Wednesday, December 6

TRACK 1 TRMC T&E/S&T Cyberspace Test Technology Overview

Title of Presentation: TRMC T&E/S&T Cyberspace Test Technology Overview
Presenter: Pete Fiery, MITRE
Authors: Dr. Mike Shields, Chief Scientist, TRMC T&E/S&T CTT and Min Kim, Deputy EA, TRMC T&E/S&T CTT

TRMC T&E/S&T CTT (Cyberspace Test Technology). It will go over the domains and mission of the CTT. In addition, the presentation will touch on the highlights of the on-going cyber T&E projects.

Title of Presentation: Vader Modular Fuzzer (VMF) – USG Fuzzing Capability
Presenter & Author: Arch Owen, Program Manager for Weapon Security, Draper Laboratory

TRMC T&E/S&T CTT (Cyberspace Test Technology) has initiated an effort to expand USG (United States Government)-wide awareness and experience in fuzzing, and to provide tools suited to DoD needs - specifically tools that are affordable, usable in closed spaces, suited to unique testing needs (e.g. real time embedded systems), easily adapted, incorporate the latest fuzzing techniques, and can be quickly learned by non-fuzzing experts. In order to support this initiative, the CTT is developing Vader Modular Fuzzer (VMF), a suite of fuzzers and modules that allow users to tailor fuzzers to specific needs. In addition, USG Fuzzing Working Group is stood up to promote adoption of VMF and share knowledge on fuzzing. This presentation is to update the T&E community on the VMF development status, the features included in current phase (Phase 3 of 4-year project) and how to get started with VMF.

Title of Presentation: Measure and Share: TRMC T&E/S&T Cyberspace Test Technology's project to improve Cyber T&E impacts across DoD
Presenter: Bharath Selvarai, DeciSym,. LLC
Author: Dr. Donald Pellegrino, CEO, DeciSym, LLC

The Measure and Share Initiative is to Measure the Efficacy of Cyber Test and Evaluation, and Share the results at an appropriate classification level by providing a relevant perspective to the DoD stakeholders.

The Goals of this initiative are:

- Improve T&E Results
- Improve JTF and Service Commanders Cyber Knowledge
- Enable Better Acquisition Outcomes
- Improve Intelligence Community Reporting Impacts

The initial focus has been a development of a distributed, secured data storage system designed to enable organizations to store the data (for example, system models, test plans, test results, etc.) at appropriate classification levels.

This presentation will describe the Measure and Share Initiative in depth including the Concepts of Operations, current status and a way forward.

Title of Presentation: Automated Attack Framework for Test & Evaluation (AAFT)
Presenter: Owen Camp, Research and Development, The Applied Research Laboratory, The Pennsylvania State University (ARL PSU)
Authors: Andrew Shaffer, Research and Development Engineer and Bruce Einfalt, Senior Research Engineer, ARL PSU

Red Team cybersecurity testing is critically important to ensure that new systems will perform as expected without compromising mission success. Unfortunately, no individual Red Team can keep up with the torrent of new threats that are being discovered every day. Also, a lack of cybersecurity Red Team availability often delays system accreditation and forces procurement programs to move forward with less mission assurance than is desired.

The Automated Attack Framework for Test & Evaluation (AAFT) enables Red Teams to keep pace with the threat by providing a framework for Red Teams to collaboratively capture and share information about threat cyberattacks in a format that is intelligible to an autonomous cybersecurity testing system. It also improves Red Team utilization and efficiency by automating the execution of threat cyberattacks and emulating basic and intermediate-level cyber threats so that Red Teams can focus on emulating more sophisticated threats, increasing the overall scope of cybersecurity testing that can be performed.

AAFT creates a simple layer of abstraction for diverse cyberattack tools, enabling autonomous algorithmic selection and execution of multi-tool attack sequences leading to user-specified attack objectives within specified timing and risk parameters. These autonomy algorithms can emulate the Tactics, Techniques and Procedures employed by known threats and optimize attack selections to achieve specified objectives by combining currently known target system information with information about all permissible attack options. The optimal attack strategy is dynamically recomputed after each stage of an attack has been executed, making AAFT highly adaptive to diverse testing environments. AAFT's autonomy algorithms automatically incorporate the new capabilities of any properly specified cyberattack tool to generate new potential attack paths, allowing the system to easily integrate with new custom and open source attack tools as soon as they are developed. The autonomous attack engine also automatically maintains a complete forensic attack log for all of the attacks that it executes during each test event to facilitate post-test analysis.

AAFT's autonomy algorithms and architecture advance test and evaluation by autonomously managing basic and intermediate-level cybersecurity Red Team testing from start to finish. These capabilities support continuous comprehensive penetration testing, enabling significant reductions in system reauthorization costs. They also provide a capable "adversary on demand" to support Blue Team training. The entire AAFT system is designed for distribution as a virtual machine instance that can be easily deployed on standard computing hardware with little if any software configuration required before use, making it suitable for widespread deployment.

The AAFT project has officially been in development as a Test Resource Management Center project since May 2020 and considerable progress has been made in all major areas of system development. The basic AAFT framework has now been implemented and a wide range of different cyberattacks have already been integrated for use in AAFT-enabled automated testing. Development of the AAFT system is ongoing, and plans are in place to scale up the complexity and scale of the attacks that AAFT can autonomously execute.

TRACK 2 T&E in Support of Agile Development Process

Title of Presentation: DevSecOps Evaluation Framework Dashboard
Presenter: Mr. Patrick Quilter, President ALPI, Scientific Test and Analysis Techniques Center of Excellence (STAT COE)
Additional Author(s): Dr. Steve Oimoen and Mr. Andrew Pollner, STAT COE

The Scientific Test and Analysis Techniques Center of Excellence (STAT COE), sponsored by the Office of the Director, Operational Test and Evaluation (DOT&E), has developed a DevSecOps Evaluation Framework (DSO-EF) to assess the effectiveness of DevSecOps (DSO) implementation processes and ensure alignment with best practices. While DSO offers numerous advantages, it also introduces new complexities into software-development processes which further necessitate the effective test and evaluation (T&E) of systems developed using this DSO approach.

