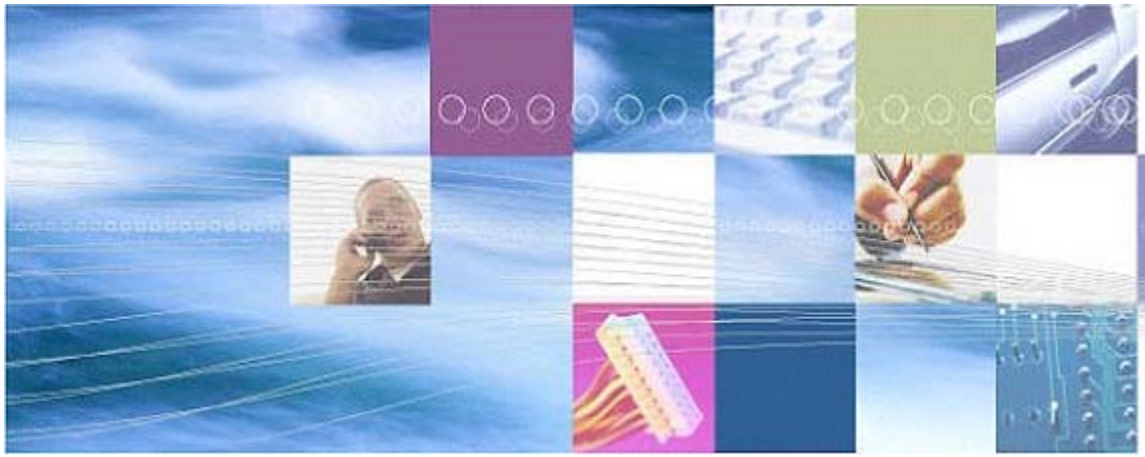


WindRiver®

HOW SMART THINGS THINK™

Tornado for DO-178B

COTS software for certifiable applications

William Boyer-Vidal (Account Manager)
Olivier Charrier(Field Application Engineer)

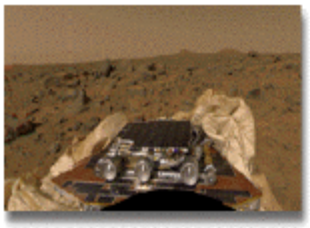
Olivier.Charrier@windriver.com
http://www.windriver.com

Review of commercial RTOS in Safety-Critical Systems

- In recent years, a number of applications have used a commercial RTOS in safety-critical applications
- In the 1990s, Wind River did not offer a safety-critical VxWorks product, but a number of programmes had used VxWorks for safety critical programmes.
- Key influencing factors:
  - **RTOS maturity with proven track record,**
  - **Supported on over 35 processor architecture families**
  - **Deployed on over 150 million processors worldwide**
  - **Entire VxWorks source code available from Wind River in order to certify RTOS as part of programme's DO-178B certification activities.**

FAA DO-178B certified Honeywell GlobalStar 2100 running VxWorks

VxWorks® in High-Integrity Systems



Mars Pathfinder

Mission Computer on IBM RAD6000 rad-hardened processor

http://www.windriver.com/customer/html/jpl.html

Honeywell GlobalStar 2100

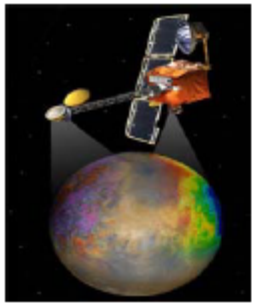
DO-178B certified Flight Management System

http://www.windriver.com/customer/html/honeywell_ss.html

NASA Deep Space One

Flight Computer on IBM RAD6000 rad-hardened processor

http://www.windriver.com/customer/html/jpl.html



NASA Mars Odyssey

Command & Control and Data Transfer Network

http://www.windriver.com/html/odyssey_mission.html

http://www.jpl.nasa.gov/releases/2001/release_2001_208.html

VxWorks® in High-Integrity Systems

Space Station X-38 Crew Return Vehicle

Entire Control System on 68040
(Navigation & guidance, flight control surface operation, life support, communications, deorbit propulsion)

http://www.windriver.com/html/x38.html
http://www.windriver.com/press/html/20011212.html
http://www.dfrc.nasa.gov

Space Shuttle

Checkout and Launch Control Systems on PowerPC processor

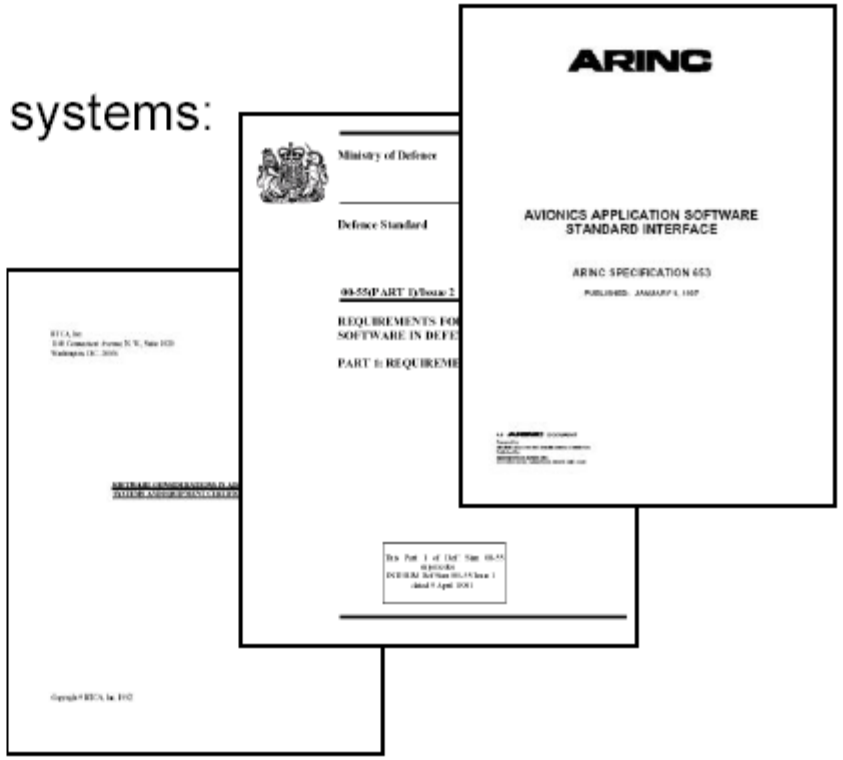
http://www.windriver.com/customer/html/jpl.html

