Safety Assurance in Digital Safety Systems

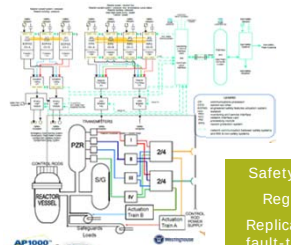
From Airplanes to Atoms

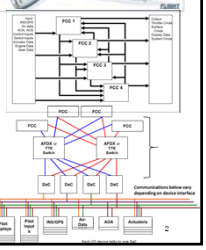
Nuclear Regulatory Commission
Regulatory Information Conference
Session TH35
12 March 2015

Dr. Darren Cofer
cofer@ieee.org

Rockwell Collins

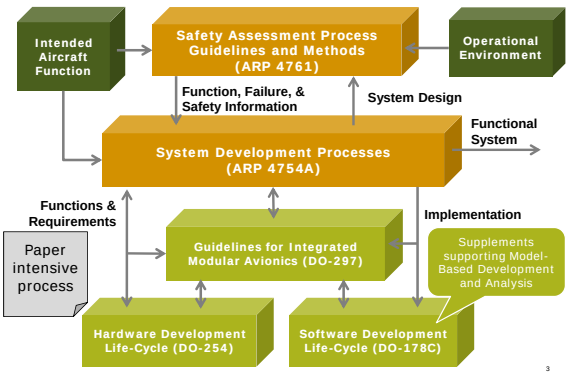
Similar concerns…





- Safety-critical
- Regulated
- Replication for fault-tolerance
- Software intensive
- ⬅ Fail-safe
- Fail-op ➡

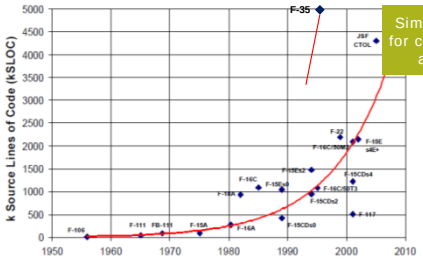
Certification Process for Civil Aviation



Rockwell Collins

Software is growing!

"Software providing essential JSF capability has grown in size and complexity, and is taking longer to complete than expected," the GAO warned. **Pentagon: Trillion-Dollar Jet on Brink of Budgetary Disaster,** Wired 3/21/12



Similar curve for commercial aircraft

Source: D. Gary Van Oss (USAF), "Avionics Acquisition, Production, and Sustainment: Lessons Learned – The Hard Way," NDIA Systems Engineering Conference, Oct 2002.

4

Rockwell Collins

- 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

What can NRC learn from civil aviation experience?

5

Rockwell Collins

Analytic 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

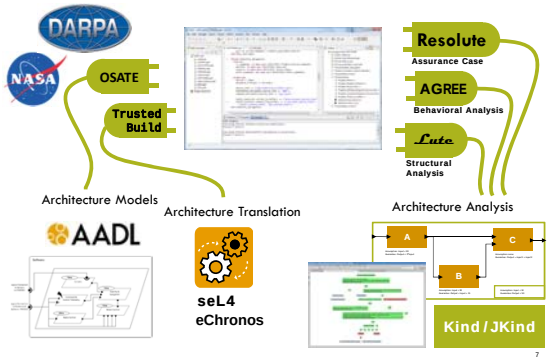
Motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analyses on software-based systems can contribute to establishing the correctness and robustness of a design

Analogy: FEA for structures

6

Rockwell Collins

Research Results:
Mathematical Analysis Tools for Software-Based Systems



7

Rockwell Collins

8

Rockwell Collins

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 capable to be applied to 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

9

Rockwell Collins

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

10

Rockwell Collins

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

11