

Cyber-Vulnerabilities in Aviation Today

Robert F. Behler
Deputy Director and COO



Software Engineering Institute

Carnegie Mellon University®

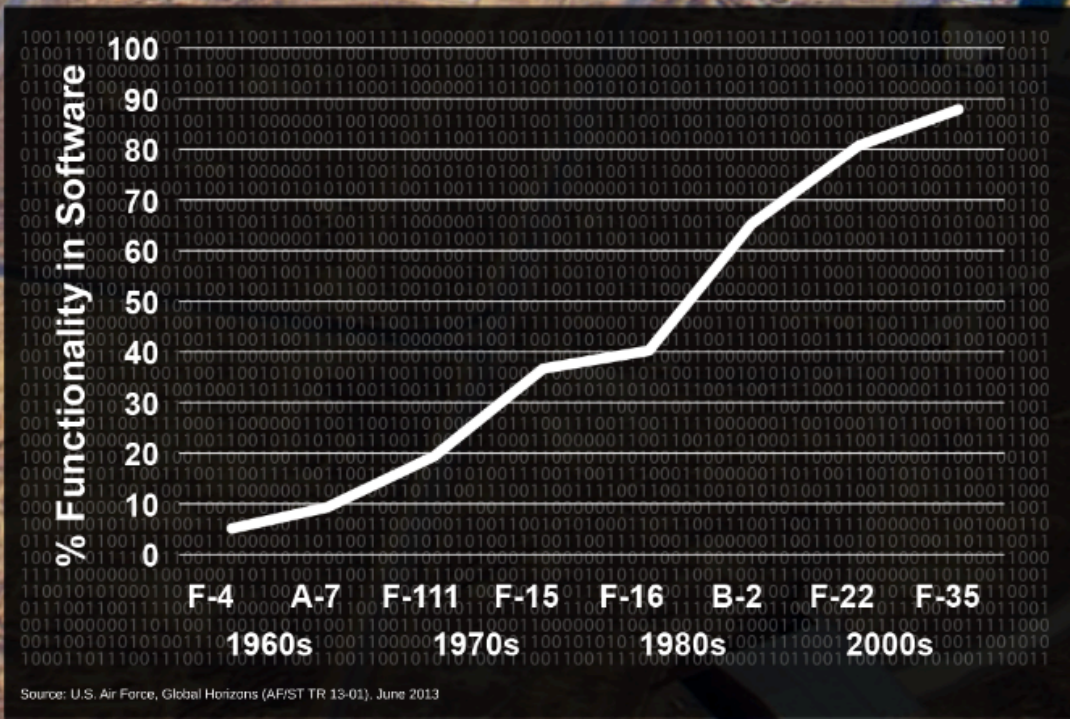
The aircraft industry is in the software business

```
10011001010100011011100111001100111100000011001000110111001110011001110011001100101010001110
01001110011001111000110000001100110010101000110111001110011001100111100000011001000110111001110011
110001100000011011001100101010001110011001111000110000001100110010100001101110011100110011111
01100110010101000111001100111000110000001101100110010101000111001100111100011000000110011001
10010001101110011100110011100110011001010100011100110011110001100000011011001100101010001110
110111001110011001111000000110010001101110011100110011110011001100101010001110011001111000110
1100011000000110011001010100011011100111001100111100000011001000110111001110011001111001100110
01100110010101001110011001110001100000011001100101010001101100110011001111000000110010001
100111001100111100011000000110110011001010100011100110011110001100000011001100101010001101100
1110011001110011001100101010001110011001110001100000011011001100101010001110011001111000110
001111000000110010001101110011100110011110011001100101010001110011001111000110000001101100110
00110010101000110111001110011001111000000110010001101110011100110011110011001100101010001100
1001110011001111000110000001100110010101000110111001110011001111000000110010001101110011100110
100011000000110110011001010100011100110011110001100000011001100101010001101110011100110011110
110011001010100011100110011110001100000011011001100101010001110011001111000110000001100110010
001000110111001110011001111001100110010101000111001100111100011000000110110011001010100011100
10111001110011001111000000110010001101110011100110011100110011001010100011100110011110001100
100011000000110011001010100011011100111001100111100000011001000110111001110011001111001100110
10011001010100011011100111001100111100000011001100110011110000001100100011011100111001100110
0011001100111100011000000110110011001010100011100110011110001100000011001100101010001110011001
011110000001100100011011100111001100111100110011001010100011100110011110001100000011011001100
011001010100011011100111001100111100000011001000110111001110011001111001100110010101000111001
00111001100111100011000000110011001010100011011100111001100111100000011001000110111001110011001
000110000001101100110010101000111001100111100011000000110011001010100011011100111001100111100
100110010101000111001100111100011000000110110011001010100011100110011110001100000011001100101
010001101110011100110011110011001100101010001110011001111000110000001101100110010101000111001
011100111001100111100000011001000110111001110011001111001100110010101000111001100111100011000
000110000001100110010101000111001100111100011000000110011001010100011011100111001100111100
100110010101000111001100111100011000000110110011001010100011100110011110001100000011001100101
010001101110011100110011110011001100101010001110011001111000110000001101100110010101000111001
011100111001100111100000011001000110111001110011001111001100110010101000111001100111100011000
0001100000011001100101010001101110011100110011110000001100100011011100111001100111100110011001
1001100101010001101110011100110011110000001100110011001111000000110010001101110011100110011001
000110000001100110010101000111001100111100000011001000110111001110011001111001100110010101000111001
111100000011001000110111001110011001111001100110010101000111001100111100011000000110110011001
110010101000110111001110011001111000000110010001101110011100110011110011001100101010001110011
0111001100111100011000000110011001010100011011100111001100111100000011001000110111001110011001
001100000011011001100101010001110011001111000110000001100110010101000110111001110011001111000
001100101010001110011001111000110000001101100110010101000111001100111100011000000110011001010
100011011100111001100111100110011001010100011100110011110001100000011011001100101010001110011
```