MEDS cockpit upgrade

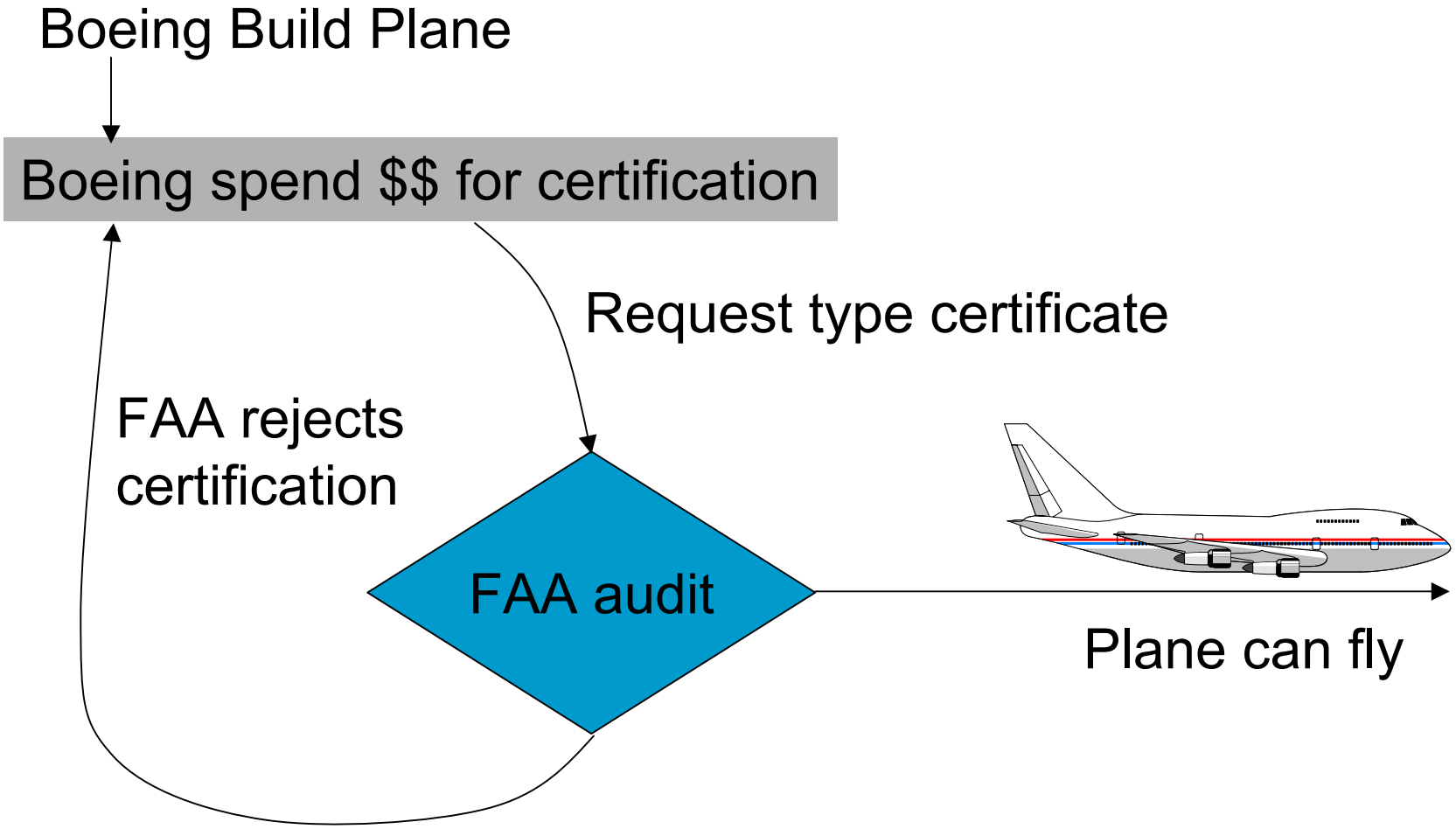
http://mae.pennnet.com/Articles/print_screen.cfm?PUBLICATION_ID=32&ARTICLE_ID=97983

So why develop certifiable VxWorks products?

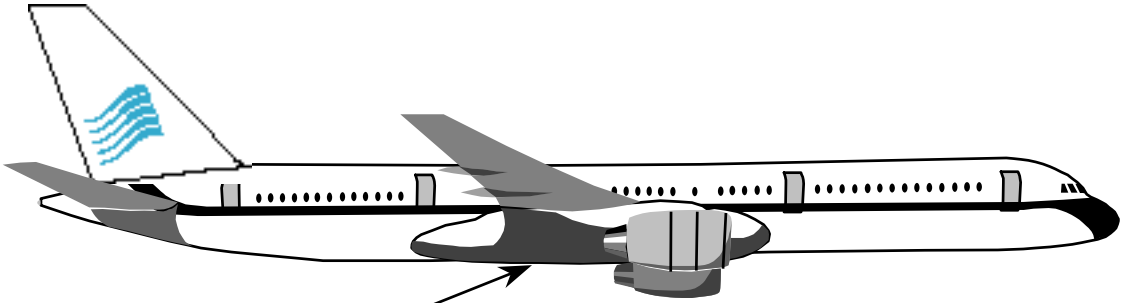
- Customer demand for a certifiable true COTS product
  - **Providing reuse of certification evidence**
  - **Enabling faster time to market**
  - **Reduced programme costs**
  - **Functionality**
- Standards compliance for safety-critical systems:
  - **RCTA/DO-178B**
  - **UK MoD Defence Standard 00-55**
  - **RTCA/SC-182: ACR MOPS**
  - **ARINC-653**

