Cybersecurity Pre-Workshop Tutorials

NOTE: Pre-Workshop Tutorials require a separate fee from the Workshops.
Single Tutorial - $205, Two Tutorials - $385

Tuesday, 18 Oct. 8:00 AM – 12:00 PM

Cybersecurity Assessment of MIL-STD-1553

Adam McCorkle
Georgia Tech Research Institute

The MIL-STD-1553 serial data bus standard has been around for over 4 decades and continues to be an integral network architecture on modern military aircraft, ground vehicles and both surface and subsurface ships. This presentation will provide a brief overview and history of the standard and its applications, and then discuss potential vulnerabilities related to the physical, electrical, and functional characteristics that are inherent in implementations of the standard. In particular, modern cyber-attack techniques will be discussed that could potentially be applied to penetrate an implementation of the MIL-STD-1553 data bus. An approach to assess the severity of each of these intrusions and potential attack countermeasures will be discussed that could potentially be applied to existing implementations of MIL-STD-1553 in order to mitigate these risks and to also drive engineering decisions for newly developed systems. This discussion in its entirety can aid with the development of a penetration testing program for a particular system or system of systems implementing the MIL-STD-1553 data bus. Current MIL-STD-1553 cyber hardening efforts across the DoD community will also be reviewed.

A Process for Distributed LVC in T&E

Michael O'Connor
TRIDEUM Corporation

Integration and execution of large distributed Live, Virtual, Constructive (LVC) events consume substantial time and resources. While the underlying distributed LVC technologies are mature, the processes for integrating events are not. The IEEE Std 1730-2010 Distributed Simulation Engineering and Execution Process (DSEEP) standard defines a process model for developing an event. DSEEP defines a set of seven steps divided into activities. The process model provides representative inputs and outputs for each activity. However, the user still must instantiate the process and develop artifact templates. The development of a robust process based on DSEEP is a substantial effort.

The goal of the process is to produce a verified distributed LVC environment to conduct the event. While distributed LVC environments can be created without using a process, doing so adds significant risks. The first risk is that the integration fails, and it may be difficult to discover the reason. The second risk is that the unverified environment produces invalid results that might not be apparent until the results are used.

An instantiation of DSEEP was developed based on the authors' integration and execution of many distributed LVC events. This implementation has nine steps, divided into 27 activities. This process adds two additional steps to the process. One of the steps adds a tabletop wargaming step to work through the requirements. The second additional step develops a digital twin of the target system. A detailed set of processes, templates, and guidance on how to perform the selected activities is provided. The process covers the integration of simulations and tactical systems to meet the objectives of the LVC event.

The tutorial will provide an overview of the complete process with selected steps described in more detail. This tutorial will provide the detailed inputs, tasks, outputs, and examples for each activity in the step. The process includes solution approaches related to distributed LVC environments using multiple distributed simulation architectures, live entities, and cyber activities.

The process described in this tutorial was developed to support distributed LVC Test and Evaluation and has been extended to support cyber testing.

Introduction to Cyber Resilience Test and Evaluation

Jean Petty
Cyber Resilience T&E Manager, Department of Homeland Security (DHS)

This tutorial will familiarize attendees with Cybersecurity and Test and Evaluation as it applies to US Federal Government Programs and the U.S DOD. Note that the ideas and concepts presented also apply in principal to any acquisition program. Topics that will be addressed include Cyberspace as an operational domain, Cybersecurity threats, malware, DHS and DOD systems acquisition and associated Cyber T&E policy and process including "Cloud" Programs, requirements analysis, evaluation frameworks, cyber tabletop exercises, cooperative vulnerability assessments, adversarial assessments, cyber ranges and lessons learned.

Tuesday, 18 Oct. 1:00 PM – 5:00 PM

Cybersecurity Solutions with JMETC, TENA, and TRMC BDA

Gene Hudgins
TENA/JMETC, KBR

The Test and Training Enabling Architecture (TENA) was developed as a DoD CTEIP project to enable interoperability among ranges, facilities, and simulations in a timely and cost-efficient manner, as well as to foster reuse of range assets and future software systems. TENA provides for real-time software system interoperability, as well as interfaces to existing range assets, C4ISR systems, and simulations. TENA, selected for use in JMETC events, is well-designed for its role in prototyping demonstrations and distributed testing.

Established in 2006 under the TRMC, JMETC provides readily available connectivity to the Services' distributed test capabilities and simulations. JMETC also provides connectivity for testing resources in the Defense industry and incorporation of distributed testing and leveraging of JMETC-provided capabilities by programs and users has repeatedly proven to reduce risk, cost, and schedule. JMETC is a distributed LVC testing capability developed to support the acquisition community during program development, developmental testing, operational testing, and interoperability certification, and to demonstrate Net-Ready Key Performance Parameters (KPP) requirements in a customer-specific Joint Mission Environment.

JMETC is the T&E enterprise network solution for secret testing and uses a hybrid network architecture – the JMETC Secret Network (JSN), based on the SDREN. The JMETC MILS Network (JMN) is the T&E enterprise network solution for all classifications and cyber testing. JMETC provides readily available

connectivity to the Services' distributed test capabilities and simulations, as well as industry test resources. JMETC is also aligned with JNTC integration solutions to foster test, training, and experimental collaboration.

