Test Case Design via Model Based Systems Engineering

Marshall Bronston, Col (USAF Ret.)
Professional Research Engineer
Marshall.Bronston@gtri.gatech.edu
520-352-2513
Systems-of-Systems = Complexity

- Methods for efficient cybersecurity test campaign design are needed
- Full mesh interfaces: \( c = \frac{n(n-1)}{2} \)
- Test program change impact mitigation
Agenda

- MBSE in a Systems Modeling Language context
  - Requirements
  - Structure
  - Behavior
  - Parametric
- Cyber security T&E
- Application of MBSE to generate useful and appropriate test cases
- Use of MBSE and its inherent automation to provide linkages and traceability between mission needs, requirements, design, and test activities
Model-Based Systems Engineering

Document-Centric

Model-Centric

Valdez
System Modeling Language (SysML) Views

- **SysML Diagrams**
  - **Structural Diagrams**
    - Block Definition Diagram
    - Internal Block Diagram
    - Parametric Diagram
  - **Behavioral Diagrams**
  - **Cross-Cutting Diagrams**
    - Requirements Diagram
    - Use Case Diagram
    - Sequence Diagram
    - Activity Diagram
    - State Machine Diagram
Behavior - Use Case Diagram Example

- Expected system behaviors
- Provides insight to white/gray/black box testing
- Actor interactions
- Threat/hacker interactions (mis-actor/mis-use)
Specify appropriate venues, instrumentation, red team constraints, etc.
Structural Diagrams – “BDD” Example

- Requirements are allocated to components
- Block Definition Diagram: major parts of an architecture
  - Ground segment
  - Vehicle (1..*)

```
This block definition diagram provides a high level description of critical voice and data elements associated with communications between control elements and the actual TELAR.
```
Structure – Internal Block Diagram Example

End-to-End comm flow/RF chain/Data structures
Behavior – State Machine Example

- Activity
- Sequences
- States
Behavior – Activity Diagram Example
Parametric Diagram - Example

- Inside SysML model – closed form calculations
- Calls to other model environments – optimized for problem type
- Avoids recreating validated models
Linkages and Views

- Diagrams provide views of the model
- Model provides linkages
- Views are tailored to aspects of interest
- Model depth developed to suit the need
- Changes to the model (e.g. manipulate the diagram) reflected in the model
- Broken model elements are highlighted in views
Agenda

• MBSE in a Systems Modeling Language context
  – Requirements,
  – Structure,
  – Behavior
  – Parametric
• Cyber security T&E
• Application of MBSE to generate useful and appropriate test cases
• Use of MBSE and its inherent automation to provide linkages and traceability between mission needs, requirements, design, and test activities
Cyber Security T&E

- Goal: efficient test campaign design
- Stakeholder concern traceability
- Scope test events
  - Objectives
  - Scenarios
  - Instrumentation
  - Red Team
Measurement Decomposition

- Stakeholder concern (e.g. DT, OT) determines scope and focus
- Test construct based on system requirements
- Priorities/risks drive test requirements
Test Scope

- Fidelity
- Depth
- Breadth

It is also okay to mix levels of fidelity among different functional elements in a single execution.

MOP/Technical Performance - Example

System Performance Parameters
- Track Update Timeliness/accuracy
- Number/Type of Tracks
- Common Awareness
- Interoperability of Link feed interfaces
- Effectiveness of Collab. Tasks
- Process Execution Time

Technical Performance Parameters
- Message Latency
- Geographical COP Differences
- # of planned targets
- Alternatives Analyzed
- Interactive/Exchange
- Task Latency
- Effective Bandwidth
- Quality of Service

Fundamentals of Cybersecurity T&E
Agenda

• MBSE in a Systems Modeling Language context
  – Requirements,
  – Structure,
  – Behavior
  – Parametric
• Cyber security T&E
• Application of MBSE to generate useful and appropriate test cases
• Use of MBSE and its inherent automation to provide linkages and traceability between mission needs, requirements, design, and test activities
Test Case

- **Purpose:** specify test requirements
  - Types (Pen, Security, Software Integration Lab, TEMPEST, Anti-Tamper/ Detection, Encryption, Cross Domain, etc.)
  - Environment (cyber range, live network, lab, anechoic chamber, open air range, etc.)

- **Build/manage in model**
  - Often winds up being/looking like a run card
  - Views (run cards, etc.) can be rendered via SysML
  - Can build as a collection of events
  - Consider value of traces/linkages in model

- **Includes:**
  - Required Test Environment/Conditions
  - Steps/procedure: input/expected outcome/”verdict”
# Case Mapping to Create a Test Campaign

## Decisions

Decision points within the program are listed across the top row of the table, with Decision Support Questions that support the decisions defined directly beneath.

## Evaluation

High level evaluation measures are referenced in the far left columns. The evaluation measures are referenced from the Systems Engineering Plan, PPP, and requirements documentation.