This paper describes the development of the DSO-EF and demonstrates how it can provide clarity and oversight to the DSO process. Initially, the STAT COE decomposed Department of Defense Chief Information Office (DOD CIO) guidance into activities (overarching processes) and tasks (specific items) and organized them in a spreadsheet. As the framework expanded, it evolved into a relational-data model, an application programming interface (API), and an interactive dashboard. The DSO-EF now serves as a versatile tool to support developmental test (DT), operational test (OT), reliability and maintainability (R&M), and security teams in understanding and tracking DSO lifecycle activities, as well as required T&E activities and tasks.

The DSO-EF dashboard enables data tagging and query-based task identification specific to DT, OT, automation, security, reliability, maintainability, and model-based systems engineering (MBSE). By providing visibility into the DSO process, the tool facilitates collaboration and horizontal integration among T&E organizations and various disciplines, harnessing the full potential of DSO.

Keywords: DevSecOps, test and evaluation, software development, DSO Evaluation Framework, agile development, adaptive systems, STAT COE

Title of Presentation: Leveraging Flexible and Interactive Model Based T&E Tools to Improve Efficiency and Effectiveness of Execution Phase Test Programs
Presenter and Author: Joe Murphy, Sr. Business Development Director T&E Solutions, Ansys Government Initiatives

This presentation will explore how a computer aided engineering (CAE) approach to detailed test design, real-time decision support, and post-flight analysis can serve to accelerate the adoption of Model-Based Test & Evaluation, and enhance and accelerate workforce readiness for overall adoption of DOD programs' digital transformation.

Utilizing a quickly composable modeling capability to adapt to program evolving level of characterized system designs provides a powerful way to transform current methods of detailed test design. Pre-test analysis using this approach allows test practitioners to design their test events in a CAD/CAE like fashion in a "try before you fly approach" resulting in significantly more productive test activity.

Taking these composed models into control rooms for use along-side current control-room tools provides a real-time decision support method that can greatly improve test-point success rate and provide a post-flight while you fly capability. The insights derived in real-time allows test conductors to "call audibles" to pilots and other test-resources to affect in-flight contingencies and save test events from failed test-points.

A "richer" post-flight quick-look which includes simulated playback along with modeled capabilities provides for faster insights for decision support. Utilization of post-flight reconstruct within these composed modeling environments allow for faster and more effective verification and reporting back to program stakeholders.

These flexible and quickly composable modeling environments have become increasing important as test events employ multi-domain resources and autonomy.

Additionally, these approaches enable a feedback loop to MBSE and digital prototypes & twin models' verification and evolution through a program lifecycle.

Title of Presentation: A Collaborative Approach to Verify and Validate a Complex Air Traffic Control System

Author and Presenter: Amnon Pollak, Test Director, Federal Aviation Administration Automation and Agency Support Branch, ANG-E582
Additional Author(s): Matthew Thornton, Test Director, Leidos Corporation

This paper presents an innovative approach used by the Federal Aviation Administration (FAA) and the system developer, Leidos Corporation, to collaboratively complete the test and evaluation (T&E) of a complex air traffic control system, Terminal Flight Data Manager (TFDM), leading to its deployment at the Cleveland air traffic control tower (ATCT).

As demand on the National Airspace System (NAS) grows, smarter Next Generation Air Transportation (NextGen) System technologies are making air travel more efficient, safer, and environmentally friendly. The FAA is committed to updating terminal automation systems and implementing Air Traffic Control (ATC) capabilities that improve air traffic operations in the NAS. TFDM is such a system.

TFDM is a tower-based NextGen system that improves surface management and efficiency and enables real-time digital data exchange throughout gate-to-gate aircraft operations. TFDM supports new services that provide automation to current, manually-intensive operations and replaces critical, outdated systems in the NAS. The TFDM airport surface management concepts have been validated with operational users through concept engineering and prototype development activities. When fully implemented, TFDM will save approximately 313 million gallons of fuel and reduce over 3 million metric tons of carbon emissions during its lifetime, and also improve the experience of the flying public.

TFDM modernizes ATCT equipment by improving exchange of electronic flight data and enabling collaboration and decision-making capabilities between the gate and the tower. This requires the TFDM system to interface with essentially all FAA air traffic control systems and airport specific sensors in near real-time to exchange data. Testing such a complex system can be challenging. In particular it requires a test environment that includes actual systems in a dynamic environment that enables real-time

operational data exchange with end-user inputs.

This paper presents an innovative approach that enabled the FAA and the TFDM system developer, Leidos, to combine a Leidos simulation-based factory and the FAA's enterprise laboratory test capabilities to jointly conduct system tests for requirement verification, early discovery of unexpected interface compatibility issues, and opportunity for more realistic operational behavior for evaluation by end users.

It describes how this joint test initiative, with clearly delineated responsibilities between Leidos and the FAA, was able to take advantage of the developer's laboratory environment for early testing while applying the Government's more operationally focused laboratory environment for risk reduction and end state testing. This FAA-Leidos collaborative test method also enabled the test team to establish an iterative test approach, within an agile software development framework, by leveraging early look engineering software builds for timely feedback and performing risk reduction tests for continuing software improvements.

The FAA and Leidos were also able to overcome challenges of the COVID-19 pandemic by implementing Leidos' clientless remote desktop gateway tools in the FAA's laboratory environment, thus enabling remote virtual tests. This permitted continued, uninterrupted TFDM test activities even during the height of the pandemic.

As a result, the TFDM system tests were successfully completed to achieve initial operational capability (IOC), with the first operational TFDM system fielded at the Cleveland ATCT on October 24, 2022.

