Safety Assurance in Digital I&C Systems

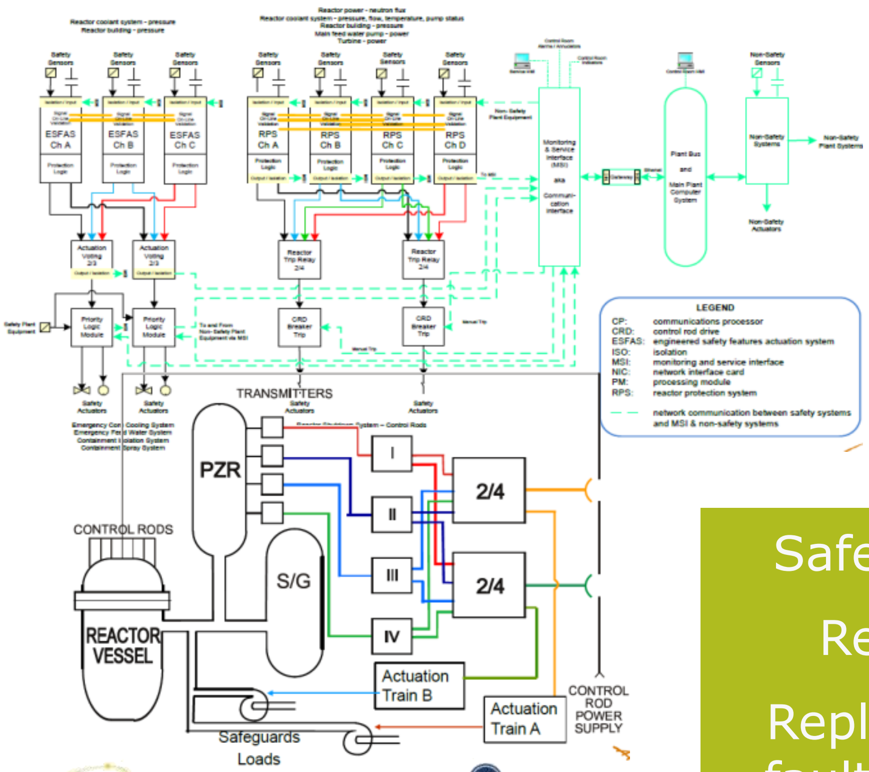
From Airplanes to Atoms

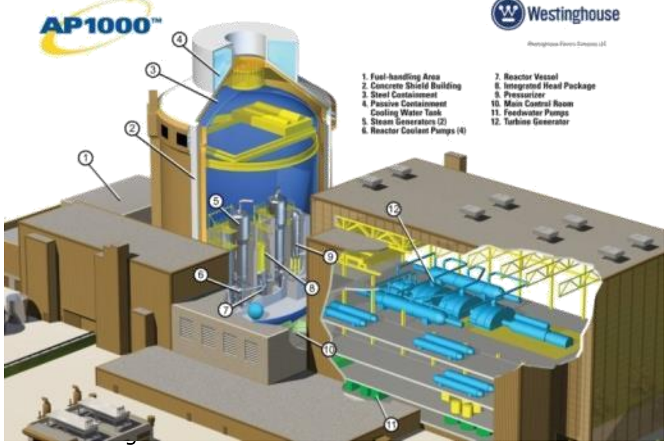
Nuclear Regulatory Commission
Digital I&C Systems
Commission Meeting
17 December 2015

