DOE and Test Automation for System of Systems T&E

Larry Harris, Navy SPAWAR PMW-120 APM–T&E
Luis Cortes, MITRE Corporation
Jim Wisnowski, Adsurgo
Darryl Ahner, OSD STAT COE
Jim Simpson, JK Analytics
Bottom Line Up-Front (BLUF)

• Many Programs of Record (PoRs) are improving their individual performance through innovative applications of emerging thrust areas and methodologies – AGILE Testing, Test Automation, Design of Experiments (DOE), and Cyber Security Testing

• Even though the performance of the majority of these PoRs depends on other PoRs, they are not evaluated as a System of Systems (SoS) earlier in the acquisition cycle
Motivation

- **Refocus Developmental Test** on mission end-to-end performance to improve the likelihood of success in Operational Test
- **Optimize test designs** and **increase software test coverage** to obtain the right information at the right price
- **Deliver an integrated and interoperable capability** to the Fleet
- **Leverage the application of emerging thrust areas** for Systems Engineering and Test & Evaluation
- **Demonstrate System-of-Systems (SoS) T&E** concept that integrates thrust areas under a single, comprehensive application
An efficient, disciplined, and informative process that takes advantage of advanced techniques and methods to provide quantifiable results for the verification and validation of technical requirements and operational capabilities
Introduction
Thrust Areas Policy & Guidance

• In addition to the TEMP Guidebook, recent directives require Program Managers to take advantage of innovative, disciplined, effective, and efficient test methodologies to characterize system behavior across an appropriately selected set of factors and conditions

• Design of Experiments – DoDI 5000.02 (2015)
• Modeling and Simulation in T&E – DOT&E Memo
SoS Test Concept
Value and Benefits

- Provides potential reduction in unit and systems level testing (could be as much as 2/3 test times!)
- Provides a scenario based test tool that verifies and validates KPPs, KSAs, other PoR requirements
- Provides more effective and efficient method for certification of systems prior to field deployment
- Reduces variance, cost, and maintenance of systems in the field
- Provides a Lab test environment for future DTs, OA, and OTs
- Lays foundation for future Cyber Security testing, with automation and SoS-level focus
- Serves as baselining event for providing metrics on value of Cyber Built-in ‘vs’ Bolted-on.
- Provides metrics or comparing AGILE ‘vs’ Non-AGILE development and the factors that affect the comparison
SoS Overall Notional Architecture

- Hosted Sys 1
- Hosted Sys 2
- Hosted Sys 3
- Connected Sys 1
- Connected Sys 2
- Connected Sys 3

Primary System

Infrastructure
SoS Notional Architecture
Example 1 - Units With Identical Systems
SoS Notional Architecture
Example 2 - Units With Different Systems

Unit 1
- Subsystem 1
- Subsystem 2
- Subsystem 3
- Subsystem 4
- Subsystem 5

Unit 2
- Subsystem 1
- Subsystem 2
- Subsystem 3
- Subsystem 4
- Subsystem 5

Unit 3
- Subsystem 1
- Subsystem 2
- Subsystem 3
- Subsystem 4
- Subsystem 5

Information Exchange
## DOE Table

### COMMs PoR Example

<table>
<thead>
<tr>
<th>Response Variable</th>
<th>Test Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT-B1/IT-C1</td>
<td>IT-C2/IT-D1/IT-D2</td>
</tr>
<tr>
<td>- Chat Latency</td>
<td>- Chat Latency</td>
</tr>
<tr>
<td>- Data LAN Transfer Timeliness</td>
<td>- Data LAN Transfer Timeliness</td>
</tr>
<tr>
<td>- Common Operating Picture (COP) Timeliness</td>
<td>- COP Timeliness</td>
</tr>
<tr>
<td>- Imagery Display Timeliness</td>
<td>- Imagery Display Timeliness</td>
</tr>
</tbody>
</table>

### Factors | Levels |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Loading</td>
<td>- high &gt;74 percent user CCE devices in use</td>
</tr>
<tr>
<td></td>
<td>- low &lt;51 percent user CCE devices in use</td>
</tr>
<tr>
<td>Enclave</td>
<td>UNCLAS, SECRET, SR, and SCI</td>
</tr>
<tr>
<td>Transmission Type</td>
<td>Super Hi Frequency (SHF) satellite communications</td>
</tr>
<tr>
<td></td>
<td>Hi Frequency</td>
</tr>
<tr>
<td>File Size</td>
<td>Large ≥5 MB medium 1 to 5 MB</td>
</tr>
<tr>
<td></td>
<td>small &lt;1 MB</td>
</tr>
<tr>
<td>Transport Method</td>
<td>upload</td>
</tr>
<tr>
<td></td>
<td>download</td>
</tr>
<tr>
<td>Platform Type</td>
<td>Unit Level</td>
</tr>
<tr>
<td></td>
<td>Force Level</td>
</tr>
<tr>
<td></td>
<td>Subsurface</td>
</tr>
<tr>
<td></td>
<td>MOC</td>
</tr>
<tr>
<td></td>
<td>Aviation</td>
</tr>
<tr>
<td>Air Temperature</td>
<td>As occurs</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>As occurs</td>
</tr>
</tbody>
</table>

- Systematically Vary
- Record
What is Automated Software Test (AST)?

• “The application of automation technology throughout the software testing lifecycle with the goal of delivering capability faster and more affordably.”
  *Innovative Defense Technologies*

• Important aspects of AST
  - Applies to software-only or software-intensive systems and offers alternative to manual testing
  - Requires specialized software to control the input feeds, execution, and data collection of the test
  - There are various levels of automation complexity
  - Automation can be applied in all phases of software development and testing, from unit tests to software integration tests, to functional tests to performance tests
  - The software tools consist of open source and commercial products, that work can operate on the front-end (GUI) and the back-end (objects) of the system
  - Automation capability has both costs (licensing, expertise, automation scripts) and benefits (faster execution, more testing)

• Without automation, testing is limited to what we can do with limited manual testers
Test Automation Simulation and Stimulation

- Stallion
- jBehave
- Sikuli
- Selenium
- TestNG
- JMeter

- Perform VV&A assessment of simulator to ensure realistic and scalable generation of input data that would be experienced in operational environment
- Determine key factors (e.g. volume of message traffic) that would span the space of operational conditions and implement combinations
Cybersecurity T&E in SoS Environment

• Cybersecurity testing is required in most software-intensive systems at both the DT and OT milestones

• Cybersecurity vulnerability assessments and penetration testing can only be effectively performed in a SoS environment

• Cybersecurity testing benefits from a rigorous planning, design, and analysis process
Software SoS Cybersecurity Test Factors and Metrics

**INPUTS**
(Factors)
- Adversary Activity Type
- Adversary Level of Effort
- Defensive Activity
- Adversary Skill Level
- Adversary Access
- Sysop Login Steps
- Number of Users

**OUTPUTS**
(Responses)
- Time to Detect Intrusion/Exploitation
- Time to Mitigate Intrusion/Exploitation
- Vulnerability Severity Category Code
- Time to Restore Mission Capabilities
- Reduction in Mission Effectiveness
Summary and Conclusion

• Focus is on leveraging T&E state-of-the-art practices and inject them software-intensive programs by integrating some key thrust areas in a single SoS application

• DoD services and organizations are making progress in integration testing of linked systems in SoS testing under realistic conditions