Pre-Workshop Tutorials

Tutorials are a separate fee from the workshop. The fee to attend a tutorial is $300 for one 4-hour tutorial or $500 for two 1/2 days.

Tuesday, August 29 – Morning Tutorials 8:00 am to 12:00 pm

Automated Compliance, Performance, and Security Testing of 5G Systems

Binil George, Robert Donohoe, and Kevin McKenna, Lockheed Martin

5th generation of mobile cellular services offer enhanced mobile broadband, ultra-low latency, and extreme high density communication services as well as a modular, composable system architecture designed to mesh computing solutions. OUSD (R&E) sees multiple opportunities to employ 5G technology to meet a variety of enhance DoD tactical and enterprise communications challenges. This tutorial will present a brief background on 5G technology and how to integrate compliance, performance, and security testing of 5G solutions into a DevSecOps pipeline. The approach presented will highlight work Lockheed Martin has done in collaboration with Keysight Technologies to stand-up and operate a 5G testbed and CI/CD Pipeline that builds, deploys, configures, and tests 5G solutions.

Lessons Learned from Safety Science Applicable to Cyberspace Test and Evaluation

Michael Lilienthal, PhD, CTEP, CPE, EWA-GSI

Several studies and subject matter experts have concluded most cyber breaches are caused by human error. Program managers developing new weapon systems find the human error causal factor very seductive. Unfortunately, fixing only human error symptoms can easily become a continuous fight without identifying and mitigating contributory root causes. Safety engineers who also examine human error as part of accident investigations and hazard analyses repeatedly find complex systems almost always fail in complex ways. Safety engineering objectives dovetail with those of cybersecurity to achieve the goal of a high level of functional safety and cybersecurity resiliency during conception, design, operation, testing and maintenance of cyber-physical systems. The value that the safety science approach adds to cybersecurity is determining why people behaved in the way they did and what weaknesses in the system allowed the breach (loss/accident) to occur. Cybersecurity tests can benefit from the progress safety science has made in its methods of accident investigations and hazard analysis to supplement their analysis of emerging systems for cyber vulnerabilities and cyber survivability.

The tutorial reviews a case study of an actual cyber incident as well as a real world example of a naval incident to provide context for the T&E of a system that includes the human operating subsystem (HOS). Current directives and MIL-STDs for the HOS relevant to cybersecurity will be discussed. Categories of errors users make along with intentional and unintentional violations that contribute to a cybersecurity breach will be discussed. We will discuss how the effects of fatigue, system usability, workload, mental models, training, and the like will alter the cyber vulnerability and resiliency of a SUT. This will provide suggestions for the design and execution of OT&E. Class demonstrations will illustrate aspects of the limitations of human cognition, fatigue, mental models, and memory to reinforce the tutorial. Tools used for aircraft accident investigation and hazard analysis will be presented as potential frameworks to complement cyber resiliency especially in the context of a mission/system of system 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.

Mission Based Cyber Risk Assessment (MBCRA) Tutorial and Exercise using the Unified Risk Assessment and Measurement System (URAMS)

William D. Bryant, Technical Fellow, MTSI

Mission Based Cyber Risk Assessments (MBCRA) help set the foundation of good cyber testing by focusing limited test resources on the most significant risks. There are numerous MBCRA approaches available including Cyber Table Tops (CTT) and the Mission-based Risk Assessment Process for Cyber (MRAP-C). The Unified Risk Assessment and Measurement Process (URAMS) is another MBCRA and while it is lighter weight and faster than some methods, many of the principles and techniques use apply broadly across many different MBCRAs.

URAMS starts with an engineering analysis, and our preferred tool is Systems-Theoretic Process Analysis for Security (STPA-Sec). This tool was developed from leveraging the safety analysis work done at MIT and has since been used with great effectiveness across a range of military weapon systems and civilian aerospace systems. STPA-Sec is grounded in systems engineering and is focused on mission-level losses as the true drivers of relevant security design. STPA-Sec also enables analysis of a system's security posture early in the lifecycle, which enables true "baking in" of security.

From the analysis, a set of risk scenarios are developed that are specific to the system under consideration and its expected operating environment. Then, those risk scenarios are scored using any of a wide range of available scoring tools. URAMS scoring tools are characterized first by the model of risk and what factors are assumed to contribute to overall risk, and second by the type of input. Inputs can be provided as single point values, single point values with a confidence, three-point estimates, or 90% confidence intervals. Selection of input type depends on the training and experience of the assessors, as well as how important uncertainty is to the decision makers. While human subject matter experts (SMEs) are

utilized as the basis for scoring in URAMS, automated and algorithmic based approaches can and should be used to inform those SMEs.