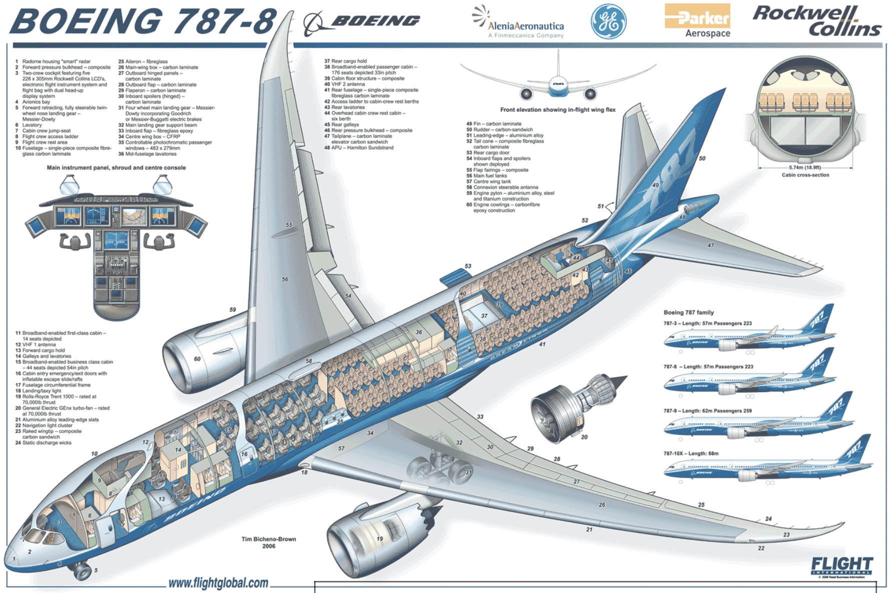
Dr. Darren Cofer
cofer@ieee.org

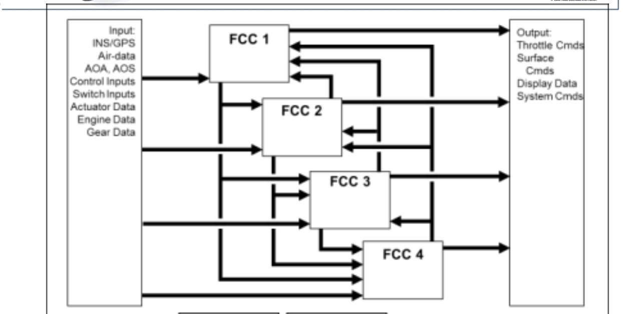
Rockwell Collins
Building trust every day

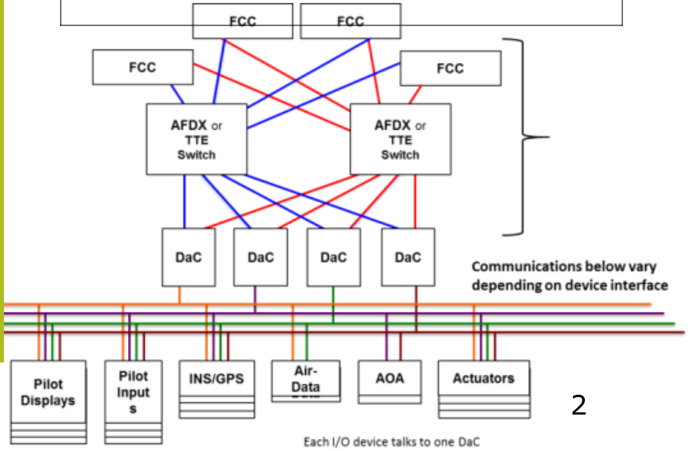
Similar concerns…


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
Actuation Voting 2/3
Reactor Trip Relay 2/4
CRD Breaker Trip
Priority Logic Module
Safety Actuators
Monitoring & Service Interface (MSI) aka Communication Interface
Plant Bus and Main Plant Computer System
Non-Safety Sensors
Non-Safety Systems
Non-Safety Plant Systems
Non-Safety Actuators
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
Emergency Core Cooling System
Emergency Feed Water System
Containment Isolation
Containment Spray System
TRANSMITTERS
PZR
S/G
CONTROL RODS
REACTOR VESSEL
I
II
III
IV
2/4
2/4
Actuation Train B
Actuation Train A
CONTROL ROD POWER SUPPLY
Safeguards Loads




BOEING 787-8
BOEING
AleniaAeronautica
Parker Aerospace
Rockwell Collins
Main instrument panel, shroud and centre console
Front elevation showing in-flight wing flex
Cabin cross-section
Boeing 787 family
787-3 – Length: 57m Passengers 223
787-8 – Length: 57m Passengers 223
787-9 – Length: 62m Passengers 259
787-10X – Length: 68m
Tim Bicheno-Brown 2006
FLIGHT INTERNATIONAL
www.flightglobal.com





