FM@COLLINS

FM@SCALE
25 SEPTEMBER 2019
ARLINGTON VA

DR. DARREN COFER
TRUSTED SYSTEMS
DARREN.COFER@COLLINS.COM

Collins Aerospace

https://www.quantamagazine.org/formal-verification-creates-hacker-proof-code-20160920/

WHY SHOULD COLLINS AEROSPACE CARE ABOUT FORMAL METHODS?

By analyzing requirements, models, and software early in the development process, we can eliminate defects, reducing costly rework and even more costly escapes.

- Satisfy certification objectives?
  - Maybe (see DO-333)
- Eliminate testing?
  - Some, but not all
- Be the **most trusted** source of aviation and **high-integrity** solutions in the world?
  - Definitely!

THE REAL REASON WE WILL USE FORMAL METHODS

- To reduce costs
  - Automation of tedious reviews and testing that humans are terrible at anyway
  - Reduce cost of rework
  - Reduce cost of escapes

THE REAL REASON WE WILL USE FORMAL METHODS

- To reduce costs
  - Automation of tedious reviews and testing that humans are terrible at anyway
  - Reduce cost of rework
  - Reduce cost of escapes

    (Undetected design error that compromises safety)

The New York Times

Boeing Says Charges Tied to 737 Max Grounding to Reach $8 Billion

Boeing 737 Max planes parked at the municipal airport in Renton, Wash. The Max planes have been grounded after two were involved in deadly crashes.
Lindsey Wasson for The New York Times

By David Gelles

July 18, 2019

The financial fallout from the troubled 737 Max jetliner continues to swell for Boeing, which on Thursday announced $7.3 billion in costs that will hit its bottom line.

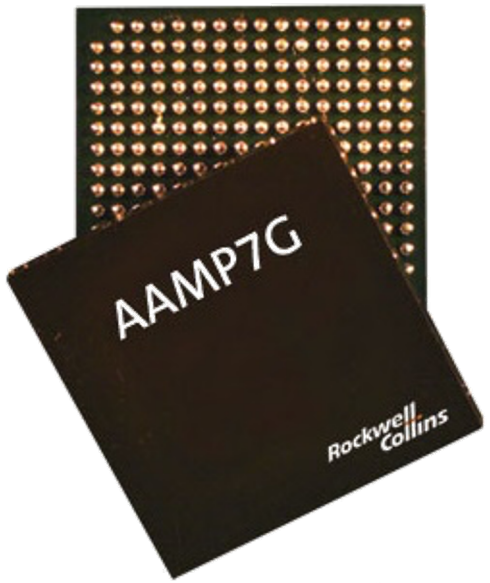
FM@COLLINS : SUCCESSES

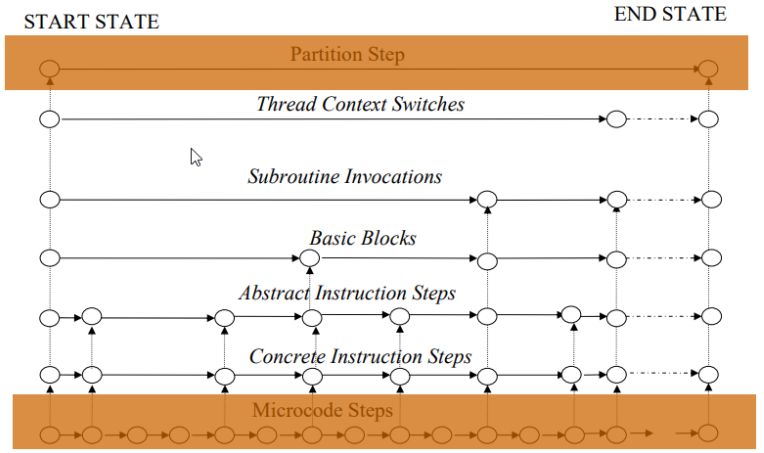
DO IT ONCE

TURNSTILE / AAMP7 / SEL4

- Large, sustained effort by formal methods experts to produce a product or other reusable artifact
- AAMP7G microprocessor with intrinsic partitioning
- Turnstile cross-domain guard
- GH Integrity certification
- seL4 microkernel