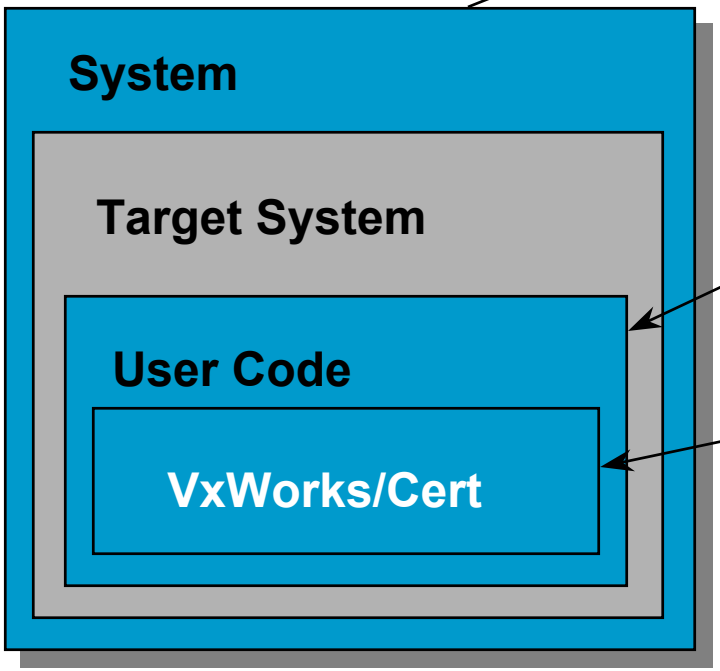


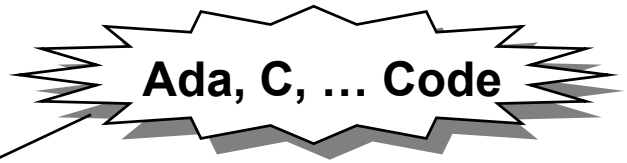
Industry Paid - Certification

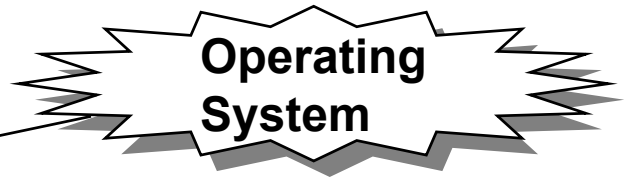


Software Components of a System









System cannot be certified unless VxWorks is verified

The COTS Advantage

- Shorter time to market
  - Increased productivity through leading tools
  - More engineers familiar with products
  - Support not in-house function
- Allows you to concentrate on *your* value component – application development
- Widespread adoption leads to:
  - Reduced costs
  - Increased robustness
  - Longer time-in-market

Avionics COTS

- DO-178B Glossary Entry:

> *Commercial off the shelf (COTS) software* – Commercially available applications sold by vendors through public catalog listings. ***COTS software is not intended to be customized or enhanced***. Contract-negotiated software developed for a specific application is not COTS software."

Avionics COTS Problem?

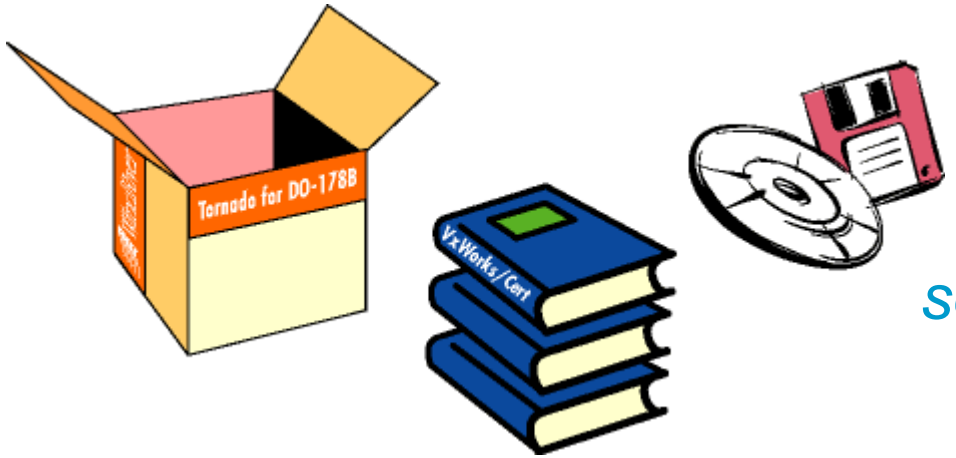
- Still have to comply with DO-178B objectives
- But, generally:
  - Certification material not available
  - Prohibitive development costs
  - Stifle innovation
- Options:
  - Buy source code, develop certification material
  - Buy consultancy services from vendor

‘Service-based’ Certification

- Drawbacks:
  - True cost hidden
  - Feature set not guaranteed
  - Support
  - Ownership of certification material unclear

Wind River's Solution

- A true DO-178B COTS product, including:
  - Certifiable multitasking RTOS
  - Leading development tools
  - Supporting DO-178B certification material



DO-178B Level A[*]

software development Out-of-the-Box

Wind River DO-178B expertise

- **October 1999: Joseph Wlad (WindRiver) in charge.**
  - 16 years of avionics design, development, test and evaluation including:
    - Douglas Aircraft Company, MD-11 Test and Certification
    - United Airlines B747 Fleet engineering and modification
    - Trimble Navigation Engineering Manager (development and FAA approval of GPS sensors)
    - Wind River OS certification Manager
      - 3 engineers to support testing and release of our product
  - FAA DER: Systems and Equipment and Software, Long Beach ACO

Wind River Certification Process

- Certification work undertaken by Verocel under exclusive contract to Wind River:
  - **George Romanski - President**
    - British ex-patriate, with experience of UK & US programmes
    - Formerly Director of Safety Critical Software at Aonix
    - Author of Aonix Safety-Critical Handbook
    - Co-author of the Ada Ravenscar Profile Definition
    - Member of Ada 95 HRG
    - Member of RTCA/SC-190 Committee (Guidelines for DO-178B)
  - **Jim Chelini - Chief Operations Officer**
    - Formerly Manager of Safety-Critical Software at Aonix
    - Member of RTCA/SC-190 Committee (Guidelines for DO-178B)
    - Member of RTCA/SC-182 Committee (Avionics Computing Resource)

VEROCEL URL http://www.verocel.com

Definition of the Certifiable VxWorks

- *Objective:* definition of a true subset of the VxWorks API that may be certified and its rationale
- *Guidelines:*
  - FAA guidelines to Level A objectives as defined by DO-178B
  - Requirements from RTCA/SC-182 (ACR MOPS) and ARINC 653
  - API of the subset to remain consistent with VxWorks
  - Elimination of function compromising predictability and leading to memory fragmentation
  - Elimination of function compromising a safety-critical application
- *Approach:* examination of the source code and architecture, multiple analysis pass

Definition of the Certifiable VxWorks

- **Start with examination of the source code and architecture**
  - determine functions which are predictable and certifiable
  - eliminate unnecessary functionality and any features that may compromise a safety-critical application
- **Define a true subset of VxWorks that may be certified**
  - removed:
    - network protocol support and file systems
    - shared memory for multiple processors
    - Object-oriented features: Dynamic links, other C++ features
    - Debug facilities, BSPs, and various tools
    - Dynamic allocation and de-allocation of memory

