Testing of Avionics

Dr Stephen Wright

Department of Engineering Design and Mathematics
University of the West of England

steve.wright@uwe.ac.uk

Programme

- Certification authorities
- Certification standards
- Development life cycles
- Tools

Avionics in boxes

Avionics Growth

- F-4A (1958) - 1000 lines-of-code

- F/A-18 (1978) – 1 million lines-of-code

- F-22 (1997) - 1.7 million lines-of-code

- F-35 (2006) - 8 million lines-of-code

Certification Authorities

- National aviation authorities certify aircraft for flight over their territory

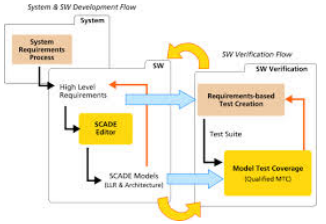
- America: Federal Aviation Administration
- Europe: European Aviation Safety Agency
- United Nations: International Civil Aviation Organization

Aircraft Certification

- A *type certificate* is issued to confirm that an aircraft design is airworthy
- Certified that the aircraft meets Minimum Operational Performance Standards
- MOPS are enforced by agreed procedures
- Procedures are published by non-profit industry organisations
- DO-178 series, DO-254 series (and DO-160 series)

Standards

- DO-254 - electronic hardware
- DO-178C - software
- DO-160G - environmental test conditions



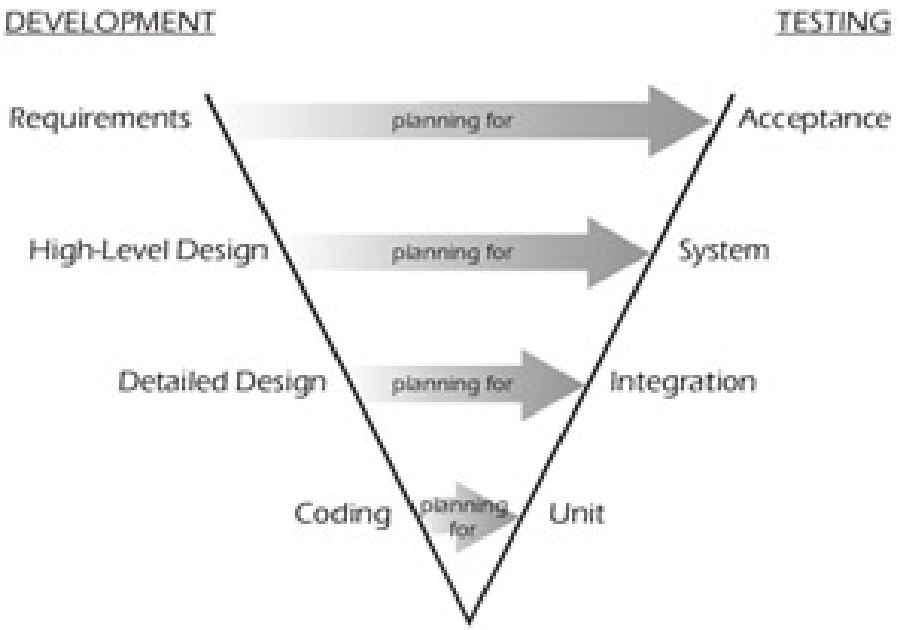
- Note that documents are sometimes republished under a different name by another authority

Avionics development life cycle

- Standards do not prescribe particular methods of design and test (some are recommended)
- Standards only enforce a structured life cycle
- Therefore it is impossible to certify the hardware/software retrospectively
- Standards enforce a V-Model

V – Model*

- Validation – confirming that specification is correct
- Verification – confirming that implementation is correct with respect to specification
- Each level of requirements, specification etc. provides the basis of each level of verification (this is the V)



DO-178C

- Published 2012
- Updated from DO-178B (1992)
- Published by RTCA Inc. and EUROCAE
- Defines Design Assurance Levels
- Demands V-Model development with documented traceability between levels
- Recommends certain techniques (e.g. Formal Methods and Model Based Design)

Jargon Buster

Radio Technical Commission for Aeronautics = technical guidance for use by US government regulatory authorities and industry