Safety-critical

Regulated

Replication for fault-tolerance

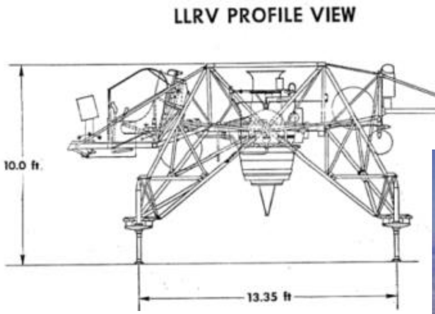
Software intensive

Fail-safe

Fail-op

History of Digital Flight Control

- Reduce weight & cost
- Improved automation
- Advanced functionality
- Safety through redundancy



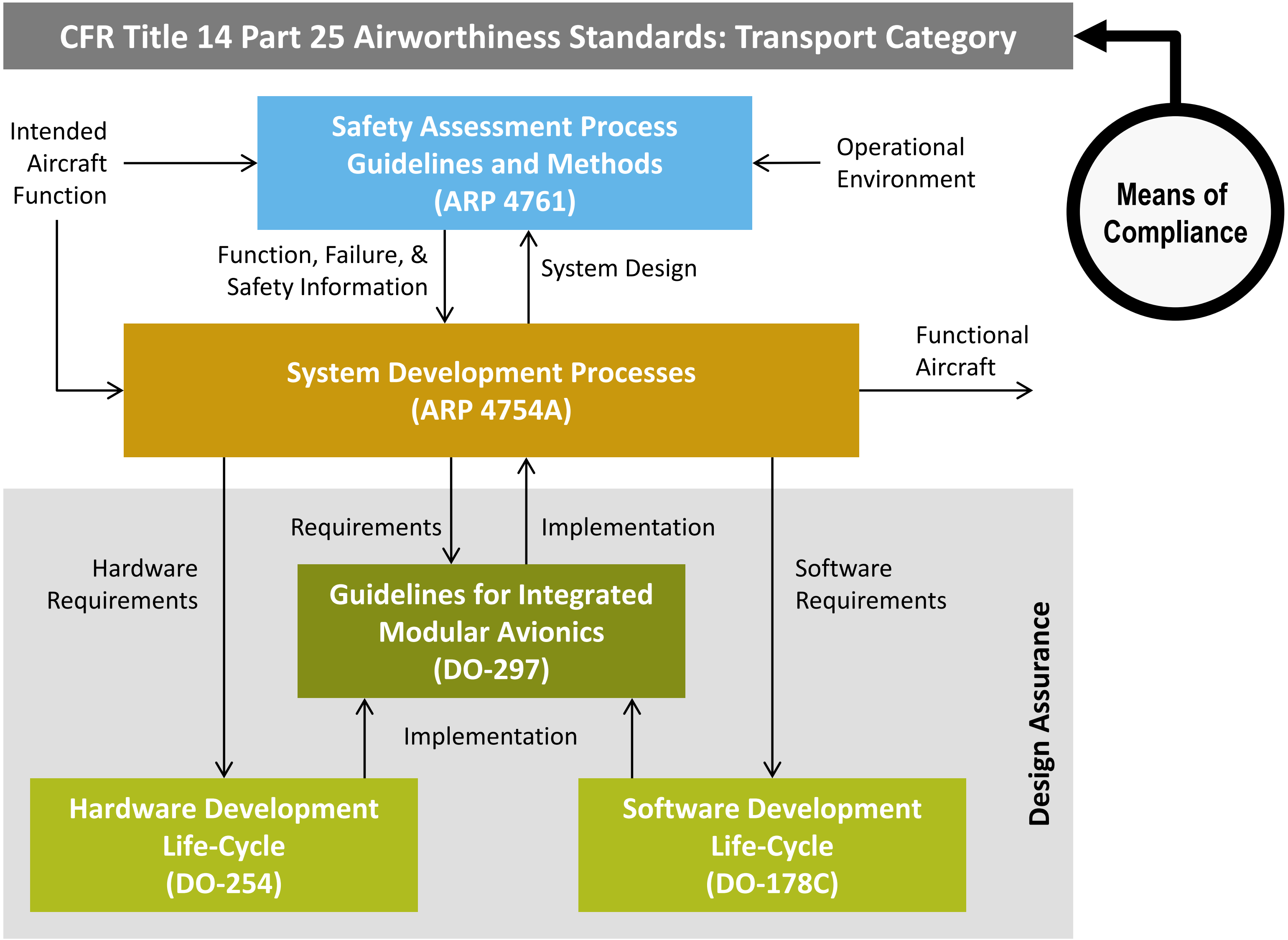
1964: LUNAR LANDING RESEARCH VEHICLE (Analog electronics with no mech. backup)

