High Integrity Software for High Integrity Systems

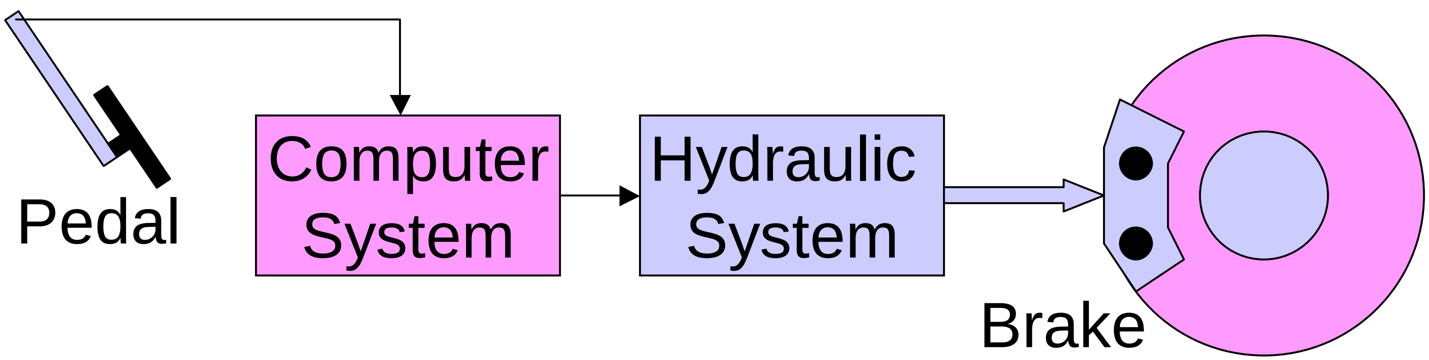
George Romanski
Romanski@Verocel.com

Outline

- System safety
- Safety standards
- Safety objectives
- Military avionics
- Ground based systems
- Future policy
- Directions

Brake-by-Wire Safety Solutions

- System Design - Limit speed to 5 mph
- Hardware Design - use mechanical/hydraulic backup
- Replicate Computer systems - no common mode errors
- Software assurance through compliance with standards (e.g. DO-178B)



DO-178B / ED-12B

- Acceptable means of compliance to the regulators of software in avionics systems

Not the only means of compliance !

But, if you choose a different approach

Must show DO-178B/ED-12B objectives have been met

Intent of DO-178B

- Describe objectives for Life-Cycle Processes
- Describe process activities
- Describe evidence required at different assurance levels

SC-190, WG-52 Committee

- 150 Registered Members
- Consensus based
- 4 years - Report published
  - Annual Report for Clarification of DO-178B (DO-248A)
  - Annual Report for Clarification of ED12B (ED-94A)
- Position Papers
  - Document corrections
  - FAQ’s (Clarifications)
  - Discussion Papers
- CNS/ATM - Work Continues

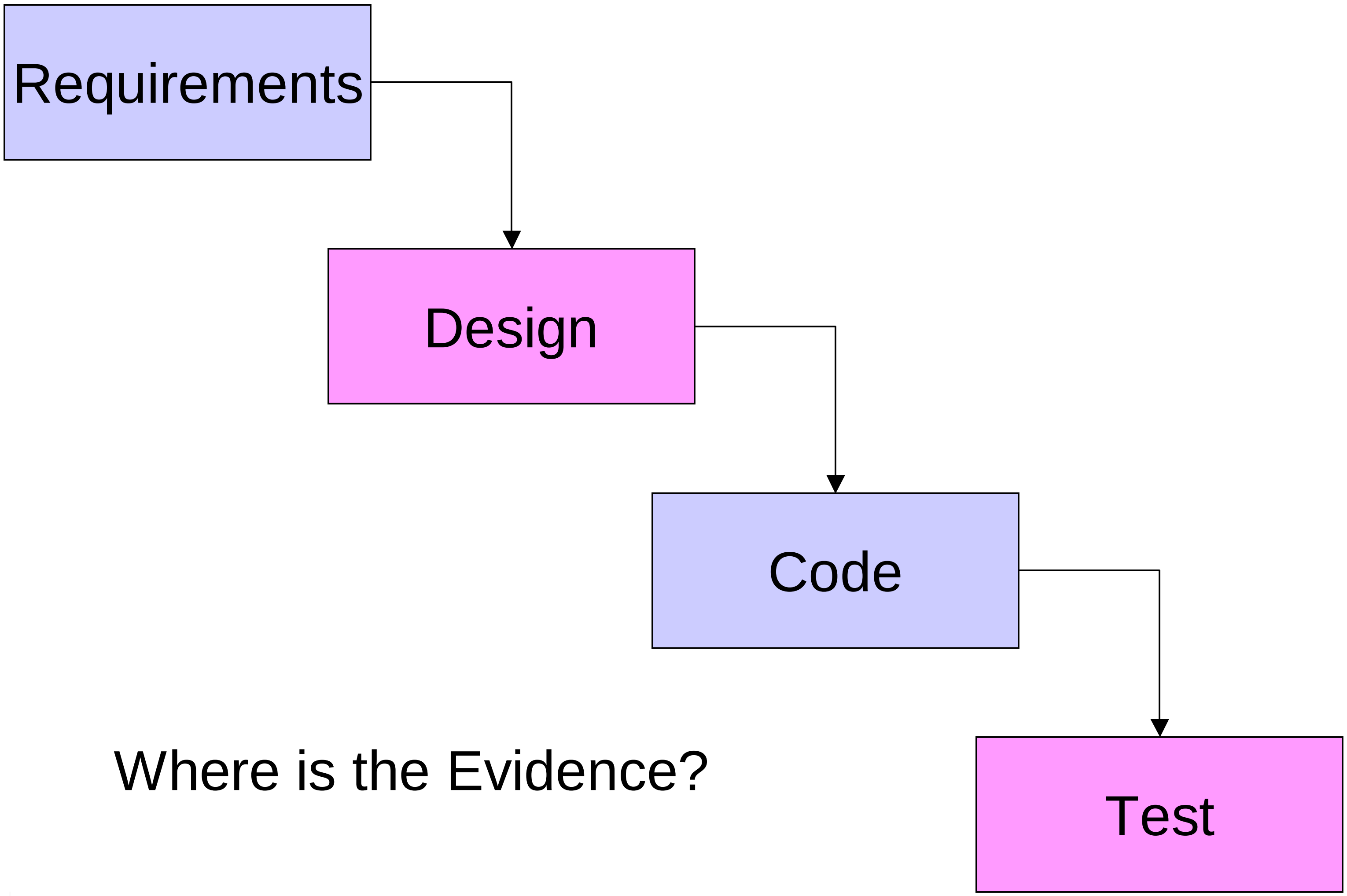
Typical DO-248A clarifications

- Is recursion permitted in airborne applications?
  - Yes, but it must be bounded (…etc)
- Is Source-code to Object-code traceability required?
  - Yes, if providing coverage analysis at source code and level A
  - No, if providing coverage at machine code
- If some run-time functions are inlined, is coverage still required
  - Yes, cannot conceal coverage obligations

Typical DO-248A clarifications Cont.

