Safety Assurance in Software Systems

From Airplanes to Atoms

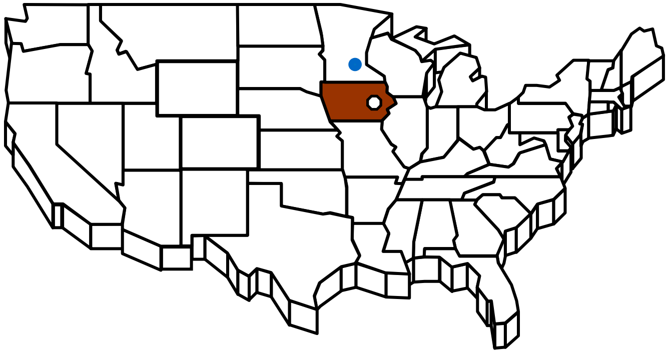
MDEP Conference on
New Reactor Design Activities
Session 2 – Digital I&C: Current &
Emerging Technical Challenges
12 September 2017

Dr. Darren Cofer
cofer@ieee.org

Rockwell Collins: Advanced Technology Center

Trusted Systems Group

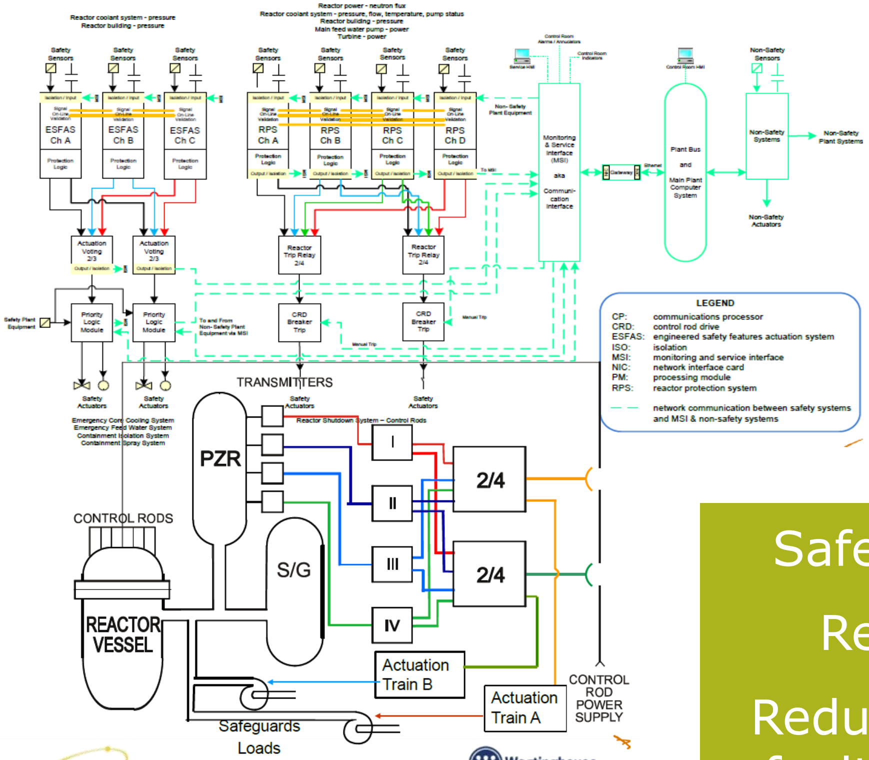
- Formal methods for verification
- Model-based development
- Practical and effective tools
- Certification (DO-178C)

