Developmental & Cybersecurity Evaluation Framework

Dr. Suzanne Beers & Peter Christensen
The MITRE Corporation supporting DASD(DT&E)

31st Annual International Test and Evaluation Symposium:
T&E to Achieve Better Buying Power 2.0
7 October 2014
Briefing Purpose & Overview

- Developmental Evaluation Framework (DEF) part of TEMP’s SE-V story:
  - How acquisition, technical and programmatic *decisions* will be informed by evaluation
  - How system will be *evaluated*
  - How *test and M&S events* will provide data for evaluation
  - What *resources* are required to execute test, conduct evaluation, and inform decisions

- Cyber Evaluation Framework guides programs through forest of cyber/IA guidance
  - System/software assurance
  - Risk Management Framework
  - Vulnerability Assessment
  - Interoperability
Articulate a logical evaluation strategy that informs decisions

- How acquisition, programmatic, technical and operational decisions will be informed by evaluation
- How system will be evaluated
- How test and M&S events will provide data for evaluation
- What resources are required to execute test, conduct evaluation, and inform decisions

DT&E story thread: decision – evaluation – test & resources
Developmental Evaluation Framework (DEF)

- **Capabilities questions**
- **Decision Support Questions (DSQ)**
  - DEO 1
  - DEO 2
  - DEO 3
  - TM 1
  - TM 2
  - *TM 3

Technical measures

KPP/KSA/CTP - related

System Engineering decomposition:
Evaluate system capability - Inform decisions
# Developmental Evaluation Framework

<table>
<thead>
<tr>
<th>Developmental Evaluation Objectives</th>
<th>System Requirements and T&amp;E Measures</th>
<th>Decisions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Decision #1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DSQ #1</td>
</tr>
<tr>
<td>Functional evaluation areas</td>
<td>Technical Reqmts Document Reference</td>
<td>Description</td>
</tr>
<tr>
<td>System capability categories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td>3.x.x.5</td>
<td>Technical Measure #1</td>
</tr>
<tr>
<td>Performance</td>
<td>3.x.x.6</td>
<td>Technical Measure #2</td>
</tr>
<tr>
<td>Performance</td>
<td>3.x.x.7</td>
<td>Technical Measure #3</td>
</tr>
<tr>
<td>Performance</td>
<td>3.x.x.8</td>
<td>Technical Measure #4</td>
</tr>
<tr>
<td>Interoperability</td>
<td>3.x.x.1</td>
<td>Technical Measure #1</td>
</tr>
<tr>
<td>Interoperability</td>
<td>3.x.x.2</td>
<td>Technical Measure #2</td>
</tr>
<tr>
<td>Interoperability</td>
<td>3.x.x.3</td>
<td>Technical Measure #3</td>
</tr>
<tr>
<td>Interoperability</td>
<td>3.x.x.4</td>
<td>Technical Measure #4</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>PPP 3.x.x</td>
<td>SW Assurance Measure #1</td>
</tr>
<tr>
<td>RMF</td>
<td>RMF Control Measure #1</td>
<td>Cont Assess</td>
</tr>
<tr>
<td>Vulnerability Assess</td>
<td>Vul Assess Measure #1</td>
<td>Blue Team</td>
</tr>
<tr>
<td>Interop/Exploitable Vuln.</td>
<td>Vul Assess Measure #2</td>
<td>Red Team</td>
</tr>
<tr>
<td>Reliability</td>
<td>4.x.x.1</td>
<td>Technical Measure #11</td>
</tr>
<tr>
<td>Reliability</td>
<td>4.x.x.2</td>
<td>Technical Measure #12</td>
</tr>
<tr>
<td>Reliability</td>
<td>4.x.x.3</td>
<td>Technical Measure #13</td>
</tr>
<tr>
<td>Reliability</td>
<td>4.x.x.4</td>
<td>Technical Measure #14</td>
</tr>
</tbody>
</table>

**Identify major decision points for which testing and evaluation phases, activity and events will provide decision supporting information.**

Cells contain description of data source to be used for evaluation information, for example:

1) Test event or phase (e.g., CDT#1, CDT#2, CDT#3, CDT#4)
2) M&S event or scenario
3) Description of data needed to support decision
4) Other logical data source description