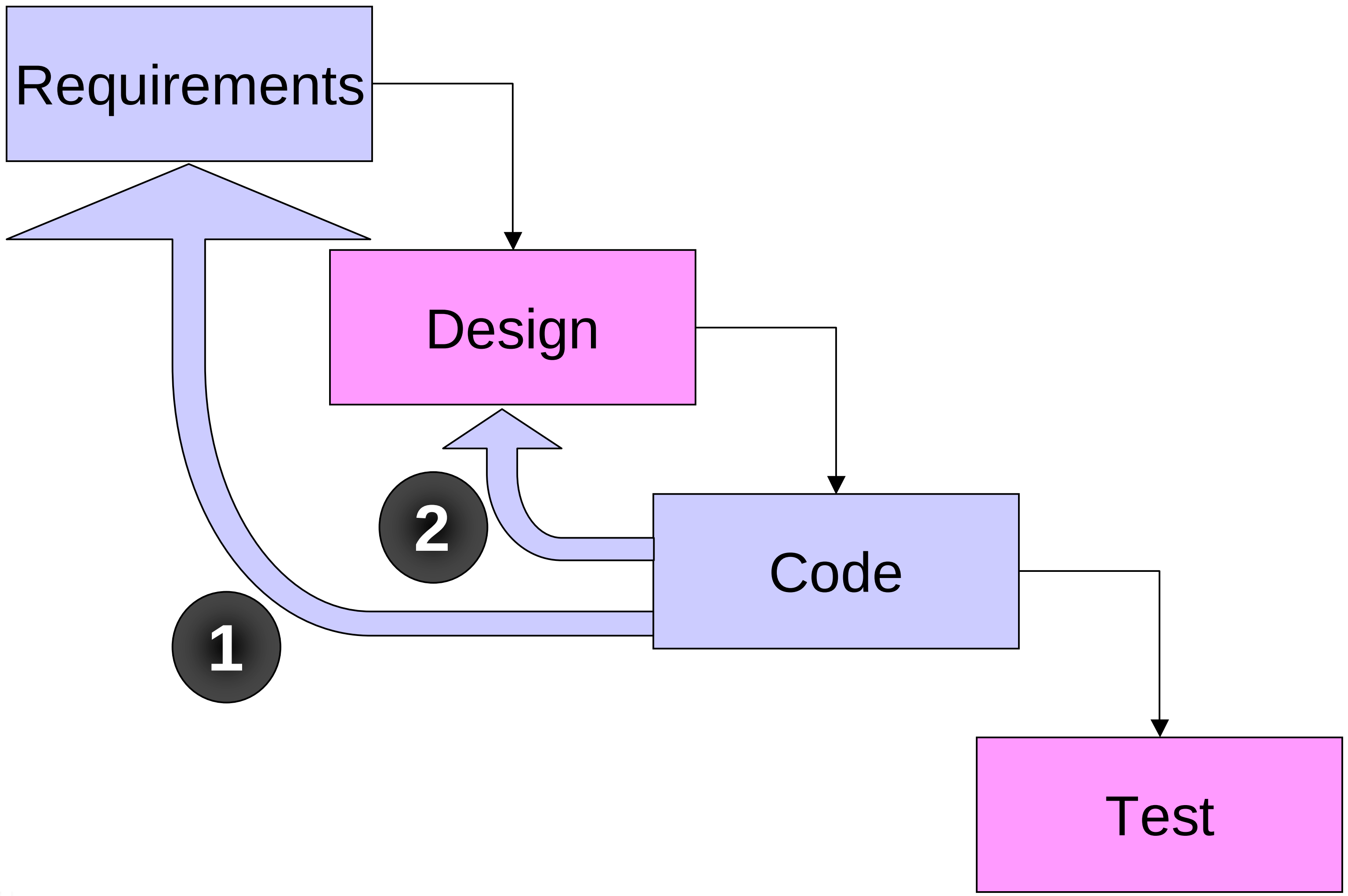
- Can compiler features be used to simplify coverage analysis at object code?
  - Yes! (e.g. short-circuit operations)
  - But, the compiler (feature) is being used as a verification tool so compiler (feature) must be qualified as a verification tool
- What are the issues for reverification of COTS software?
  -

