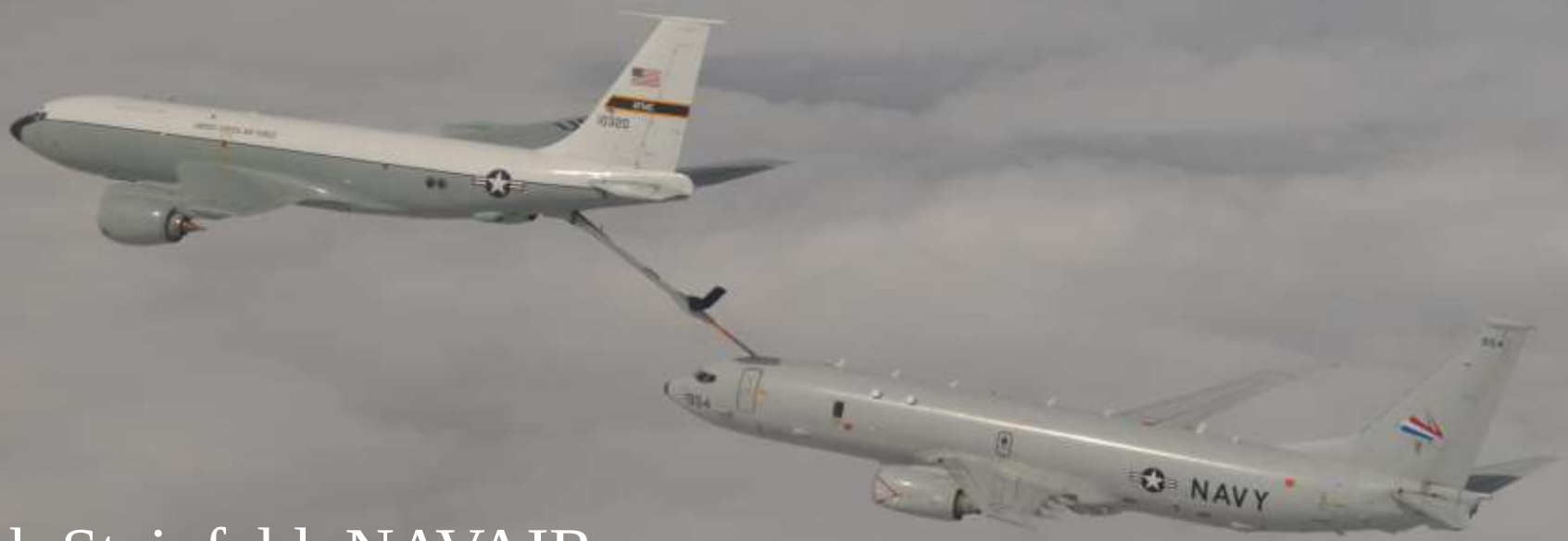
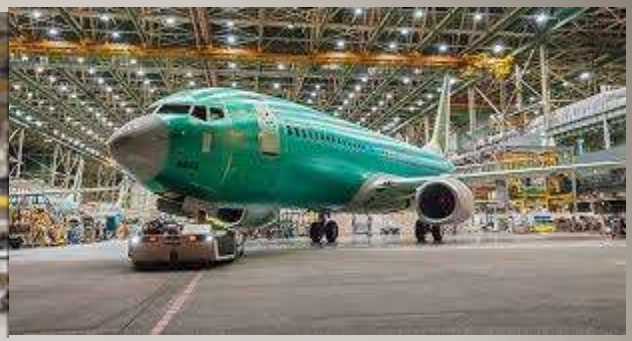
The Green Airplane and Cyber



Hank Steinfeld, NAVAIR

Paola Pringle, NAVAIR

What is the ‘Green Airplane’?

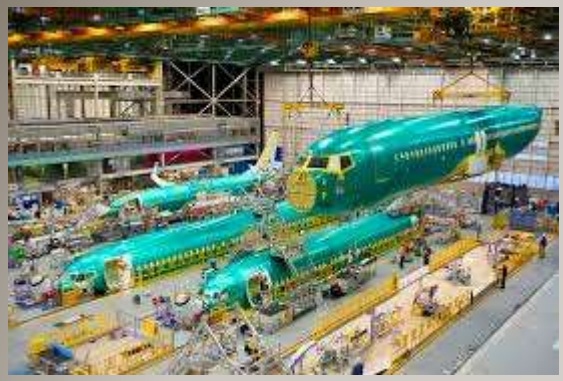


- The green airplane is the product that is the derivative source. In short it is the root aircraft from which we create our military application aircraft.

- The green airplane may include airframe, cockpit, basic flight systems, support systems, or any combination of these. In any case these will be, in general, commercial and non military in nature.

