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 spec compliance or system characterization on one end (Developmental Test and Evaluation, or DT&E), or mission functionality/effectiveness

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

From www.edwards.af.mil/shared/media

http://www.edwards.af.mil/shared/media

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 straight forward and easy to implement
- Don't reinvent the wheel

$$IQ_{gear\ up} \propto IQ_{ground} \div 2$$

$$IQ \approx \text{Time to test point } \textit{(in seconds)}$$

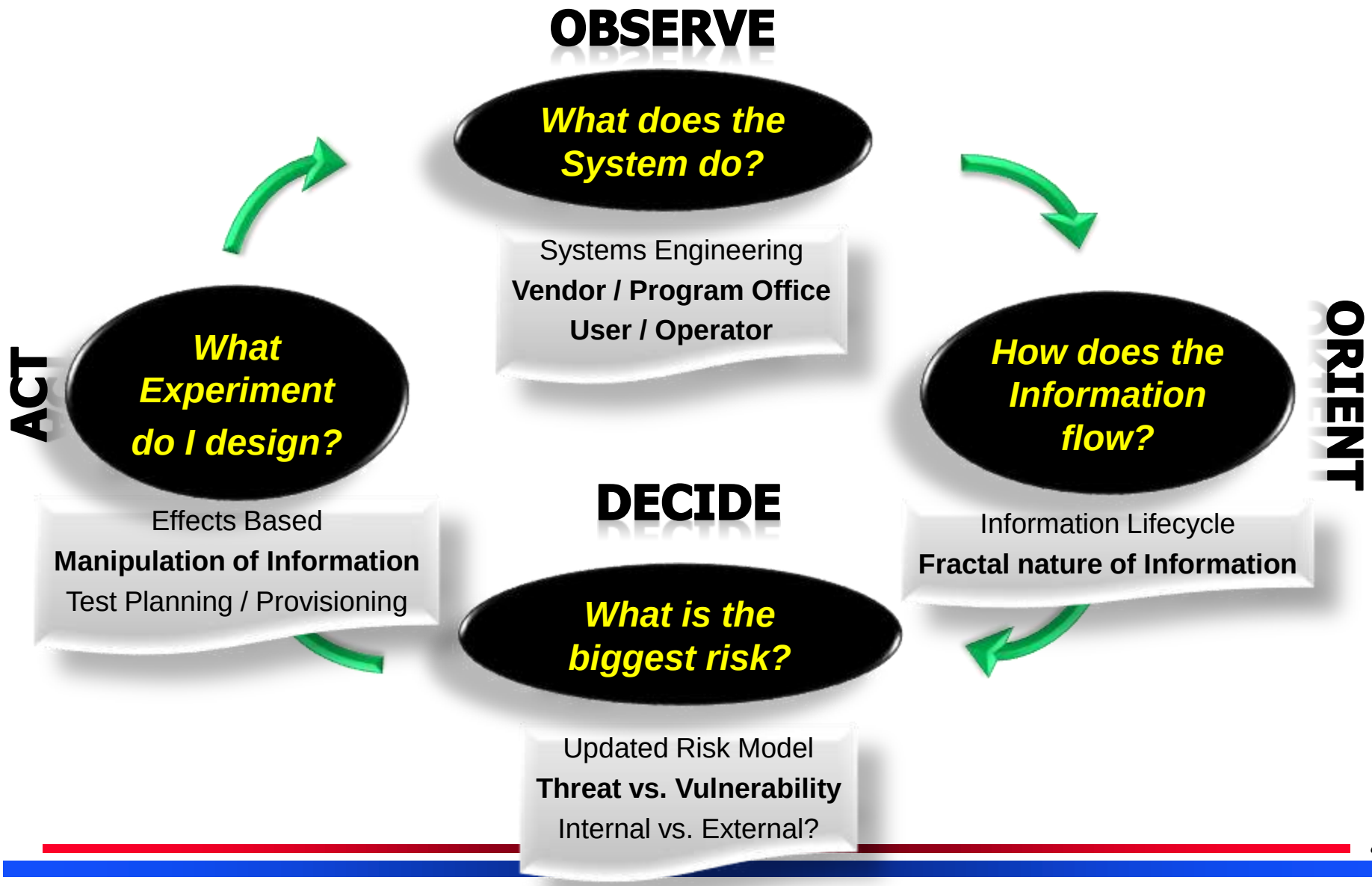
http://www.michaelcovel.com/wp-content/uploads/2013/