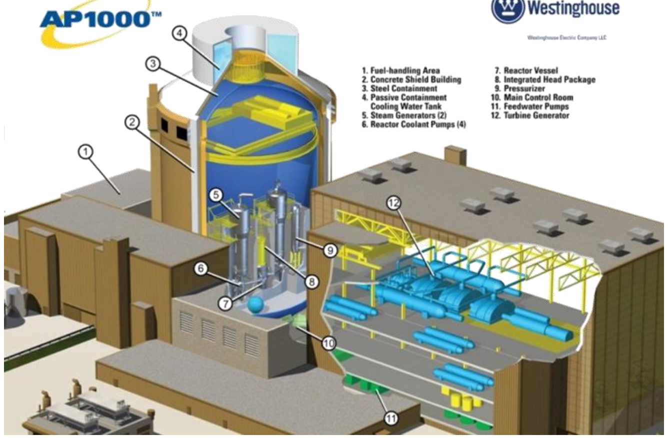


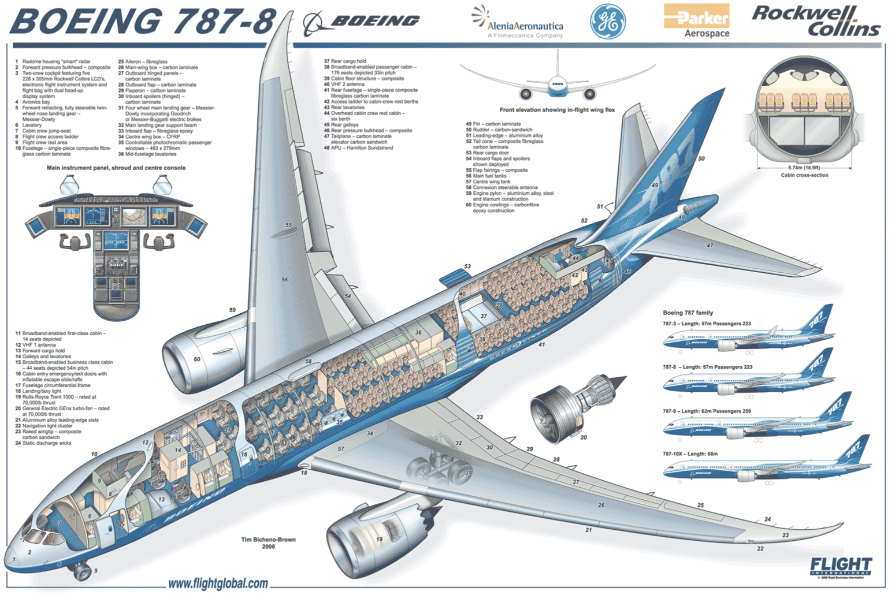
Domains

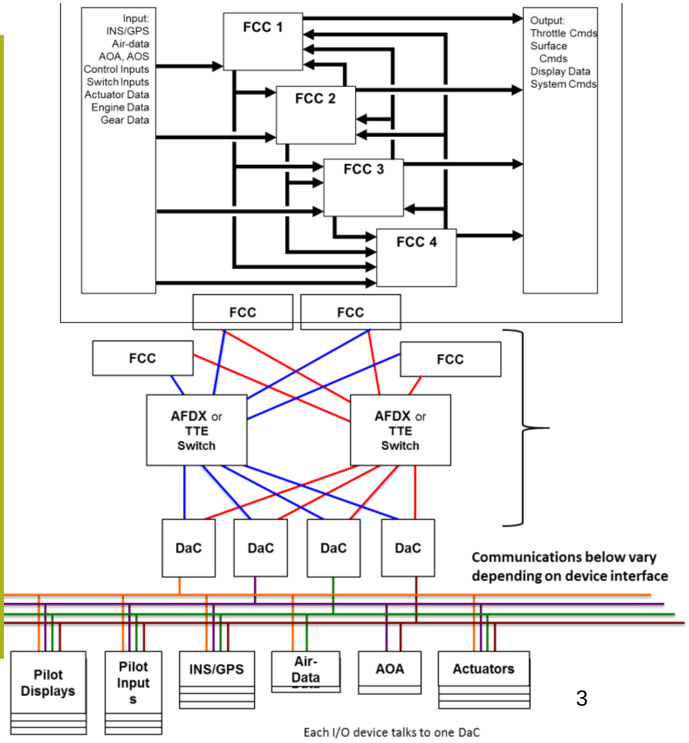
- Avionics systems
- Commercial and military
- Manned and unmanned
- Safety and security

Similar Concerns...


