forced to use costly commercial off the shelf (COTS) products, along with the recurring expenses associated with license renewals, specialized training, and product support.

To further sweeten the deal, AFRL also opted to provide users and developers with the source code for both the framework and all supporting tools. This decision was borne from the Lab's own frustration with other "black box" software tools that provided limited insight into how the tool transformed inputs into outputs. AFRL recognized that providing source code would enable savvy users to see for themselves the logic, algorithms, equations, and associated assumptions behind every AFSIM result. AFRL also realized that source code access could leverage the user community as code debuggers, knowing that inquisitive users would likely dig into the source code to understand anomalous results, unearthing logic errors and faulty assumptions that could be corrected in future software updates.

Deliberate community engagement has also been a core element of AFRL's strategy for AFSIM. In addition to actively soliciting feedback on the user experience and leveraging them to find and repair minor coding issues, AFRL has incorporated the user community into its governance model, establishing eight domain-centric working groups (Sensors, Space, Threats & Scenarios, Kinetic Weapons, Directed Energy, Standardization, Virtual Simulation and Wargaming, Cyber/C3) to help establish the vision for capability development within each group's respective domain. Each working group is a self-organized entity whose leadership structure is driven more by consensus of the subject matter experts in that group rather than AFRL dictate. Nearly half the groups are led by non-AFRL personnel, some by other military services. A central program management team integrates and prioritizes the inputs from each group in order to develop an annual execution plan within the available funding limits.

As the AFSIM community has grown, so, too, has the need to scale the AFSIM software development and maintenance effort. The AFSIM software team now consists of over 40 full-time developers and analysts to maintain both the Windows and Linux variants. Software increments for both variants are released on a six-month cycle, with user support and bug fixes provided for both the latest version and one prior version. This approach enables a steady flow of cutting-edge capabilities, while providing longer-term stability for users who do not require the latest release. Each release of AFSIM has a one year support window. As of this writing, AFSIM 2.3 is the "stable" version, AFSIM 2.4 is the latest version, and 2.5 is in development. The AFSIM development team works closely with network approval authorities to ensure authority to operate on multiple government systems across a range of security classifications. To facilitate these network approvals, the development team utilizes a continuous integration and build process which incorporates automatic builds, static code analysis, regression testing, and rigorous vulnerability scanning.

One of AFSIM's primary use cases is as a simulation platform for technology maturation. Over the past few years AFRL has made a significant investment in using AFSIM as a testbed for maturing air vehicle autonomy. Utilizing AFSIM as a simulation testbed for autonomy has created a single, unified environment for developing, maturing, and testing autonomy algorithms for basic and applied research, as well as advanced applications. Using AFSIM as a virtual testbed for accelerating air vehicle autonomy development has proven so effective that several government agencies and industry partners have also adopted it for similar efforts, to include the Defense Advanced Research Projects Agency (DARPA), Johns Hopkins University Applied Physics Laboratory (JHU APL), Georgia Tech Research Institute (GTRI), and Leidos. AFRL is also teaming with the Air Force Lifecycle Management Center (AFLCMC) and the Air Force Warfighting Integration Center (AFWIC) to make AFSIM the tool of choice for analyses of alternatives (AoAs) for future weapon system concepts. Additionally, AFWIC has incorporated AFSIM into its capability development guide. AFRL has also communicated to its industry partners that AFSIM will be a key tool it uses to evaluate their proposals. Lockheed-Martin's recent announcement that it is investing $5M into their AFSIM infrastructure is a clear indicator that industry is listening. Boeing, who developed the predecessor to AFSIM, has been a committed user for over a decade.

## CONCLUSION

Representing a $50M investment to date and another $6M per year for the foreseeable future, AFSIM is not an inexpensive framework. However, AFRL believes the DoD will ultimately recoup this investment by reducing schedule delays and the associated cost overruns through earlier identification and correction of murky requirements, invalid assumptions, and flawed design decisions. Despite its shortcomings, AFSIM is already enhancing the DoD's "model centric" approach to acquisition. AFRL's conscientious efforts to make AFSIM useful, available, affordable, and user friendly have undoubtedly helped in this regard. AFRL believes that AFSIM will be key to helping the Secretary of the Air Force attain her vision of building an innovative Air Force that "dominates time, space, and complexity in future conflict across all operating domains to project power and defend the homeland" [5]. Will AFSIM ultimately help the Air Force achieve this lofty goal? Only time will tell.

