Join us for the 8th Cybersecurity Workshop

New Domains in Cybersecurity T&E

October 18-20, 2022
Embassy Suites by Hilton Destin Miramar Beach, Destin, FL
Hosted by the ITEA Emerald Coast Chapter

- Half-day pre-Workshop Tutorials: *Earn Continuing Professional Education Credits (CPEs)*
- Keynote Speakers & Panel Discussions
- Technical Exchange Sessions
- Hands-on Lab Experience.
- Networking Opportunities: *Make professional connections to grow your business network and seek out partnerships*

Register now at www.itea.org

Week at-a-Glance

EVENTS	DATE	TIME
Tutorials Separate fee and registration	Tuesday, October 18	8:00 a.m. to 12:00 p.m. 1:00 p.m. to 5:00 p.m.
Red Team/Blue Team Hands-on Lab Experience	Thursday, October 20	1:30 p.m. to 3:00 p.m. 3:15 p.m. to 5:15 p.m.
Technical Sessions	Wednesday, October 19 Thursday, October 20	3:15 p.m. to 5:15 p.m. 1:30 p.m. to 5:15 p.m.
Special Features Including guest speakers and a networking reception	Wednesday, October 19 Thursday, October 20	8:00 a.m. to 12:00 p.m. 5:30 p.m. to 7:30 p.m. 8:00 a.m. to 12:30 p.m.

Pre-workshop Tutorial

Separate fees are associated with these courses

Tuesday, October 18 – Morning Sessions (8:00 a.m. to 12:00 p.m)

An Introduction to Human System Integration (HSI) Aspects of Cyberspace Test and Evaluation
Michael Lilienthal, PhD, CTEP, CPE, EWA Government Systems Inc.

The human subsystem of a weapon, control, or maintenance system in many cases is the most vulnerable to cyber-attack. This tutorial will introduce human capabilities and limitations (cognitive, physical, sensory, and team dynamics) that testers need to consider as they develop their test and evaluation (T&E) plans to assess the cyber resiliency of a system under test (SUT) in a cyber contested environment.

Human System Integration (HSI) is the science that ensures the capabilities and limitations of human users (operators, maintainers, and supporters) are best matched with the constraints presented by system technology. HSI seeks to identify and remove system elements that require excessive cognitive, physical, or sensory skills; result in mission-critical errors; require avoidable training costs; or produce safety or health hazards.

This tutorial will review the current policies, guidelines, and tools of HSI for use during developmental and operational T&E. Their applicability to cybersecurity T&E will be discussed.

The tutorial will present how the categories of errors users make (both intentional and unintentional), the effects of fatigue, system usability, workload, training, and the like will alter the cyber vulnerability and resiliency of a SUT. In class demonstrations will illustrate aspects of the limitations of human cognition and memory to reinforce the tutorial. Reviews of case studies of actual cyber incidents will provide context for human factors that contributed to the incidents will be part of the tutorial. The Human Factors Analysis and Classification System (HFACS), the process which classifies human error and latent organizational factors in aviation accidents will be presented as a potential framework for use in cyber resiliency T&E.
The challenges of evaluating human teaming with autonomous and automated systems for cyber vulnerabilities will be discussed along with other emerging technologies being introduced to the multidomain battlespace.

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 principle 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.

Pre-workshop Tutorial continued

A full description and fees associated with these courses are located on the website

Tuesday, October 18 – Afternoon Sessions (1:00 p.m. to 5:00 p.m.)

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.

Snapshot of the Agenda

Wednesday, October 19

8:00 a.m. to 8:30 a.m.
Opening Ceremony & Welcome

Bruce Einfalt, President of ITEA
Shelby Pearce, Program Chair
Andy Overbay, Technical Chair

8:30 am to 10:00 a.m.
Keynote & Featured Speaker

George Rumford, (SES) Director (acting) and Principal Deputy, Test Resource Management (TRMC)
Brig Gen Rawls, Commander, Air Force Operational Test and Evaluation Center (AFOTEC)

10:00 a.m. to 10:30 a.m.
Refreshments

10:30 a.m. to 12:00 p.m.
Featured Speakers

James Wells (SES), Director Office of Test and Evaluation, Department of Homeland Security (DHS)
Sarah Standard, OUSD R&E, Developmental Test, Evaluation, and Assessments (DTE&A)

12:00 p.m. to 1:00 p.m.
Luncheon

1:00 p.m. to 3:00 p.m.
Hands-on Lab Experience

3:00 p.m. to 3:15 p.m.
A quick break

3:15 p.m. to 5:15 p.m.
Technical Sessions running concurrently

Session 1: Cybersecurity Test Technology (Part 1)
Chair: **Min Kim**, Deputy Executing Agent for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