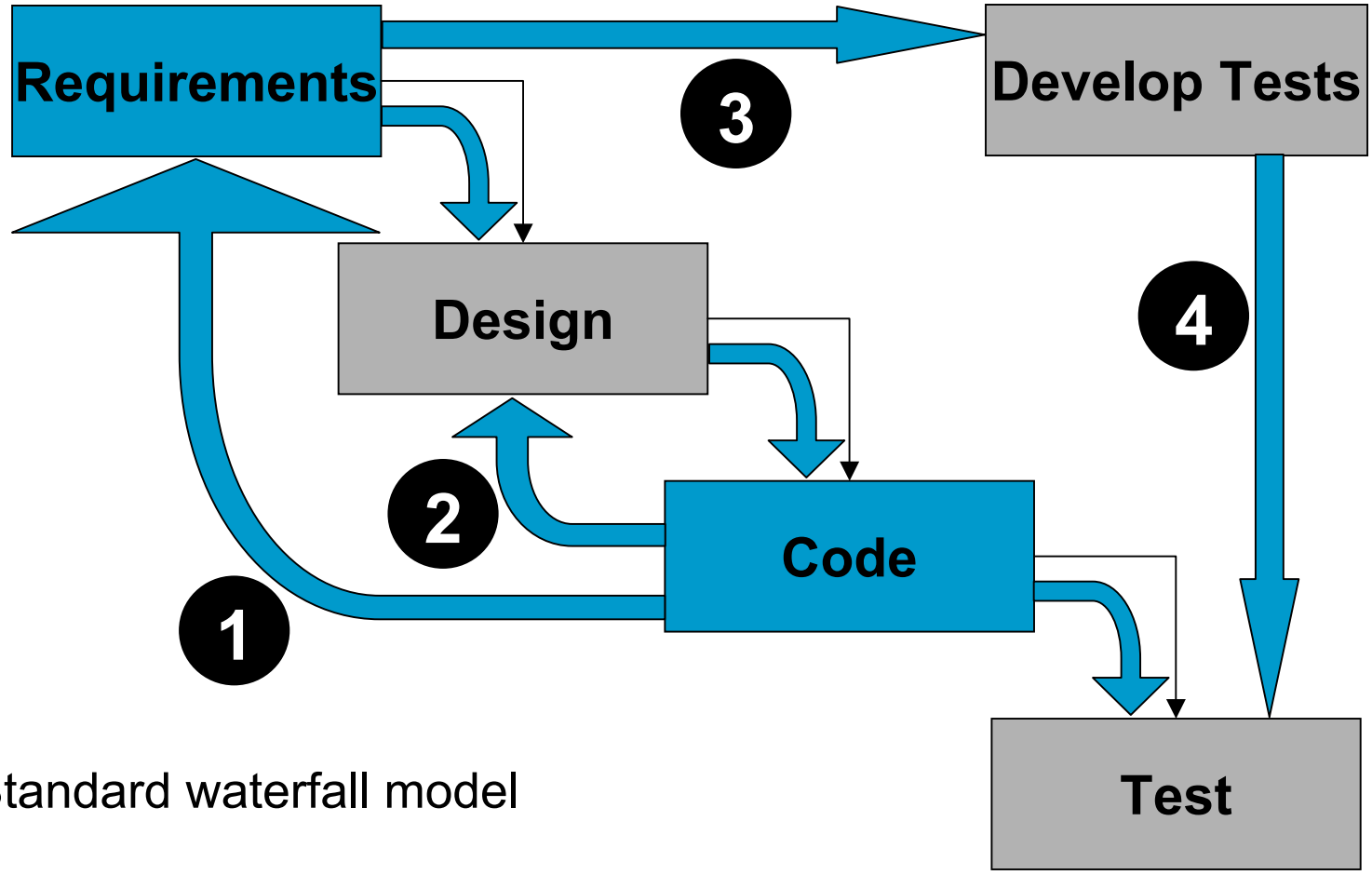
Definition of the Certifiable VxWorks

- **Create a subset definition and rationale**
  - **results in a scaled-down version of VxWorks**
    - 15K SLOC
- **Create Software Hazard Analysis**
  - Identifies potential failure conditions in the software, their potential impact, and proposed mitigation
  - updated at each phase of the software lifecycle
- **Create a Plan for Software Aspects of Certification (PSAC) that describes the reverse engineering strategy**
  - Provides the Certification Authorities an overview of the means of compliance and insight into the planning aspects for delivery of the product

Software Development Process

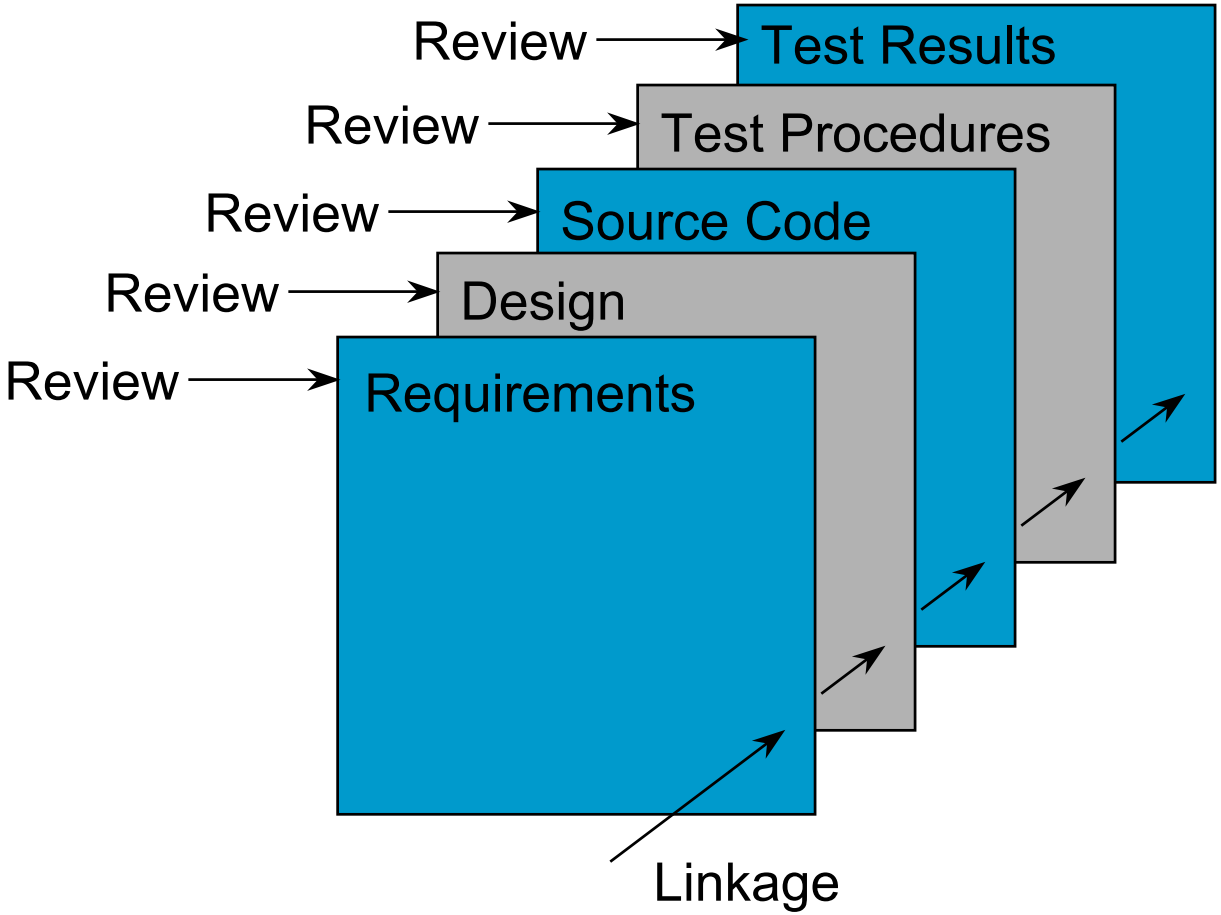
- **Wind River Products comply with ISO requirements**
  - Not ISO 9000-3 (S/W Quality) compliant
- **Therefore, adaptation are required to comply with DO-178B objectives**