Presentation: Model Based Test Engineering: Incorporating Test Engineering into the Digital Engineering Transformation
Author and Presenter: Johnston A. Coil, LinQuest Corporation

As more programs adopt digital engineering transformation, test engineers must take advantage of the opportunities this change presents. Utilizing Model Based Systems Engineering (MBSE) principles and applying them to test engineering enables the test program to access authoritative structural, behavioral, and requirements data on the system under test and take advantage of the MBSE principles of simplifying complexity, relationships between model elements, and model element re-use. This paper presents a Model Based Test Engineering (MBTE) metamodel that federates with system under test models; provides improved linkages between requirements, test procedures, safety, and test resources; improves test program insights through automated reporting; and is applicable for testing of physical systems, hardware in the loop, digital twins, or hybrid testing. Application and lessons learned are provided from case studies of reverse-engineering document based test plans and from the execution of a MBTE pilot program at the 780th Test Squadron, Eglin AFB, FL.
The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. government.

TRACK 3 Artificial Intelligence and Machine Learning

Replacement – here

Title of Presentation: Transportable Modelling and Simulation System for Test & Evaluation
Presenter and Author: Jarrod Cornforth, Dstl
Additional Author: Bex White, Ms, Dstl

The UK Ministry of Defence (MOD) is currently undertaking a Test and Evaluation (T&E) Transformation programme, a modernisation programme focusing on moving UK Defence beyond evaluation-for-acceptance, to evaluation-for-advantage. This will be achieved through drawing upon modern technology advances such as modelling and simulation, data analysis and digital engineering.

The Defence Science and Technology Laboratory (Dstl) is developing a standardised approach for performing synthetic T&E using test benches. This will include designs for a standard test bench approach based upon previous research performed within Dstl. The outcome from the investigations and demonstrations will shape how T&E will be performed using a more digitised approach (including Digital Twins) that will enable more rapid evaluation based on endorsed threat information. These test benches will permit easy sharing, through common approaches and federation, to encourage collaboration with industrial and international partners to enable the evaluation at sub-system, system and system of system levels at appropriate classifications. This should include up to 2-way communication between different classified components of the synthetic environment and the inclusion of hardware-in-the-loop.

Title of Presentation: Model-Derived Evidence for PBX Mechanical Properties in Support of Qualification
Presenter: Andrew Cunningham. QinetiQ
Authors: Andy Rix, Senior Scientist, QinetiQ , Peter Gould, Principal Scientist, QinetiQ

Mechanical properties of energetic materials are a critical underpinning factor in the safety of weapons systems, and a knowledge of their response is vital to ensure Safety and Suitability for Service. Significant benefit may be achieved via the application of Modern Digital Engineering combined with predictive Modelling and Simulation. This work covers model-derived evidence, achieved via the implementation of an eXplainable Artificial Intelligence (XAI) model, which uses an existing mathematical model for the prediction of composite energetic material mechanical properties, as well as verification and validation of that model. Testing is currently the method whereby mechanical property information is fed into Qualification of energetic materials that, thereafter, informs Type Qualification of the weapon systems using that energetic material. Such testing carries significant burdens of time, resource and safety.

In the event of material obsolescence, weapon system requirement change, etc. the predictive model will allow energetic material certification more rapidly and with reduced risk. Work in the programme has examined Regulatory approaches to model-derived evidence and understood the reasons why models based on mathematical algorithms and modern digital techniques can be as acceptable as currently trusted empirical model evidence. Furthermore, the work has recommended methods whereby empirical evidence can be better acquired. The work has incorporated advances in data management and aims to demonstrate how verification and validation, including uncertainty quantification, can be applied to build trust in predictions. Evidence has been gathered regarding facilitation of an enterprise approach with sharing of information across industry, regulators and independent advisors.

This work is in funded-by and supports UK MOD's Research and Development Test and Evaluation (RDT&E) T&E transformation programme, this is a modernisation programme focused on moving UK Defence beyond evaluation for acceptance, to evaluation for advantage.

Title of Presentation: Predictive Resilience Modeling
Presenter and Author: Lance Fiondella, Associate Professor, University of Massachusetts Dartmouth
Author: Priscila Silva, PhD Student, University of Massachusetts Dartmouth

Resilience is the ability of a system to respond, absorb, adapt, and recover from a disruptive event. Dozens of metrics to quantify resilience have been proposed in the literature. However, fewer studies have proposed models to predict these metrics or the time at which a system will be restored to its nominal performance level after experiencing degradation. This talk presents alternative approaches to model and predict performance and resilience metrics with elementary techniques from reliability engineering and statistics. We will also present a free and open source tool developed to apply the models without requiring detailed understanding of the underlying mathematics, enabling users to focus on resilience assessments in their day to day work.

Track 4 Data Analytics / Modeling and Simulation

Title of Presentation: A T&E strategy to validate the physics-based modelling of an uncrewed aerial system (UAS) applied to a mission engineering thread
Presenter and Author: Mr Tim Grabert, Nova Systems, Australia
Additional Authors: Mr Peter Nikoloff, Mr Jeet Shah, and Mrs Jamie Smith, Nova Systems Australia

A T&E strategy to validate the physics-based modelling of an uncrewed aerial system (UAS) applied to a mission engineering thread. This paper describes the test and evaluation strategy used to collect the necessary data to validate physics-based models used in the mission engineering analysis of a UAS test range surveillance system.

The ability of the Mission Engineering Approach to provide the warfighter with decision-quality information is dependent upon access to models with a requisite level of fidelity. Consequently, the capability to verify and validate models of Mission Elements (systems) is a fundamental enabler of the Mission Engineering Approach as described in the US DoD Mission Engineering Guide (2020).

A series of designed experiments were conducted in a synthetic physics-based modelling and simulation environment that aimed to characterize, and subsequently optimize the FIND, FIX and TRACK mission tasks assigned to a small UAS equipped with an electro-optic sensor for a defined land-based operational scenario.