- It is to be expected that as a commercial item, data will be propriety in nature and could extend to flight performance as well as system architecture and design.

The challenge



Understanding the common and the deltas

What we have control over and what we are expected to accept

737-700

C-40

P-8A

How does the root design impact the military application

It is only Software!

- **Software hazard analysis was applied to any system containing software that provided information to the pilot. At one time, this could be applied to a digital watch!**
- **CYBERSAFE level 1 now looks at the attack surface resulting in exploitable vulnerabilities that impact the safety of flight of the aircraft**
  - This results in a corollary that this attack surface is also present in the root commercial aircraft.
- **What testing has been conducted on the commercial aircraft?**
- **Are there military systems that impact the results of testing or of systems present in the 'green aircraft'?**
- **What are the obligations of military testers to notify commercial aircraft manufacturers of discovered vulnerabilities and how do we maintain appropriate security and classification?**

Scope of the Problem

Common commercial/military systems on 'green aircraft'	Military unique systems
IFF- Mode A/C/S	IFF- Mode 1/2/3/4/5
ADSB-out	
TCAS	
TAWS/EGPWS	
Electronic Charts	
Navigation/GPS	SASM
Health monitoring system	
Engine control and data monitoring FADEC	May have military unique FADEC
Fuel management	May have military unique algorithm
Automatic Flight Control	
Pressurization	
Communications management	Will accommodate military configuration
Time	Time may have encryption

Commercial systems are unencrypted or secured

What is the Attack Surface?

- **For the green airplane, the attack surface includes elements that are intended to be interactive and interoperable such as CNS/ATM, TCAS, and civilian operations**
- **The green airplane opens up the supply chain to areas which are normally secured in DoD, simply because they are shared with the commercial world**
- **Access to the integral elements of the aircraft are available to both adversary and ally since the commercial product is sold world-wide**

History and Background

- **Computer security expert/hacker is alleged to have hacked into the guts of the flight control computer system on a United Airlines Boeing 737-800 through its television system and scrolled through a menu of vital aircraft functions.**
- **He also told them that on one occasion he had taken over control of an engine in flight.**
- **The Federal Aviation Administration is orders Boeing to modify the technology aboard late-model 737 aircraft to prevent computer hackers from damaging the planes.**
- **The order published in the Federal Register was effective immediately, although the agency allowed a comment period until July 21. Boeing indicated, at the time, they were taking institutionalized actions in line with similar protections for the 747-8, 777 and 787. (June 2014)**
- **The latest FAA order applies to 737-700, -700C, -800, -900ER, -7, -8 and -9 aircraft. The special conditions apply to these aircraft because their technology is connected more thoroughly than other planes with computer networks outside the aircraft, making the 737 more vulnerable, according to FAA. (June 2014)**
- **Over the past two years, there has been an increasing number of cyber-security incidents reported in the aviation industry. (Oct 2015)**

Cyber awareness: asking the uncomfortable questions

- **Could someone compromise the flight controls of an aircraft and control it?**
- **Could someone compromise the FADEC or engine controls and cause engine failure (shut down/overspeed) in flight?**
- **Could someone cause a loss of pressurization such that the crew and passengers are rendered unconscious?**
- **Could someone compromise the navigation system and cause an aircraft to be lost?**
- **Could someone compromise the communications system of an aircraft rendering it unable to respond to air traffic control?**
- **Could someone compromise the information in the cockpit causing the pilot to land the aircraft at the wrong airport?**
- **Could someone compromise the fuel management system causing fuel starvation and loss of the aircraft?**

How do we test for these and other questions

How and when do we test?

- Our test organizations are geared to testing the weapon system
- We have limited capability to test the ‘green airplane’ in that we can test performance, but have limited capacity to test cyber at this time
- While we have a structural test article for the P-8A, due to proprietary issues, we have limited information regarding the ‘green airplane’
- With the cost of a derivative aircraft well over $100 M, testing in cyber which could be destructive, is not realistic when applied after initial delivery
- CYBERSAFE requires that systems be evaluated/assessed prior to fleet introduction. For derivative aircraft, these aircraft are already in service; therefore, we are backfilling information
- Test agencies must develop new tools to evaluate cyber threats

NDI testing on aircraft in a periodic fashion

What resources are available

- **Usually the OEM is the only source for detailed information on the green airplane.**
- **Weapon systems labs may not have live feeds and are dependent on sim/stim for the outside data sources such as altitude, airspeed, air temp, etc.**
- **DoD expertise in a number of these areas is limited as the result of a continued and steady reduction in force approach that has transferred risk to the OEM and therefore increased reliance on outside test agencies.**
- **Each DoD Service has a piece of the information, but not all**
- **Cyber test facilities and ranges do exist at the avionics and general service facilities such as the National Cyber Range is being sponsored by Test Resource Management Command for DoD**