Reactor coolant system - pressure
Reactor building - pressure
Reactor power - neutron flux
Reactor coolant system - pressure, flow, temperature, pump status
Reactor building - pressure
Main feed water pump - power
Turbine - power
Safety Sensors
ESFAS Ch A
ESFAS Ch B
ESFAS Ch C
RPS Ch A
RPS Ch B
RPS Ch C
RPS Ch D
Protection Logic
Actuation Voting 2/3
Reactor Trip Relay 2/4
CRD Breaker Trip
Priority Logic Module
Safety Plant Equipment
To and From Non-Safety Plant Equipment via MSI
Manual Trip
Safety Actuators
Emergency Core Cooling System
Emergency Feed Water System
Containment Isolation System
Containment Spray System
Monitoring & Service Interface (MSI) aka Communication Interface
Gateway
Plant Bus and Main Plant Computer System
Non-Safety Sensors
Non-Safety Systems
Non-Safety Plant Systems
Non-Safety Actuators
Non-Safety Plant Equipment
LEGEND
CP: communications processor
CRD: control rod drive
ESFAS: engineered safety features actuation system
ISO: isolation
MSI: monitoring and service interface
NIC: network interface card
PM: processing module
RPS: reactor protection system
network communication between safety systems and MSI & non-safety systems
TRANSMITTERS
PZR
S/G
CONTROL RODS
REACTOR VESSEL
Reactor Shutdown System – Control Rods
I
II
III
IV
2/4
2/4
Actuation Train B
Actuation Train A
CONTROL ROD POWER SUPPLY
Safeguards Loads







Safety-critical

Regulated

Redundancy for fault-tolerance

Software intensive

← Fail-safe

Fail-op →

Similar Challenges

- Increased use of software in safety-critical functions
- Complexity of software
- Incorporation of COTS hardware/software
- New technologies that challenge the existing certification process
- Limitations of testing for safety assurance
- Cybersecurity

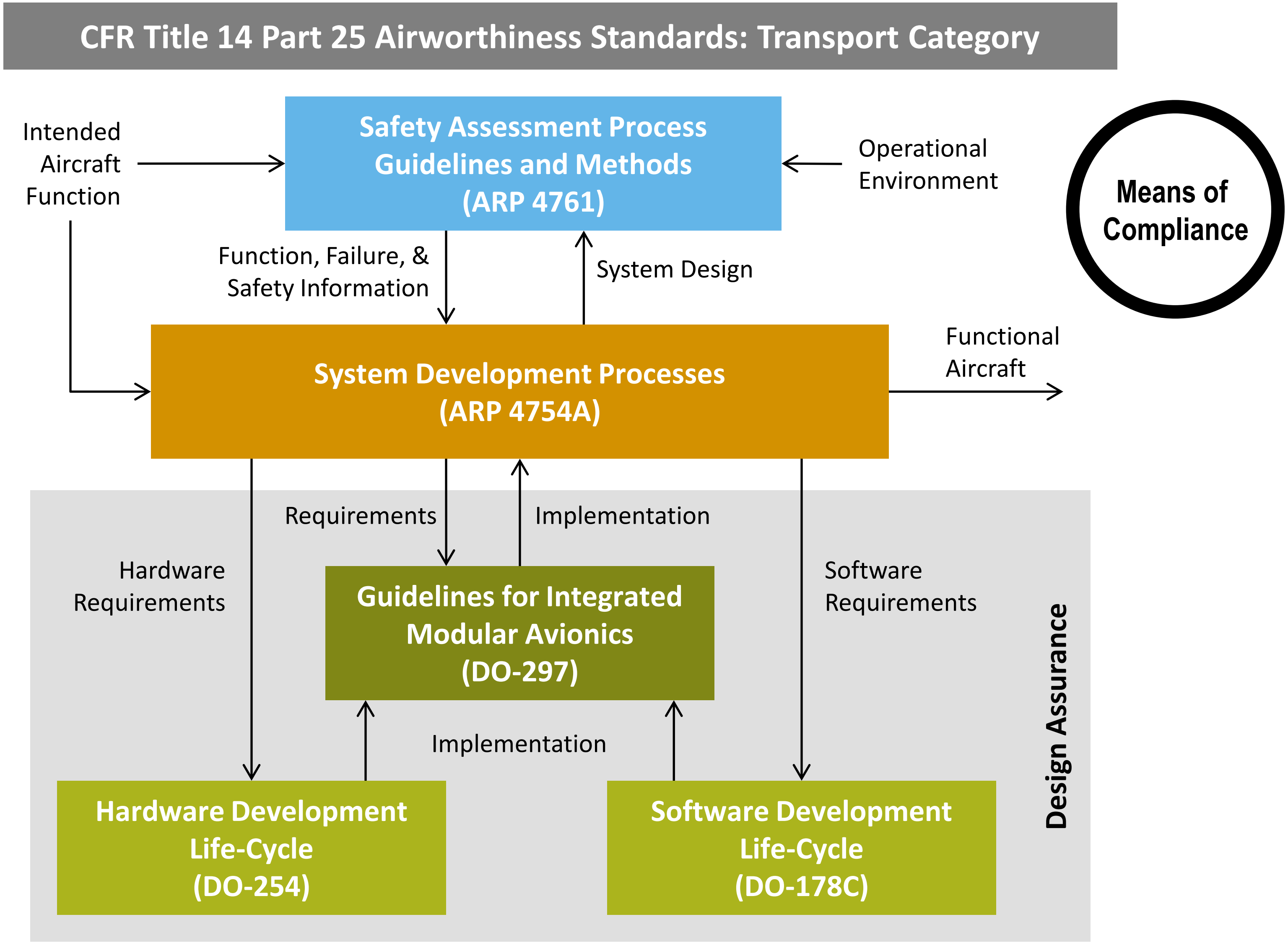
"Houston, we have a problem."