European Organisation for Civil Aviation Equipment = works together with RTCA

DO-254

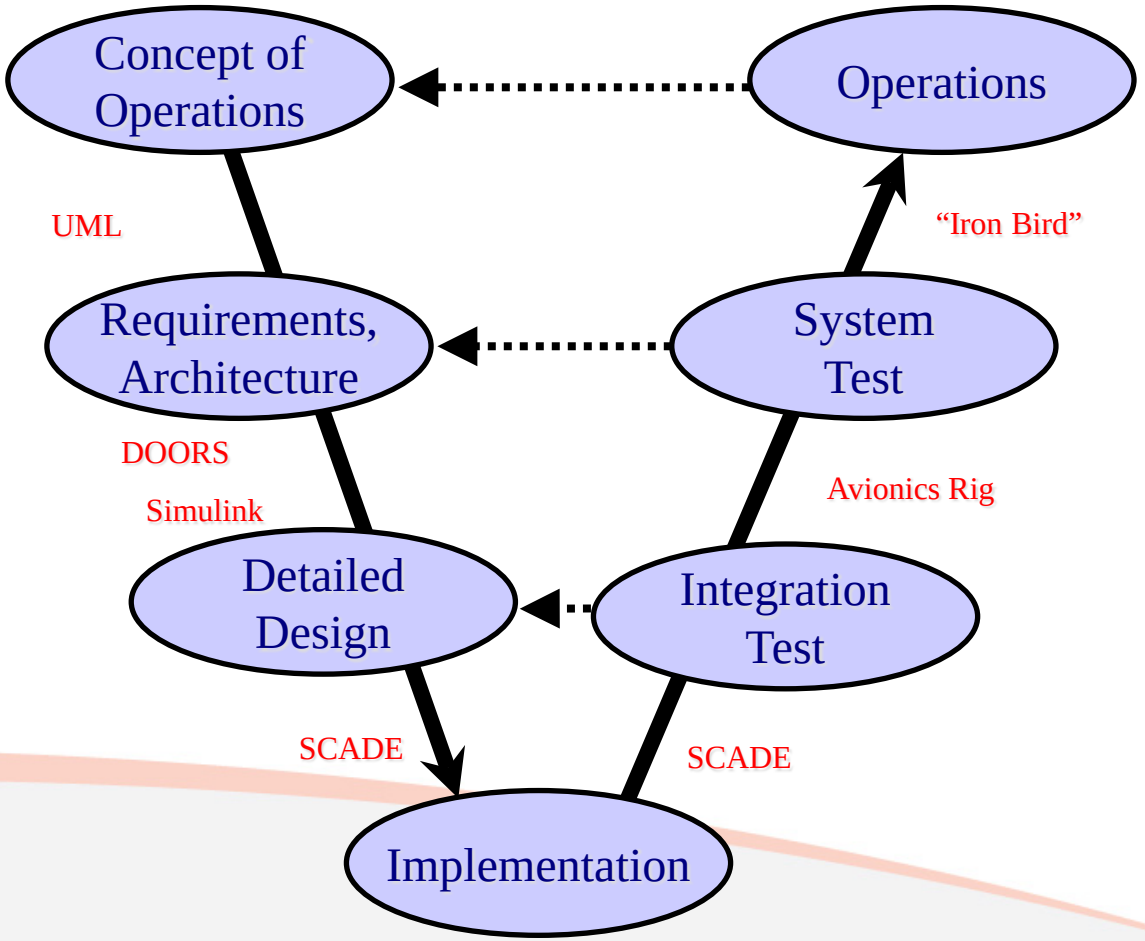
- Published 2005
- Similar form to DO-178C (e.g. V-Models, DALs)
- Covers FPGAs, PLDs, ASICs (i.e. a reaction to flexible hardware technologies)

Design Assurance Level

- Level A – Catastrophic : 10^{-9} failures/flight-hour
- Level B – Hazardous: 10^{-7} failures/flight-hour
- Level C – Major: 10^{-5} failures/flight-hour
- Level D – Minor: 10^{-3} failures/flight-hour
- Level E – No Effect: Not Applicable