Start Time	Presenter(s)	Presentation
3:15 p.m.	Dr. Mike Shields, TRMC T&E/S&T and Pete Firey, MITRE	*Measure and Share: TRMC T&E/S&T Cyberspace Test Technology's project to improve Cyber T&E impacts across DoD*
3:45 p.m.	Steve Durst, Terry Champion, Eric Renouf, Skaion	*Activity and Content Enhancement – Next Gen Traffic Generation Toolkit*
4:15 p.m.	Terry Patten, Gerald Fry, David Kelle, Brian Gzemski, and Bradley Mahan, Charles River Analytics	*The Future of Cyber Monitors*
4:45 p.m.	Dr. Himanshu Upadhyay, Dr. Leonel Lagos, Santosh Joshi, Jayesh Soni, and Michael Perez, Florida International University	*Automated Machine Learning for Cyber Security*

Session 2: Securing the SW Supply Chain and Infrastructure
Chair: To Be Announced

Start Time	Presenter(s)	Presentation
3:15 p.m.	Michael D Brown, Trail of Bits	*Automated Tools for Securing the Software Supply Chain – **by Video***
3:45 p.m.	Michael House, DESE Research Inc.	*Attack Surface Reduction through Binary Analysis*
4:15 p.m.	John Peace	*Cybersecurity Data Science (CSDS) for the Aviation Ecosystem*
4:45 p.m.	Melissa Glazener, Taylor Mitchell, Joey Mink, Reggie Johnson, Ricoh Glover, Ian Doull	*Platform Thinking: Bridging the Warfighter Gap with DevSecOps*

Session 3: Test Design, Regulations, and Best Practices

Chair: **M. John Rafferty**, USAF

Start Time	Presenter(s)	Presentation
3:15 p.m.	Steven Newton, Sarah Standard	*DoD Cyber T&E Cyber Focus Chapter and Companion Guide Deep Dive*
3:45 p.m.	Gilmore, Avery, Girardi, Medlin	*Applying Design of Experiments (DOE) to Cyber Testing*
4:15 p.m.	Steve Millar	*DevOps to DevSecOps: Making Security Part of Your Development Operations*
4:45 p.m.	Steve Seiden, Acquired Data Systems	*Cybersecurity in the Operational Technology (OT) World*

5:30 p.m. to 7:00 p.m.

Join us for a Networking Reception

Thursday, October 20

8:00 a.m. to 8:15 a.m.

Welcome & Review of the Day

8:15 a.m. to 10:30 a.m.

Keynote & Featured Speakers

Maj Gen Evan C. Dertien, Commander, Air Force Test Center, Edwards Air Force Base
AJ Pathmanathan, Director, National Cyber Range Complex
Joe Bradley, Exec Director of the CROWS *(Invited)*

10:30 a.m. to 11:00 a.m.

Refreshments

11:00 a.m. to 12:30 p.m.

Col William E. Young, Jr., PhD (USAF Ret) Commander, 350th Spectrum Warfare Wing
To Be Announced

12:30 p.m. to 1:30 p.m.

Luncheon

1:30 p.m. to 3:00 p.m.

Technical Sessions and Hands-on Lab Experience running concurrently

Session 4: Best Practices for Cyber Evaluation Tools

Chair: **Ryan Christiansen**,

Start Time	Presenter(s)	Presentation
1:30 p.m.	Megan Fischer	*Security Impact Analysis and Risk Management Boards (cyber-evaluation tools)*
2:00 p.m.	Megan Fisher; Todd Jacob, Ryan Christiansen, Evan Thomas	*Reducing the Burden of a Cyber Table Top (CTT-LITE)*
2:30 p.m.	Megan Fischer	*CTT to RMF (part of the analysis process for the CTT)*

Session 5: Assessing and Mitigating Risk

Chair: To Be Announced

Start Time	Presenter(s)	Presentation
1:30 p.m.	William D. Bryant	*Unified Risk Assessment and Measurement System*
2:00 p.m.	Dr. S. Sarathy; M. Marquez, T. Ngo, J. Goh, Dr. S-k Chin, Dr. Q. Qiu, Dr. W. Young	*Hybrid Assurance Approach for Hardware Based MLS Security*
2:30 p.m.	Michael Kaplan	*LOOKOUT: Low-Overhead Observations Keeping Operational Under Threat*

Red Team/Blue Team Hands-on Lab Experience

Chair: **Sean Conway**, Edwards AFB

Description coming soon – check back

Session 6: Cybersecurity Test Technology (Part 2)

Chair: **Min Kim**, Deputy Executing Agent for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

CUI [Controlled Unclassified Information (CUI) session] This one track will have limited participation to U.S. citizens who are employees of the U.S. Federal Government or its contractors (C), or employees of the Department of Defense or its contractors (D). If you do not meet this requirement, you will be unable to attend this one track. DoD common access cards (CAC) or personal identity verification (PIV) will be required for entry. After the one track – the session will be open to all attendees.