Standard Waterfall Process Model

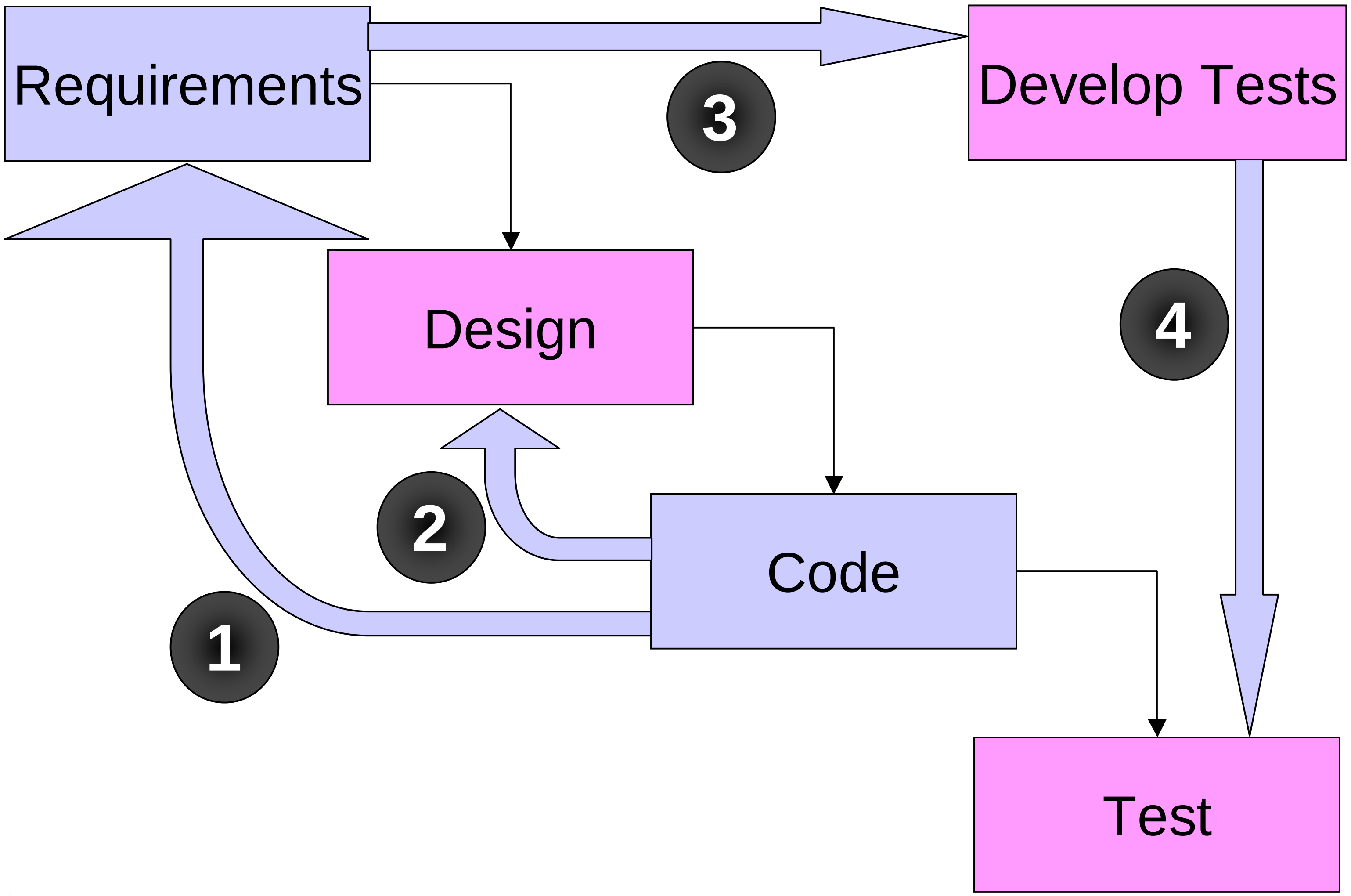


Where is the Evidence?

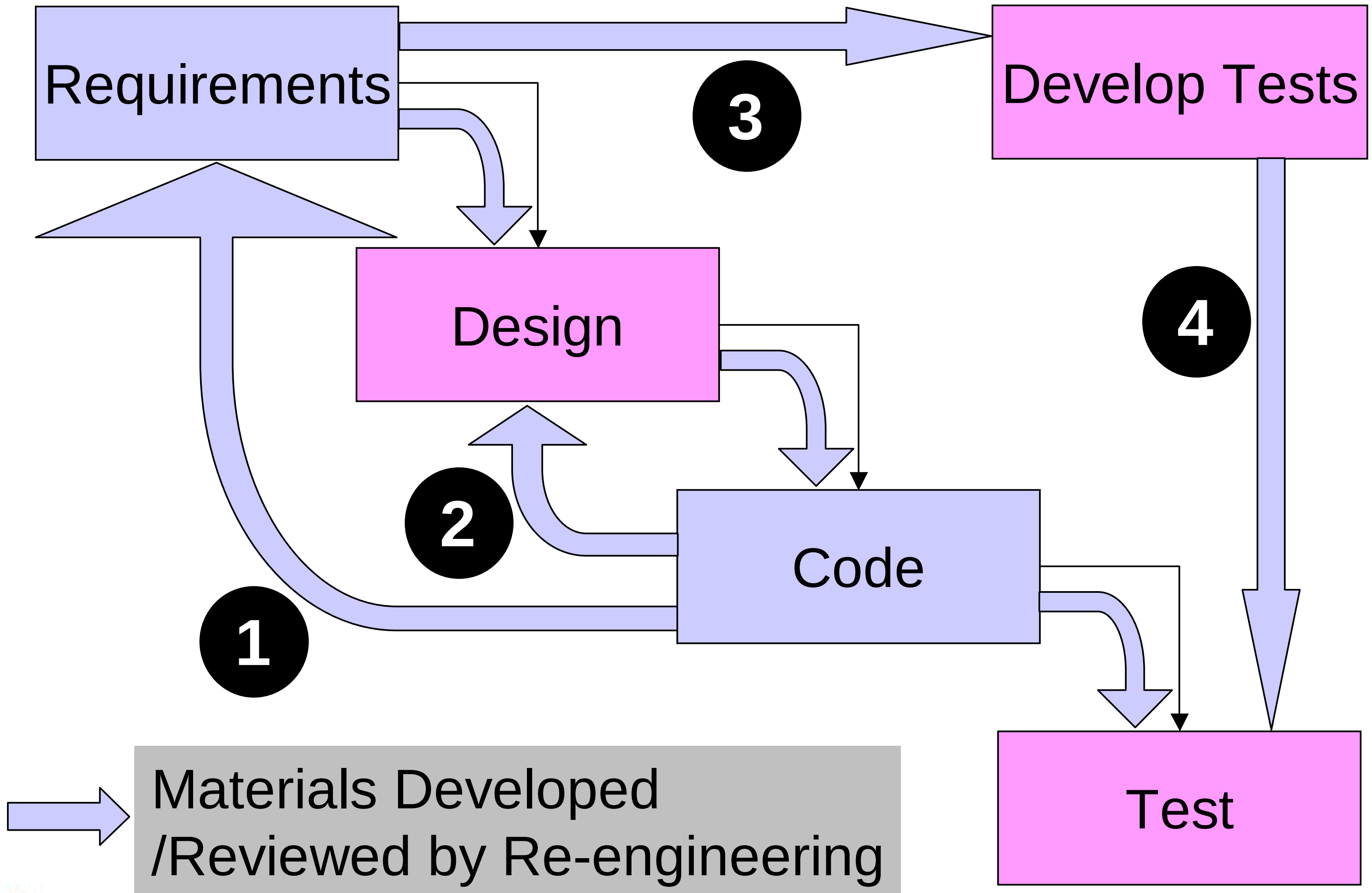
Code Exists - Requirements re-engineered



