Framework for testing Airborne Cyber Physical Systems in Contested Cyber Environments

Noel Zamot
Col (Ret) USAF

Presented at:
31st Annual International Test and Evaluation Symposium:
T&E to Achieve Better Buying Power 2.0
Oct 6 - 9 ~ Arlington, Virginia
Abstract

- Test and Evaluation (specifically, flight test) of Cyber Physical Systems (CPS, specifically air vehicle centric) in contested cyber environments presents challenges that are not currently addressed by traditional approaches. Traditionally, manned and unmanned air vehicles and their associated systems have focused on flight sciences (performance and flying qualities, or P&FQ) and recently, mission systems (evaluation of radars, sensors, EW, human machine interfaces, etc.). These approaches have historically focused on specific compliance or system characterization on one end (Developmental Test and Evaluation, or DT&E), or mission functionality/effectiveness on the other (Operational Test and Evaluation, OT&E). There has to date been no framework that enables flight test professionals to develop experiments that test the most critical aspects of a system in a contested cyber environment. This presents an unfortunate situation where as systems get more complex and more susceptible to undocumented / unknown threats, the frameworks to test these systems provide less information to make sound assessments on whether they meet mission requirements. When these systems enter OT&E or achieve Initial Mission Capability (IMC), they are often woefully unprepared to survive and operate in typical contested cyber environments.

The framework presented in this paper/presentation seeks to provide a process by which a tester can characterize a system, understand information flow, identify key threats and their associated risks, and design experiments to characterize system performance in a contested environment under the identified threats. The framework was developed in cooperation between the Air Force Research Laboratories Information Directorate and the USAF Test Pilot School. It builds upon the Observe-Orient-Decide-Act (OODA) model, combining situational awareness and cyber operations discipline from AFRL with risk assessment and design of experiments approaches from USAF TPS. The approach builds upon understanding and characterization of the system under test (SUT); the information lifecycle; the fractal nature of threats with respect to the boundary of the SUT; an established model of risk applied to cybersecurity; and the manipulation of information to create experiments that will stress the targeted portions of the system.

The resulting framework is optimized for testing federated CPS, specifically those with a measure of human input, and is not limited strictly to air vehicles. Although the framework was not designed for evaluating Internet Protocol (IP) based systems, it is adaptable for evaluating cases where information is at risk of manipulation. Future work, incorporation of specific tools, and framework development could enhance the framework.

Simply Put:
How do you think about testing complex CPS in contested cyber environments?

What if your CPS is, or is on, an aircraft?

Can I do it smartly and save money?

Early testing of CPS in contested environments can yield significant lifecycle cost savings by enabling the most critical vulnerabilities to be addressed early in the system lifecycle.
Agenda

- Background – why did we develop this? Why do we care?
- Creating the Framework: Adapting OODA
- A brief story
- Thoughts and a way ahead

If at the end of the presentation the mood is “Gee, that’s pretty straight forward. Anyone could’ve thought of THAT”...

MISSION ACCOMPLISHED
Why should I care?

• When discussing systems testing in contested environments. . . Precedent is thin
  – Software T&E, DevTest ≠ Systems test in contested environments

• An enormous amount of work is spent on layer 5 of the OSI model
  – Network testing ≠ Systems test in contested environments

• Discussions on CPS performance in contested cyber environments usually addresses
  – Spec compliance
  – Test “governance”
  – DevTest of sub components
  – Inadequate operational testing
  – Or “All of the Above” (which ≠ Systems test in contested environments)

• Much discussion about component testing, but little discussion on why and how specific areas should be tested.

• What should I test? Why? How?
Background

- 2010: USAF TPS develops “Cyber Systems Test” course
  - USAF Mission: Air, Space, Cyberspace
  - TPS taught Air & Space

- TPS collaborates with AFRL Information Directorate

- Course developed 2011-2012

- Class 11B: First class taught
Creating the Framework

- **Objective:** Develop a way of thinking - don’t direct a (convoluted) process
- **Focus on how testers think**
  - Find vulnerabilities, understand threats, prioritize risk, and design experiments
  - Two inviolable rules of flight test (FTEs know these):
- **Make it straightforward and easy to implement**
- **Don’t reinvent the wheel**

\[
IQ_{\text{gear up}} \propto IQ_{\text{ground}} \div 2
\]

\[
IQ \approx \text{Time to test point (in seconds)}
\]


Some interesting quotes

• “Had I done this in Academia, it would’ve taken me 18 months and we would’ve gotten nowhere.”
  • Unnamed Sr. Scientist for Info Assurance for World Famous Air and Space Force

• “This [approach] is not being taught anywhere else in the world – it is quite probably the first of its kind”
  • Same unnamed Sr. Scientist

• “Why don’t we apply this to everything we test?” [20 second pause]
  “Oh, wait – we already do. . .”
  • Chief Test Pilot, USAF Test Pilot School

• “Why do I have to worry about teaching cyber testing? I’d rather focus on P&FQ [performance and flying qualities].”
  • Master Instructor at USAF TPS
OODA approach to Systems Test

**OBSERVE**

*What does the System do?*

Systems Engineering
Vendor / Program Office
User / Operator

**ACT**

*What Experiment do I design?*

Effects Based
Manipulation of Information
Test Planning / Provisioning

**DECIDE**

*What is the biggest risk?*

Updated Risk Model
Threat vs. Vulnerability
Internal vs. External?