## Test

Test events that “feed” the decision are defined in the cells corresponding to decisions, DSQs, and evaluation measures.

## Resources / Schedule

Resources and schedule are defined in the TEMP, linked to decisions and test events included in the matrix.

### Table: Developmental Evaluation Categories

<table>
<thead>
<tr>
<th>Decision 1</th>
<th>Decision 2</th>
<th>Decision 3</th>
<th>Decision 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSQ #1</td>
<td>DSQ #2</td>
<td>DSQ #3</td>
<td>DSQ #4</td>
</tr>
<tr>
<td>DSQ #5</td>
<td>DSQ #6</td>
<td>DSQ #7</td>
<td>DSQ #8</td>
</tr>
</tbody>
</table>

### Functional Evaluation Areas

- **Performance**
  - Capability #1
  - Capability #2
  - Capability #3
  - Capability #4

- **Interoperability**
  - Capability #3
  - Capability #4

- **Cybersecurity**
  - SW/System Assurance
  - RMF
  - Vulnerability Assess
  - Interop/Expansible Val

- **Reliability**
  - Reliability Cap #1
  - Reliability Cap #2

### System Requirements and T&E Measures

<table>
<thead>
<tr>
<th>Performance</th>
<th>Interoperability</th>
<th>Cybersecurity</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.x.1</td>
<td>3.x.3</td>
<td>4.x.1</td>
<td>4.x.1</td>
</tr>
<tr>
<td>3.x.2</td>
<td>3.x.4</td>
<td>4.x.2</td>
<td>4.x.2</td>
</tr>
<tr>
<td>3.x.3</td>
<td>3.x.5</td>
<td>4.x.3</td>
<td>4.x.3</td>
</tr>
<tr>
<td>3.x.4</td>
<td>3.x.6</td>
<td>4.x.4</td>
<td>4.x.4</td>
</tr>
</tbody>
</table>

### Decisions Supported

- Identify major decision points for which testing and evaluation phases, activity and events will provide decision supporting information.
- Each contains description of data source to be used for evaluation information, for example:
  1. Test event or phase (e.g. CERT, ...)  
  2. M&S event or scenario  
  3. Description of data needed to support decision  
  4. Other logical data source description
# Data Supporting Net Ready KPPs

| Document/Architecture | AV-1 | AV-2 | CV-1 | CV-2 | CV-3 | CV-4 | CV-5 | CV-6 | DIV-1 | DIV-1 (OV-7) | DIV-1 (SV-1) | DIV-1 | DIV-2 | DIV-2 (OV-7) | DIV-3 | DIV-3 (OV-7) | DIV-3 (SV-1) | DIV-4 | DIV-4 (OV-7) | DIV-4 (SV-1) | DIV-4 (SV-2) | DIV-5 | DIV-5 (OV-7) | DIV-5 (SV-1) | DIV-5 (SV-4) | DIV-6 | DIV-6 (OV-7) | DIV-6 (SV-1) | DIV-6 (SV-4) | DIV-7 | DIV-7 (OV-7) | DIV-7 (SV-1) | DIV-7 (SV-4) | DIV-8 | DIV-8 (OV-7) | DIV-8 (SV-1) | DIV-8 (SV-4) | DIV-9 | DIV-9 (OV-7) | DIV-9 (SV-1) | DIV-9 (SV-4) | DIV-10 | DIV-10 (OV-7) | DIV-10 (SV-1) | DIV-10 (SV-4) | DIV-11 | DIV-11 (OV-7) | DIV-11 (SV-1) | DIV-11 (SV-4) | DIV-12 | DIV-12 (OV-7) | DIV-12 (SV-1) | DIV-12 (SV-4) | DIV-13 | DIV-13 (OV-7) | DIV-13 (SV-1) | DIV-13 (SV-4) | DIV-14 | DIV-14 (OV-7) | DIV-14 (SV-1) | DIV-14 (SV-4) | DIV-15 | DIV-15 (OV-7) | DIV-15 (SV-1) | DIV-15 (SV-4) | DIV-16 | DIV-16 (OV-7) | DIV-16 (SV-1) | DIV-16 (SV-4) | DIV-17 | DIV-17 (OV-7) | DIV-17 (SV-1) | DIV-17 (SV-4) | DIV-18 | DIV-18 (OV-7) | DIV-18 (SV-1) | DIV-18 (SV-4) | DIV-19 | DIV-19 (OV-7) | DIV-19 (SV-1) | DIV-19 (SV-4) | DIV-20 | DIV-20 (OV-7) | DIV-20 (SV-1) | DIV-20 (SV-4) | DIV-21 | DIV-21 (OV-7) | DIV-21 (SV-1) | DIV-21 (SV-4) |
|-----------------------|------|------|------|------|------|------|------|------|-------|----------|----------|-------|-------|----------|-------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|-------|----------|----------|----------|
| DCR                   | 1    | R    | R    | R    | R    | R    |    |    |   | R       |         |       |       |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |
| CONOPS                | 1    | R    | R    | R    | R    | R    | R  | R  | R    | R       |         |       |       |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |
| ICD                   | 1    | X    | R    | R    | R    | R    | X  | X  | X    | X       |         |       |       |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |
| CDD                   | 1    | X    | X    | X    | X    | X    | X  | X  | X    | X       |         |       |       |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |
| CPD                   | 1    | X    | X    | X    | X    | X    | X  | X  | X    | X       |         |       |       |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |
| IC^3.4                | X    | X    | X    | X    | X    | X    | X  | X  | X    | X       |         |       |       |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |          |          |       |