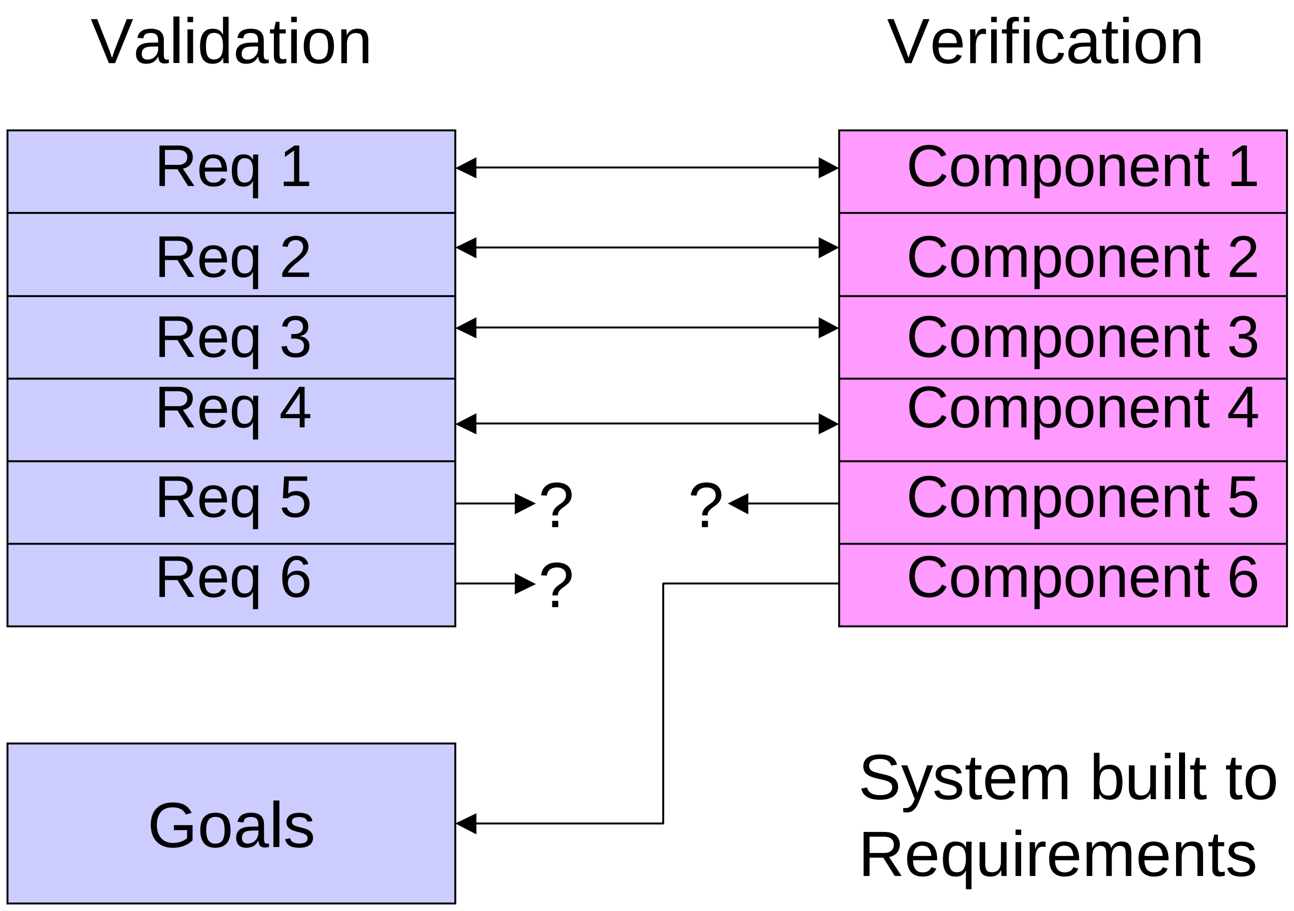
Requirements Based tests



Standard Waterfall Model

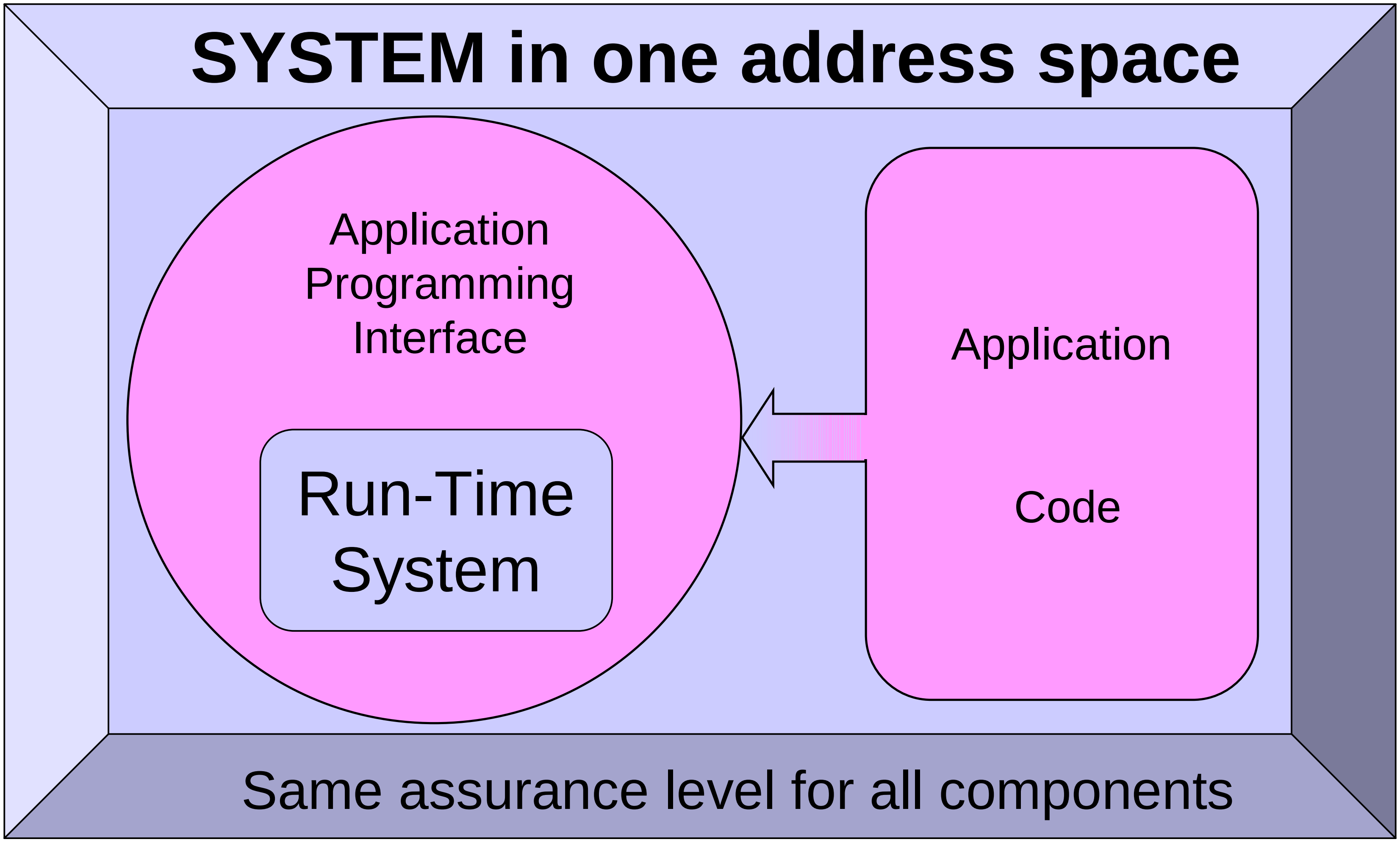


Validation and Verification



Complete and Correct

RTS an Important Component



System cannot be Certified unless RTS is Verified

Deterministic Behavior

Functionality

Resources

Time

Deterministic Behavior

- Results of a function are the inevitable consequence of its inputs:
  - Parameters
  - Global variables
- Bound on the resources used
  - Memory - no new memory after startup
  - Stack - HUGE margins
- Bound on the time taken to complete the function
  - time taken to execute a function depends on many system level parameters,
  - non-linear relationships are noted as they can cause the application to miss deadlines