  (Data61, FoC)



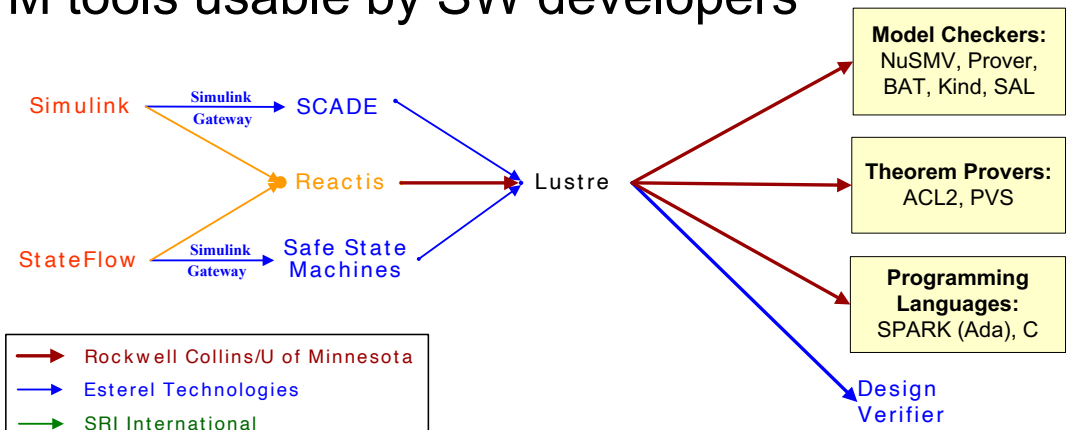


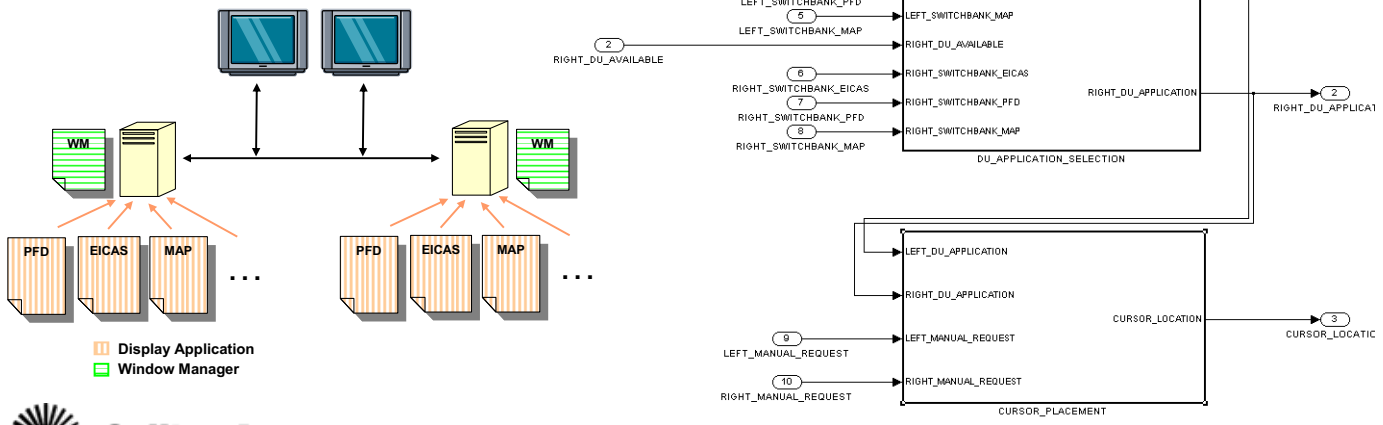
Collins Aerospace

DO IT LOTS

GRYPHON / FSV

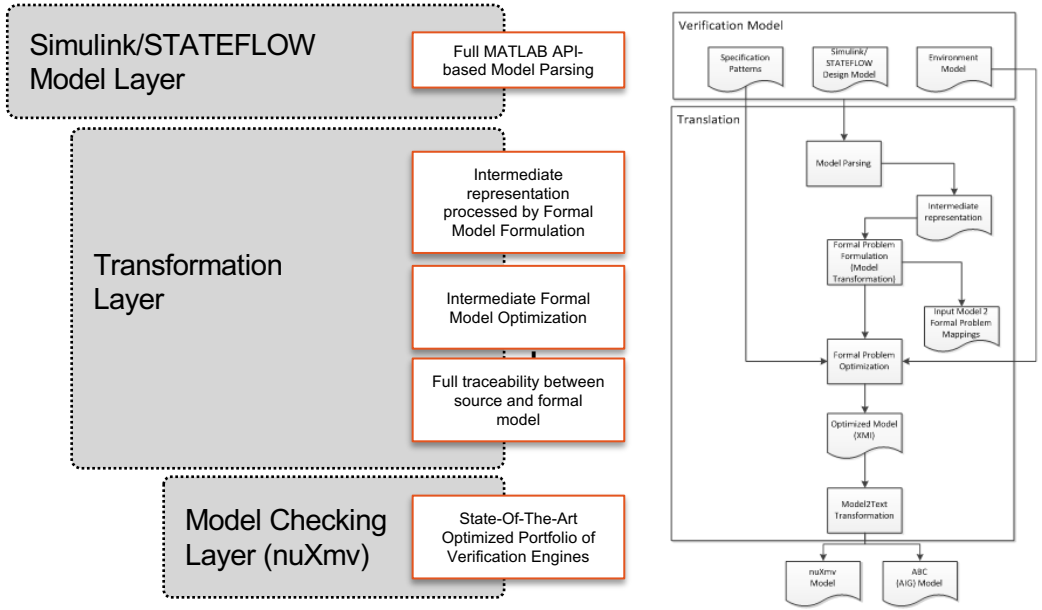
- FM tools usable by SW developers

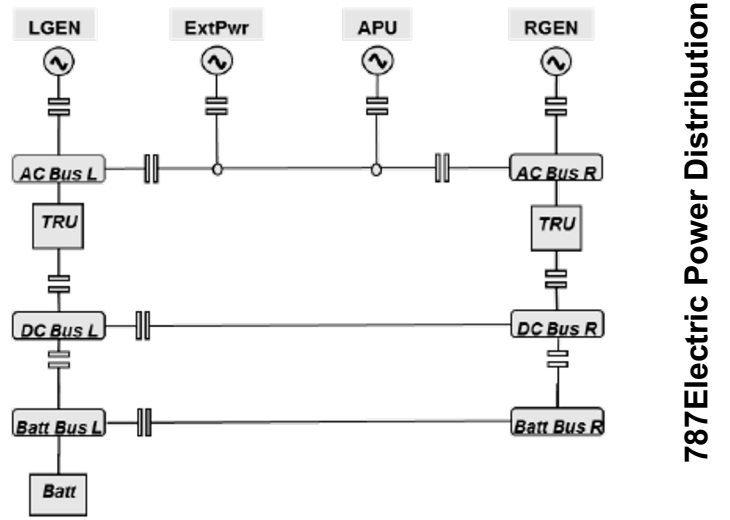




UTAS / UTRC

Formal Specs Verifier (FSV) for Formal Verification



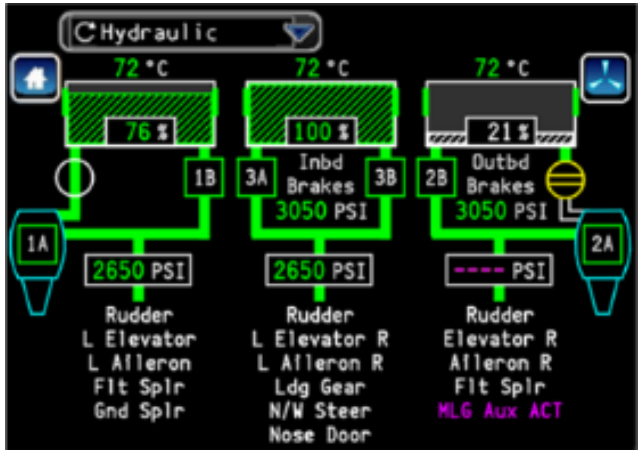


787Electric Power Distribution