What can the nuclear industry learn from civil aviation experience?

Assertion 1:

The nuclear industry can benefit from aerospace software development and verification practices.

Certification Process for Civil Aviation

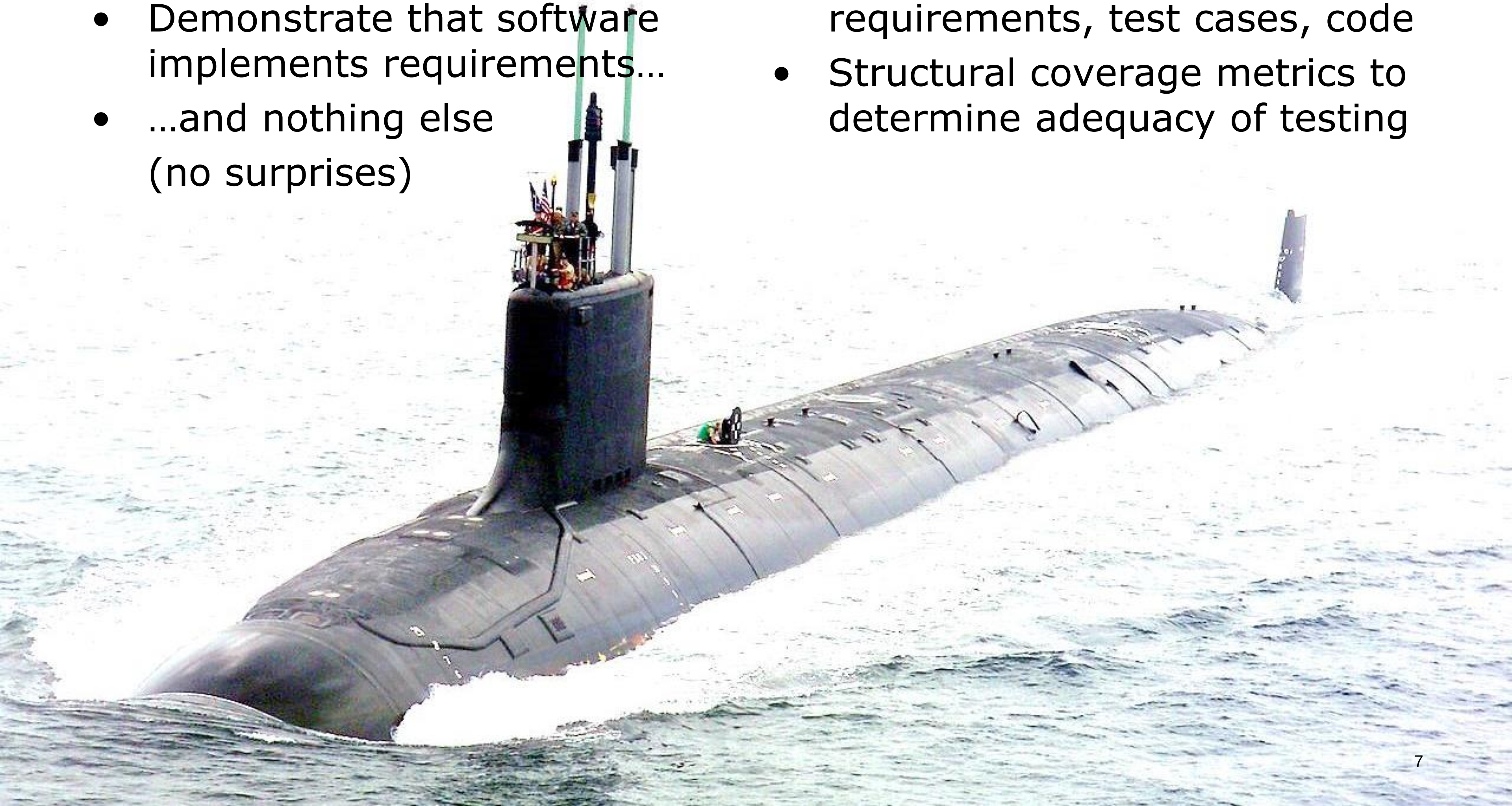

CFR Title 14 Part 25 Airworthiness Standards: Transport Category
Intended Aircraft Function
Safety Assessment Process Guidelines and Methods (ARP 4761)
Operational Environment
Means of Compliance
Function, Failure, & Safety Information
System Design
System Development Processes (ARP 4754A)
Functional Aircraft
Requirements
Implementation
Hardware Requirements
Guidelines for Integrated Modular Avionics (DO-297)
Software Requirements