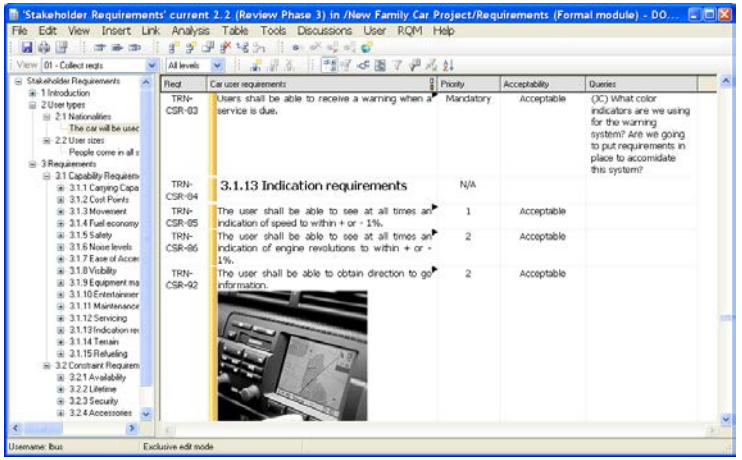
Tools

- Requirements
- Validation
- Development
- Verification
- Test

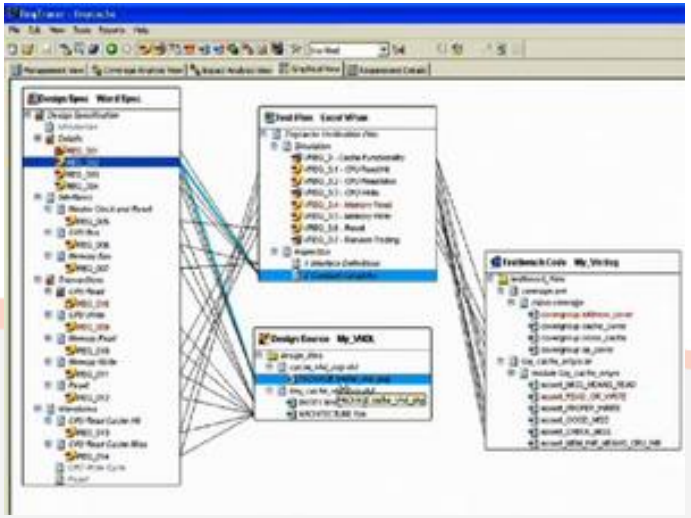


Requirements Capture

- Rational Dynamic Object Oriented Requirements System (DOORS)