1972
NASA F-8C CRUSADER
FLY-BY-WIRE

1977
SPACE SHUTTLE
ORBITER

1984
AIRBUS A380

Certification Process for Civil Aviation



CFR Title 14 Part 25 Airworthiness Standards: Transport Category

Means of Compliance

Intended Aircraft Function

Safety Assessment Process Guidelines and Methods (ARP 4761)

Operational Environment

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

Implementation

Hardware Development Life-Cycle (DO-254)

Software Development Life-Cycle (DO-178C)

Design Assurance

Why does this work?

- Conservative industry with strong safety culture
- Consensus-based process between industry and regulators to develop guidance
- Lots of testing!

DO-178B

Primarily a *design assurance* document

- Demonstrate that SW implements requirements
- and nothing else (no surprises)

Requires auditable *evidence* of specific processes

- Planning, Development, Verification, Configuration Management, Quality Assurance, Certification Liaison

Five Software Levels

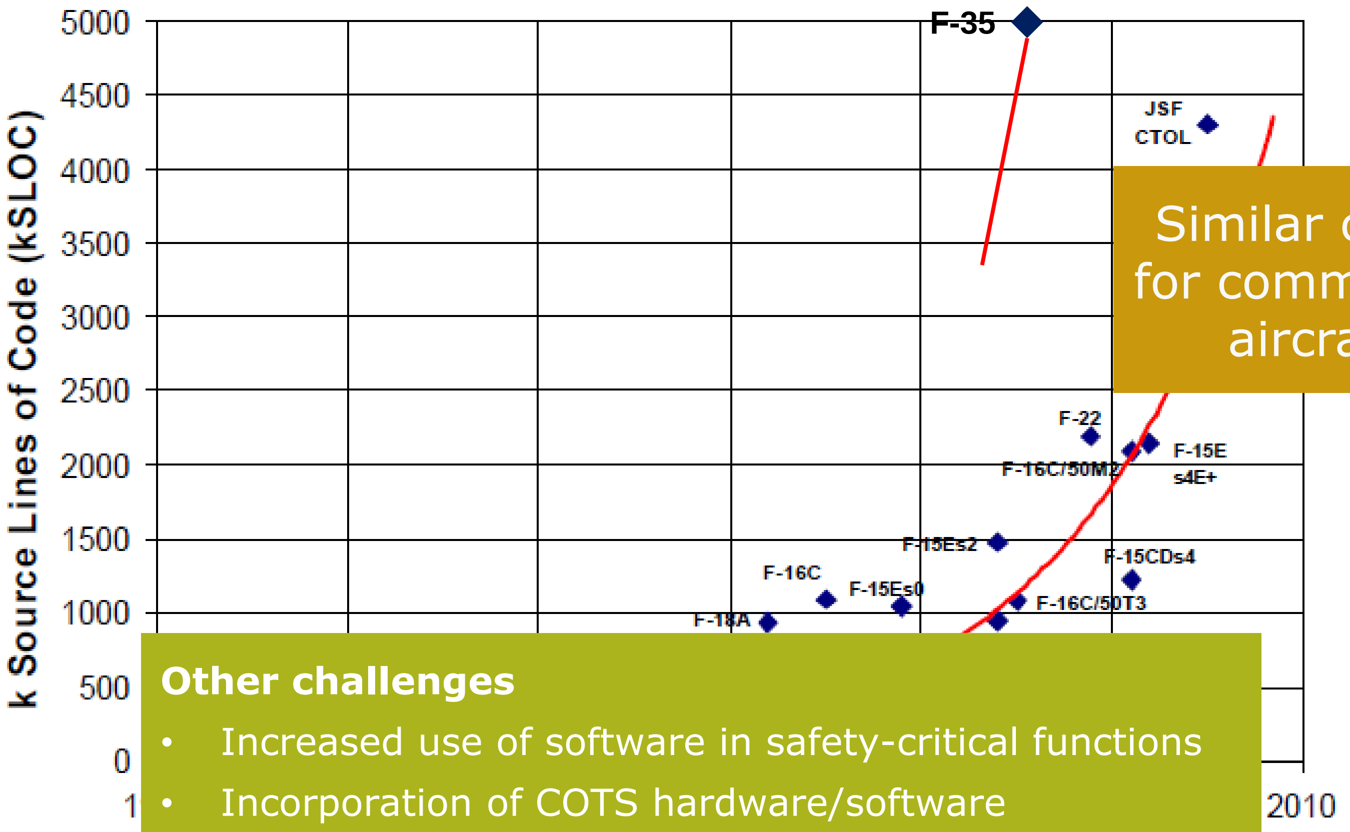
- Design Assurance Level in other contexts