The risk scenarios can then be combined utilizing a simple Monte Carlo simulation to determine what the overall risk is for a system or portfolio of systems. The ability to combine risk facilitates building a structured assurance case that includes the analyzed mission structure connected to the specific risk scenarios and their scores, which flow up through the mission elements to the overall system. Perhaps most importantly, specific evidence such as testing results, design features, etc., can also be added to the assurance case to validate the risk scores. The assurance case is presented in a format that allows decision makers to rapidly assess whether the scoring is reasonable, based upon their understanding of the mission and the evidence provided.

This tutorial will teach students how to accomplish a URAMS MBCRA by presenting some of the theory behind the approach, showing how to utilize one set of URAMS tools, and providing practical experience by working through portions of a URAMS assessment on a notional aerospace system to include scoring selected risk scenarios.

T&E Fundamentals and Certified Test & Evaluation Professional (CTEP) Foundations

Charles "Chas" McKee, President & CEO, Taverene Analytics LLC

In this high-level short course we will review T&E fundamentals which are covered in the CTEP Foundational exam. We will review the Body of Knowledge (BOK) including the four subject domains used in developing the CTEP program. These will include: Test and Evaluation Planning (Organizational planning, Requirements Analysis, T&E strategy, Evaluation approach, Test Design and Adequacy, T&E Documentation, T&E Cost Management, Contracting for T&E, Specialized Types of testing, planning and resourcing, Risk identification and management, Cyber testing, Modeling and Simulation, Reliability-Availability-Maintainability); T&E Design (Test Adequacy, Scientific Test and analysis techniques, Software Testing); Test and Evaluation Execution (Test Control Management, Data Management, and Test Safety / Certification); and Test Data Analysis, Evaluation and Reporting (Data Verification and Validation, Validation of Test Results, Evaluation, Reporting, Cyber Resilience / Cybersecurity Analysis, Model Validation, and Data Analytics).

Who Should Attend: Individuals in the T&E community (government and industry, members and non-members) who want to demonstrate their knowledge, skills and abilities in T&E and be recognized by the International Test and Evaluation Association for their professional growth. Requirements for Foundational level CTEP certification should have a Bachelor's degree and 1 year of T&E work experience or an Associates degree and 3 years of relevant T&E work experience or five years of relevant T&E work experience. Please note that the CTEP credential is becoming a "preferred" requirement in many test engineer job postings.

5G NR Specification and System Engineering Aspects

Achilles Kogiantis, PhD, and Ankur Sharma, Peraton Labs

5G wireless cellular networks, based on the 3GPP standard, are being widely deployed in the United States and the rest of the world. 5G is expected to increasingly dominate the worldwide cellular communication market due to its flexibility, wide adoption, and an ever-expanding supplier global ecosystem. The flexible 5G architecture allows multiple networks widely differing in physical, reliability and power characteristics to be supported over a common infrastructure.

This flexibility will be particularly useful to Testing Ranges where subnetworks simultaneously supporting high-bandwidth terrestrial communications, low-power sensors and broadband airborne telemetry systems can be flexibly implemented over a common 5G platform. This tutorial is intended to familiarize the Testing Range professionals with a) the key features of the 5G standards specifications – the basic vision, network architecture, the physical and MAC-layer characteristics of the air-interface, and b) the 5G system engineering aspects of deploying a new private network, dimensioning and planning, and its performance assessment. The first half of the tutorial will discuss the 5G standards specifications, while the second half will cover the 5G systems engineering aspects.

Mission Impact Assessment (MIA) Process

Teresa Barley Merklin, Cyber Fellow, Aeronautics Cyber Range, Lockheed Martin

Mission Impact Assessment (MIA) is a process used to identify and prioritize the mission essential functions of a system. Integrating MIA into the Acquisition and Development lifecycles creates a foundational understanding of cyber resiliency objectives. This process has proven to be valuable during project inception as a mechanism for eliciting meaningful cyber resiliency requirements. It also produces data which is useful for scoring Cyber Risk Assessment. For Cyber Test and Evaluation teams, the MIA process can be used as a basis for test planning as well as scoring the impacts of any findings. This tutorial provides an introduction to the process documented in the MIA Guidebook and a detailed overview of the Use Cases for using the resulting data. Each step of the process is illustrated using a case study.

Test and Evaluation in a Digital Engineering Environment

Jean Petty, Department of Homeland Security (DHS)

This short course / 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.

Who Should Attend: 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.