**Legend**

- **X** - Required
- **O** - Optional
- **R** - Recommended,
- PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs. (e.g., HQDA requires the SV-10c, USMC requires the SV-10a and SvcV-8).

**Note 1**
The AV-1 must be registered, must be “public” and “released” at the lowest classification level possible in DAKS for compliance.

**Note 2**
The technical portion of the StdV-1 and StdV-2 are built using OCO-F DISR standards profiling resource and, within six months of submitting JCIDG documentation, must be current and published for compliance. Use of non-mandated DISR standards in the StdV-1 must be approved by the PM or other duly designated Component cognizant official and documented by a waiver notification provided to the DoD CIO.*

**Note 3**
Intelligence Community (IC) requirements IAW the IC Enterprise Architecture Program Architecture Guide and development phase which clarifies the IC Policy Guidance 801.1 Acquisition.

**Note 4**
Service Views (SvcV) only

**Note 5**
1. The Sponsor* and the Program are jointly responsible for the AV-1, AV-2, CV-1, CV-2, CV-3, CV-4, CV-5, CV-6, SV-6 or SvcV-7.
2. The Sponsor* is responsible for the development of the architecture data for the OV-1, OV-2, OV-4, OV-5a, OV-6c, DIV-2, and the SV-6 or SvcV-6.
3. The Program is responsible for the development of the architecture data for the DIV-1, DIV-3, OV-3, OV-5a, OV-6a, PV-2, SV-1 or SvcV-1, SV-2 or SvcV-2, SV-4 or SvcV-4, SV-5a or SvcV-5, SvcV-10a, SvcV-10b, SvcV-10c, StdV-1, and StdV-2. * Operational user (or representative).

**Note 6**
The NR-KPP Measures data is captured in the SV-7 or the SvcV-7.

---

*MBSE in SysML Supports Document Rendering*
Agenda

• MBSE in a Systems Modeling Language context
  – Requirements,
  – Structure,
  – Behavior
  – Parametric
• Cyber security T&E
• Application of MBSE to generate useful and appropriate test cases
• Use of MBSE and its inherent automation to provide linkages and traceability between mission needs, requirements, design, and test activities
Test Data Analysis

- MBSE applied to test cases provides structured traceability
- Test case inputs and outputs feed forward to results
- Test cases and events translate laterally (event mapping)
- Test events and activities can enable vertical model integration
- Enables correlated analysis
- Analysis easily traced backwards to requirement and mission need/impact

Typical Concerns
- Movement
- Network
- Time
- Context: Uses, Emergent Behaviors, Valuations
Limitations of this Approach

- Valid well-documented Requirements and Boundaries
- Clear direction to test
- Well-trained/educated test force
- Established enterprise processes in-place
- Sufficient SUT maturity (“as tested” baseline exists)
- Flow follows NIST/Cybersecurity T&E Guidebook
- Baseline T&E follows design & developmental iteration
- Complexity of Test Requirement is sufficient to warrant this approach
Benefits of Approach

• Deals test method complexity
• Allows for library of tests/ontologies that can be re-used
• Many are already doing something similar, automate where complexity itself creates test validity risk
• Automate traces and linkages, especially for complex test campaign data collection: flaws “glow in the dark”
• Maps well to hypothesis, useful to validate model approach
• Allows analysis trace: event → outcome → requirement → need
• Natural flow supporting results analysis
• Top-down view establishes purpose and context
• Excellent communication device, swift means to maintain team continuity
• Permits apples-to-apples comparisons in a manner understandable to decision makers and test teams – repeatability
Summary

- Cybersecurity is naturally complex
- Complexity requires a systems approach
- Threat diversity forces need for systematic test & evaluation methods
- Model-Based Systems Engineering tools provide extensible views
- Automation via SysML is one way to structure clerical functions
- Maintain context of the event vs test campaign
- Tests support informed decision-making
References Cited

- DoD Cybersecurity Test and Evaluation Guidebook V1.0, 1 July 2015.
- “Team TELAR” SysML model, PMASE ASE 6005 Student Project, GIT, 2011.
- Register, A. “Fidelity Resolution and Accuracy”, GT PMASE course, spring 2010.
Artifacts and Events Mapped to the Acquisition Life Cycle

Cybersecurity T&E Guidebook