Design Assurance
Implementation
Hardware Development Life-Cycle (DO-254)
Software Development Life-Cycle (DO-178C)

DO-178 Principles

- Primarily a quality document, not safety
- Demonstrate that software implements requirements…
- …and nothing else

  (no surprises)

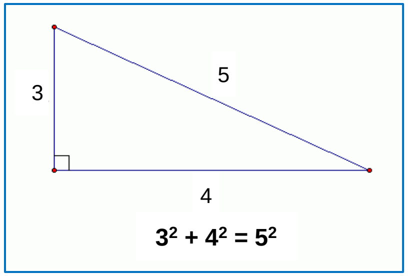
- Requirements-based testing
- Traceability among requirements, test cases, code
- Structural coverage metrics to determine adequacy of testing



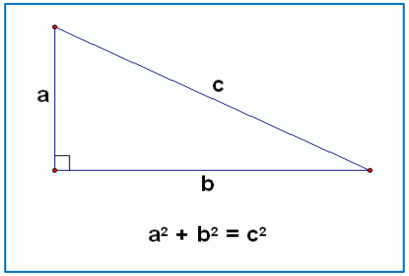
Assertion 2:

To cope with software complexity, the aerospace industry is moving toward use of formal methods.

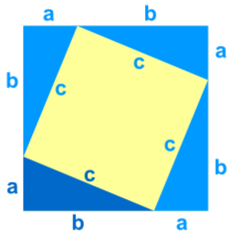
Formal Methods: Complete Exploration of Design