WindRiver DO-178B Process



Standard waterfall model

Traceability



Certification Material

- Plan for software aspects of certification
- Software quality assurance plan
- Software configuration management plan
- Software development plan
  - Software requirements standards
  - Software design standards
  - Software coding standards
- Software verification plan
- Software requirements specification
- Software design document
- Version description document
- Traceability matrix
- Software development folder
  - Design reviews
  - Code reviews
  - Test reviews
  - Functional tests
  - Coverage results
- Tool qualification documentation
- Software accomplishment summary

Target Audience and Products

- People who want to use a certifiable base to their project:
  - People bidding on projects.
  - People with existing VxWorks application evaluating if the application could be certified.
  - People in search of a ‘safe’ kernel

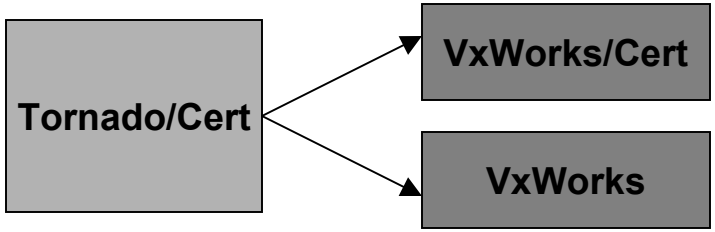
➔ **Tornado for DO-178B Starter Kit**

- People engaging in the certification of applications

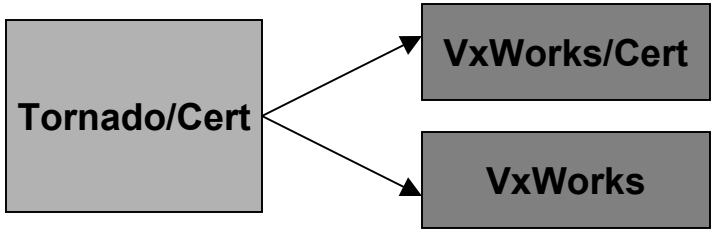
➔ **Tornado for DO-178B Certification**

Product Packaging

Tornado for DO-178B Starter Kit



Tornado for DO-178B Certification



Certification Documentation
Required to certify an application

Source Code
For VxWorks/Cert and tests

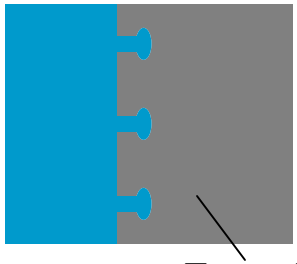
Verification Tool / Results
Coverage analysis tool and results