Collins Aerospace

DO IT LOTS

CERTIFICATION TOOLS FOR COMMERCIAL AVIONICS



Custom domain-specific tools using FM to automate:

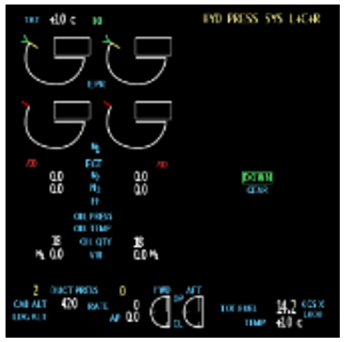
- extensive peer reviews of requirements, designs, and code
- manually generated structural tests
- process documentation

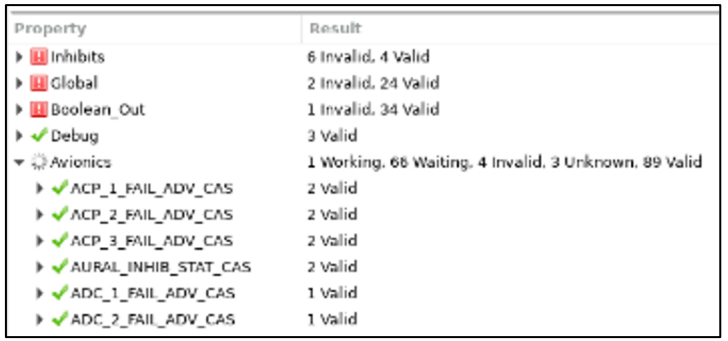
New methods use automated reasoning to improve today's labor-intensive methods