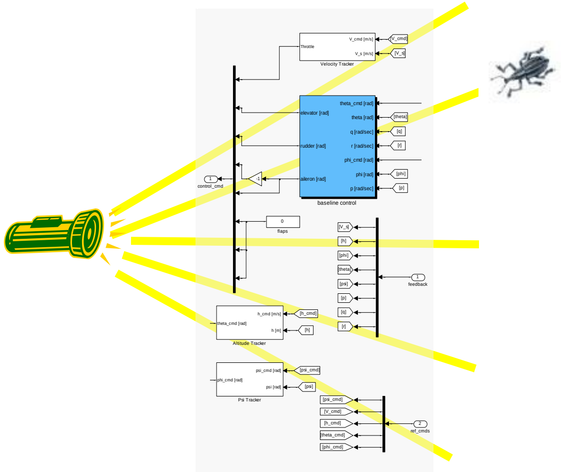


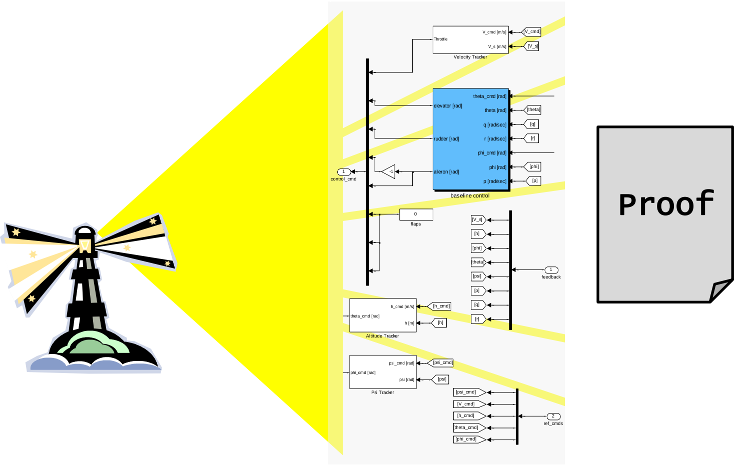
$3^2 + 4^2 = 5^2$



$a^2 + b^2 = c^2$



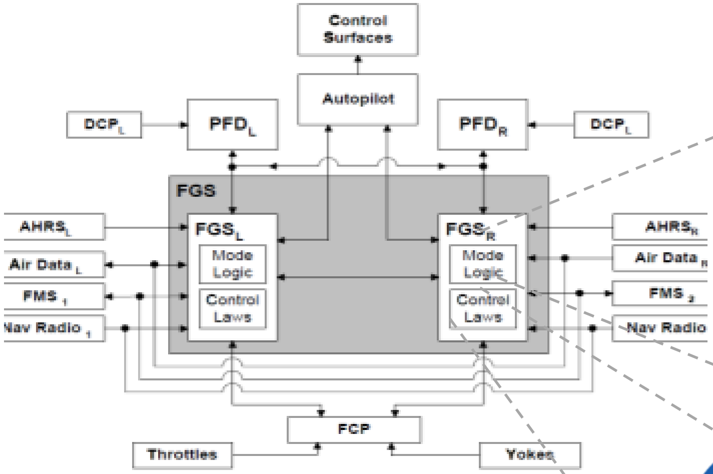




Testing can only show the presence of bugs (and only if you are lucky)

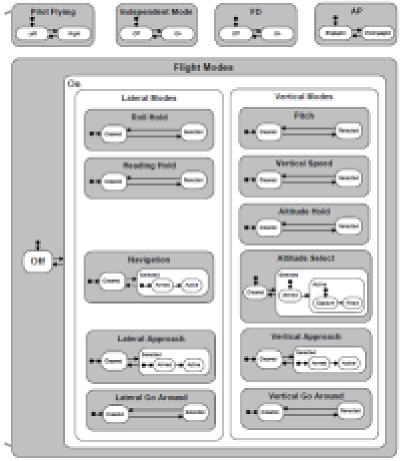
Analysis can show the absence of bugs (with evidence of correctness)

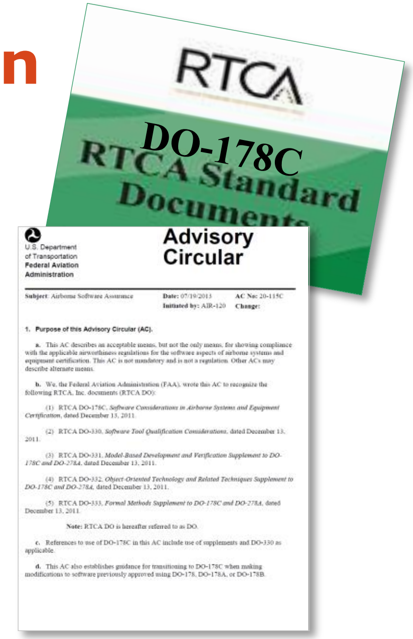
Formal Methods and Aircraft Certification