Development

Certification

Development Cycle

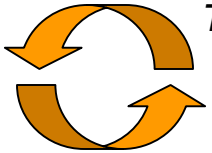
1. Develop

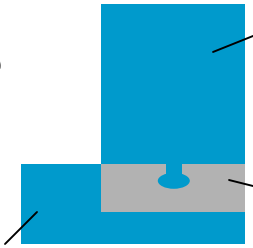


Tools

Tornado/Cert

Develop, Debug, Tune





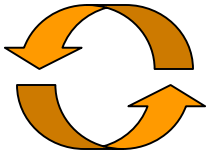
Application

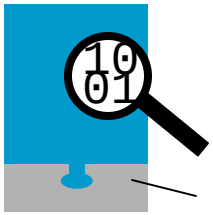
Subset API

VxWorks

2. Verify

Verification, Code coverage



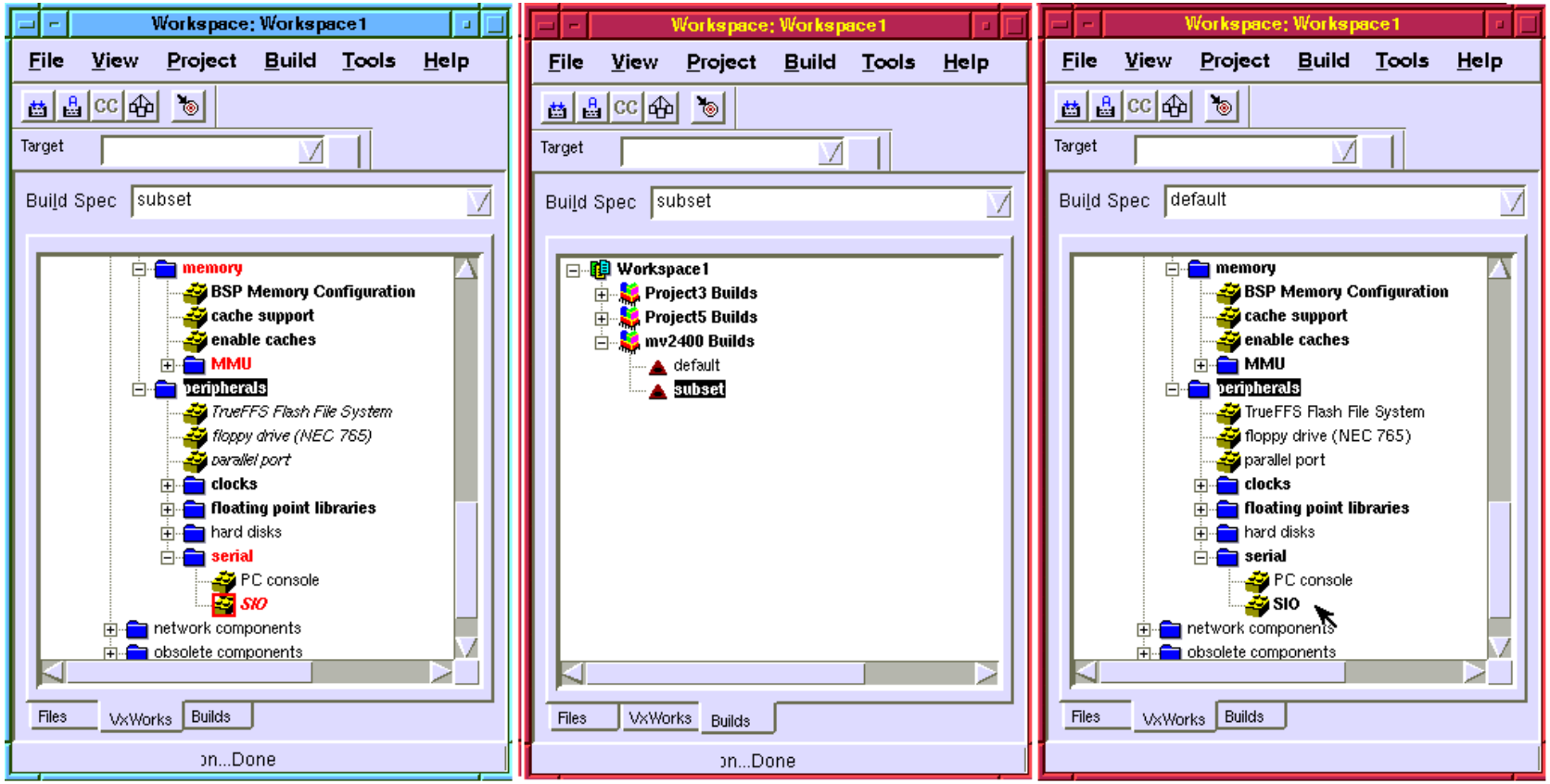


VxWorks/Cert

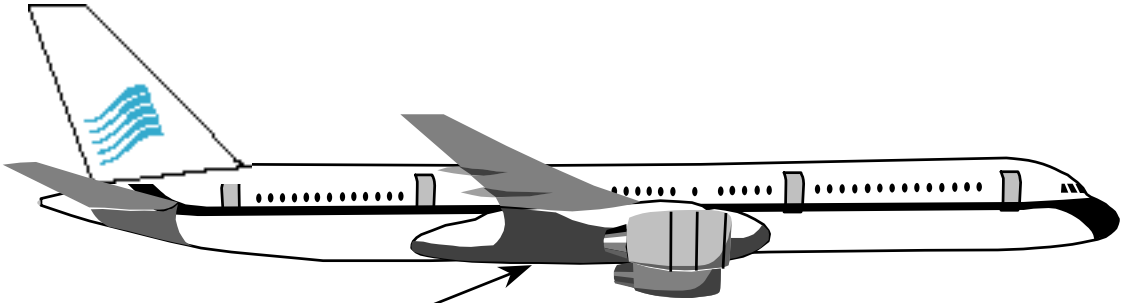
3. Deploy

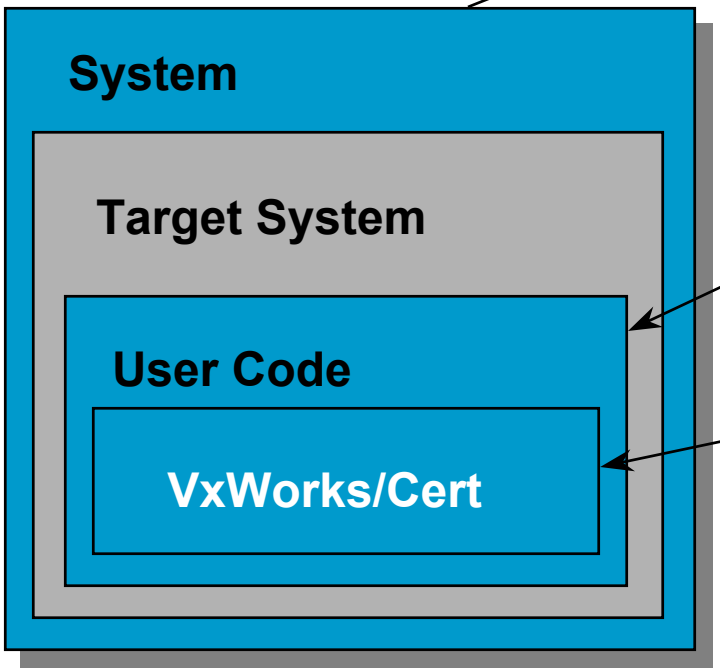
Certified application using VxWorks/Cert