Black Box Testing

- No single failure should prevent “Continuous safe flight and landing.”
- Statistical testing cannot show absence of a single state that will cause a failure
- Software has discontinuities
- Software does not follow Gauss/Normal Distribution

There is no foundation for statistical reasoning about software faults or safety

Coverage Analysis

- Analysis of testing methods and results to show effectiveness of testing
- Method to show absence of unintended function
- Should be based (as much as possible) on requirements based tests
- Rigor depends on criticality level

Note: Coverage **Analysis**
not
Coverage **Testing**

Coverage at Level B and C

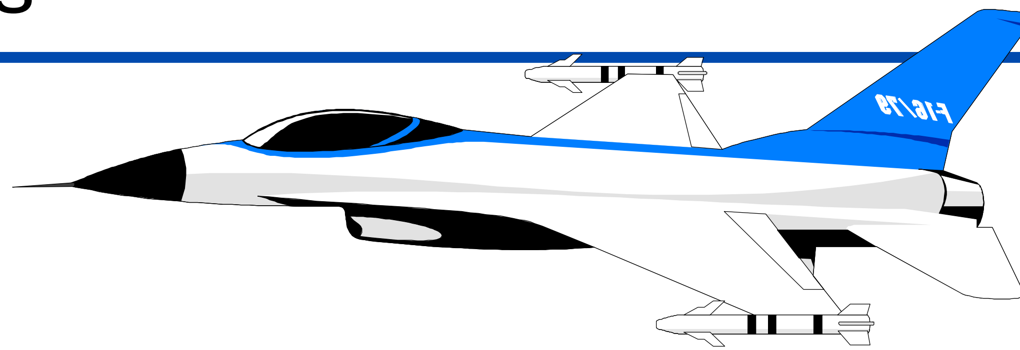
- Statement Coverage — Level C
- Decision Coverage
  - Entry Points
  - Exit Points
  - All Decisions
  - All Outcomes

Level B

Coverage at Level A

- Coverage required at Machine Code level or
- Show source to object code traceability and test at source level or
- Use different compilers and different languages or
- MCDC testing required
  – each condition must have effect on outcome

Military Avionics



- D0-178B - now mandated by congress
- Need Safety - even though:
  - Pilots have parachutes
  - Pilots don't sue
- Want safe software
  - Don't need the evidence ?
  - Must withstand an audit

The ‘Requirements’ for ATM Systems

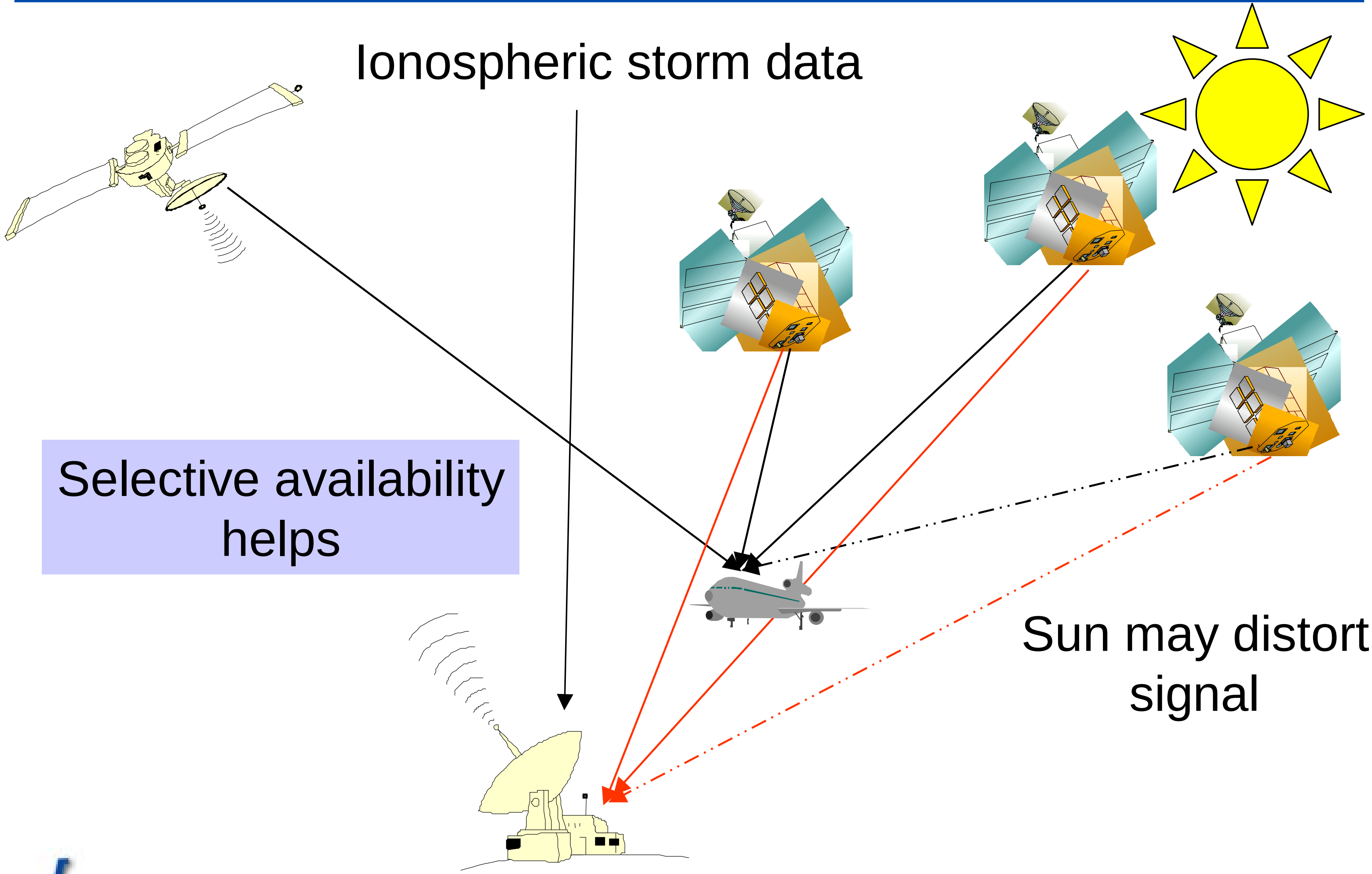
More	Safety
Increase in	Capacity
Lower	Costs
Fewer	Resource constraints

Want to use COTS !!!