## ACRONYMS

| | |
|---|---|
| AF/A9 | Air Force Studies, Analyses and Assessments Office |
| AFLCMC | Air Force Lifecycle Management Center |
| AFNES | Analytic Framework for Network-Enabled Systems |
| AFRL | Air Force Research Laboratory |
| AFSIM | Advanced Framework for Simulation, Integration and Modeling |
| AFWIC | Air Force Warfighting Integration Center |
| AoA | Analysis of Alternative |
| COTS | Commercial Off The Shelf |
| DARPA | Defense Advanced Research Projects Agency |
| DoD | Department of Defense |
| DIS | Distributed Interactive Simulation |
| DTED | Digital Terrain Elevation Data |
| GTRI | Georgia Tech Research Institute |
| GUI | Graphical User Interface |
| IADS | Integrated Air Defense Systems |
| IDE | Integrated Development Environment |
| IR&D | Independent Research & Development |
| ITA | Information Transfer Agreement |
| ITAR | International Traffic in Arms Regulations |
| JHU APL | Johns Hopkins University Applied Physics Laboratory |
| LVC | Live-Virtual-Constructive |
| M&S | Modeling and Simulation |
| MoU | Memoranda of Understanding |
| NASIC | National Air and Space Intelligence Center |
| NGA | National Geospatial-Intelligence Agency |
| RF | Radio Frequency |
| STORM | Synthetic Theater Operations Research Model |
| US | United States |

## REFERENCES

**[1]** U.S. House of Representatives, "H.R. 2500 - FY20 National Devense Authorization Bill - Subcomittee on Tactical Air and Land Forces," Washington DC, Jun. 2019.

**[2]** P. D. Clive ***et al.***, "Advanced Framework for Simulation, Integration and Modeling (AFSIM)," p. 5, 2015.

**[3]** L. Daigle, "AFRL uses new Information Transfer Agreement to share software with industry," ***Military Embedded Systems***, 2017. [Online]. Available: http://mil-embedded.com/news/afrl-uses-new-information-transfer-agreement-to-share-software-with-industry/. [Accessed: 07-Jul-2019].

**[4]** J. Knapp, "Information Transfer Agreement enables AFRL software sharing with industry," ***Wright-Patterson AFB***, 10-Mar-2017. [Online]. Available: http://www.wpafb.af.mil/News/Article-Display/Article/1109831/information-transfer-agreement-enables-afrl-software-sharing-with-industry. [Accessed: 07-Jul-2019].

**[5]** US Air Force, "U.S. Air Force Science and Technology Strategy." 17-Apr-2019.

## ABOUT THE AUTHORS

**COLONEL TIMOTHY D. WEST** is a senior US Air Force acquisition officer with command experience in Program Management, Research & Development, and Test & Evaluation. He currently serves as Senior Materiel Leader, Aerospace Systems Directorate, Air Force Research Laboratory, Ohio, where he leads the Air Force's science and technology program in aerodynamics, propulsion, electrical power and thermal management for advanced next-generation space, missile and aircraft applications. Colonel West is a graduate of the US Air Force Test Pilot School and the Air War College. He has a Bachelor of Science degree in Mechanical Engineering, Master of Science degrees in Aerospace and Industrial Engineering, and is currently pursuing a Doctorate in Systems Engineering at Stevens Institute of Technology.

**MR. BRIAN BIRKMIRE** is a computer engineer with the Power and Control Division, Aerospace Systems Directorate, Air Force Research Laboratory, Ohio. Mr. Birkmire is the AFSIM Deputy Program Manager responsible for AFSIM community / end-user management, distribution management, and assisting with technical oversight, requirements development, project planning, and roadmapping. Mr. Birkmire also serves as a software developer in the areas of modeling & simulation as well as autonomy algorithm and architecture development. He has Bachelor of Science and Master of Science degrees in Computer Engineering from Wright State University.

**Cyber Security and Information Systems**
**Information Analysis Center**
266 Genesee Street
Utica, NY 13502

# THE CENTER OF EXCELLENCE IN CYBER SECURITY AND INFORMATION SYSTEMS

*Leveraging the best practices and expertise from government, industry, and academia in order to solve your scientific and technical problems*

**https://www.csiac.org/journal/**

Design and Development Process for Assured Software - Volume 1

Journal of Cyber Security & Information Systems

Upcoming Events

Share and Invite

Read the Latest Journal

*To unsubscribe from CSIAC Journal Mailings please email us at* ***info@csiac.org***
*and request that your address be removed from our distribution mailing database.*