Using Modern System Engineering Methods for Resilient Cyber Design & Test

ITEA 6\textsuperscript{TH} CYBERSECURITY WORKSHOP (2018)

Frank Alvidrez  Spectrum Inc.
The Threat has expanded exponentially
Cyber-resiliency is like Aircraft Survivability
  - It is better to be designed in than added later
  - It’s a new paradigm of software, systems design & testing
Cyber Requirements are critical for programs success
Cyber Measures are difficult to define & test for Systems
Enterprise Architectures & System Engineering (MBSE) are critical to cyber-resiliency design & test
Sun Tzu and Cybersecurity

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle”

- Sun Tzu, Art of War Chapter III, Attack by Stratagem

Sun Tzu and Cyber War – Kenneth Geers NCIS CCD COE

Slide 3
Cybersecurity MindMap

- Summary
- Introduction
- Cybersecurity Testing
- Cybersecurity Design
- Cyber Governance Domain
- Cybersecurity Domain
- Cyber Threat Domain
- Cyber Security & INCOSE "V"
For This Presentation

- Model Used – MagicDraw 18.5
- Mac OS High Sierra V10.13.2
- Perspective – DoDAF/UAF Architect
- MBSE – SysML 18.5 SP1
- UPDM 3 (w/ Unified Architecture Framework – UAF)
- DARPA J-UCAS Initial Project Description (Public Knowledge)
- Governance – USG Cybersecurity (Public Knowledge)
- Model Available on Request (frank.alvidrez@sptrm.com)
- Mind Mapping Software – Mindjet MindManager v10.5
Cybersecurity Domain

- DoD 8500 Series
- Information Assurance
- CVPA/AA
- ISO 27001
- ES C2M2
- ISO/EIC 15408
- DoDAF v2
- Intrusion Testing
- SSOA
- Cybersecurity Framework
- ISO 51288
- NCSD
- CMMI
- Malware
- Ransomware
- DIACAP
- DoD 5000 Series
- ISA-99
- RMF
- Control system security
- Info Security
- NIST
- CERT
- JCIDS
- CERT
Cybersecurity Domain Model
CYBERSECURITY THREAT DOMAIN
Cyber Threat Types

- ADVANCED PERSISTENT THREAT
- Trojan Horse
- Malware
- Spyware
- SQL Injection
- Cross-site Scripting
- Evesdropping
- Viruses
- Spoofering
- Social Engineering
- Worms
- Phishing
- Denial of Service (DOS) Attack
- Distributed DDOS
- Sabotage
- Logic Bomb
- Collateral Damage
- Spear Phising
- Pharming
- Whaling

Source: Itlaw.wikia.com
CYBERSECURITY GOVERNANCE DOMAIN
Cybersecurity Domain Model

Slide 11
Governance Domain

Committee on National Security Systems (CNSS)

US National Cybersecurity

Defense

Intelligence

Law Enforcement

Civil

International Standards

Governance
Risk Management Framework (RMF) Process NIST 800-37 rev. 1

Source: Guide for Applying the Risk Management Framework to Federal Information Systems
Security Control Assessment (RMF) vs Cyber T&E Guidance (Review)

DoDI 8500.01
DoDI 8510.01
DoDI 5000.02
AFI 99-103

DOT&E Memo, Aug 2014

Technical Spec Compliance
Operational Requirements

T&E

Security Control Assessment (RMF Efforts)

DT & OT Cyber Test

Source: AFMC Draft T&E Cyber Capability Requirements Course
NDAA FY 2016 – Section 1647

• National Defense Acquisition Act of 2016
• Implements a number of acquisition reforms to enhance cybersecurity
• Section 1647 requires the evaluation of cyber vulnerabilities of all major DoD programs by the end of 2019
• DoD’s priority list for programs to be evaluated and reported on.

Source: DOT&E FY16 Cybersecurity
Operational Cybersecurity Testing Governance

- For DoD – DOT&E Guidance (Aug 2014)
- Cooperative Vulnerability & Penetration Assessment
- Adversarial Assessment
- Test & Evaluation Master Plans (TEMPS)
- Operation Test Plans
- Test Reports.