AUTOMATED CERTIFICATION TOOLS

Crew Alerting

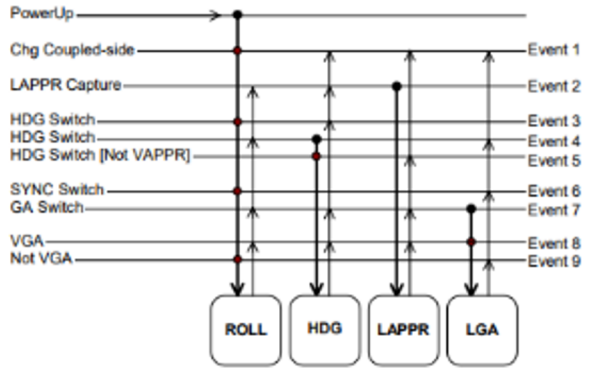
- Automated design review and test generation with structural coverage of requirements
- First cert use Sept 2018
- Saved $1.5M on M170 program





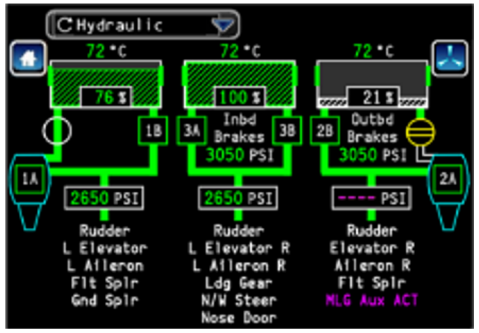
Flight Controls

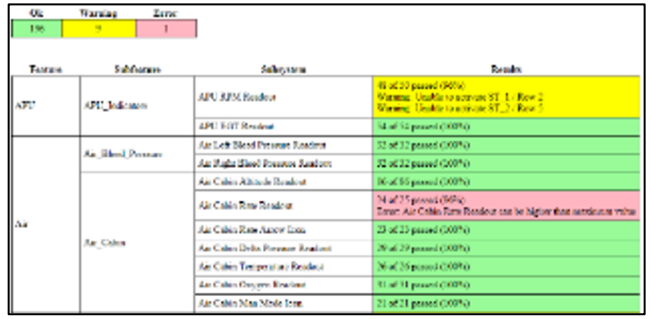
- Custom IDE automates design review and test generation
- First expected cert use 2020