Start Time	Presenter(s)	Presentation
3:15 p.m.	Susi McKee and Brad Mahan, 47th Cyberspace Test Squadron / OL-A	** CUI * NSITE (Network, System Integration and Test Environment) – CTC (Cyber Test Capabilities)*
3:45 p.m.	Arch Owen, Draper – National Security and Space	*Vader Modular Fuzzer: What, Why and How*
4:15 p.m.	Andrew Shaffer, & Bruce Einfalt	*Automated Attack Framework for Test & Evaluation (AAFT)*
4:45 p.m.	Dr. Himanshu Upadhyay, Dr. Leonel Lagos, Santosh Joshi, Jayesh Soni, and Steven Valle, Florida International University	*Cyber Threat Automation & Monitoring System*

Session 7: Future of Test

Chair: To Be Announced

Start Time	Presenter(s)	Presentation
3:15 p.m.	Leonard Moskal	*Update from the Executive Agent for DoD Cyber Test Ranges*
3:45 p.m.	Tilghman Turner; Michael O'Connor, Ken LeSueur	*Virtual Blockhouse for Remote T&E*
4:15 p.m.	Brian Pate, Davis, Durr, Conway	*SpaceCREST*
4:45 p.m.	Michael J. O'Connor; Brett Boren, Ken LeSueur	*A Hybrid Digital Twin for T&E*

Red Team/Blue Team Hands-on Lab Experience – continued

Chair: **Sean Conway**, AF

Description coming soon.

Other Important Information

Hotel & Workshop Location
Embassy Suites by Hilton Destin Miramar Beach
570 Scenic Gulf Drive
Destin, FL 32550
Phone: 850-337-7000
Room Block Cut-off: 16 September
See website for pricing and cancellation notice.

Company Visibility – Sponsor!
ITEA is a 501(c)(3) professional education association dedicated to the education and advancement of the test and evaluation profession. Sponsorship opportunities are available to highlight your company before and during the workshop. We offer a fee structure that will fit any budget, from $250 to $5000.

Education and Credit Hours
Each 4-hour pre-workshop tutorial provides 4 contact hours of instruction (4 CPEs) that are directly applicable to your professional development program, including the Certified Test and Evaluation Professional Credential (CTEP). The fee to attend a 4-hour tutorial is $205 for one class or $385 for two classes. Registration for a tutorial does not require registration for the workshop.

ITEA Membership Perk
Since ITEA is the only professional association dedicated to the Test and Evaluation community, why wouldn't you become a member? The nominal fee for a full-time government or active-duty military person is only $45. Industry partners are $95 and early career professionals and student fees are $25. Become a member prior to registering and you will receive a discount of $150 on the registration fee.

Registration The fee includes: 2 lunches, refreshments, & a networking reception.

Early Bird Registration prior to September 10
$645 – Non-Member
$495 – ITEA Member / Government Employee / Active-Duty Military
$95 – Early Career Professional*

Regular Registration September 11 – 30
$745 – Non-Member
$595 – ITEA Member / Government Employee / Active-Duty Military
$195 – Early Career Professional*

Late Registration after October 1
$845 – Non-Member
$695 – ITEA Member / Government Employee / Active-Duty Military
$295 – Early Career Professional*

*Early T&E Career Professional (less than 5 years of T&E experience) Verification required. Includes a one-year ITEA membership for Non-ITEA Member.

Special Registration Pricing
A nominal fee to help defer some of the costs associated with hosting this workshop are necessary. We are pleased to be able to offer extremely low fees to our speakers and presenters. We appreciate your understanding.

$150 – Plenary Speaker, Panel/Session Chair, Tutorial Secondary Instructor
$395 – Panelist and Technical Presenter
$50 – Full-time students (ID Required)
$400 – One day only

SUBSTITUTION AND CANCELLATION POLICY: Substitutions are permitted. Refunds are not available within ten (10) days prior to the start of the event. Requests for cancellation submitted between ten (10) to 45 days prior to start date of the event will be subject to a $250 cancellation fee. Requests for cancellation greater than 45 days prior to the start date of the event will be subject to a $100 cancellation fee.

The Planning Committee

ITEA is an all-volunteer organization. The planning committee is made up of dedicated T&E professionals from the Emerald Coast Chapter who have donated their time and energy to build an exceptional program for you. The Chapter has a robust scholarship program, and this workshop will also provide additional dollars to be added to their coffers. ITEA leadership would like to thank this hardworking team for their expertise, attention to detail, and enthusiasm as they plan and then execute this technical workshop.

Workshop Co-Chairs
Andy Overbay, BigBear.AI
Shelby Pearce, Jacobs

Contact us if you have any questions: info@itea.org 703-631-6220