Source: U.S. Air Force, Global Horizons (AF/ST TR 13-01), June 2013

whether they realize it or not

The aircraft industry is in the software business



whether they realize it or not



F-35

30M SLOC

15M on plane

15M for ground
support equipment

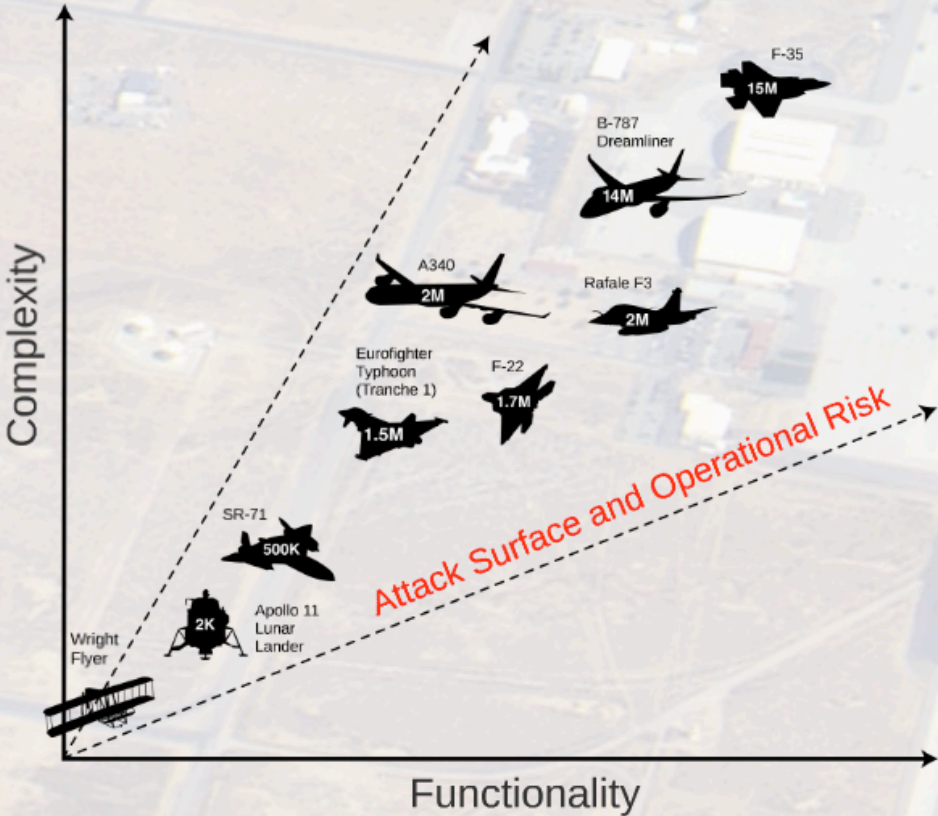


Potential Cyber-Vulnerability Pathways



26 suppliers provide components for the avionics