http://newsoffice.mit.edu/2009/ratti-copenhagen-1216

Some interesting quotes

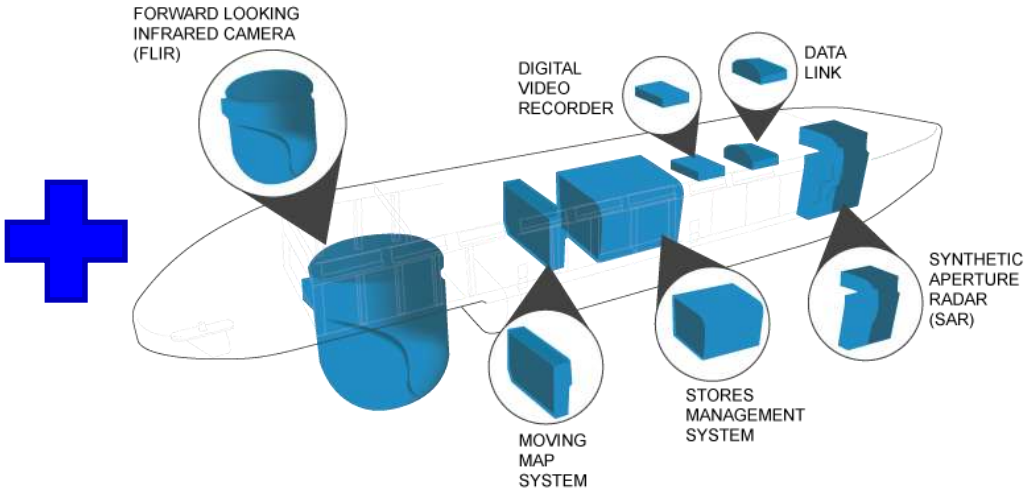
- "Had I done this in Academia, it would've taken me 18 months and we would've gotten nowhere."
  - Unnamed Sr. Scientist for Info Assurance for World Famous Air and Space Force
- "This [approach] is not being taught anywhere else in the world – it is quite probably the first of its kind"
  - Same unnamed 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