Aircraft Health Monitoring

- Automated review of generated code using CBMC
- First expected cert use 2020

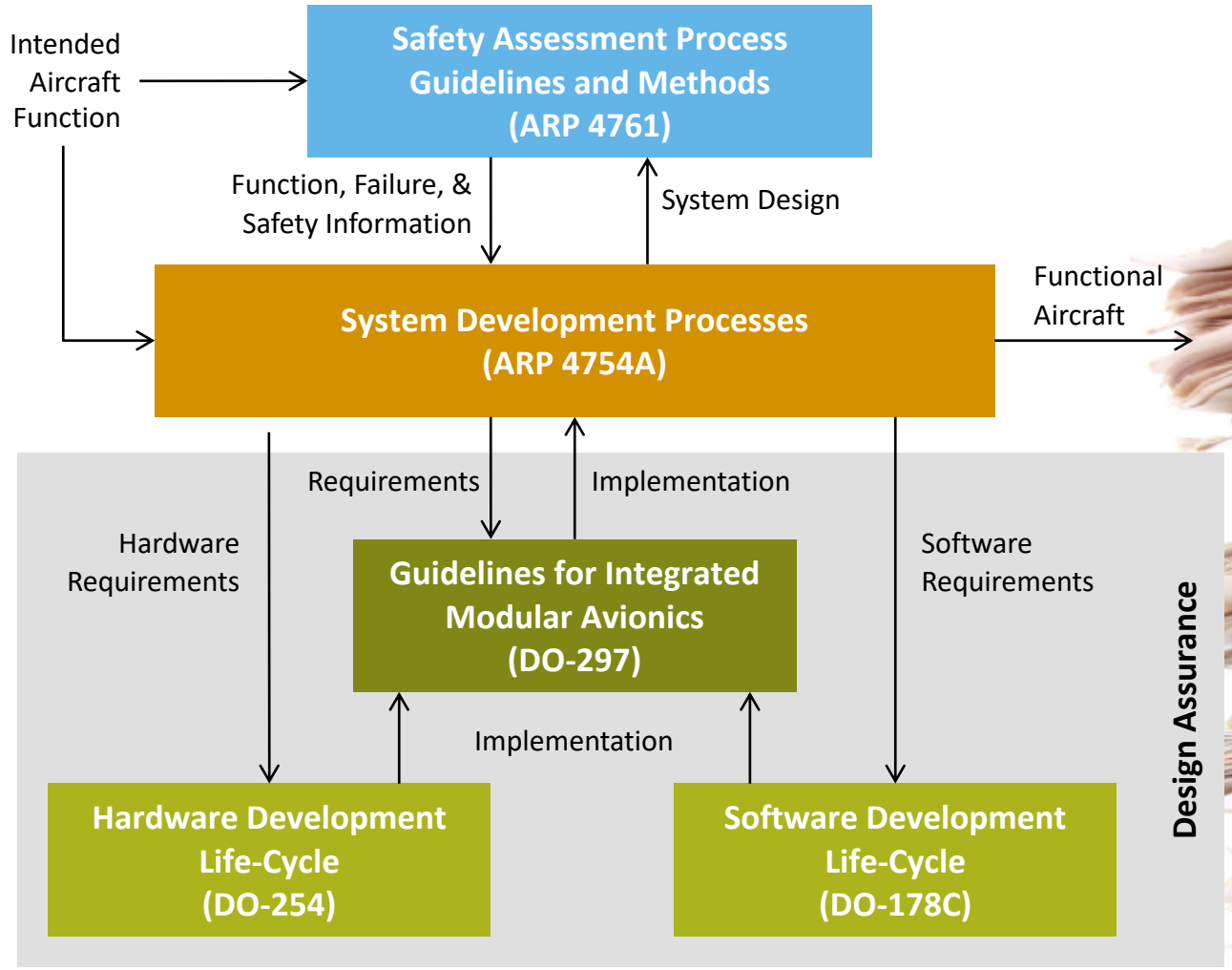


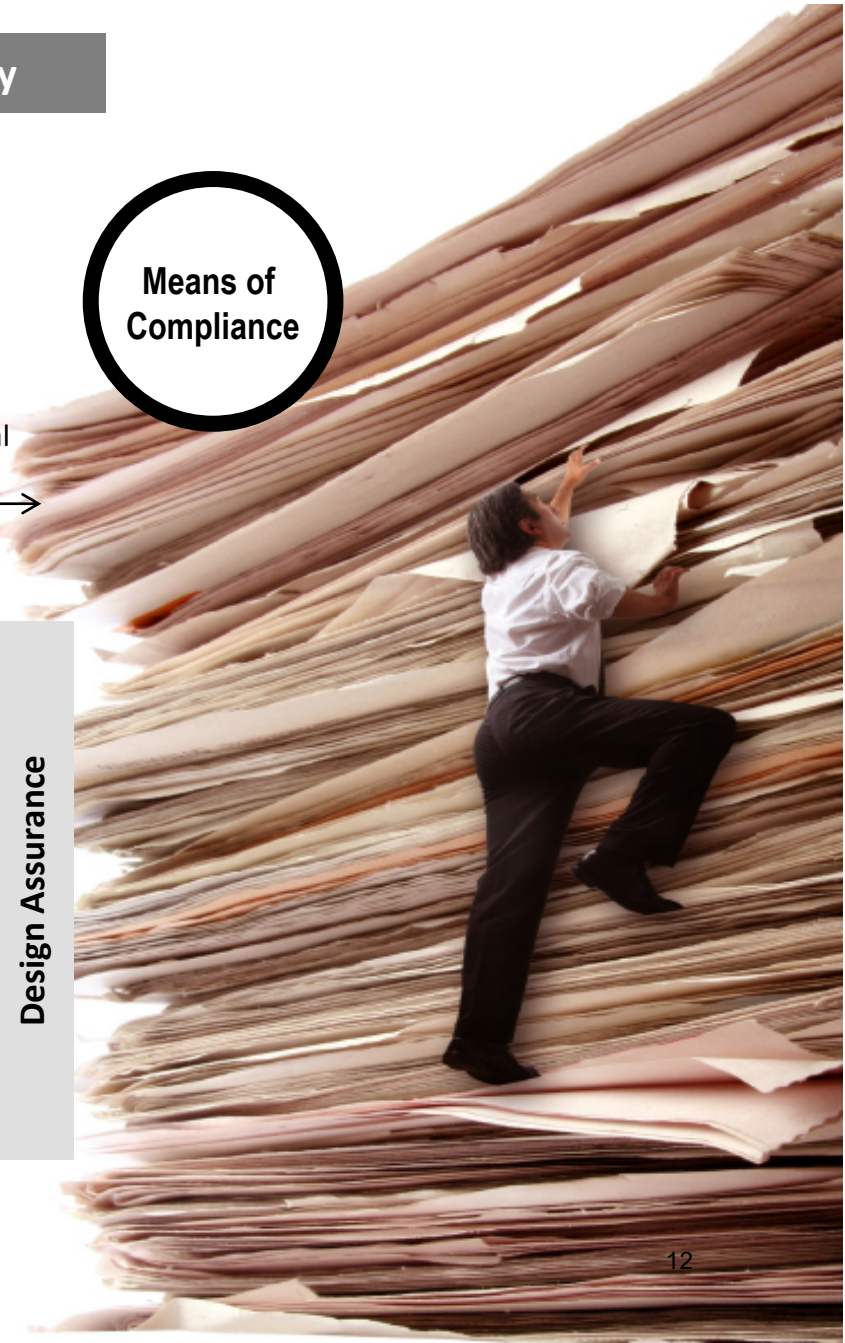


FM@COLLINS : CHALLENGES

CHALLENGES : CERTIFICATION PROCESS

CFR Title 14 Part 25 Airworthiness Standards: Transport Category





CHALLENGES : MANY DOMAINS

Safety-critical
Real-time
Networking
Security domains
Data storage

Sensing
Embedded computing
Human Interface
Maintenance/PHM
GNC

Collins Aerospace

FM@COLLINS : FUTURE

HOW CAN WE SCALE UP APPLICATION OF FORMAL METHODS FOR AVIONICS?

Collins Aerospace

1 : DO IT LOTS MORE

DEVELOP MORE DOMAIN-SPECIFIC TOOLS

- Get *really good* at rapid customization of a standard set of analysis engines for new/different application areas