**ORIENT**

*How does the Information flow?*

Information Lifecycle
Fractal nature of Information
Learn by Doing: Let’s follow a notional example

What if...
You had to test integration of two COTS products for potential use in contested cyber environments?

In no way making any statement on any of these systems – only playing a hypothetical “What if?”

From www.scorpionjet.com/gallery
Observe: What does the system do?

- **Objective:** What does the system do?
- **Skills/tasks:** Systems engineering, architecture, WBS
- **Stakeholders:** vendors, program office, users, operators
- **Key issues / questions to ask:**
  - First off, what boxes?
  - Where do I draw the box?
  - Once I draw it, what goes in and out? *What goes through my boundary?*
Orient: How does the information flow?

• Lifecycle of information
  1. Generation (Sensors)
  2. Processing
  3. Storage
  4. Communication / transmission
  5. Consumption (CAOC, users, analysts, weapons)
  6. Destruction
     » It is REALLY hard to destroy information

• Usually, the limiting factor is transmission

• What flow do I worry about?
  – Internal. . .
  – . . . Or External?
Fractal Nature of Information Flow

• “An internal threat at a higher layer becomes an external threat at a lower layer” – Dr. K. Jabbour

• Works not only in a federated system. . .

• . . . But also with the OSI model
Decide: What is the biggest threat?

- The judgment call of the process
- What are your vulnerabilities based on that information flow?
- What is the threat?
- What is the risk? (This defines “contested”, btw)
- Risk impact = Probability x consequence
- For us, Probability = Threat x Vulnerability
Back to our NOTIONAL example

<table>
<thead>
<tr>
<th>Path</th>
<th>Vuln</th>
<th>X Threat</th>
<th>= Prob</th>
<th>Consequence</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus Traffic</td>
<td>MED Weak EMIC, shielding</td>
<td>MED/LO Low ERP, directional, structured</td>
<td>MED/LO</td>
<td>Internal messaging errors: Mission Degrade</td>
<td>Med</td>
</tr>
</tbody>
</table>

The concept of a Risk Register, *correctly developed*, will guide your decision on WHAT to test.
Finally. .! Act

• So, now you know WHAT to test. . HOW do you test it?
• How do you adapt / manipulate information?
• Use the “D5” model to develop your “FTT”
• Determine objectives, then design the test.

*This is where test professionals are most comfortable*
Finally, we design an experiment

- **Test Objective:** “Determine datalink **system performance** (to include time stamped loss of signal, bus BER, network sync error, etc.) **in the presence of Ku band interference and/or smart (e.g., DRFM) jamming** under operationally relevant flight conditions . . .

- Emitter should operate at -10 deg / +40 deg waterline, with ERP at system aperture 6dB over notional Ku band downlink.
- Emitter waveforms should include . . .
- Effect duration should last from . . .
- Data collected should include . . .
Does this work? A Brief Story

• A student familiar with cargo aircraft that can drop with precision.
• . . . 4 minutes during class break.
• . . . Makes the news.
• . . . And the SPO finds out

• THEN it gets interesting.
Limitations

- The framework does not design your test - it informs you of where to best spend resources to design your test.
- Be careful when using this in an IP based scenario.
- Single pass application will not be very useful (similar to the other disciplines of flight test);
Limitations

- The framework does not design your test - it informs you of where to best spend resources to design your test
- Be careful when using this in an IP based scenario
- Single pass application will not be very useful (similar to the other disciplines of flight test);
- Your framework will only be as good as the focus you put on the "two O's" (Learn what the system does, and deeply understand what the information does);
Limitations

- The framework does not design your test - it informs you of where to best spend resources to design your test
- Be careful when using this in an IP based scenario
- Single pass application will not be very useful (similar to the other disciplines of flight test);
- Your framework will only be as good as the focus you put on the "two O's" (Learn what the system does, and deeply understand what the information does);
- The risk equation likely needs some third party involvement so you retain credibility and rigor;
- A D5 effect that does not resemble (or build on, or augment) a threat of interest may give your test incomplete information.
Summary

• Testing CPS (specifically, airborne systems) in contested cyber environments requires a disciplined approach
• Adapting existing frameworks yields a simple, robust heuristic that can guide decision-making
• Become familiar with BFO concepts like:
  Information lifecycle
  Fractal nature of information flow
  Nuanced risk analysis
  Manipulation of information during experiments
• Once you have thought through WHAT and WHY you should test, (only then) should you focus on HOW to test

Disciplined thinking before you bend metal or burn resources
Usually ends up saving a ton of money
QUESTIONS