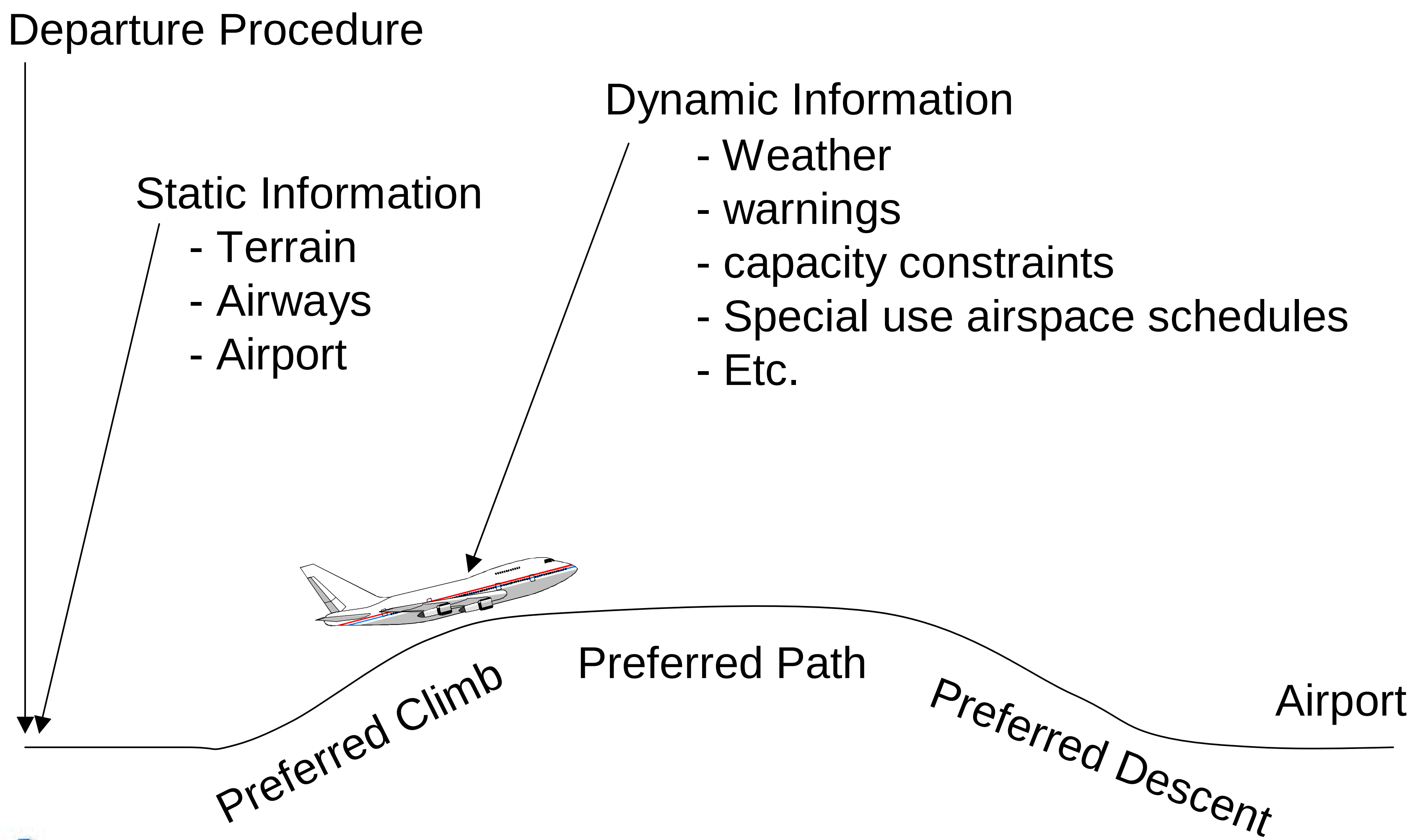
The ‘Challenges’ for ATM Systems

Current technology	Becomoing obsolete
New Technology	Increasing in cost
Air Traffic in Europe	Increasing 6% pa.
Air Traffic in US	Increasing 4% pa.