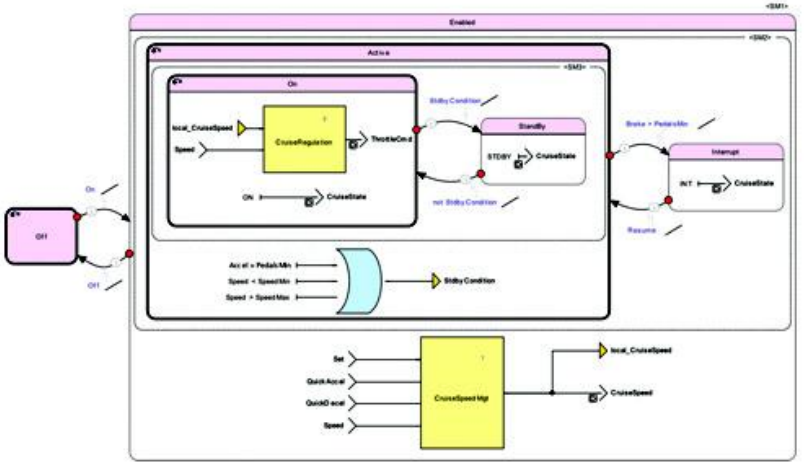


- Visure

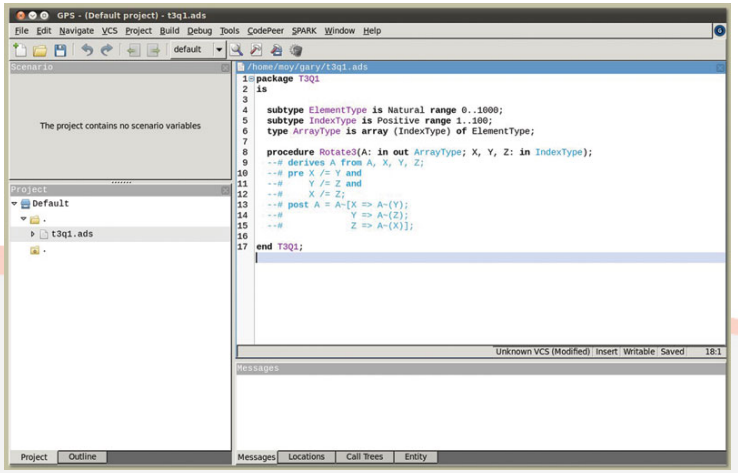


Development

- Esterel SCADE



- Altran SPARK Pro



asureSIGN™ at the heart of HW/SW V&V

Requirements
- Excel
- Doors
- Jira
- etc

SystemC Simulation

UCIS API

XML API

asureSIGN™

Run API

Manual API

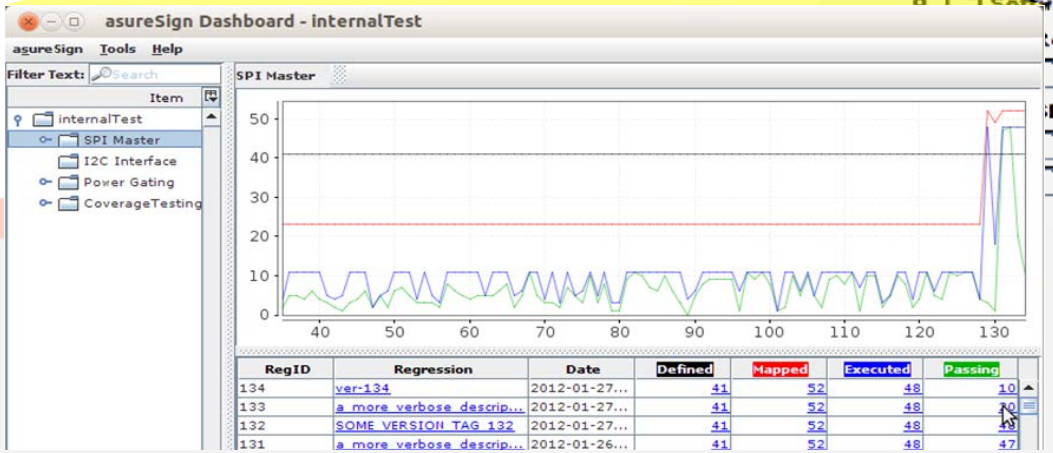
Hardware Simulation
- Coverage — Cadence
- Assertions — Mentor, Aldec
- Etc.

Formal Verification
- OneSpin

Directed test results

Automated SW Test Tool

Lab Results



Matlab

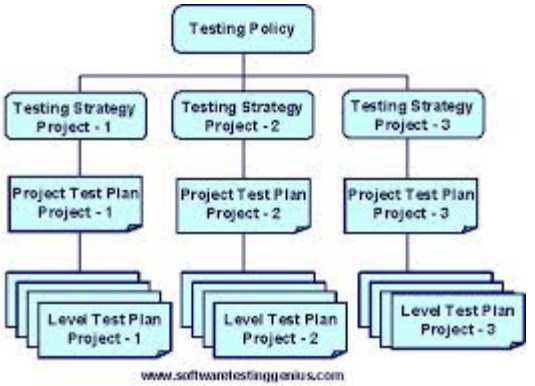
SW Test tools

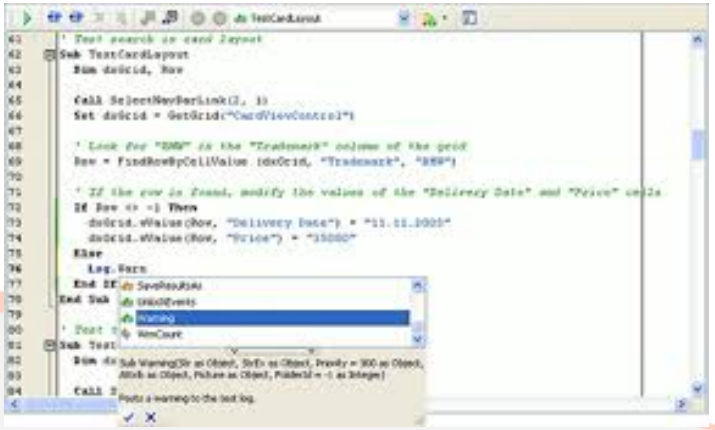
Requirements Engineering

bettertogether

Software Unit Testing

- Individual modules (functions) are tested in isolation
- Unit testing performed outside the “target” avionics hardware
- DO-178C allows some unit testing to be replaced by static analysis techniques