Increased Attack Surface



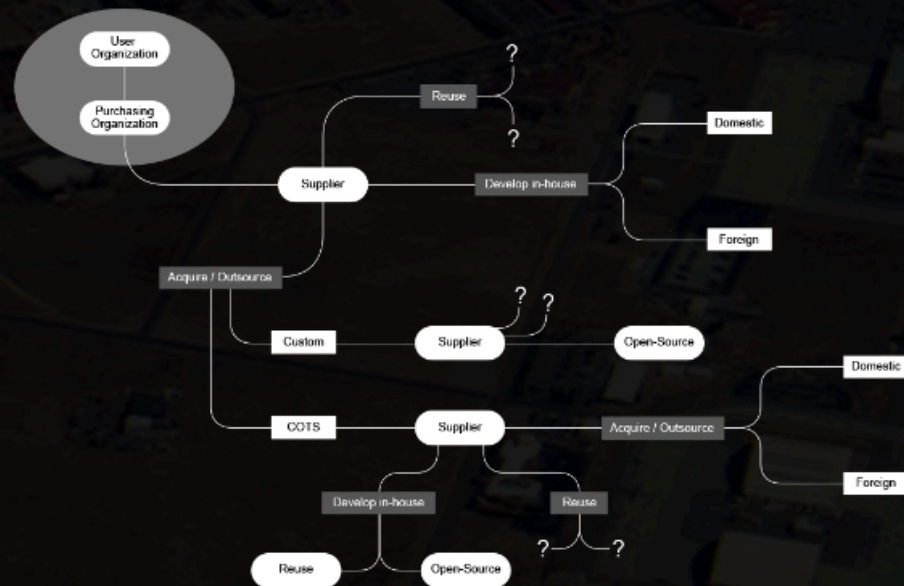
Defects in software may be exploited

Software defects per KSLOC in a recent aircraft program

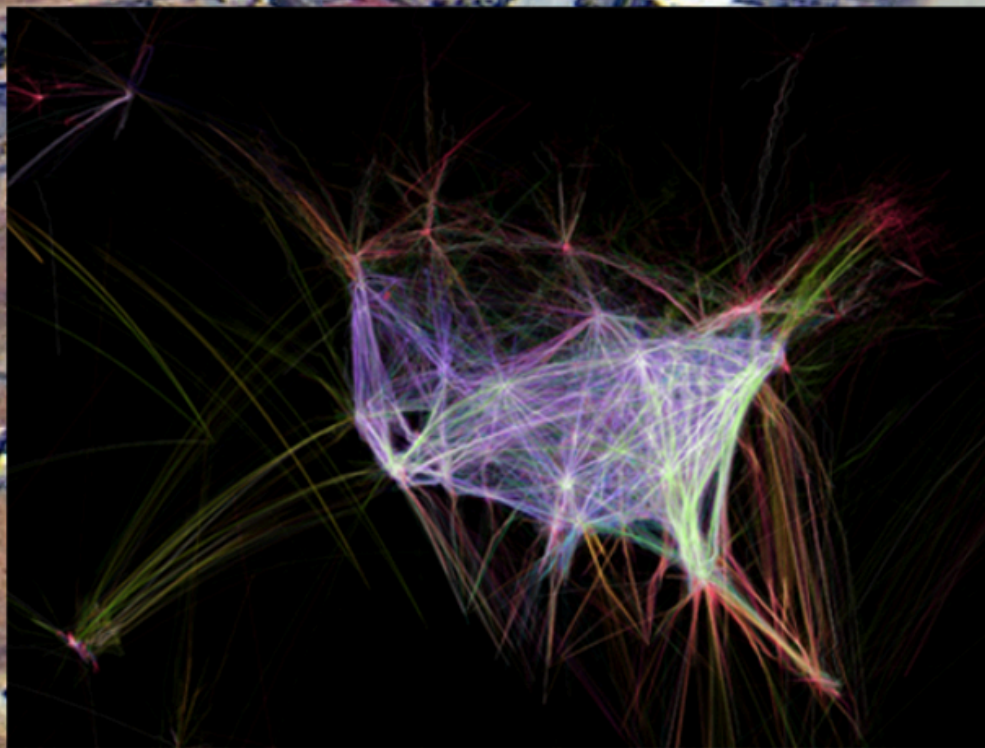
Type of Development	Number of Defects Discovered	KSLOC	Defects per KSLOC
Software Project 1	36	32	1.13
Software Project 2	66	89	0.74
Software Project 3	260	443	0.59