The Services must work together and share data

Applying the Cyber Kill-Chain

- **We need to understand how an adversary could gain access to our systems**
- **We need to understand the technology and risks associated with the commercial systems**
- **We need to understand the effects that can be generated and then how to recognize when this has occurred**
- **Notional attack**
- **Gain access via health monitoring system**
  - Compromised maintenance personnel or maintenance computer
- **Create malware package which targets engine monitoring system**
  - Package could send spurious warnings such as erratic oil pressure or high engine temperature, or exhaust gas temperature
- **Upload package at routine maintenance period adding trigger such as weight off wheels**
- **At next flight, when aircraft takes off, the malware package activates causing the pilot to abort flight and land**

What is our obligation to the OEM or commercial traveler?

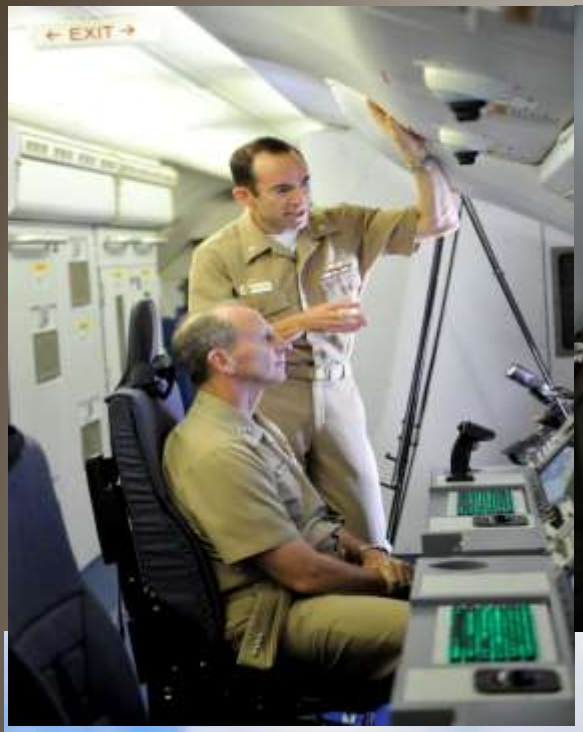
- **Consider the question that as a result testing, a vulnerability is discovered in the flight control computer which is shared across a number of both DoD and Commercial platforms**
- **DoD will recommend (could be mandatory) correction to the defect, but the defect is not a part of the weapon system, but rather the 'green airplane'**
  - NAVAIR Cyber does have a relationship with FAA and so would report to FAA if a suspected cyber incident occurred
  - **The program would also advise the OEM which may not be the commercial source but the military division**
  - **NAVAIR and Air Force Systems Command are working to share information in order to broaden base. This will likely include the sharing of tools and techniques in the future**

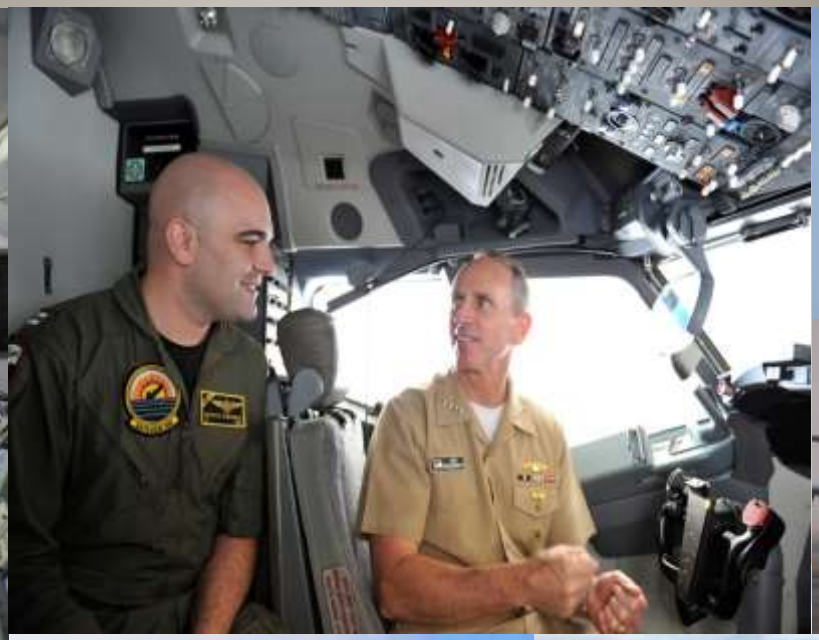
The Services are testing in areas the OEM is not