Learn by Doing: Let's follow a notional example

From www.scorpionjet.com/gallery

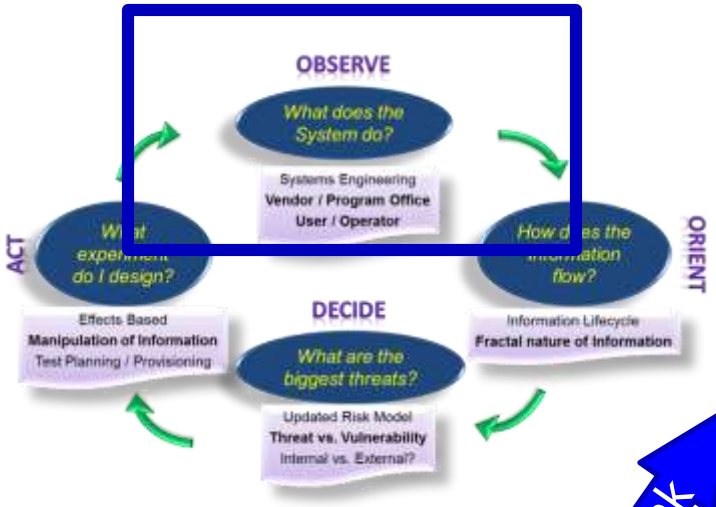


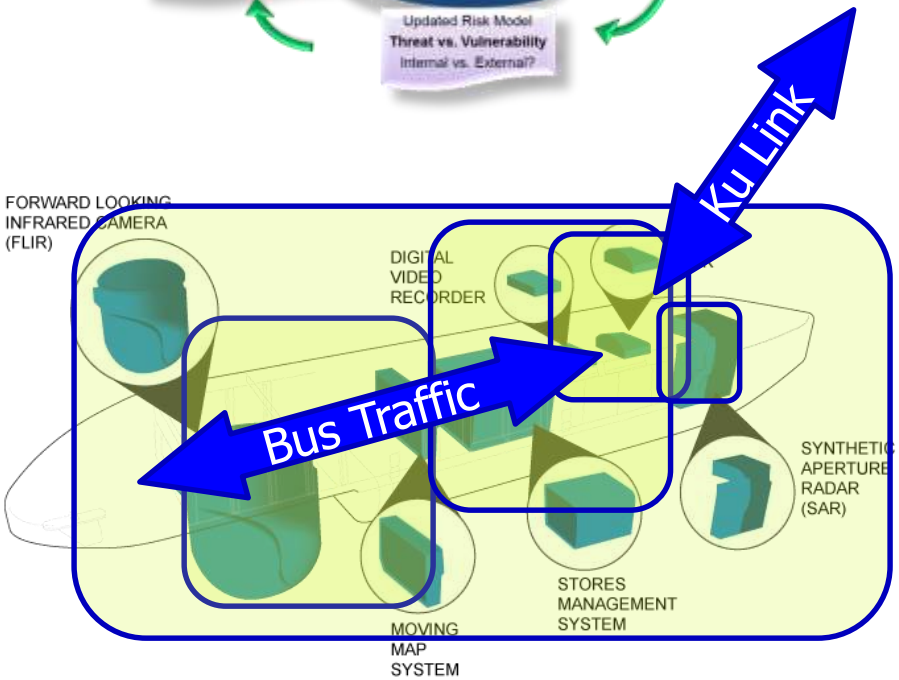
What if. . .
You had to test integration of two COTS products for potential use in contested cyber environments?

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

Observe: What does the system do?

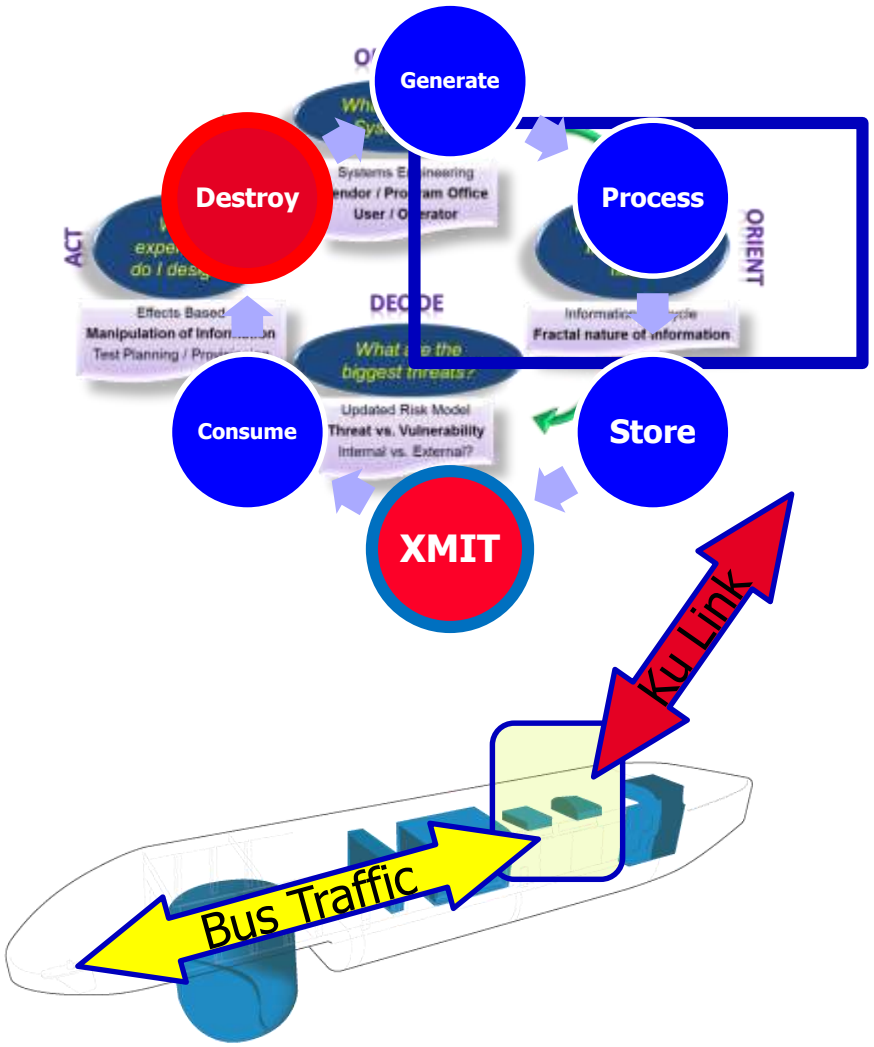
- Objective: What does the system do?
- Skills/tasks: Systems engineering, architecture, WBS
- Stakeholders: vendors, program office, users, operators
- Key issues / questions to ask:
  - First off, what boxes?
  - Where do I draw the box?
  - Once I draw it, what goes in and out? *What goes through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





Orient: How does the information flow?