Adapted from: NAVAIR report, NAWCWD TP 8642

The supply chain creates vulnerabilities



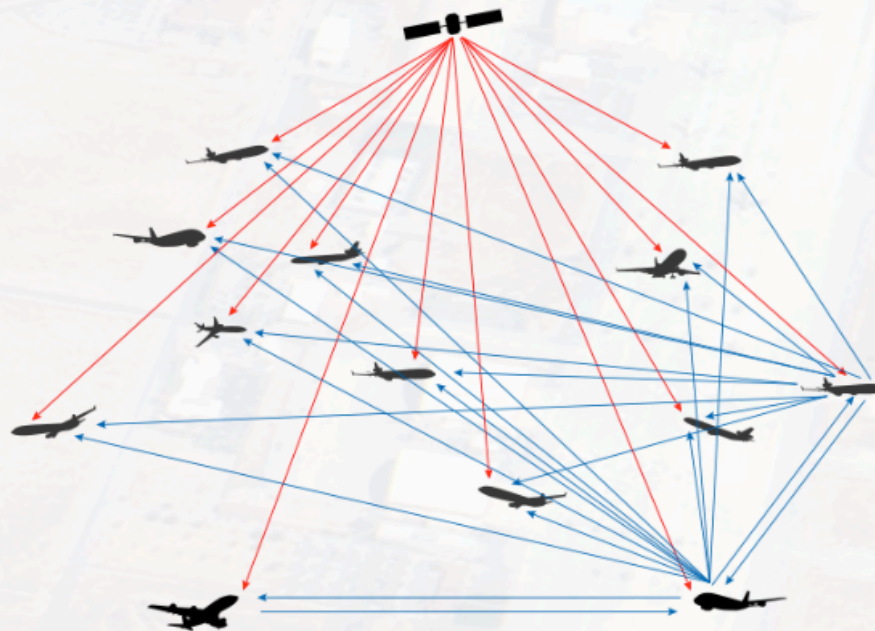
Aircraft operate in a very complex environment



Automatic Dependent Surveillance-Broadcast (ADS-B) will replace radar with GPS

Greater functionality

Greater complexity



Increased attack surface and lack of security
Every aircraft will be a node on a network