---

**Decisions Suppoted**

- **Decision #1**: Performance Capability #2
- **Decision #2**: Performance Capability #1
- **Decision #3**: Interoperability Capability #3
- **Decision #4**: Reliability Cap #2

---

**Resources**

- Define
- Inform
- Data
- Execute

**Schedule**

- Define
- Inform
- Data
- Execute
Sensors, weapons, mission command (MC), and communication networks for the Army Air Defense Artillery (ADA) Future Force
### Decision Support Questions

#### Functional Integration (3.0.2)
**Ready for IOT&E**
(Capabilities demonstrated)

#### Functional Integration (3.1)
**MS-C**
(Capabilities demonstrated or on track)

### Decision Support Questions

**DSQ#1**: Ready to integrate?

**DSQ#2**: Capability performing to include/exclude in SW build?

**DSQ #3**: Capability sufficient for intended use for next phase?

### DEO/Capabilities

**System specification capabilities (3.2.x)**

<table>
<thead>
<tr>
<th>Performance:</th>
<th>Paragraph</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.1</td>
<td>Geodetic Registration</td>
</tr>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.2</td>
<td>Sensor Control</td>
</tr>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.3</td>
<td>Common Tactical Air Picture</td>
</tr>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.4</td>
<td>Estimate Launch and Impact Point Prediction</td>
</tr>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.5</td>
<td>Track Capacity</td>
</tr>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.6</td>
<td>Saturation Alleviation</td>
</tr>
<tr>
<td>3.2 Integration</td>
<td>3.2.2.2.7</td>
<td>Single Integrated Air Picture / Early Warning</td>
</tr>
</tbody>
</table>

### Requirements/Technical Measures

**System Specification sub-capabilities (mix of 3.2.x.x and 3.2.x.x.x to capture capability description at TEMP level of detail)**

### Test events / Data sources

- **CT**: Contractor Test
- **IV**: Integration Event
- **SHWIL**: SW/HW in the Loop
- **Range**: Range/Flight Test
IA Policy Guidance “Shock & Awe”
Cyber EF Roadmap Guides
T&E Path
Cyber EF Roadmap guides program-specific tailoring

- Categories of cyber evaluation
  - System/SW assurance
  - Compliance (C&A, RMF)
  - Vulnerability assessment (Red team, Blue team)
  - Interoperability (NR-KPP)

- Cyber capabilities within each category
- Source documents, examples of measures
- Test activities, data sources
# System & Software Assurance

## Risk Management Framework

**Overarching Developmental Issue**

*Does the system satisfy the specified and derived cybersecurity technical requirements for confidentiality, availability, and integrity; and is the system able to sustain critical mission tasks in a cyber-contested environment?*

| **Issue 1, Systems and Software Assurance** | 
| --- | --- |
| Are the system and the software developed securely? |
| DT objectives evaluate: | Measures Sources: |
| • Software vulnerabilities have been eliminated in critical components (source: CVE, CWE, Common Attack Pattern Enumeration and Classification) | • Software Development Plan |
| • Secure software development processes | • PPP Table 5.3.3.1 (example measures: number/category of SDRs, CVEs eliminated, CWEs remaining) |
| • Secure software development environment | • Information Assurance Strategy or equivalent |
| • Anti-tamper protections implemented | • PPP Appendix D: Anti-tamper plan |
| • Supply chain risks mitigated | • Supply chain risk addressed in PPP Section 5.3.4, in RFP and contracts |

<table>
<thead>
<tr>
<th><strong>Test Activity/Data Sources:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Contractor T&amp;E/ Functional Qualification Testing/ Government ST&amp;E</td>
</tr>
<tr>
<td>• Anti-tamper Implementation Plan/Report</td>
</tr>
<tr>
<td>• Supply Chain Risk Management Report</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Issue 2, RMF Requirements</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system satisfy baseline cybersecurity technical standards?</td>
<td></td>
</tr>
<tr>
<td>DT objectives evaluate:</td>
<td>Measures Sources:</td>
</tr>
<tr>
<td>• Identified attack surfaces</td>
<td>• SAP, DoDI 8510.01, NIST Special Publication 800-53/53A, CNSSI 1253, and cybersecurity acquisition strategy (example measures include percentage of controls verified, number/category of outstanding deficiencies)</td>
</tr>
<tr>
<td></td>
<td>• Include technical standards appropriate for the attack surface</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Test Activity/Data Sources:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• ST&amp;E/ Security Controls Assessor/ ACAs/ vulnerability assessment team</td>
</tr>
<tr>
<td>• Contractor T&amp;E and government technical standard testing as appropriate</td>
</tr>
</tbody>
</table>
## Issue 3, Vulnerability Assessment