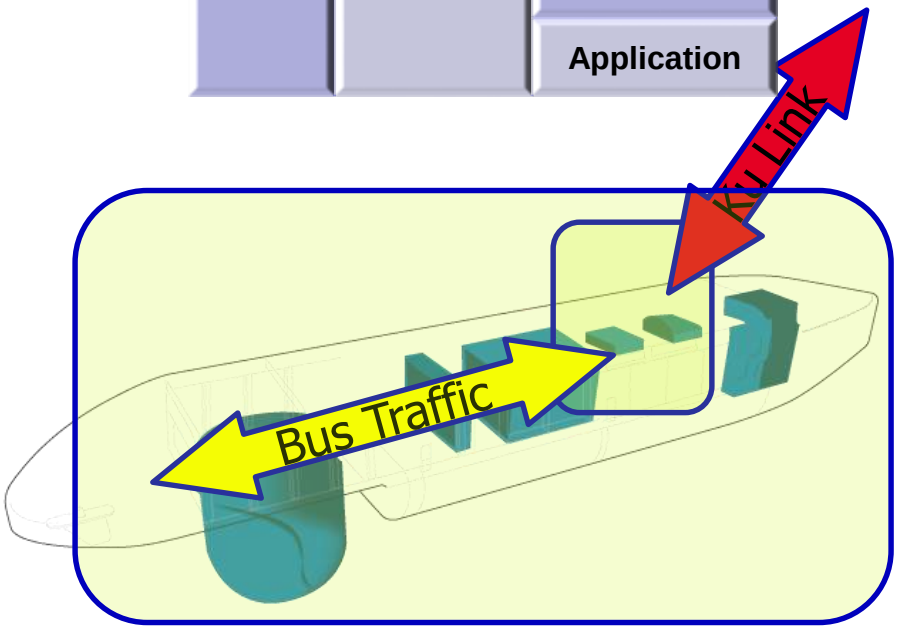
- Lifecycle of information
  1. Generation (Sensors)
  2. Processing
  3. Storage
  4. Communication / transmission
  5. Consumption (CAOC, users, analysts, weapons)
  6. Destruction
     - » It is REALLY hard to destroy information
- Usually, the limiting factor is transmission
- What flow do I worry about?
  - – Internal. . .
  - – . . . Or External?



Fractal Nature of Information Flow

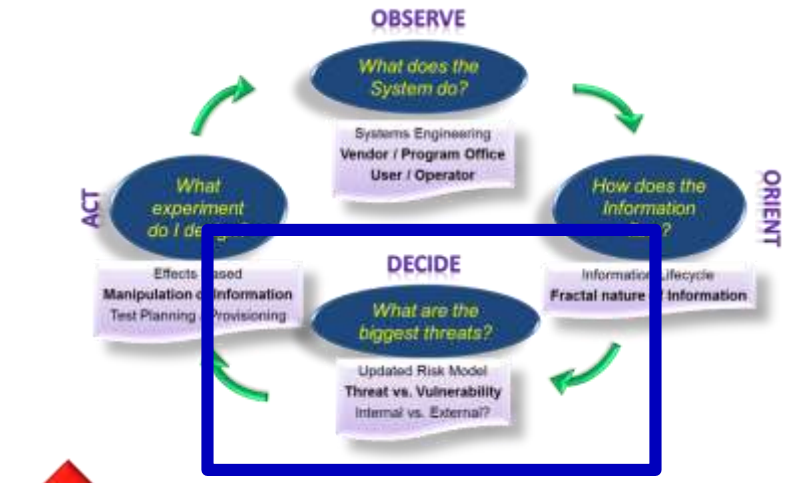
- "An internal threat at a higher layer becomes an external threat at a lower layer" – Dr. K. Jabbour
- Works not only in a federated system. . .
- . . . But also with the OSI model