Requirements-based testing

Traceability

Structural coverage metrics

But onboard software is growing!



Similar curve for commercial aircraft

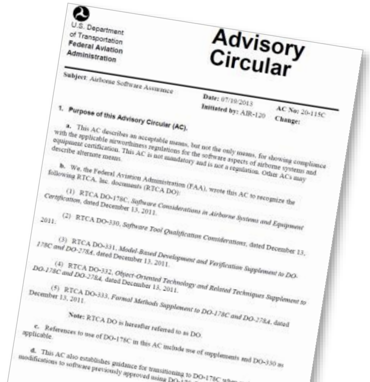
Other challenges

- Increased use of software in safety-critical functions
- Incorporation of COTS hardware/software
- New technologies that challenge existing processes
- Limitations of testing for safety assurance

Source:
Learned

sons

DO-178C (and friends)



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.

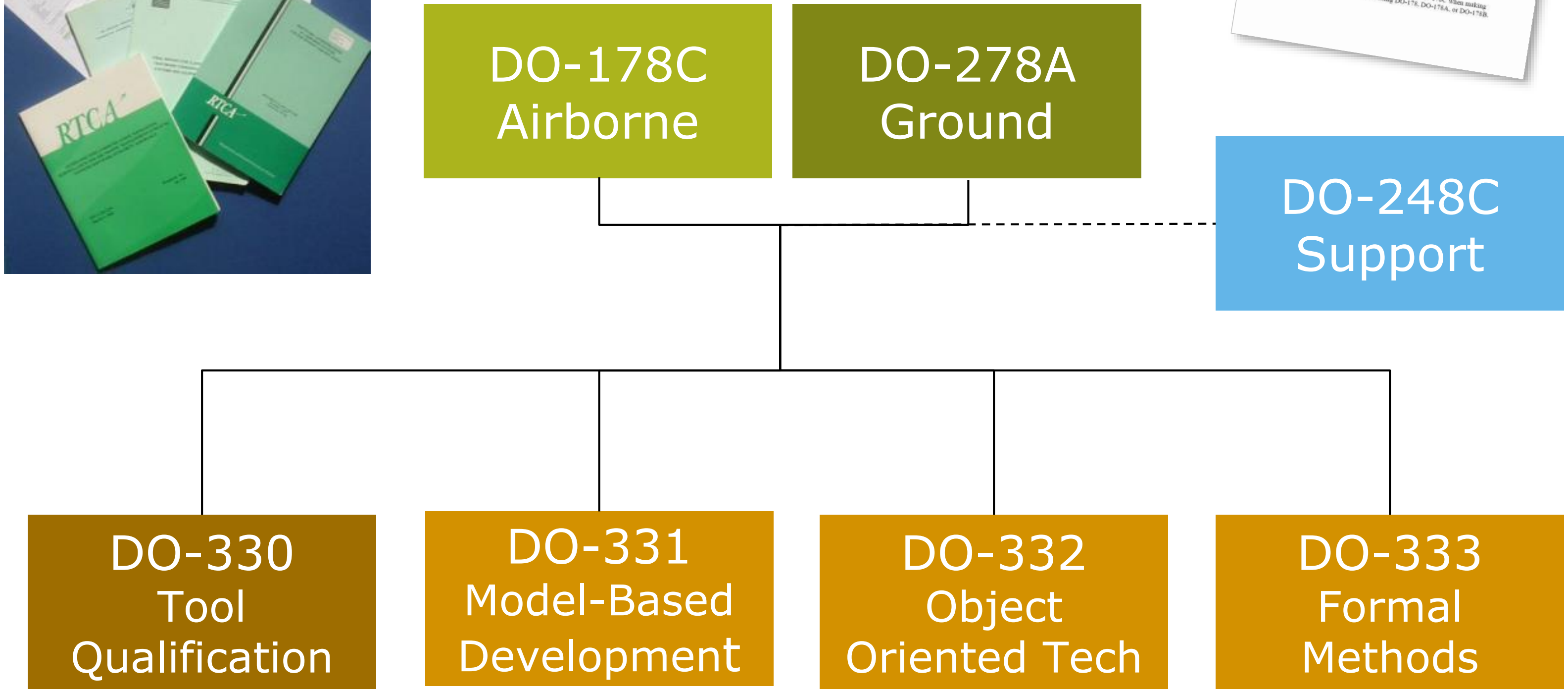
(4) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(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.