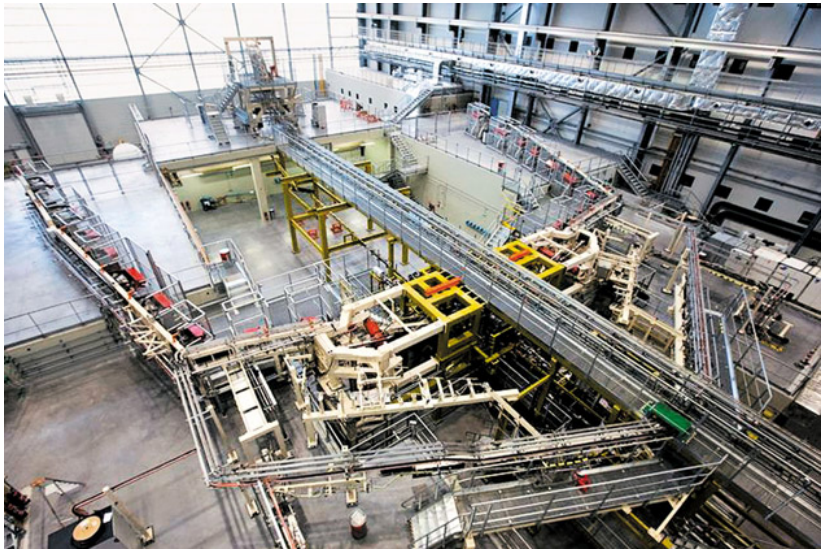
System Integration Benches

- Simulate all physical devices electronically

- Model all systems that interact with SuT in software

Further Testing

- Further testing on "*iron bird*" rigs
- Finally go to *flight test*



Aircraft Flight Test

Flight test is *to be avoided as much as possible*

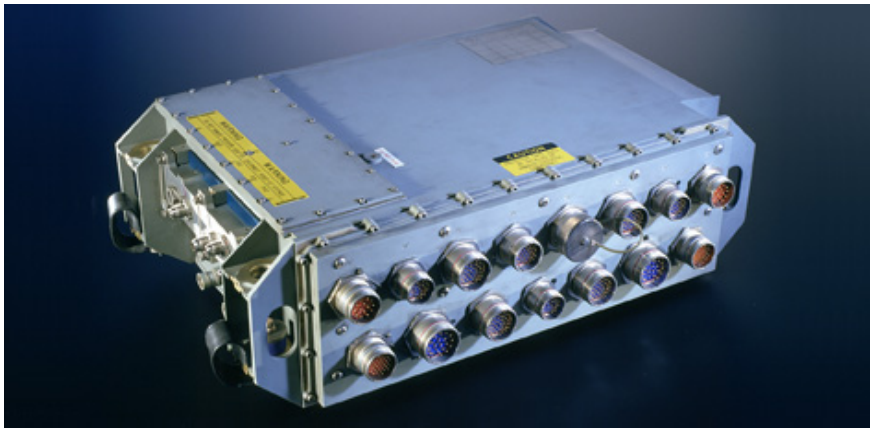
Gulfstream G650, 2011

Airbus A400M, 2015

Boeing 767 Production Flight Test

Costs

- Software production: ~10 loc/day @ ~$100/hour = $800M
- Civil aircraft, avionics about 30% of total cost
- Some military aircraft can be as high as 75%
- Full Authority Digital Engine Controller - $100,000 - $200,000



The future

- Model Based Design
- Formal Methods
- DO178D?
- Generic safety-critical standards

In summary

- Avionics test driven by combination of **certification** and **commercial** goals

- Avionics test is well behind automotive/consumer test

Questions?