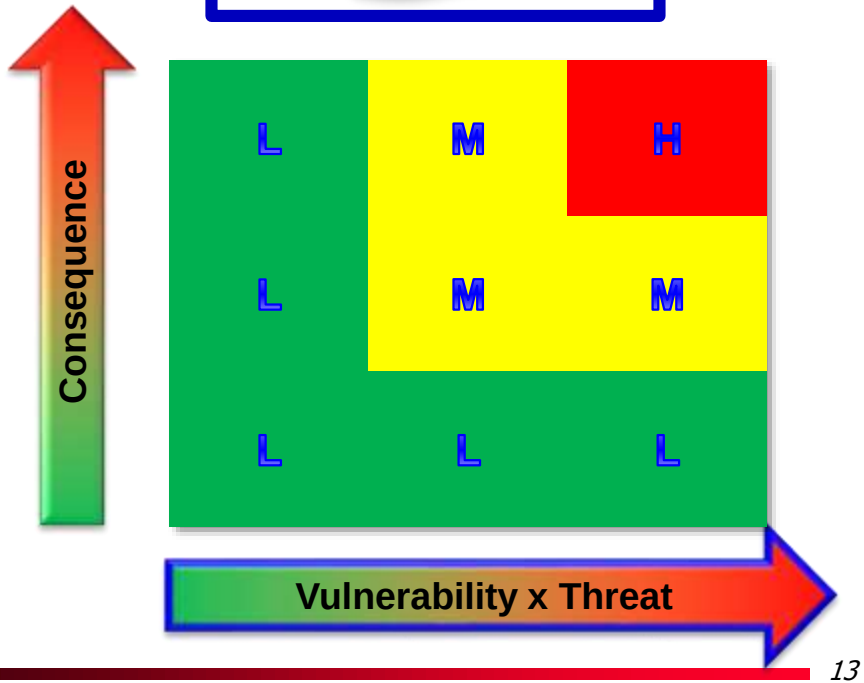
Media	Bits	Physical
	Frames	Datalink
	Packets	Network
Host	Segments	Transport
	Data	Session
		Presentation
		Application



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

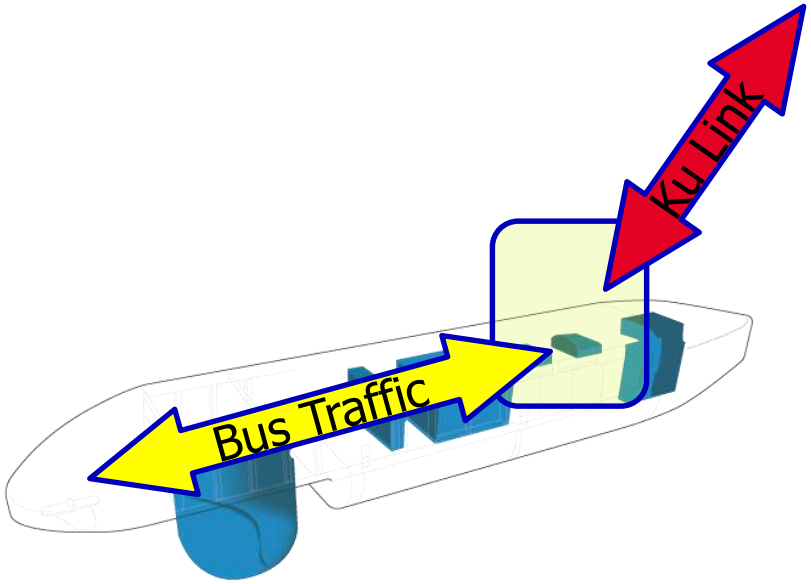




Back to our NOTIONAL example

Path	Vuln	X Threat	= Prob	Consequence	Impact
Bus Traffic	MED Weak EMIC, shielding	MED/LO Low ERP, directional, structured	MED/LO	Internal messaging errors: Mission Degrade	Med