New Tools for Software Analysis

- Mathematical techniques for the specification, development, and verification of software aspects of digital systems
  - Formal logic, discrete mathematics, and computer-readable languages

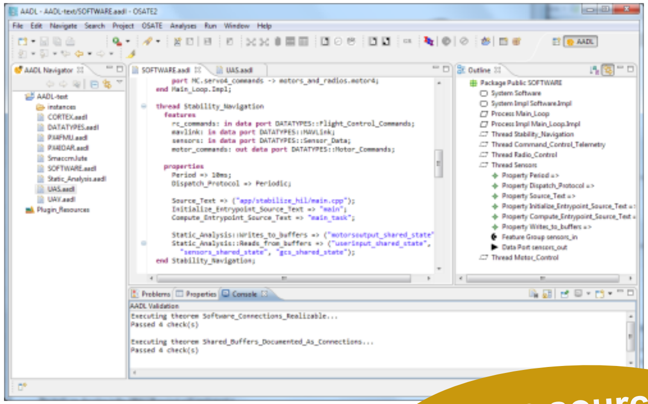
Motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analyses on software-based systems can contribute to establishing the correctness and robustness of a design

Analogy:
FEA for structures

Research Results:
Mathematical Analysis Tools for Software-Based Systems

OSATE

Trusted Build


AADL - AADL-text/SOFTWARE.aadl - OSATE2
File Edit Navigate Search Project OSATE Analyses Run Window Help
AADL Navigator
SOFTWARE.aadl
UAS.aadl
Outline
AADL
Problems
Properties
Console

AADL-text
- instances
- CORTEX.aadl
- DATATYPES.aadl
- PX4FMU.aadl
- PX4IOAR.aadl
- SmaccmJute
- SOFTWARE.aadl
- Static_Analysis.aadl
- UAS.aadl
- UAV.aadl

Plugin_Resources

```
      port MC.servo4_commands -> motors_and_radios.motor4;
  end Main_Loop.Impl;

  thread Stability_Navigation
    features
      rc_commands: in data port DATATYPES::Flight_Control_Commands;
      mavlink: in data port DATATYPES::MAVLink;
      sensors: in data port DATATYPES::Sensor_Data;
      motor_commands: out data port DATATYPES::Motor_Commands;

    properties
      Period => 10ms;
      Dispatch_Protocol => Periodic;

      Source_Text => ("app/stabilize_hil/main.cpp");
      Initialize_Entrypoint_Source_Text => "main";
      Compute_Entrypoint_Source_Text => "main_task";

      Static_Analysis::Writes_to_buffers => ("motorsoutput_shared_state"
      Static_Analysis::Reads_from_buffers => ("userInput_shared_state",
        "sensors_shared_state", "gcs_shared_state");
  end Stability_Navigation;
```