Trucks jam GPS, close Newark airport



Climate control

Engine ignition

Air-bag system

Collision avoidance system

Electronic stability control

Entertainment system

Alarm system

Tire-pressure monitoring

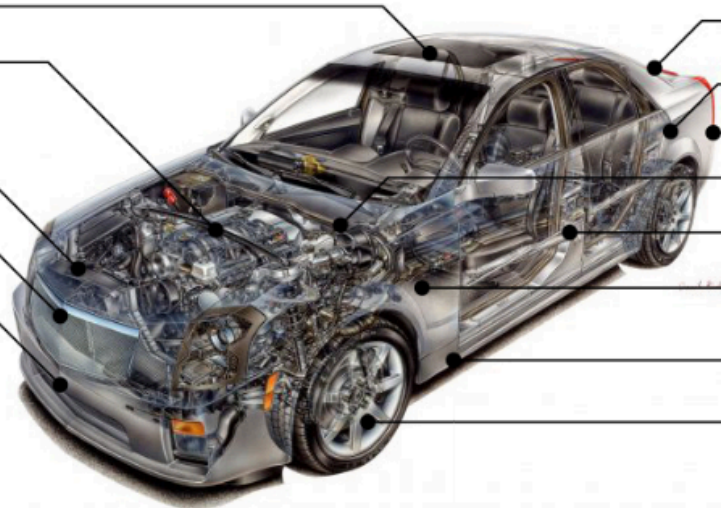
Cruise control

Electronic seat control

Power steering

Automatic transmissison

Antilock brakes

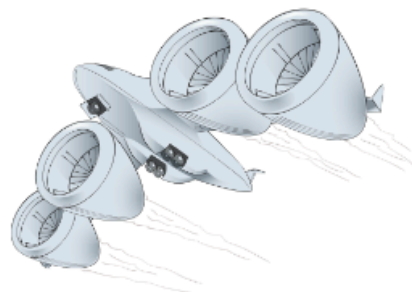


2016 Luxury Car
100M SLOC

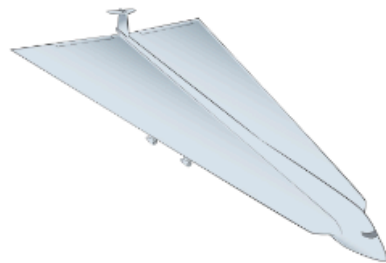


60
MINUTES

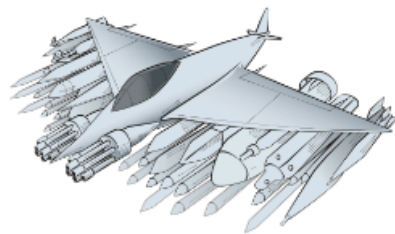
Engineering Perspectives



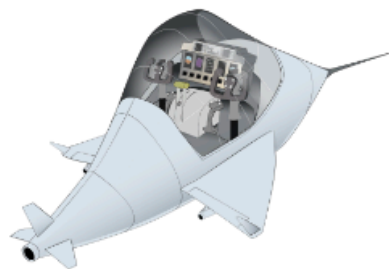
Propulsion Engineer



Aero Engineer

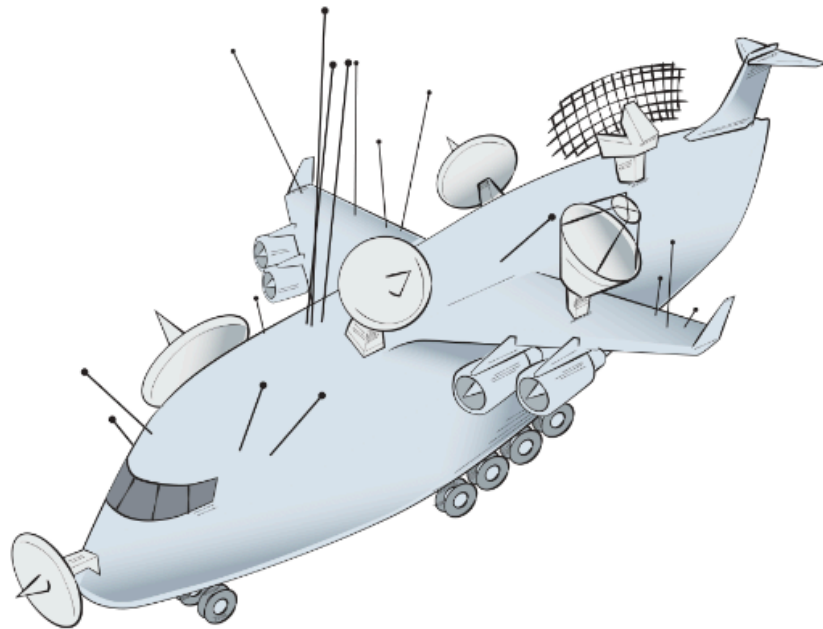


Armaments Engineer



Avionics Engineer

Engineering Perspectives



**Cyber-Vulnerabilities
Engineer**

Taxonomy of Cyber-Threats

Exploits pre-existing
known vulnerabilities

\$10K's

- Password theft
- Insider threat
- Credit card fraud
- Malware
- Spear fishing
- Identity theft

← NUISANCE

EXISTENTIAL →

Taxonomy of Cyber-Threats

Exploits pre-existing known vulnerabilities

\$10K's

- Password theft
- Insider threat
- Credit card fraud
- Malware
- Spear fishing
- Identity theft

Discovers unknown vulnerabilities

\$1M's

- Zero day attacks
- Logic bombs
- Supply chain issues
- Intellectual property theft - aircraft designs
- Fuzz testing to identify vulnerabilities

NUISANCE

EXISTENTIAL

Taxonomy of Cyber-Threats

Exploits pre-existing known vulnerabilities

\$10K's

- Password theft
- Insider threat
- Credit card fraud
- Malware
- Spear fishing
- Identity theft

Discovers unknown vulnerabilities

\$1M's

- Zero day attacks
- Logic bombs
- Supply chain issues
- Intellectual property theft - aircraft designs
- Fuzz testing to identify vulnerabilities

Creates vulnerabilities using full spectrum

\$1B's



Russia



China



North Korea



Iran

NUISANCE

EXISTENTIAL



James Clapper
U.S. Director of National Intelligence

"Cyber poses a very complex set of threats, because profit-motivated criminals, ideologically motivated hackers or extremists, and variously capable nation-states like Russia, China, North Korea, and Iran are all potential adversaries who, if they choose, can all do great harm."

James Clapper in testimony
to the Senate Intelligence Committee
on February 26, 2015

Software-reliant platforms need to be tested to minimize the maximum regret



Software Engineering Institute

Carnegie Mellon University