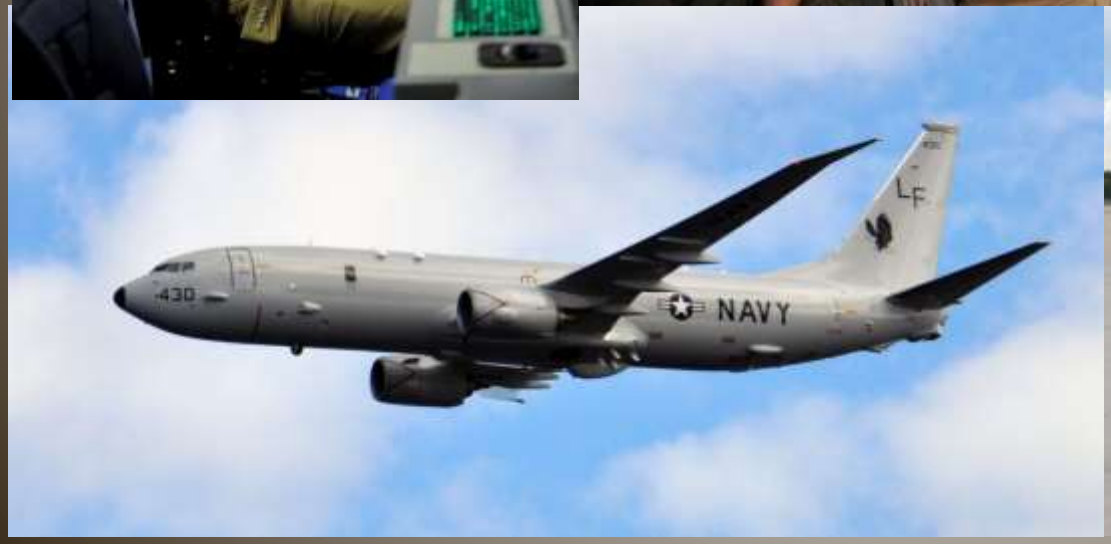
What Now?

- **The Services are testing where the Commercial OEM is not**
- **Data are being collected, but must be shared between services**
- **The OEM must have a secure means to transmit critical data provided by the Military customer to the Commercial source**
- **Military Cyber testers must develop new tool sets to address areas that have historically not been in the repertoire of Developmental Test**
- **Cost of test being high, both Developmental and Operational Test need to share information to advance the range of test and not plow the same turf over again**

Questions



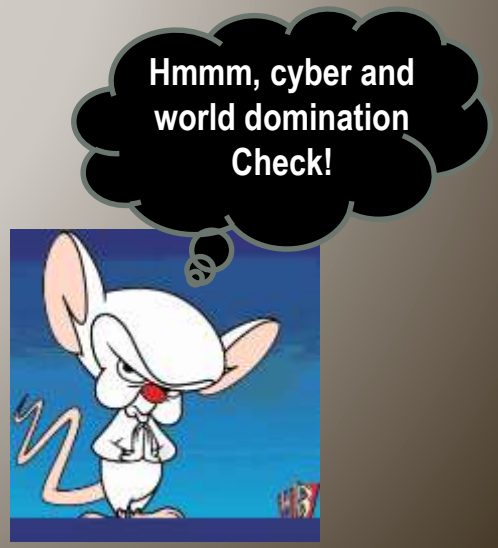




Contact Information

Hank 'Wizard' Steinfeld, APM T&E P-8A Inc 3, P-3C
APM T&E PMA-264
ASW SoS APM T&E
PMA-290 Cyber Test Strategy Lead
301-342-3041
henry.steinfeld@navy.mil

Ms. Paola Pringle
Integrated Warfare Test and Evaluation Division, 5.1L
Cyberspace T&E Branch 51L300E
P-8A Increment 3 Interoperability LTE
(805) 816-3038
paola.pringle@navy.mil



The Commercial Side

- **The latest FAA order applies to 737-700, -700C, -800, -900ER, -7, -8 and -9 aircraft, one of the most popular types of planes for the last 20 years. The special conditions apply to these aircraft because their technology is connected more thoroughly than other planes with computer networks outside the aircraft, making the 737 more vulnerable, according to FAA. (June 2014)**
- **The chief of Europe's top airline safety agencies warned that cyber-criminals could hack into critical systems on an airplane from the ground.**
- **Patrick Ky, director of the European Aviation Safety Agency, told European aviation journalists at a meeting of the Association des Journalistes Professionnels de l'Aéronautique et de l'Espace (AJPAE) that his organisation had hired a penetration tester to find and exploit vulnerabilities in the ACARS (Aircraft Communications Addressing and Reporting System) used to transmit messages between aircraft and ground stations.**
- **Over the past two years, there has been an increasing number of cyber-security incidents reported in the aviation industry. (Oct 2015)**