<table>
<thead>
<tr>
<th>Do exposed vulnerabilities adversely affect system resiliency?</th>
</tr>
</thead>
</table>

Operational scenarios and critical missions should be based on authoritative sources, including CONOPS and capabilities documents. Representative cyber threats should be developed based upon STARs and cyber-attack scenarios developed by vulnerability assessment teams and approved by appropriate authoritative source. Cyber kill chain as exercised by the adversary includes the following steps: reconnaissance, weaponization, delivery, exploit, control, execute, maintain. Cyber defense in response to adversarial actions includes actions to redirect, obviate, impede, detect, limit, and expose adversarial actions. The lexicon reference is Intended Effects of Cyber Resiliency Techniques on Adversary Activities.

DT objectives evaluate:

- System and supporting networks resilience and ability to disrupt the cybersecurity kill chain
  - Deny and disrupt attacks
  - Degrade attacks
  - Deceive attacks
- Capability to:
  - Detect exploitations
  - Recover from system degradation

### Measures Sources:

- Interoperability metrics and measures should be derived from the NR-Key Performance Parameter (KPP). Measures include:
  - Support military operations
  - Enter and be managed in the network
  - Exchange information
  - Support net-centric military operations.

Cybersecurity metrics and measures may be derived from program technical documentation, or other sources (e.g., the DoD Strategy for Operating in Cyberspace and Resilient Military Systems Cyber Threat Defense Science Board Task Force). The measures below are derived from MP 120053, Rev. 1, *Cyber Resiliency Metrics*, dated Apr 2012. Example metrics include:

- Percentage of cyber resources properly configured
- Number of attempted intrusions stopped at network perimeter/deflected to honeypot
- Percentage of mission-essential capabilities for which multiple instantiations are available
- Length of time between initial disruption and restoration
- Quality of restored data
- Quality of choices made during design and engineering that affect resiliency
- Length of time between initial disruption and restoration.

### Test Activity/Data Sources:

- Assessment: Blue Team has full knowledge and access to the system and all supporting components.
<table>
<thead>
<tr>
<th>Issue 4, System interoperability and functionality in response to exploited cyber vulnerabilities</th>
<th>Is the system sufficiently interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?</th>
</tr>
</thead>
</table>
| DT objectives evaluate:  
- Entry and management on a network  
- Secure exchange of information  
- Support for net-centric military operations  
- Response to exploited cyber vulnerabilities  
- Support for military operations in a cyber-contested environment. | Measures Sources:  
- Interoperability measures derived from capabilities documents, Information Support Plan, integrated architectures, Technical Standards (CJCSI 6212.01F)  
- Cybersecurity measures and scope of Red Team testing will be based on cyber evaluation measures developed during all prior phases, to potentially include threat portrayals and penetration testing. Test Activity/Data Sources:  
- Assessment: Red Team functions as an adversary without knowledge or access to the system. |
Core Teams: Applying Evaluation Framework to Programs

**DEF Core Team**
- Small, focused group of T&E and program acquisition SMEs
  - Chief Developmental Tester, acquisition strategy SME, requirements SME
- Develop DEF by facilitated discussion
  - Decision support questions (DSQ) – T&E generated knowledge needed to inform decisions
  - Developmental Evaluation Objectives (DEO) – system capabilities
  - Technical Measures (TM) – “inch deep-mile wide” quantification of capabilities

**Cyber EF Core Team**
- Small, focused group of T&E, program cybersecurity SMEs
  - Chief Developmental Tester, cybersecurity SME, requirements SME
- Tailor generic Cyber EF roadmap to program specifics
  - Draw metrics from PPP, Anti Tamper (ATP) and Supply Chain Risk Management (SCRM) Plans, Risk Management Framework (RMF)
Summary & Way Ahead

- DEF focuses system evaluation (in mission context) to inform decisions
- Cyber EF guides cybersecurity evaluation

Way Ahead
- DASD(DT&E) is ready, willing, able, and anxious to help your program succeed!
- Contact us for your DEF and/or Cyber EF Core Team