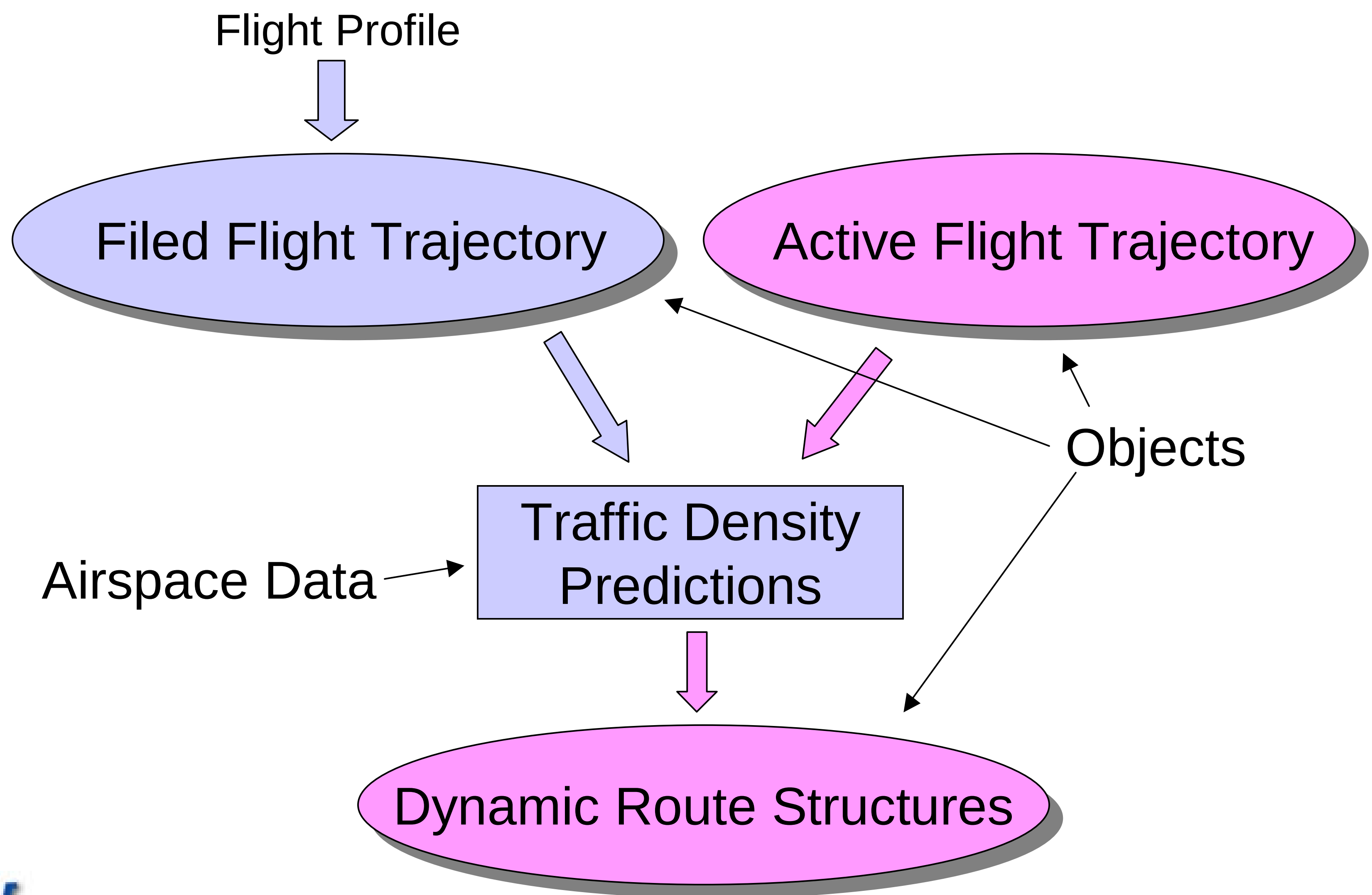
WAAS


Ionospheric storm data
Selective availability helps
Sun may distort signal

The “Flight Profile”



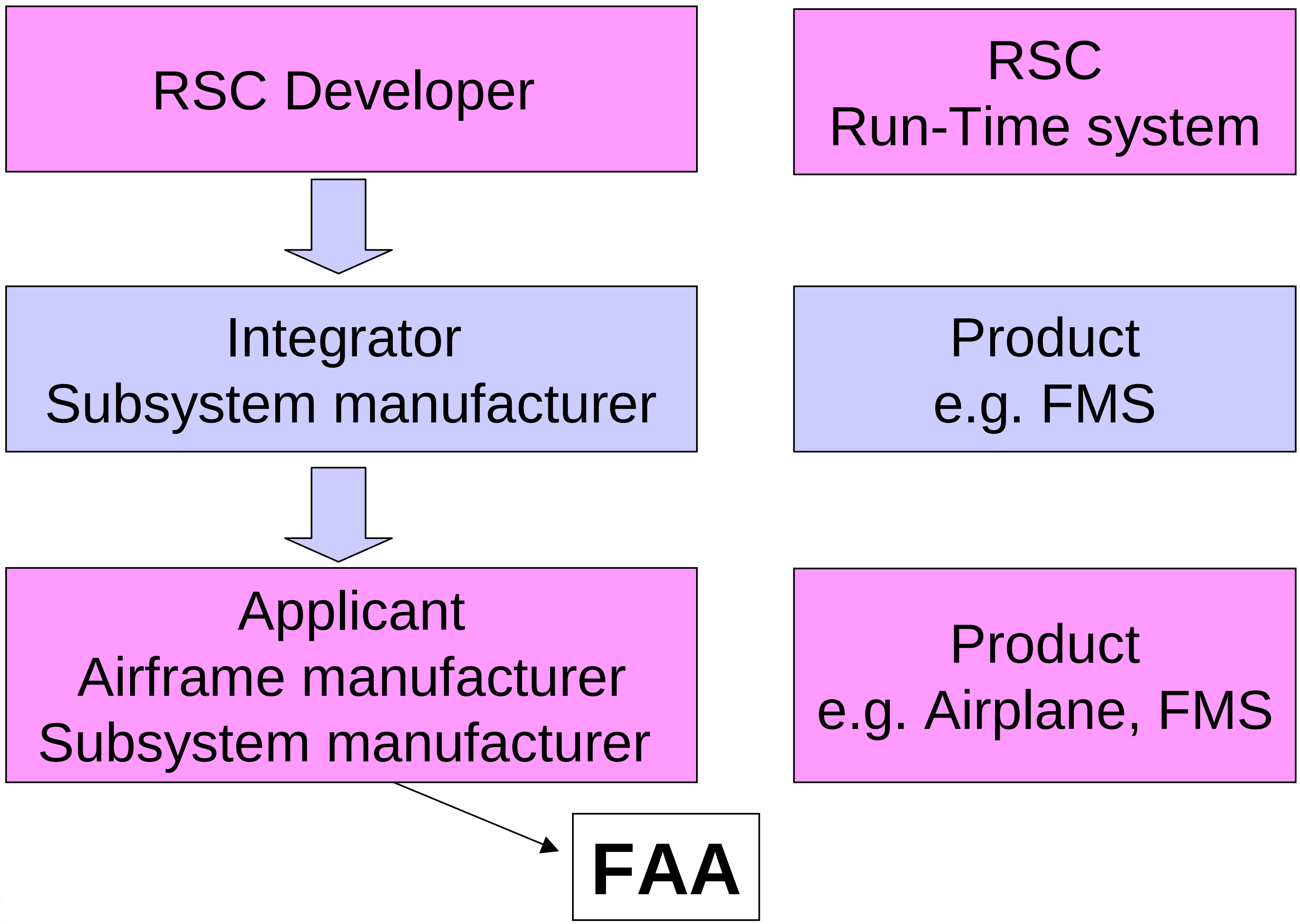
Object Oriented 'Free-Flight'



Object Oriented Technology

- Pressure from industry to use it
- Industry expect lower certification costs - eventually
- Certification authorities nervous