Response surface methods were used in the synthetic environment to generate figure-of-merit metrics relating to sensor performance and target object coverage. The physics-based model of the system under test included parameters for sensor platform dynamics, sensor resolution, weather effects, geospatial data and other mission architecture elements.

The response surface figure-of-merit values predicted in the simulation runs were then compared with test and evaluation data collected from the real mission system to provide an estimate of model confidence, and to facilitate the tuning of the physics-based models to better reflect demonstrated system performance.

This validation strategy included designing the necessary interfaces to enable real mission data collected from the system under test (mission element) to be replayed in the same modelling and simulation environment used to run the simulations.

The benefits of using a common synthetic environment to perform both modeling and simulation and post-mission data analysis will be explored, as well as a review of the efficacy of the overall validation strategy.

Title of Presentation: An Approach for the Evaluation of Open Systems Architecture Compliant Systems
Presenter and Author: Dr. Joshua Walker, Senior Research Engineer, Georgia Tech Research Institute (GTRI)
Additional Authors: Brian Schreiber, Research Engineer II, GTRI, Justin Vuong, Research Engineer I, GTRI

The Georgia Tech Research Institute (GTRI) performs a role as compliance evaluator for multiple Electronic Warfare (EW) Open Systems Architecture (OSA) programs. In this role, GTRI develops the testbed framework to support compliance evaluation activities for hardware and/or software and utilizes that test infrastructure to perform the evaluation for potentially compliant vendor systems. With experience in this role, GTRI determined the need for a test approach that adapts to the challenges associated with the evaluation of OSA-compliant systems. Evaluation of OSA-compliant systems is fundamentally different from a traditional testing approach for functional evaluation. OSA-compliant systems can vary highly between vendors, with potential differences in operating systems, interfaces, protocols, stimulation mechanisms, and containerization. Efficiency of test design is a primary objective, necessitating an agile test approach that stresses reusability of test artifacts, processes, and methodologies across vendors. Additionally, OSA requirements can be written at a higher level than traditional functional requirements to facilitate flexibility of design among compliant systems. While this is a necessary aspect to OSA requirements definition, it can lead to a higher level of variability of interpretation, resulting in further development and evaluation challenges.

This presentation will discuss the test approach for the compliance evaluation of multiple vendor

systems developed to be compliant with a software-centric OSA for Multi-Function Radar Frequency (MFRF) systems. This includes an overview of the project test objectives, challenges associated with the compliance evaluation of OSA-compliant systems, and solutions for these challenges devised during the execution of the project. Test objectives for the project centered around the need to develop and adapt a common set of automated test stimuli and procedures for multiple disparate systems. Achieving commonality minimizes the amount of unique test infrastructure developed for an individual system. While this approach introduced several challenges specific to the test environment, subsequent challenges emerged from the compliance evaluation process when interacting with vendors that were concurrently developing systems to be evaluated while in open competition with each other. These challenges had to be overcome through the development of additional test infrastructure and by cooperation among the OSA stakeholders for the overall success of the OSA.

Title of Presentation: Demonstration of Bayesian Analysis using Light Aircraft Performance Testing
Presenter and Author: Dr. Kyle Kolsti, Director, STAT COE

Bayesian statistics is attracting attention across the DOD as a potential tool for combining information from different sources. If applied appropriately, incorporating knowledge from previous testing or subject matter experts may offset some of the uncertainty caused by small sample sizes. These advantages are accompanied by additional considerations and assumptions compared to the more familiar frequentist methods. To convey both advantages and nuances of Bayesian statistics, this presentation demonstrates an application of Bayesian statistics in predicting the turn performance of a light aircraft. The data were collected at the U.S. Air Force Academy over three semesters as part of the Introduction to Flight Test course. The demonstration includes notional elicitation of knowledge from subject matter experts to design the prior distributions, use of a physics-based mathematical model, and comparison of predictions across multiple flights and sample sizes. The goal of the presentation is to increase awareness and understanding of Bayesian statistics with a practical example.

Title of Presentation: General Autonomous Platform T&E Test Bed Approach
Presenter and Author: Jarrod Cornforth, Dstl
Additional Author: Kamran Memon, Ansys

UK MOD capabilities are under development that use autonomous functions, including but not limited to robotics, with greater investment in artificial intelligence and machine learning. Such capabilities must be tested and evaluated to assure they are compliant with user needs, including performance, regulatory, legal and ethical requirements, before they can accepted into service.

Currently such Test and Evaluation (T&E) for a specific capability can be conducted in isolation from other capabilities. But this can raise the risk of duplication of effort, inconsistencies and variations of approach and limits opportunities to learn lessons and exchange knowledge within the defence community. The creation of a general ‘test bed’ capability approach for autonomy should achieve efficiencies through coherence and consistency.

In March 2022, the UK MOD autonomy T&E demonstrator displayed how synthetic environments can be used to augment and de-risk live T&E, alongside generating sufficient data to support regulatory assurance and approval. Perceived benefits from the demonstration include generating more data for T&E, whilst reducing the time, cost and dependency on environmental factors when undertaking live

tests. The opportunities in performing T&E earlier in the product development lifecycle and its impact on reducing risk were also displayed.

Alongside this, the task demonstrated how Modelling & Simulation using multi-layered and multi-fidelity synthetic environments, can be used in the development of software (including artificial intelligence) and highlighted the advantages of collaboration between small and medium enterprises to deliver benefit to UK MOD. A key output was the demonstration indicated that the technology had reached a sufficient maturity to justify research into development of a general autonomous platform T&E test bed approach.

Building upon this demonstrator, we have commissioned additional work to identify the capability requirement for a future autonomy test bed and perform a practical live demonstration of an example of such a general capability. The output of this project will enable the rapid development of a 'Capability early adopter'. The demonstration is to be performed at a live active range with suitable terrain and challenges (e.g. representative of an operational environment including energetics) to permit the capture of the benefits, issues and costs of developing an approach into a coherent capability for the evaluation of an autonomous system.