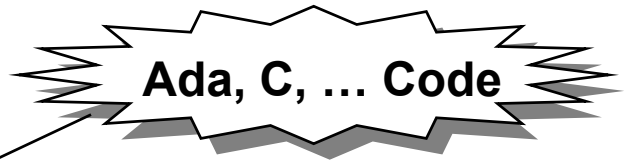
Updated Project Facility

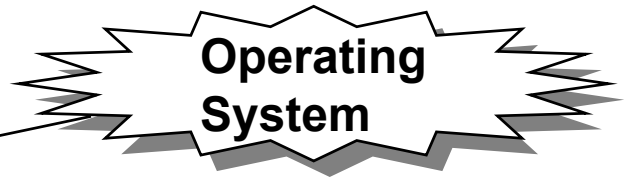


Software Components of a System



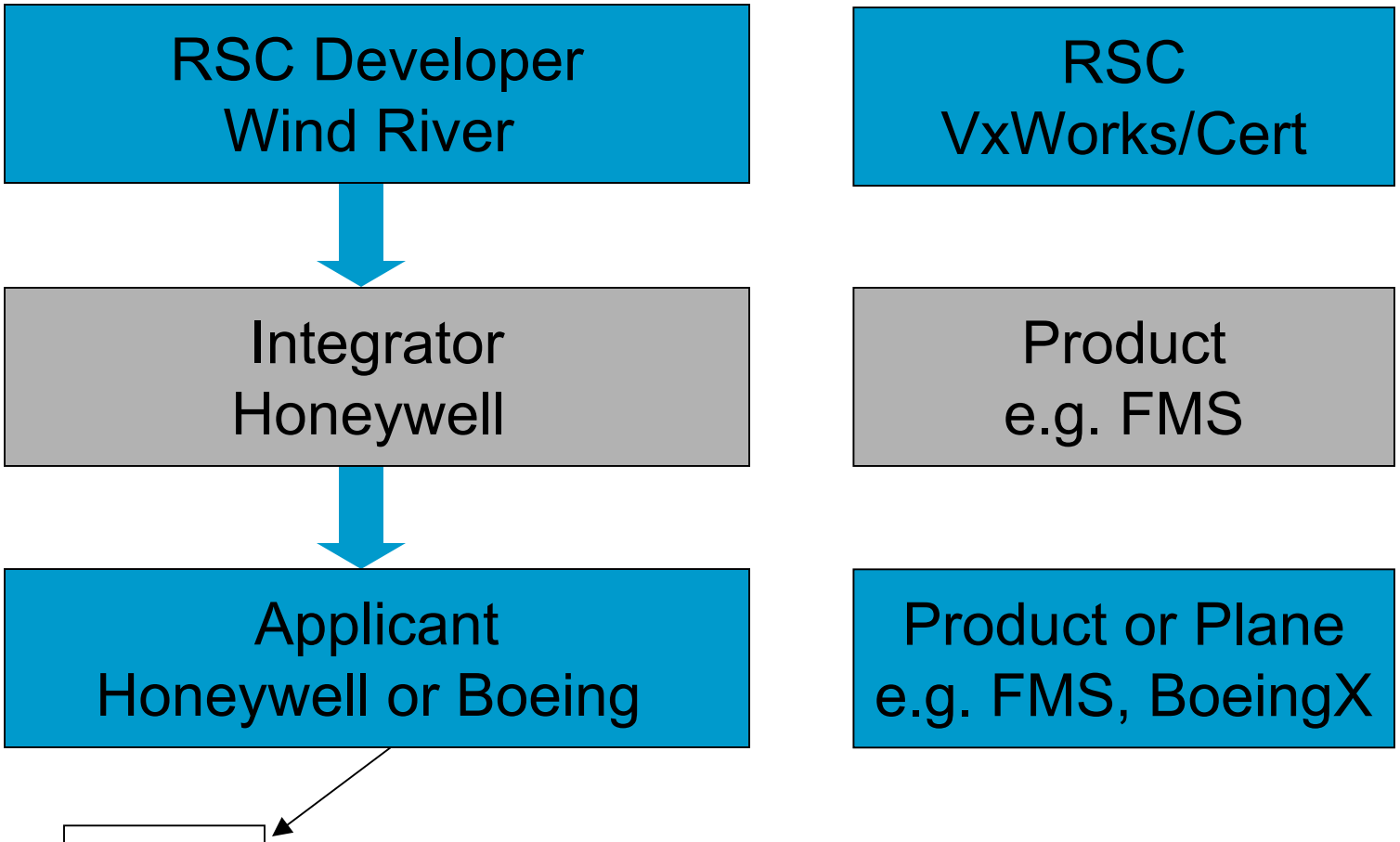






System cannot be certified unless VxWorks is verified

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

WindRiver in the Certification Process

System
I.e Boeing 777
Airbus A3xx

Subsystem
I.e. Flight Management System

Letter of intent to develop
A system or subsystem
(TSO or TC/STC requirement)

Project Number Assignment

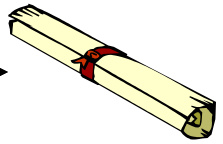
FAA or Certification Authority

Application Development
Certification Material for:
• Application Software
• VxWorks

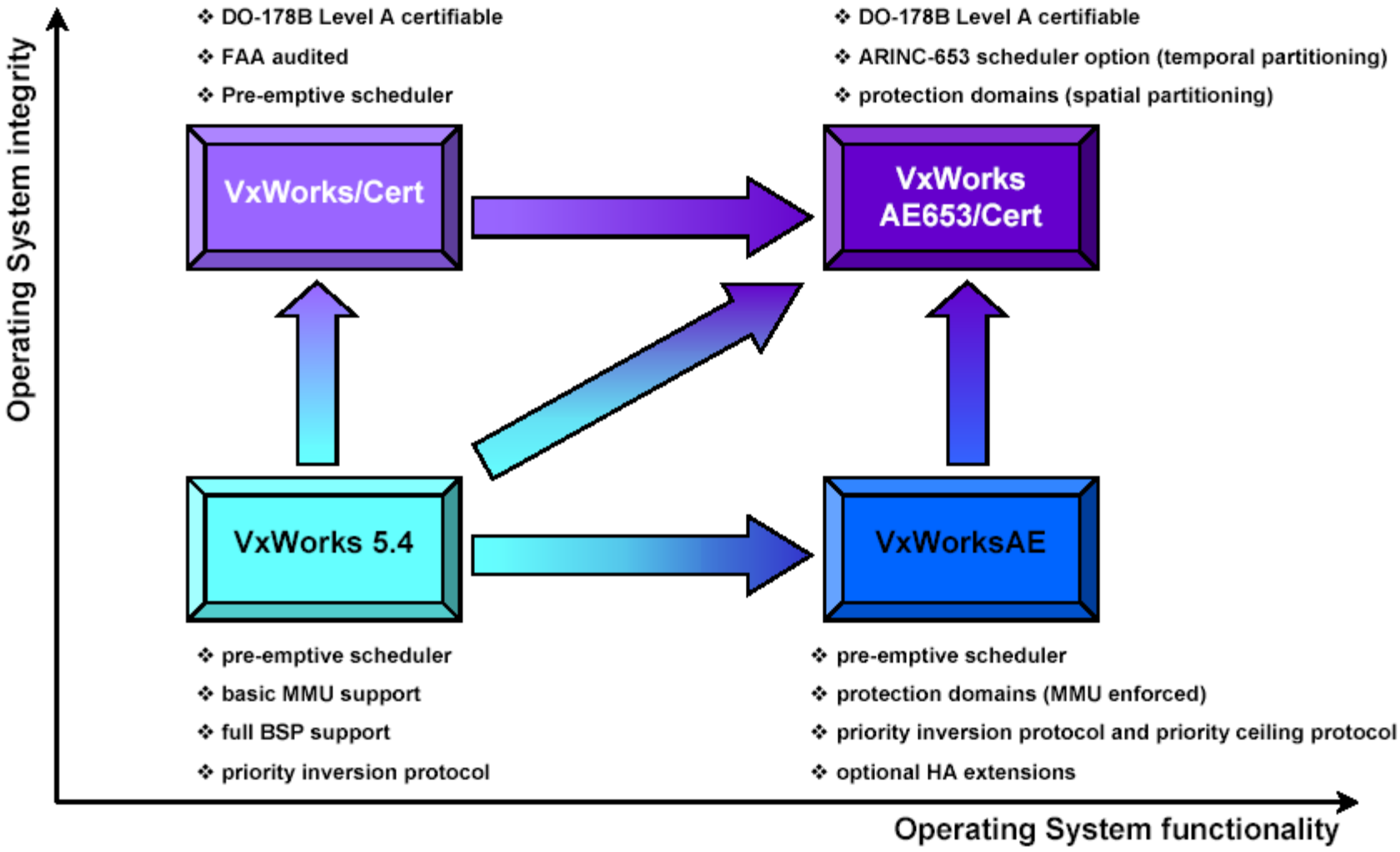
Reusable Software
Components
I.e VxWorks