TRMC Enterprise Big Data Analytics (BDA) and Knowledge Management (BDKM) has the capacity to improve acquisition efficiency, keep up with the rapid pace of acquisition technological advancement, ensure that effective weapon systems are delivered to warfighters at the speed of relevance, and enable T&E analysts across the acquisition lifecycle to make better and faster decisions using data that was previously inaccessible, or unusable. BDA is the application of advanced tools and techniques to help quickly process, visualize, understand, and report on data. JMETC has demonstrated that applying enterprise-distributed BDA tools and techniques to T&E leads to faster and more informed decision-making that reduces overall program cost and risk.

This tutorial will inform the audience as to the current impact of TENA, JMETC, and BDA on the T&E community; as well as their expected future benefits to the range community and the warfighter.

Basic Overview of Telemetry

Gary Thom
Delta Information Systems

This course provides a very high-level introduction of basic telemetry concepts and components. The course begins with onboard vehicle under test discussing sensors, signal conditioning, commutation, modulation and transmission. It continues on the ground with receivers, data distribution, decommutation, processing and display. The course includes additional concepts like IRIG 106 Chapter 10 and 11 recording and distribution formats as well as IRIG 106 Chapter 7 packet data over PCM.

ARCUS Cloud – Cyber Tools and Ranges

Peter Walsh
Jackpine Technologies Corp.

Arcus is a leading-edge cloud and security orchestration service, purpose built for the unique requirements of the DoD. Fielded at multiple classification levels, Arcus is a next generation, fully proven, DevSecOps Service (IaaS, PaaS, SaaS), offering hybrid workflows (containers, virtual machines, and/or physical systems) across hybrid clouds (local, other DoD, and commercial), to support hybrid missions.

Programs across multiple services and agencies - USAF, SPACE FORCE, DISA, JAIC, JFHQ-DODIN, Army, and others use Arcus to address a variety of mission requirements, including:

• Test Automation • Training • Cyber Security • Digital Engineering • Cyber Operations • Cloud Migration • Software Development • and more!

Major DoD success have been born and incubated inside Arcus. It has over 15 million hours of use by thousands of users, in scores of programs, launching over 300,000 deployments.

Built from the ground up with the goal of meeting the distinctive security, network, and operational constraints of the DoD, Arcus not only complies with the DoD Cloud Computing Security Requirements Guide but also automates compliance when provisioning infrastructure and resources for its users. The service and the team navigate the delicate balance between security compliance, actual security, and getting things done. The baked in rigor has enabled Arcus to received multiple Risk Management Framework (RMF) Authority to Operate (ATO) approvals. The umbrella ATO enables programs to start working inside the platform on Day One.

Arcus has been used regularly within the DoD to deploy environments to support test; cyber ranges; exercises; tool development; malware assessment; acquisition evaluations; Red Team certification; and Red Team operations.

In this session, we will introduce Arcus and explore its use for test environments and cyber ranges. Users can define and create simple to complex environments, on-demand, to support their specific use cases. We will delve into two specific examples to review their architecture, workflow, automation, and unique features.

These include:

Defense Cyber Operations (DCO) platform
- Automated deployment of enterprise products
- WAN architecture
- Traffic generators & data loading
- Multiple environments on demand
- Automated test options

Red Team Operations Platform
- Anonymous redirectors
- Use of commercial clouds
- Workstation automation
- Phishing campaign
- Tooling (Kali, Redmine, Cobalt Strike, etc.)

We will also show a short demo of how the technology is used for digital twins and IoT environments.

Interested participants will have the opportunity to work inside the Arcus platform and follow along for a hands-on experience. A laptop and a PKI credential (CAC or ECA) are required to participate in the hands-on portion.

T&E in a Digital Engineering Environment

Jean Petty
Cyber Resilience T&E Manager, Department of Homeland Security (DHS)

This tutorial will review digital engineering concepts in general and then deep dive into specifics for test and evaluation (T&E) in a digital engineering environment. The course will review concepts, methods, tools, and best practices for five Digital Engineering topic areas including models, an authoritative

source of truth, technological innovation, innovative infrastructure, and workforce. Each topic area will be addressed in general, followed by discussion of specific issues and challenges for T&E. Discussion areas will include:

- How planning and the evaluation components of T&E need to evolve in the DE environment, given Model Based Systems Engineering, Mission Engineering, and automated testing.
- The characteristics of T&E tools within the DE environment and considerations and methods for automated tools selection.
- Data access, data sharing, and hurdles for building an authoritative source of truth.
- Special concerns for Cyber T&E in a Digital Engineering environment.
- Digital Engineering infrastructure and infrastructure providers.
- T&E workforce within a Digital Engineering ecosystem.
- Gaps in current infrastructure, capabilities, workforce, etc.

This course is intended for T&E professionals who are new to Digital Engineering or are beginning to implement Digital Engineering in their T&E practices. The course will include lecture, discussion, and interactive exercises.