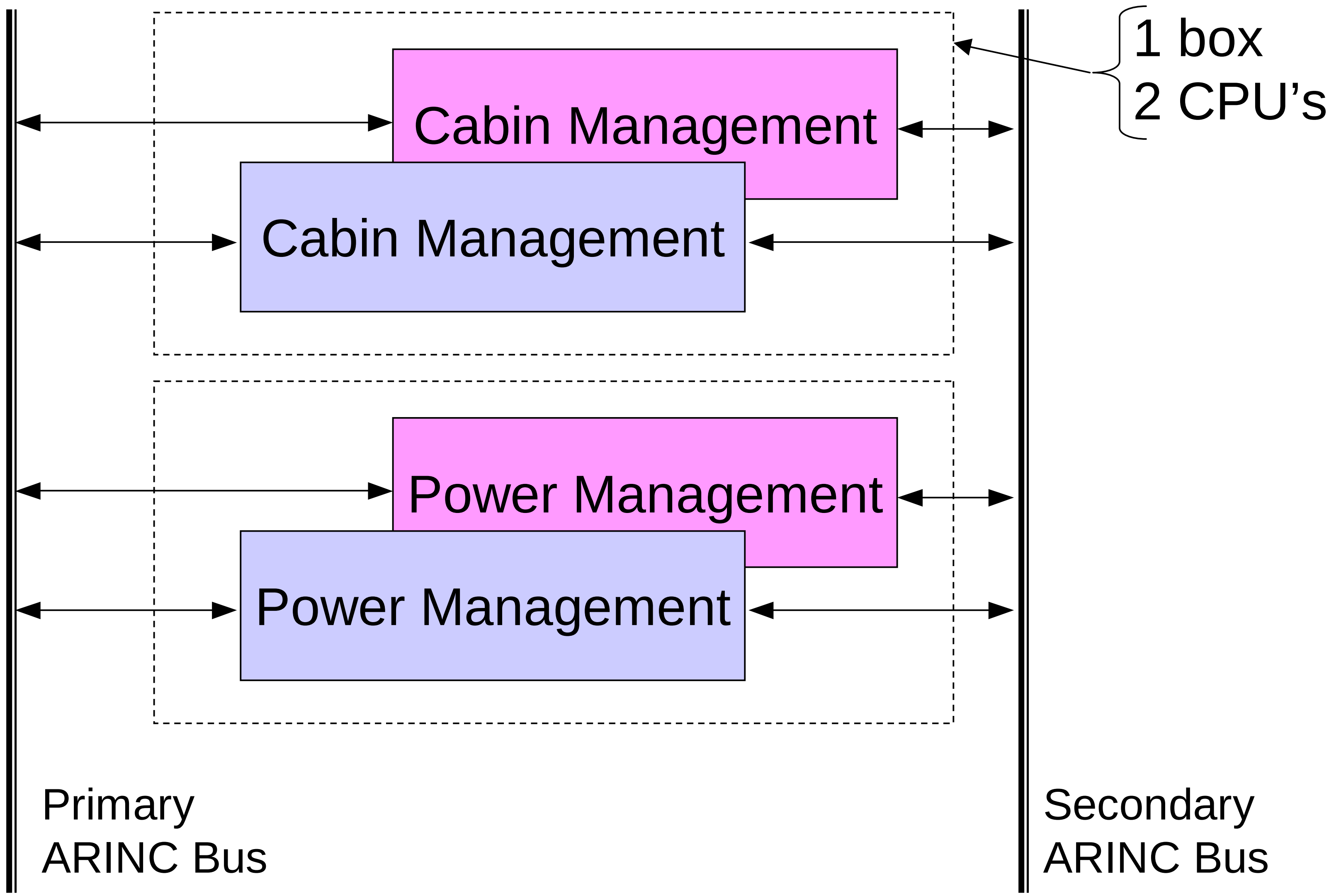
Reusable Software Components (RSC)



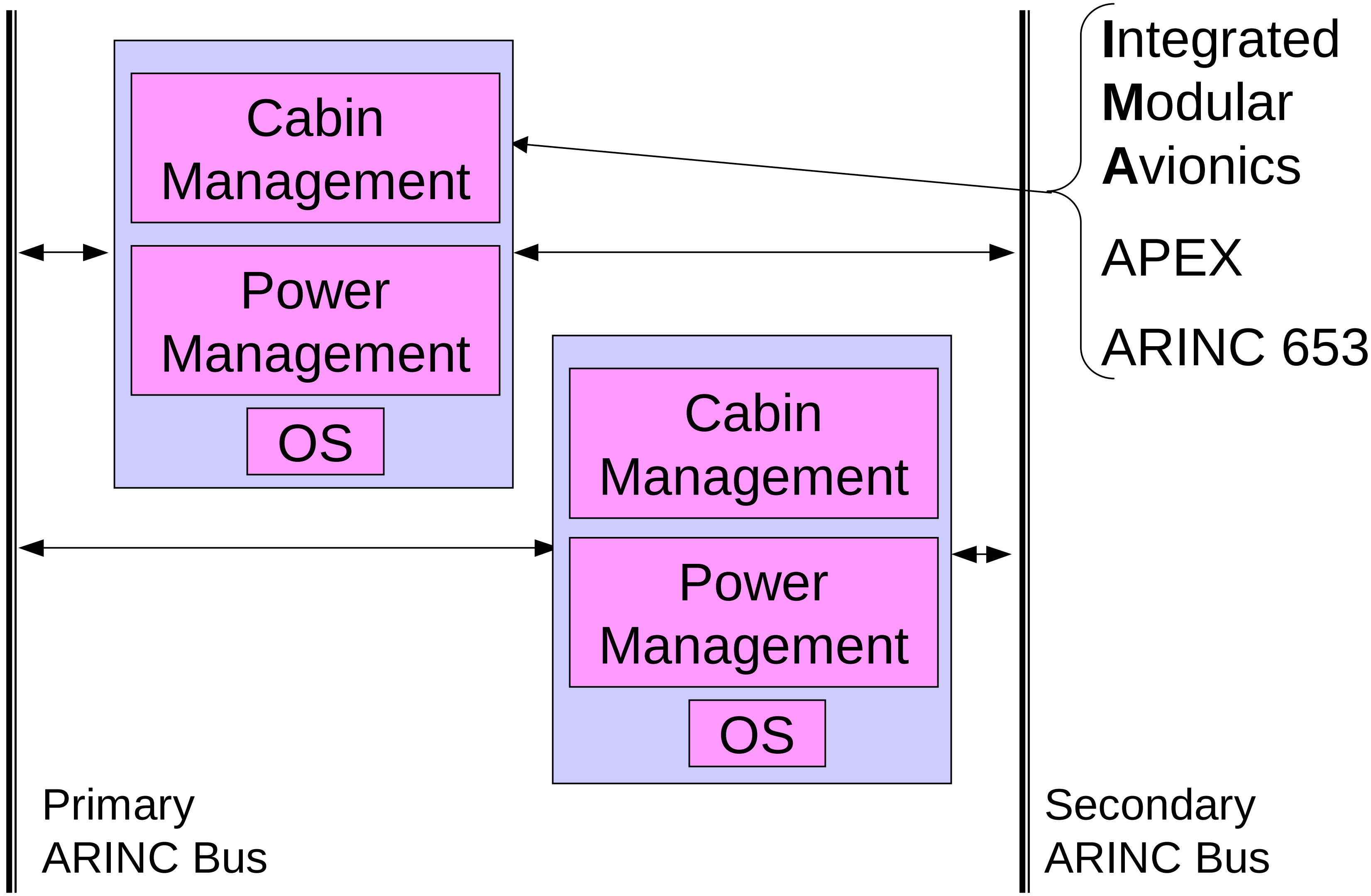
Reusable Software Component - Credit

- Applicant applies for Type Certificates for Product
- Applicant supplies DO-178B materials for RSC
  - Software Level (A, B, C, D)
  - Identified Processor type
  - Identified Compiler
- FAA provides letter to RSC developer which documents certification credit
- Eliminates / Reduces reverification on new project

Multiple Systems



Partitioned Systems



The Partitioned Promise

- Cheaper to verify components
- Cheaper to re-verify components
- Lowers criticality level - lowers certification costs
- Less software to audit when component changed/upgraded

Don’t Argue with the Auditors

- Arguing with the auditors is like mud wrestling with a pig

- After a while you find out the pig really likes it!