Company or FAA assigned
DER Review

Letter of approval

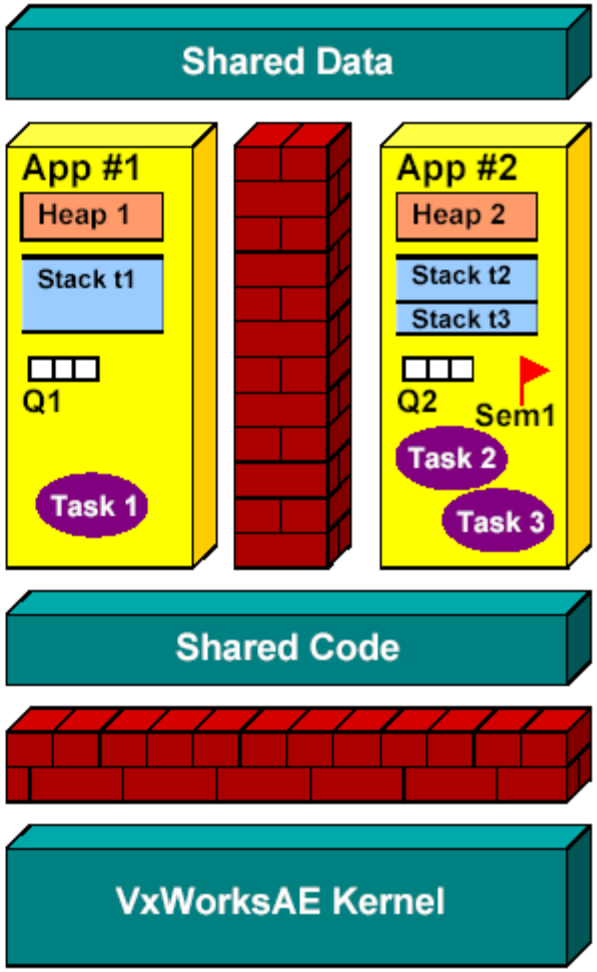


VxWorks for High Integrity Systems

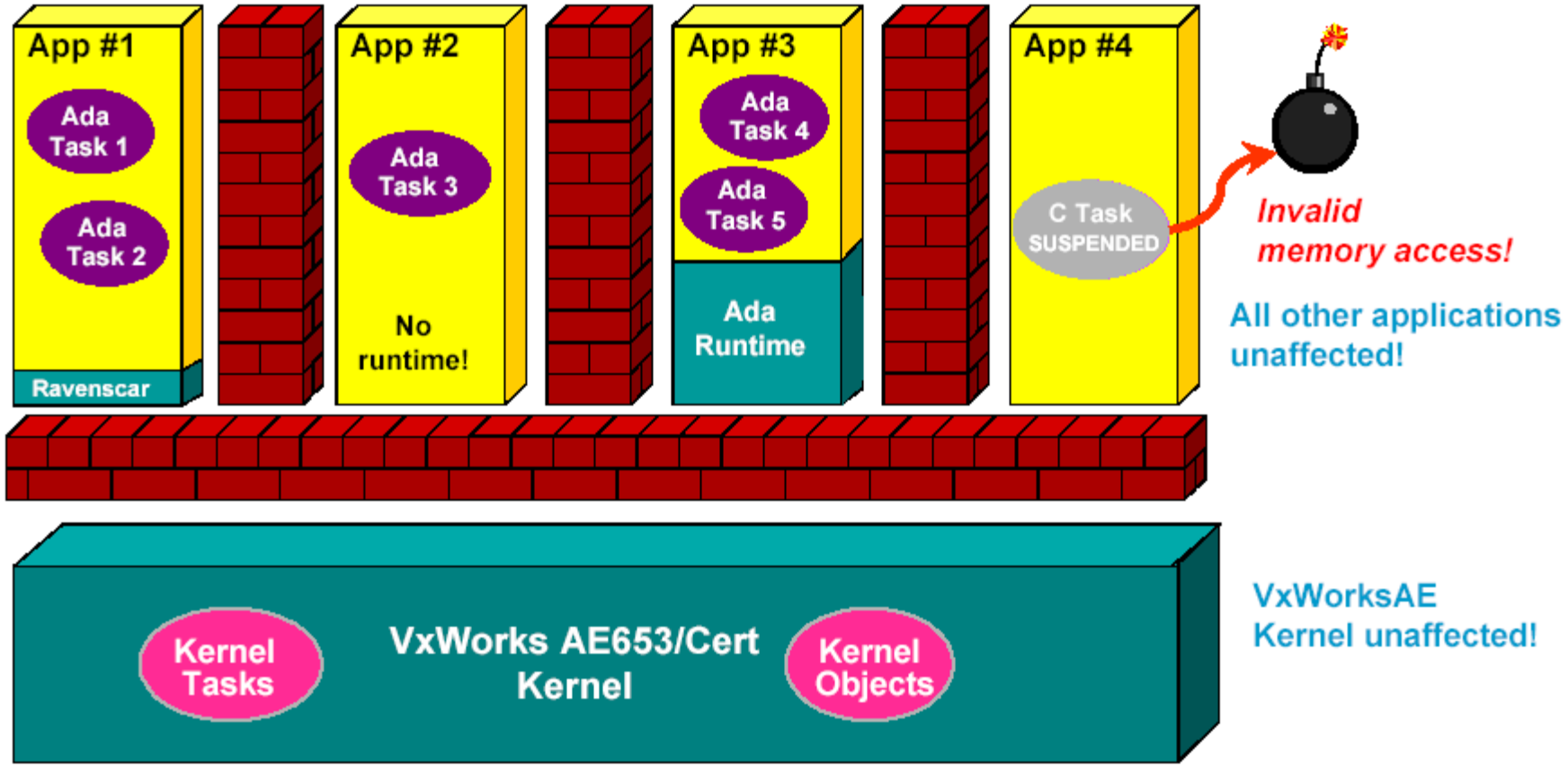


Application Protection Domains

- Each protection domain contains an application consisting of:
  - One or more application tasks
  - Task stacks
  - Domain heap
  - Application objects (message queues, semaphores, etc.)



VxWorksAE - The RTOS of choice for avionics



DO-178B: The Wind River Advantage

- Tornado for DO-178B
  - True COTS solution
  - Leverage existing VxWorks expertise
  - Benefit from Tornado and other Wind River tools for development
  - Facilitate the testing for certification, thus resulting in better time to market and cost reduction
  - Solution tailored to the needs of the application
    - Starter kit
    - Certification kit