We will present the outcomes of both these demonstrations and the benefits that can be derived from these approaches.

Thursday, December 7

Track 5 Digital Engineering

Title of Presentation: Ensuring the continued relevance of UK T3E services through Capability Development
Presenter and Author: Andrew Cunningham, Capability Development Lead, QinetiQ

QinetiQ provides strategic Test, Trials, Training and Evaluation (T3E) services to UK Defence through the Long Term Partnering Agreement (LTPA) and it is important that these remain relevant to defence and keep up with the pace of technological change to continue to deliver the required outputs.

Capabilities such as Autonomous Systems, Novel Weapons, and Cyber and Electromagnetic Activities (CEMA) all bring new challenges to the delivery of Test and Evaluation (T&E), whilst new technologies such as Model Based System Engineering (MBSE), Big Data, Digital Twins and improvements in physics based models bring considerable opportunities.

Within the LTPA, the development group is responsible for identifying the impact of these challenges and opportunities and making recommendations on changes and investments to the current suite of T3E

services. Over the past 3 years within the development group, work has been ongoing to understand the key capability and technology drivers, their impact on the suite of T3E services currently delivered, and opportunities for investments in these to ensure they continue to remain relevant. This work has made recommendations on areas of focus and has informed the development of the MOD's Strategic Direction for future T&E.

Title of Presentation: Building Confidence in Model Systems
Presenter and Author: Steve Summers, NI (formerly National Instruments)
Additional Author: Ben Robinson, NI

System models are an increasingly important part of system design, deployment, and maintenance. Models are no longer heuristic, used only for directional or demonstrative purposes. Models are becoming more accurate individualized representations of the artifacts they are connected to. They are expected to reflect the performance of the system throughout the lifetime of the system, ageing appropriately according to the actual usage conditions.

These true-to-life models, or digital twins, can accelerate the design process, reduce test costs, and improve maintenance. It is now possible to accurately forecast component and system failures with more accuracy than ever before.

More defense organizations are creating and maintaining digital models parallel to the design process. But these models are only as valuable as the confidence in those models. Most of us would not fly in an aircraft that has been modeled, but hasn't been tested. The challenge to engineers in design and test is using the data collected during the early stages of development to increase the accuracy of the models in later stages of release and use.

New technologies are making it possible to create more accurate models, with more detailed data collected during system use. In this session, we will discuss technologies and strategies for increasing the accuracy of models and building confidence in those models.

Title of Presentation: Redstone Test Center's Approach to Digital Engineering & LVC M&S In Support of Army Modernization
Presenter and Author: Jeff Tolleson, Director, PeopleTec
Additional Author: Will Harrell, Chief Technologist, Redstone Test Center

We propose this topic be briefed as a panel discussion comprised of both Redstone Test Center (RTC) government personnel and PeopleTec experts. RTC will support this panel. Should a panel not be possible, 1-2 people will present it.

PeopleTec is the prime contractor and lead developer of the Redstone Test Center's Approach to Persistent Integrated Developmental Test (RAPID) program, an effort aimed at enabling RTC's digital transformation to better support Army modernization programs' (e.g., PM FLRAA, PM FARA) digital acquisition and developmental test requirements. RAPID consists of two primary efforts: the Developmental Test Collaboration Environment (DTCE) and the Digital Trinity Lab. The DTCE is a cloud-based authoritative source of truth for users to store, view, and sort their test data. PM FLRAA will use the DTCE as their digital engineering solution and will store OEM component test data in it. The DTCE

includes a custom front-end test management tool to assist flight test engineers in planning and executing tests. The DTCE will also store and test digital twins to assist in developmental testing. The Digital Trinity Lab will integrate digital artifacts (e.g. FLRAA virtual prototype) with legacy subsystems (e.g. ASE) to simulate future increment aircraft. The Lab will also provide a MOSA conformance testing capability to ensure OEM deliveries meet the PM's MOSA requirements. All components of RAPID are designed in MBSE diagrams to best align and integrate with other digital engineering systems.

Title of Presentation: Benefits & Challenges of applying Digital Twins & Hybrid Analytics in Testing & Evaluation Programs

Presenter and Author: Vitor Lopes Pereira, M.Sc., Senior Product Sales Manager – Digital Twins, Ansys Inc.

Testing & Evaluation (T&E) Programs are always looking for opportunities to reduce cost and risks while accelerating time to field. It's well understood that most time, costs, and effort in a Program is associated with the T&E phase. Hence, the recent push on Programs to shift-left and minimize some of these by bringing modeling and simulation (M&S) capabilities earlier in the process.

Digital Twins (DT) are an upcoming technology focused on connecting real-world assets to their digital counterparts and back at a desired frequency and fidelity. The goal is to keep them synchronized and collect additional insights on how these assets are operating to augment decision making. Fulfilling this goal is not a trivial task, but recent advancements in technology have made DT more tangible and accessible. DoD Programs are always looking to develop and operate at the edge of technology to provide advantages over adversaries. This is certainly true with adopting DT, but how, where, when and why?

The main challenges with DT are associated with a balance between accuracy and speed, an element of flexibility, adaptability, interoperability, and scalability. The holy grail of Digital Twining today is Hybrid Digital Twins (HDT) that benefit from both physics and data. To achieve models that operate at high frequency and fidelity from the combination of physics and data, several "twin enabling" techniques have been adopted, such as reduced order models (ROM), Bayesian inference, gaussian methods… This work focuses on examples and the value of using HDT and applying twin enabling techniques to T&E.

Virtual Prototyping HDT rely on techniques to combine and solve models of different sources and fidelity, as well as speeding up the runtimes through ROM workflows. Adopting these empowers engineers to run simulations for different operating conditions in a fraction of time leading to more mature initial prototypes.