Package Public SOFTWARE
- System Software
- System Impl Software.Impl
- Process Main_Loop
- Process Impl Main_Loop.Impl
- Thread Stability_Navigation
- Thread Command_Control_Telemetry
- Thread Radio_Control
- Thread Sensors
  - Property Period =>
  - Property Dispatch_Protocol =>
  - Property Source_Text =>
  - Property Initialize_Entrypoint_Source_Text =:
  - Property Compute_Entrypoint_Source_Text =
  - Property Writes_to_buffers =>
  - Feature Group sensors_in
  - Data Port sensors_out
- Thread Motor_Control

AADL Validation

```
Executing theorem Software_Connections_Realizable...
Passed 4 check(s)

Executing theorem Shared_Buffers_Documented_As_Connections...
Passed 4 check(s)
```

Resolute

Assurance Case

AGREE

Behavioral Analysis

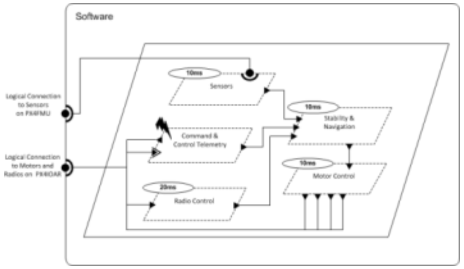
open source tools

Architecture Models

Architecture Translation

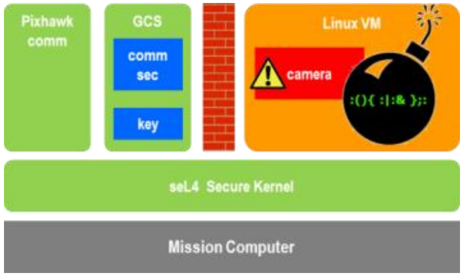
Architecture Analysis

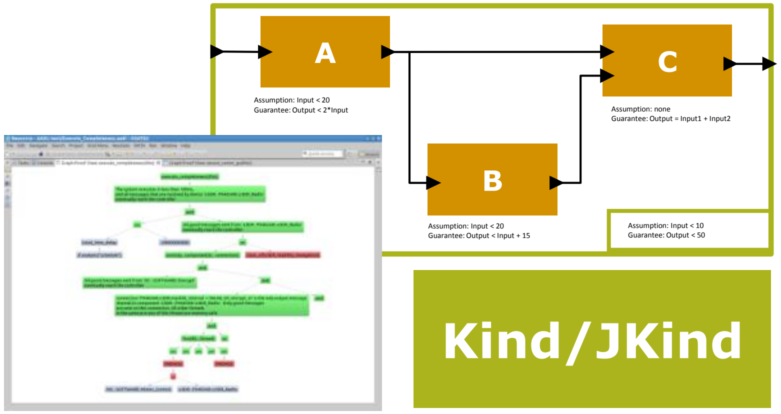
AADL


Software
Logical Connection to Sensors on PX4FMU
Logical Connection to Motors and Radios on PX4IOAR
10ms
Sensors
10ms
Stability & Navigation
Command & Control Telemetry
10ms
Motor Control
20ms
Radio Control

seL4

Security. Performance. Proof.





Kind/JKind

Lessons
learned

Tools

- Model-Based Development tools have been **successfully adopted** by aviation industry for safety-critical software
- Analysis tools for software-based systems are **sufficiently mature** and practical for application in real projects
- Success at the software component (unit) level is being replicated at the system level to **manage complexity**
  - Verification of safety properties of system architecture
  - Assurance case integrated with system architecture model

Certification

- Certification processes **change slowly**
  - Concerns of industry
  - Concerns of regulators
- Certification guidance for airborne software has been able to evolve to address **new technologies**
  - Joint effort of industry and regulators
- **Case studies** are helpful to bridge the gap between theory and practice
  - Pilot projects can help in the transition

Cost matters

- Most defects occur in requirements/design phases
- Defects are more expensive to correct later in process
- Analysis tools can be used to **reduce costs**
  - Early detection/elimination of design defects
  - Automation of routine verification activities
- Multiple studies show good ROI

Loonwerks

More info available at
Loonwerks.com