  - Maximum automation (low-hanging fruit)
  - Target existing domain-specific specifications
  - Evidence generation for certification objectives

2 : PROVABLE SYSTEM SAFETY/SECURITY

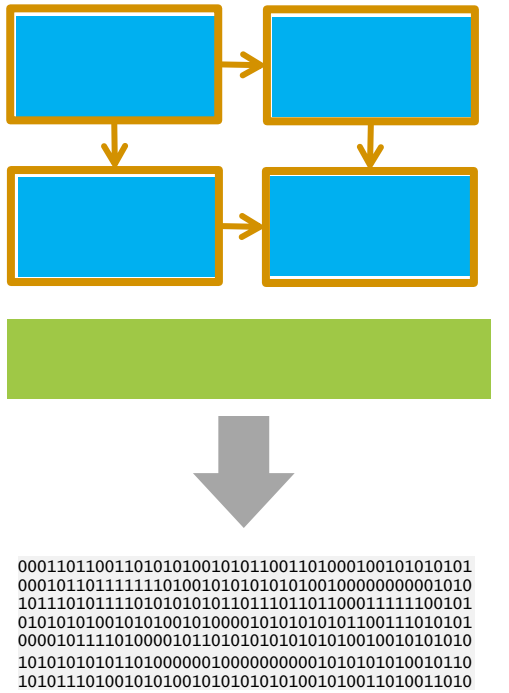
- Standardize on a system architecture language for integrating
  - System design
  - System safety
  - Cybersecurity
- Identify standard properties (requirements) needed for all aircraft/systems/components
  - With some configuration

- Architecture Analysis and Design Language (AADL)
  - Analogous to “infrastructure as code”

ARCHITECTURE-DRIVEN ASSURANCE

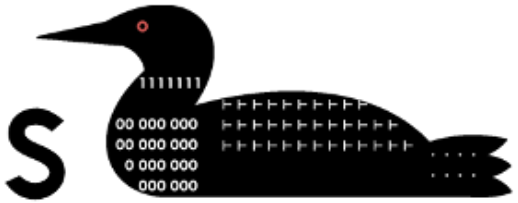
HACMS / CASE / AMASE APPROACH

- Architecture model is correct (AADL)
  - Properties, structure, behavior, interaction of components, interfaces, contracts
  - Verify system safety/security properties (in the presence of faults/threats)
- Components are correct
  - Consistent/realizable contracts
  - Components verified to implement contracts
- System does what the model says
  - Verified kernel (seL4)
  - No other information flows (memory safety, isolation)
  - OS executes model correctly (incl. timing)
- System implementation corresponds to model
  - Automatic build from component and architecture models with proof of compliance to architecture specification



Collins Aerospace

Loonwerks



Code, papers, videos available at:

Loonwerks.com

github.com/Loonwerks

Collins Aerospace