Virtual Validation HDT rely on techniques to combine physics models and test data to compensate for missing physics and quantify uncertainty. Test data can be utilized to enhance the fidelity an associated digital counterpart to represent real-world behavior. Then, less critical tests may be performed virtually while leaving more critical tests to be performed physically.

Virtual Testing HDT rely on techniques to package the final models in platform agnostic deployable units that can be shared for testing engineers to run without the need for simulation expertise. It provides testing engineers with a virtual environment to execute testing and link results back to requirements.

Test Augmentation Finally, HDT can be connected to a physical prototype and its testing harness to provide additional insights as virtual sensors and minimize the required sensing infrastructure. The twin is fed telemetry data measured at specific locations to predict variables virtually at additional spots, some of which may not be feasible and/or represent additional costs, time, and effort.

HDT and associated enabling techniques are being deployed to various stages of T&E Programs to reduce costs, risk, and accelerate time to field.

Track 6 Electronic Warfare

Title of Presentation: Enabling T&E of Cognitive EW Systems through Hybrid Digital Twins
Authors and Presenters: Mr. David Zurn, and Dr. Craig Arndt, Principal Research Engineers, Georgia Tech Research Institute

Program test managers and test engineers should carefully consider Digital Twinning approaches for addressing training and testing challenges for Artificial Intelligence/Machine Learning (AI/ML) systems. A hybrid Hardware in the Loop (HITL) and Digital Twin (DT) architecture is discussed for a notional Cognitive EW system. This architecture may provide effective training and testing for complex AI/ML systems that incorporate extensive Cyber-Physical interactions. Several key DT capabilities are identified for addressing AI/ML training and testing challenges –

- Simulation of the system and its's operational environment with sufficient realism
- Ability of the DT to create training and testing data
- Ability to efficiently virtualize hardware models, system firmware and software components into the Digital Twin, allowing for efficient Continuous Integration/Continuous Delivery (CI/CD)

To better understand whether a DT can provide these capabilities, a specific detailed Cognitive EW receiver use case is developed. A high-level hybrid HITL DT architecture for this use case is discussed along with specific functional use cases, such as training and testing data set generation and validation, AI/ML component training and DT validation. Using lessons learned from the Cognitive EW Receiver use case, considerations and limitations for using DT for the Cognitive EW Receiver are discussed.

Title of Presentation: How Do You Test a Cognitive EW System?
Presenter and Author: Jeremy Twaits; Solutions Marketing Manager – Aerospace, Defense & Government; NI

Electromagnetic warfare (EW) systems must remain flexible and adaptable, adding new capabilities as they vie for spectrum dominance against opposing systems. To achieve this, EW researchers and systems engineers are developing novel techniques based on new waveforms and algorithms, multifunction RF systems, and cognitive and adaptive modes of operation.

New cognitive techniques can furnish significant advantages, such as faster decision making and the ability to learn and adapt to changing scenarios, but validating their efficacy and reliability can be challenging. The traditional approach to testing has been to define several test cases or scenarios, simulate threat systems in a system integration lab or open-air range, and assess how the EW systems

dealt with those threats.

For legacy systems with a fixed set of capabilities, this may be sufficient. They are pre-programmed to deal with a specific set of threats or engagement scenarios, limiting the number of test scenarios. For a novel, cognitive EW system, which learns and adapts its behavior as new scenarios are encountered, there are infinite possible test cases. In addition, such systems must learn how to handle as-yet-unknown threats, making it very difficult to predictively assess their performance.

This presentation will discuss what EW test engineers and directors can learn from the automotive industry, which has encountered its own challenges already with the shift towards advanced driver assistance systems (ADAS). This has driven automotive suppliers to move autonomous vehicle testing as early as possible in the design cycle, favoring modelling and simulation over road testing. We'll look at how cognitive EW systems could be tested on the virtual battlefield, long before tactical deployment, focusing on challenges related to computing power, data movement, and signal representation. We'll also explore practical aspects including which elements of an EW system will continue to require over-the-air or physical testing versus elements that can be adequately covered by modelling and simulation scenarios.

Title of Presentation: Modular EW Test and Evaluation System
Presenter and Author: Hajin Kim, Principal Engineer, GaN Corporation

The Electronic Warfare (EW) environment continually evolves with communications technology advancements transitioning to the battlefield. EW systems use electromagnetic spectrum signals (electro-optical, infrared, and RF) for jamming, countermeasures, counter-countermeasures, anti-jamming, electronic masking, probing, reconnaissance, intelligence, and security applications.

These system capabilities mean correlating evolving EW test and evaluation (T&E) systems. Both indoor and outdoor T&E environments require realistic representations of the electromagnetic environment, including multiple threats, EO/IR/RF noise, and relevant signals from various sources for multiple engagement scenarios. EW T&E systems provide a way to significantly reduce the cost of development and full-range testing by allowing precise and realistic test events to be conducted in labs, simulated environments, and outdoor ranges. To achieve realism for the T&E community, GaN has been developing a modular interface architecture and test modules that can be used in HWIL labs or test ranges.

We will present several modules developed by GaN that support the EW T&E environment. One of the systems is Software Programmable EW module, a programmable threat simulator for lab and open-air range testing. This system provides arbitrary RF signals to mimic or jam radar or RF transmitter systems. Additionally, the system accepts a waveform file and transmits the waveform. The system utilizes software defined radio to operate from 30 MHz to 3 GHz. The effort to increase the frequency is ongoing to support up to 20 GHz.

GaN developed the System-of-Systems Controlled Environment Test Infrastructure (SCETI) which is the largest cablecam system in the world and a unique test capability for the U.S. Army. SCETI provides a test environment capable of emulating relevant aircraft flight dynamics to assess operational system performance. SCETI provides a reconfigurable aerial platform capable of precise, accurate, and repeatable 6-DOF movement while providing power and interfaces. Systems may be moved throughout

a representative flight volume using scripted patterns, manual controls, or external TENA-enabled control sources.