Flight Guidance System

Mode Logic





RTCA

DO-178C
RTCA Standard
Documents

U.S. Department
of Transportation
Federal Aviation Administration

Advisory Circular

Subject: Airborne Software Assurance

Date: 07/19/2013
Initiated by: AIR-120

AC No: 20-115C
Change:

1. Purpose of this Advisory Circular (AC).

a. This AC describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the software aspects of airborne systems and equipment certification. This AC is not mandatory and is not a regulation. Other ACs may describe alternate means.

b. We, the Federal Aviation Administration (FAA), wrote this AC to recognize the following RTCA, Inc. documents (RTCA DO):

(1) RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(2) RTCA DO-330, *Software Tool Qualification Considerations*, dated December 13, 2011.

(3) RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*, dated December 13, 2011.

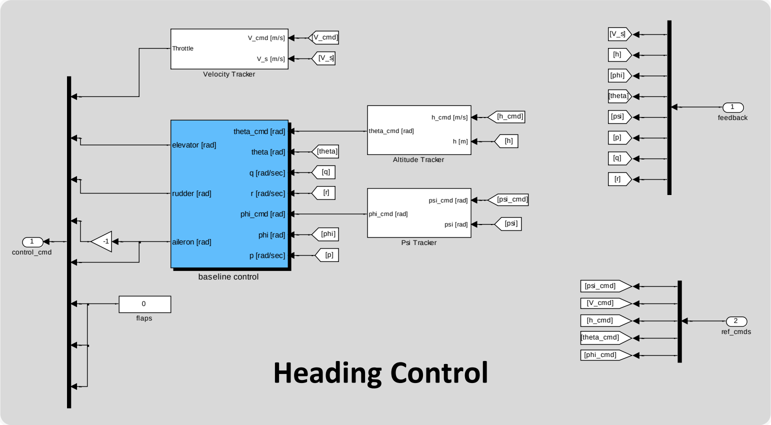
(4) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(5) RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

Note: RTCA DO is hereafter referred to as DO.

c. References to use of DO-178C in this AC include use of supplements and DO-330 as applicable.

d. This AC also establishes guidance for transitioning to DO-178C when making modifications to software previously approved using DO-178, DO-178A, or DO-178B.



Heading Control

DO-178C/DO-333 Case Study

- Theorem Proving demonstrated on the FGS design model
- Model Checking demonstrated on the Mode Logic Simulink model
- Abstract Interpretation demonstrated on the Heading Control Law source code

Formal methods reduce cost and increase confidence through early detection and elimination of errors

Assertion 3:
Formal methods can also address cybersecurity concerns for high-assurance systems.

High-Assurance Cyber Military Systems

Boeing Unmanned Little Bird Helicopter

High-Assurance Cyber Military Systems

- Final Demonstrations
  - Boeing Unmanned Little Bird (ULB): Mesa AZ, Feb 2017
  - Quadcopter: Sterling VA, Apr 2017
- Demonstrated cyber-resiliency of both vehicles
  - “Before” and “after” flight demonstrations
  - *Attacked in-flight*
  - Comprehensive evaluation by “white hat” cyber-attackers
- Cyber-resiliency achieved through application of formal methods
  - Model checking of architecture properties
  - Synthesis/verification of software components
  - Comprehensive proof of correctness of operating system

Formal methods are practical and effective for achieving cybersecurity in real aerospace systems

For More Information…

- HACMS final demo video
  - https://insights.rockwellcollins.com/2017/07/06/video-high-assurance-cyber-military-systems-hacms/
- DARPA Blocks Cyberattacks on Unmanned Little Bird In Flight (Aviation Week)
  - http://aviationweek.com/awindefense/darpa-blocks-cyberattacks-unmanned-little-bird-flight
- Cybersecurity Skeptics Now Embracing Formal Methods (ACM Ubiquity)
  - http://ubiquity.acm.org/article.cfm?id=3081880
- DO-178C/333 Certification Case Studies Using Formal Methods
  - http://loonwerks.com/projects/do333.html

cofer@ieee.org