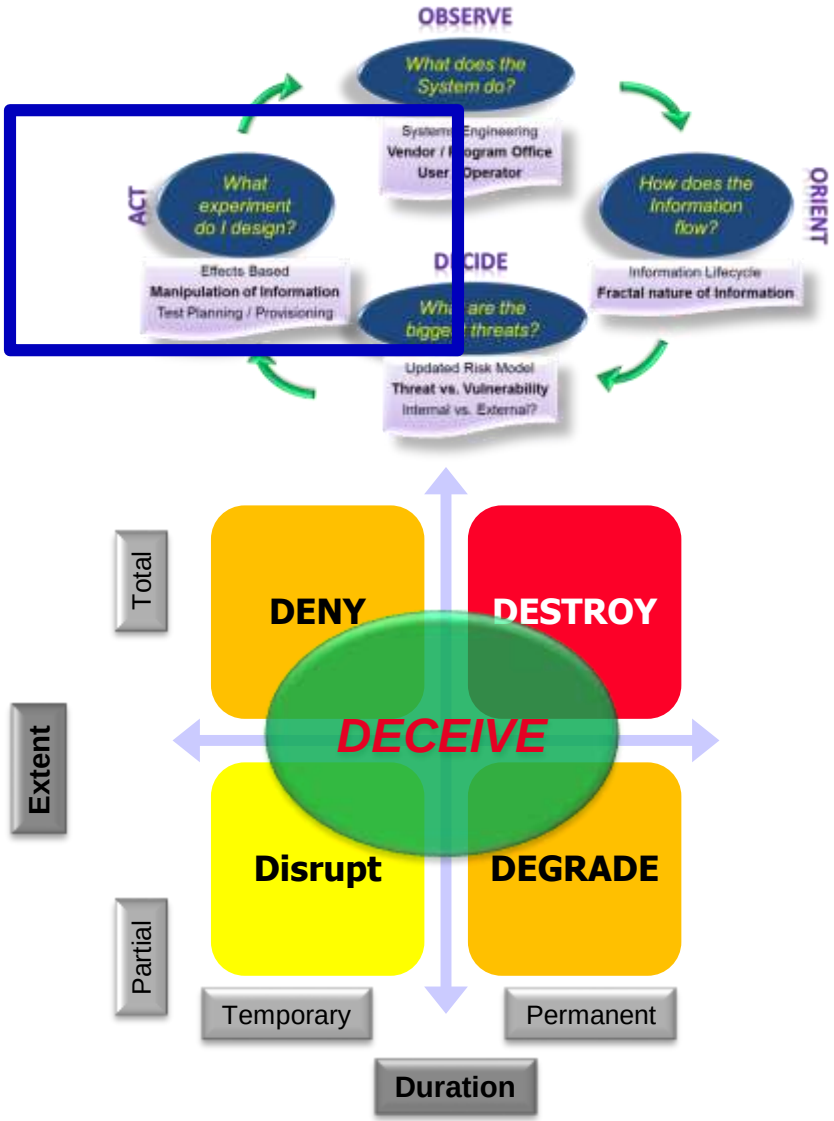
The concept of a Risk Register, ***correctly developed***, will guide your decision on WHAT to test.