Originally focused on testing aircraft sensor assemblies when exposed to Degraded Visual Environment (DVE) conditions, SCETI performs EW, hostile fire detection sensor test, counter UAS performance tests, missile seeker captive carry, and EO/IR signature collection. Another EW T&E capability is Aviation System Test & Integration Lab (AvSTIL), an integrated HWIL facility for testing Aircraft Survivability Equipment (ASE) installed on aircraft. AvSTIL consists of EW T&E systems to inject and project scenarios into a SUT to make it think it is in flight and subject to threats. GaN utilizes TENA Compliant Open Architecture with SW and instrumentation systems suite for data collection and analysis. This architecture utilizes adapters for increased test environment development, testing speed, testing quality monitoring, automated analysis, and results in cost-avoidance for testing systems.

By use of modular architecture and multi domain EW T&E systems, GaN has developed dynamic simulators to modular EW T&E capabilities.

Title of Presentation: Signal Classification using Deep Learning
Presenter and Author: Jeremy Twaits; Solutions Marketing Manager, Aerospace, Defense & Government, NI

In this presentation, we will show how to use software defined radios to capture wideband signals and train a semantic segmentation network using deep learning for spectrum monitoring. The approach is used in the lab-based prototyping and assessment of algorithms that can classify and label signals in a broad spectrum.

We will discuss the application of semantic segmentation to spectrograms of wideband wireless signals to identify spectral content. We will demonstrate an approach to:

- Generate training signals
- Apply transfer learning to a semantic segmentation network to identify 5G NR and radar signals in time and frequency
- Test the trained network with synthetic signals
- Use software defined radios to test the network with over-the-air (OTA) signals

---

Track 7: Software & Cyber Testing

A Realistic Wireless Penetration Test of a VA-Representative Network as Performed by DoD Operators
Presenter: Adam Beard, National Cyber Range Complex – Unclassified

The National Cyber Range Complex-Unclassified (NCRC-U) presents a comprehensive demonstration of a wireless penetration test as would be performed by real-world Department of Defense (DoD) cybersecurity operators. This session offers an in-depth exploration of a realistic scenario where DoD cyber operators conduct a thorough assessment on a simulated network designed to replicate the infrastructure of a Veteran's Affairs (VA) hospital.

The primary objective of this session is to provide a detailed and transparent view of the process followed by DoD cyber operators during a penetration test, from initial reconnaissance to post-exploitation analysis. The presentation emphasizes not only the technical aspects of a test, but also delves into the decision-making and rationale behind each action taken by the DoD operators.

Key topics covered in this session include network reconnaissance, vulnerability assessment, exploitation techniques, and data exfiltration methodologies. The demo will showcase the utilization of cutting-edge tools and methodologies employed by DoD experts in a controlled environment, highlighting the critical steps in safeguarding sensitive healthcare systems. By immersing attendees in this realistic penetration test, the NCRC-U aims to enhance understanding of cybersecurity challenges faced by the healthcare industry and underscore the importance of robust testing and evaluation protocols. Participants will gain valuable insights into the mindset and strategies of DoD operators, ultimately contributing to a more resilient and secure technological landscape

---

Title of Presentation: Next Generation Test Dominance: DevSecOps Platforms to Delivery Capabilities at the Speed of Relevance
Presenter and Author: Melissa Glazener, Value Stream Director, Plaform Development, BrainGu

One of the key differentiators in the success of next-generation warfighting is the ability to control and dominate the flow of information in the battlespace. As data is generated through the planning cycle and into execution, using DevSecOps platforms autonomously enables mission data relevance, increasing the lethality of the knowledge generated. Mission applications will live in a DevSecOps platform unhindered by security, bringing to bear the full weight of an optimized, secure environment to diminish the effects of distance.

BrainGu is partnered with the Advanced Battle Management System and PEO C3BM's to deliver our DevSecOps Platform product StructsureTM. This partnership transitions Cloud Based Command and Control to a modern microservice-based cloud environment, including automated pipelines in a collaborative development environment.

A collaboration environment enables the very essence of rapid experimentation for the warfighter. Delivering the capability for developers to test and deploy their applications continuously provides them with a rich source of feedback to iteratively improve and release their designs. Every warfighter and operator can attest that feedback from the operational edge is essential in creating features and delivering capability at the speed of relevance.

This combination of rapid experimentation, taking advantage of warfighter feedback during development, rapid testing through automation features, and deploying applications in StructsureTM accelerates approval to a continuous authority to operate and paves the future road to autonomous machine learning-assisted Battle Management. For example, the ability to dynamically generate ideal courses of action which are influenced by planning through a mission application capability like Web-based Information Dominant Warfare (WIDOW), informed by Blue Friendly Order of Battle, and placed on the operator's display in real-time alongside sensor information.

In Next Generation Warfighting Test and Evaluation Dominance, especially in an extended-range environment, StructsureTM facilitates rapid experimentation for battlefield employment. StructsureTM Edge is a distributed, decentralized capability that enables the performance of experiments and testing where data is generated. StructsureTM deployment target design provides a means for real-time hosting and running of mission applications. StructsureTM brings test-focused mission application data closer to the test article, which can reduce RF spectrum utilization during tests and disseminates analytics for test data federation. Our DevSecOps platform design assures a resilient, scalable, reliable, and secure environment with reusable tooling in which test experiments are stored, executed, and modified.

These platform capabilities in modern cloud-native architectures reduce reliance on air-gapped systems and human analytics. The pace of operations requires viable compute technologies capable of rapid mission application federation to deliver real-time data fusion for decision dominance results.