“The DOD acquisition process must deliver systems that provide secure, resilient capabilities in expected operational environment. Operational testing must examine system performance in the presence of a realistic cyber threat.” - Dr. Gilmore, Director DOT&E
CYBERSECURITY RESILIENT DESIGN & TEST DOMAIN
INCOSE SE – “V”
Development of a
Cybersecurity Blue Book

- Key planning document to identify the “enterprise” cybersecurity landscape (using UAF, DoDAF, Zachmann, MBSE, etc. toolsets)

- Updated and living document

- Provide background, threat, vision, operation context, and at least the following views:
  - CV-1, CV-2, OV-1, OV-2, OV-3, OV-4, OV-5a, OV-5b (with swimlanes) OV-6c, SV-1, SV-2, SV-4, DIV-1, DIV-2, DIV-3 along with selected SysML products (Use Cases, Requirements Diagrams, Test Cases, etc.)

- Use throughout the acquisition process and testing (DT & OT)
DARPA J-UCAS Example Model

- Source: DARPA Archive J-UCAS public release
- Updated for demonstration purposes only
- Initial Requirements from DARPA “Operationalized” System
- Advanced capabilities in Autonomous Operations
- Initial Program Boeing X-45C & Northrop Grumman X-47B
- Common Operating System
- Carrier Suitable, ISR, SEAD, Penetrating, Persistent UCAV
DARPA J-UCAS OV-1

- Dangerous Missions – Denied Airspace
- Survivable Air Vehicles
- Advanced Sensors & Weapons
- Network-Centric Architecture
- Distributed Command & Control
- Intra-operable Platforms
- Collaborative Operations
- Land or Sea Based System
- Global Operations
RF Spectrum

Mission Planning & Weapons

OFP Distribution & Maintenance

Weapons & Employment

Cyber Test Boundaries

Cyber Areas of Concern
Mission, Hazards and Losses – an overview

- **Mission** is what your system is designed to do.
- **MEFs** are the essential actions required for execution.
- **Losses** prevent successful MEF from happening.
- **Hazard** is the condition that drives the loss.

You’ll build a model that will help you determine what information could cause your hazards.

**TEST TO THAT**
# Failure Mode Analysis - FMEA

<table>
<thead>
<tr>
<th>#</th>
<th>Id</th>
<th>Name</th>
<th>Classification</th>
<th>Item</th>
<th>Failure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>F-6</td>
<td>Systems Check Failure</td>
<td>electrical</td>
<td>J-UCAS ACFT SYSTEMS</td>
<td>Aircraft Systems Fail</td>
</tr>
<tr>
<td>2</td>
<td>F-4</td>
<td>Failure to Connect</td>
<td>electrical</td>
<td>CV Mission Control System</td>
<td>Fail to Connect to CV</td>
</tr>
<tr>
<td>3</td>
<td>F-1</td>
<td>Mission Plan Failure</td>
<td>software</td>
<td>Mission Planning System</td>
<td>Loss of Mission Planning</td>
</tr>
<tr>
<td>4</td>
<td>F-2</td>
<td>Failure to Start</td>
<td>mechanical</td>
<td>Propulsion</td>
<td>Propulsion Sys Fail</td>
</tr>
<tr>
<td>5</td>
<td>F-3</td>
<td>Failure to Launch</td>
<td>electrical</td>
<td>J-UCAS ACFT</td>
<td>Systems Failure</td>
</tr>
<tr>
<td>6</td>
<td>F-5</td>
<td>Failure to Load Weaps</td>
<td>mechanical</td>
<td>Weapons</td>
<td>Weapons Check Fail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Effect Of Failure</th>
<th>Final Effect Of Failure</th>
<th>SEV</th>
<th>Cause Of Failure</th>
<th>OCC</th>
<th>Prevention Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual System Fail</td>
<td>CV OPS Fail</td>
<td>4</td>
<td>Hydraulic Subsystems Failure</td>
<td>1</td>
<td>Sub-sys Maint &amp; IBIT</td>
</tr>
<tr>
<td>Connection Not Established</td>
<td>CV OPS Fail</td>
<td>4</td>
<td>Electrical Subsystem Failure</td>
<td>3</td>
<td>Comm Sys Maint &amp; IBIT</td>
</tr>
<tr>
<td>Mission Plan Delay</td>
<td>Mission Plan Fail</td>
<td>4</td>
<td>Malware Attack</td>
<td>2</td>
<td>Cybersecurity Monitoring Software</td>
</tr>
<tr>
<td>Fail to Start</td>
<td>CV OPS Fail</td>
<td>4</td>
<td>Propulsion Subsystem Failure</td>
<td>2</td>
<td>Propulsion Sys Maint &amp; IBIT</td>
</tr>
<tr>
<td>Launch Delay</td>
<td>CV OPS Fail</td>
<td>4</td>
<td>Launch System Failure</td>
<td>1</td>
<td>Launch Systems Maint &amp; IBIT</td>
</tr>
<tr>
<td>Weapons Not Loaded</td>
<td>CV OPS Fail</td>
<td>2</td>
<td>Weapons Subsystems Failure</td>
<td>2</td>
<td>Weaps Sys Maint</td>
</tr>
</tbody>
</table>
OV-5 Activity Hierarchy