Finally. . ! Act

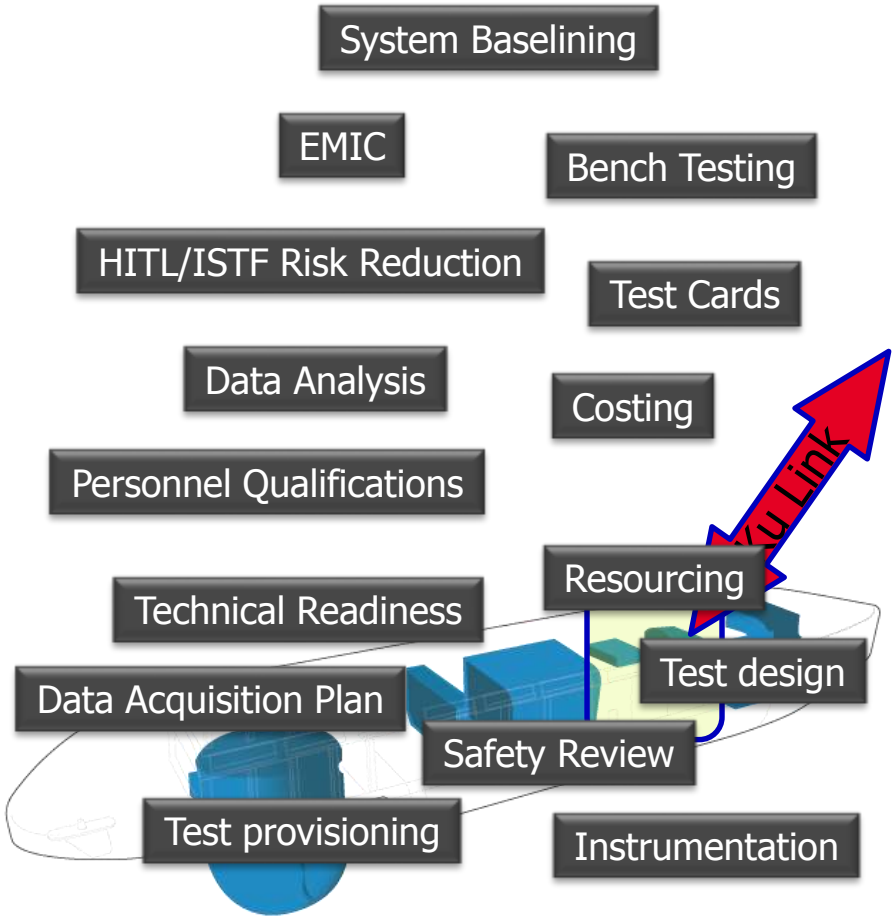
- So, now you know WHAT to test. . HOW do you test it?
- How do you adapt / manipulate information?
- Use the “D5” model to develop your “FTT”
- Determine objectives, then design the test.

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.

http://www.amc.af.mil/shared/media/photodb/photos/100121-F-4177H-734.JPG

Air Force
Print News Today
Air Force news from around the world

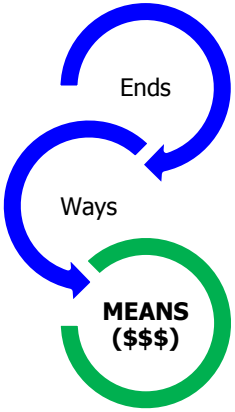
USAF TPS teaches students to fly, fight, win in cyberspace

by Laura Mowry
Staff writer

5/8/2012 - **EDWARDS AIR FORCE BASE, Calif.** -- The United States Air Force Test Pilot School has a long, rich history of educating the best of the best in air and space. Apollo 13 astronaut, Fred Haise; X-15 pilot, Joe Engle; and the first man to break the sound barrier, Chuck Yeager; are just a few of the notable Test Pilot School alumnae who have cemented their places in history books for their impressive accomplishments in both

http://www.edwards.af.mil/news/story_print.asp?id=123301314

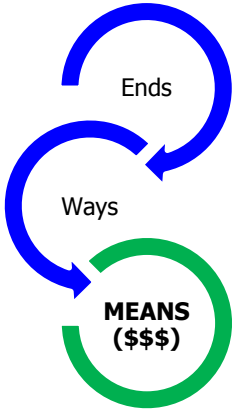
Limitations



Media	Bits	Physical
	Frames	Datalink
	Packets	Network
Host	Segments	Transport
	Data	Session
		Presentation
		Application

- 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);

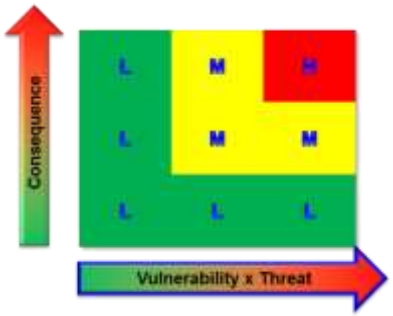
Limitations

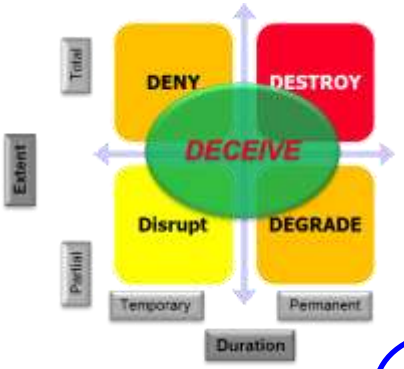


Media	Bits	Physical
	Frames	Datalink
	Packets	Network
Host	Segments	Transport
	Data	Session
		Presentation
		Application

- 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