Title of Presentation: Spider Prime: A Software Testbed Framework for the Evaluation of Open Systems Architecture Compliant Systems
Presenter and Author: Jacob Slattery, Research Scientist I, GTRI
Additional Authors: John Lillard, Alex Bustos, and Dr. Joshua Walker, Senior Research Engineer, GTRI

The Georgia Tech Research Institute (GTRI) performs a role as compliance evaluator for multiple Electronic Warfare (EW) Open Systems Architecture (OSA) programs. In this role, GTRI develops the testbed framework to support compliance evaluation activities for hardware and/or software and utilizes that test infrastructure to perform the evaluation for potentially compliant vendor systems. This presentation will provide an overview of Spider Prime, which is the software component of GTRI's automated testbed framework for OSA-compliant systems. Spider Prime provides this automated testing framework through the use of web technologies, modern software practices, and an agile development process. This presentation will discuss the software challenges associated with the development of an OSA software testbed and the architectural decisions made to address those challenges. The discussion will conclude with an overview of the features and functions of Spider Prime, and future implementation objectives for continued development. The evaluation of OSAcompliant systems requires a flexible testing framework in order to adapt to the high variability of vendor systems. While these systems align with a specific OSA standard, much of the internal design is unique to allow vendor freedom to produce the most successful system. These differences, while expected, must be minimized from the perspective of compliance evaluation in order to develop an efficient testing process and methodology. Spider Prime provides the ability to interface with independent OSA-compliant systems through the development of non-invasive code that wraps around any available control and communication interfaces. Through these interfaces, it stimulates the system under test to induce evaluated behaviors and records all data available to use for later processing. It includes mechanisms for parsing this data and executing predetermined test cases, evaluating expectations against observed behavior and producing automated results to display to the tester. While this post-processing method of compliance evaluation accomplishes the goals for current programs, continued development for Spider Prime is expected to provide mechanisms for real-time testing, characterization testing, enhanced data analysis, and expanded visualization of recorded data, leading to a higher level of utility in the evaluation of OSAcompliant systems.

Track 8: Test Design

Title of Presentation: QinetiQ's T&E Sovereign Skills Program
Presenter and Author: Scott Busby, Solution Architect, QinetiQ Pty Ltd

QinetiQ's Test and Evaluation Sovereign Skills Program: Leveraging global resources to deliver long-term solutions for the complex T&E workforce gap.

QinetiQ is a global company providing T&E services to customers around the globe. As the range of geographies within which we operate expands we have recognised the need to address the perennial challenge of the development of skills. This challenge is enhanced as many nations desire a sovereign skills base to provide an enduring national capability. Our new T&E Sovereign Skills Program (TESSP) was developed to address these joint challenges. The fundamental design of the program allows accelerated learning though an extended deployment to the UK where we provide a broad portfolio of T&E services.

The TESSP is aimed at new T&E professionals recruited into specific roles. Following selection for the program, the participants undertake on-line training in various elements of range operations and T&E delivery to give them a basic understanding. They then deploy to the UK for a three month secondment to various T&E facilities, guided by the domain experience they require. Shaping everything they do is a personalised training plan, with identified outputs that need to be achieved. The TESSP combines theory packages curated in house by the QinetiQ program team, practical experience at relevant ranges and T&E facilities, and mentoring from senior T&E professionals and systems engineers.

The first cohort from Australia completed their program in May 2023. Building on the experience of this cohort, QinetiQ is now refining and improving the content, delivery and outcomes of the TESSP for future cohorts, the next of which starts in June made up of UK personnel.

The TESSP is capable of training across the full range of T&E related roles. Each intake is tailored to the home countries' capability priorities with the number of participants dictated by the need across relevant capabilities and domains. As the program matures, it will open to other Defence, public service and industry participants providing opportunities to share practice, language and standard approaches to T&E delivery amongst partners. Continuous feedback from managers, participants and instructors enable the TESSP to remain current, agile and aligned to customer's needs as well as participant's developmental goals demonstrating the potential a global company can unlock to solve domestic problems.

Title of Presentation: Improving Flight Test Data Management for Advanced Defense Operations
Presenters and Authors: Austin Ruth, Research Engineer II, GTRI and Grace Kaylor, Research Engineer I, GTRI

Evolution of systems is a significant pain point within the DoD due to the fact that it antiquates presently fielded technology. DevSecOps and MLOps are prime practices taking the commercial industry by storm, defining paths to continuous delivery (CD) and continuous integration (CI), and therefore influencing the scope of work within the DoD. With software and algorithms becoming the key to the battle, the oftenoverlooked concept of data management is pivotal. More specifically, the flight test data analysis automation domain teams must first be able to manage, process, and deliver data products; this we

have coined as Flight Test Data Modernization. By deploying the proper infrastructure, data can be moved from point A to point B (e.g. Cloud to Edge) with containerized processing applications. As a result of this, we can deliver a rich data product for end users or algorithms. Once data products have been delivered, machine learning and artificial intelligence models can be retrained and redeployed rapidly with the most current data. In this presentation, we will showcase optimized Data Modernization infrastructure and outline key actions to be taken in DevSecOps and MLOps domains. We will also discuss the benefits of adopting this practice for a myriad of use-cases.

Title of Presentation: DevSecOps Evaluation Framework: The DevSecOps approach to Test and Evaluation
Presenter: Brittany Fischer, STAT COE
Authors: Joseph Lazarus, Operations Research Analyst Lead and Dr. Leonard Truett, Senior STAT Expert, STAT COE

We will provide an overview of the DevSecOps Evaluation Framework (DSO-EF) and its application to the Test and Evaluation (T&E) process. The DSO-EF is a comprehensive process and toolset for adapting to the impacts of emerging technology on Reliability and Maintainability within the DevSecOps lifecycle. By aligning T&E activities and injections (e.g., Automation, STAT, and Security) with the DSO-EF, organizations can achieve a more efficient and effective T&E process.

Title of Presentation: Test Design Optimization
Presenter and Author: Dr. Mark Kiemele, Air Academy Associates

Coming Soon.