Free Form Operational Taxonomy

- Conduct Mission Planning
  - Download Threat Data
  - Download WX Data
  - Generate Keep-out Zones
    - Select Target
    - Input Weapons Data
    - Generate Mission Module
Attributes of a Good Requirement

• **Must be verifiable (testable)**
• Must be unambiguous
• Must be traced (stakeholders) & traceable (derived from)
• Concise (no additional information is needed)
• Must be complete
  ─ Contain all of the possible conditions
• Expressed in terms of needs vice solution (design independent)
  ─ Address the “who” or “what’ and not “how”
• Must be consistent with other requirements
• Must be at the appropriate level of system hierarchy
Organizing Requirements by Package
Detailed Requirements Diagram

- **J-U CAS Requirements**
  - Id = "1"
  - Text = "The J-U CAS Shall be a CV, Capable, Long Range, Autonomous, Survivable, Penetrating, Cyber-Secure, ISR Maritime Combat Asset"

- **Aero Performance**
  - Id = "9"
  - Text = "The J-U CAS Shall be capable of loitering for 2 hours at a range of 1000 NM and return without air refueling"

- **Carrier Suitability**
  - Id = "9"
  - Text = "The J-U CAS Shall be able to operate from a standard USN CV in a normal operational environment without disruption of the normal deck sequence"

- **Survivability**
  - Id = "10"
  - Text = "The J-U CAS Shall be able to survive in a defined 2020 Anti-Access/Area Denial (A2/AD) Environment"

- **Autonomy**
  - Id = "11"
  - Text = "The J-U CAS Shall be a CV, Capable, Long Range, Survivable, Penetrating, Secure ISR Maritime Combat Asset"

- **Surveillance**
  - Id = "12"
  - Text = "The J-U CAS Shall be able to provide real time beyond line of sight (BLCS) surveillance of maritime and land based targets and provide target quality imagery for decision makers"

- **Cyber Resiliency**
  - Id = "13"
  - Text = "The J-U CAS System Shall be able to operate in a secure, protected and robust Cyber-Resilient Environment"
Detailed Cyber-Resiliency Requirements
Detailed Cyber Resiliency Example

**Detailed Cyber Security Operational Test**

**BLUE TEAM**
- **Blue Team Cooperative Test**

**RED TEAM**
- **Red Team Adversarial Test**

**BLUE TEAM**
- **Requirement**
  - J-UCAS Requirements
  - Id = "1"

**RED TEAM**
- **Requirement**
  - Cyber Resiliency
  - Id = "13"
  - Text = "The J-UCAS System Shall be able to operate in a secure, protected and robust Cyber-Resilient Environment."

**Requirement**
- Mission Planning
  - Id = "13.3"
  - Text = "The Risk to Mission Essential Functions (MEFs) Shall be LCW from the Cybersecurity Threats from the Mission Planning System."

**Rationale**
- Generally Performed to Support M/S C
Enterprise Cyber Team & Possible Test Locations

Test Team – CVPA/AA

- DoD Approved Blue Teams
- DoD Approved Red Teams
- Other DoD Testing Organizations
- DOD&E Representative Operational Organization (AFOTEC)
- Local Test Organization

Possible Test Locations

- Operational Bomber Wing
- USAF Test Center
- Bomber Contractor
- Bomber Depot
- Bomber Hardware in the Loop (HILT) Lab
SUMMARY

- Cybersecurity is a growth industry
  - Threats are outpacing the trained workforce
  - Not limited to DoD
  - Threat Actors are Adapting
  - Campaigns are well funded
- Cyber Resiliency needs to be designed in
- Enterprise Architectures and advanced SE techniques are critical to protecting the Enterprise
- Cyber Testing is difficult but doable.
Thank You