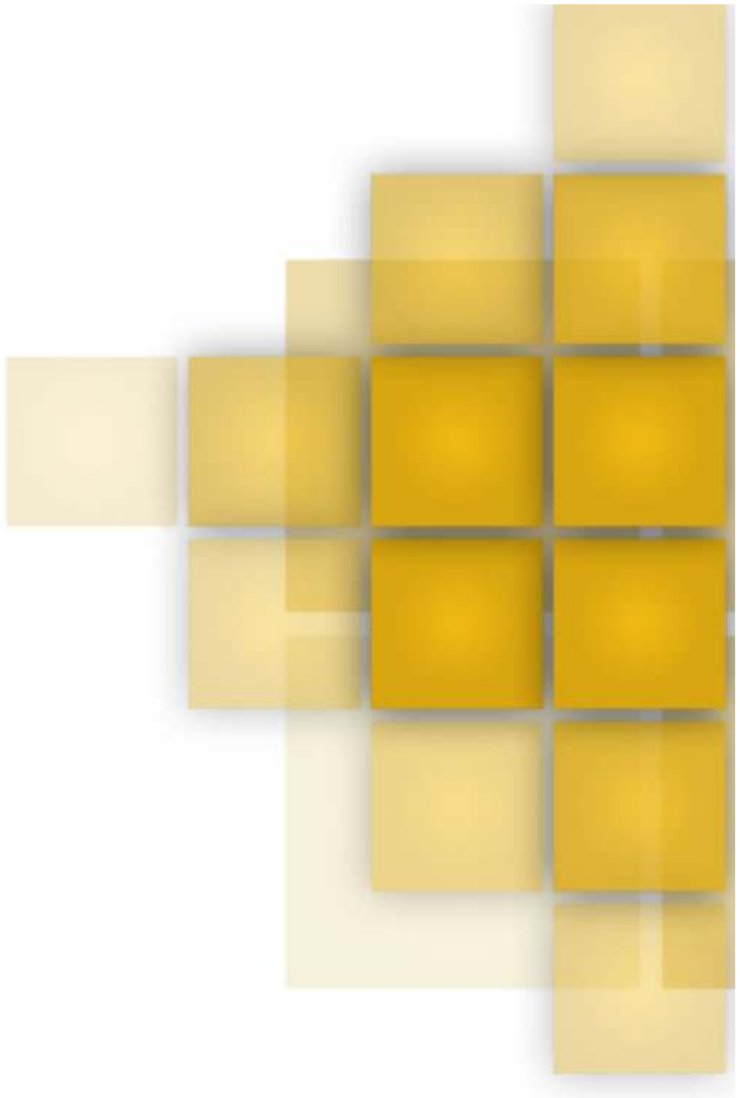
WIND RIVER

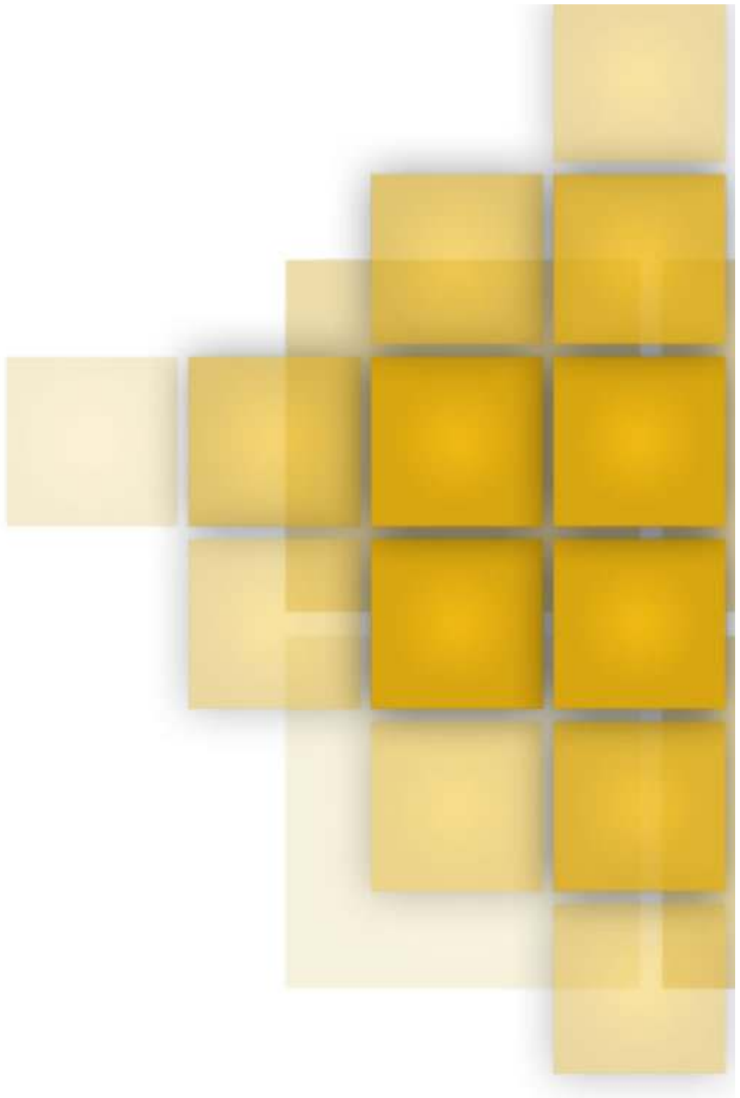


Safety Critical Solutions by Wind River

Olivier Charrier
Principal Technologist, Safety Systems

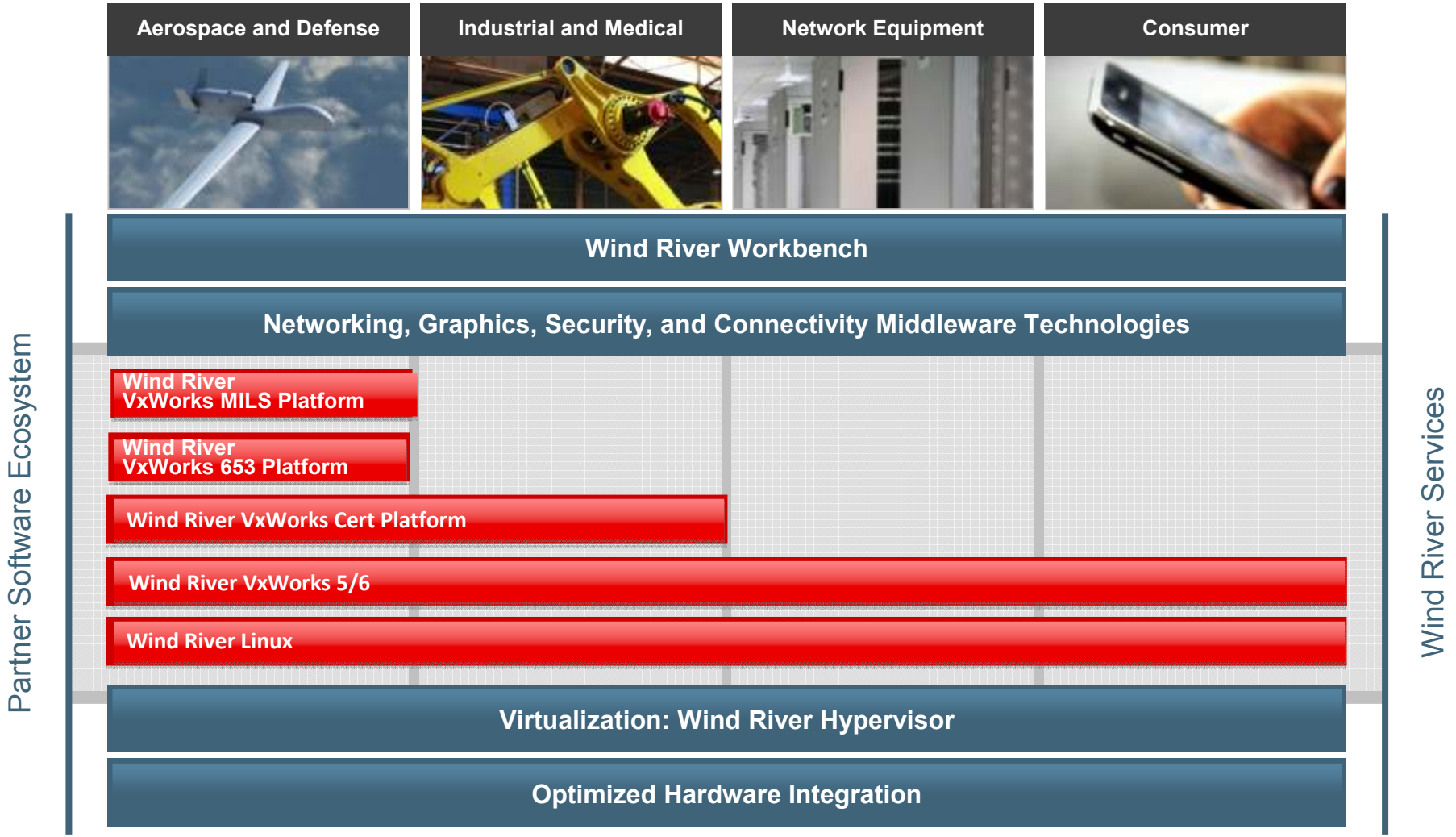
Agenda

- Wind River Solutions
- On the Avionics side
- On the Industrial, Railway and Medical Side
- Wind River VxWorks Cert
- Wind River VxWorks 653
- VxWorks Cert / 653 Common Features
- Certification Evidences



Wind River Solutions

Wind River Platform Solutions



VxWorks Cert for DO-178B/IEC 61508

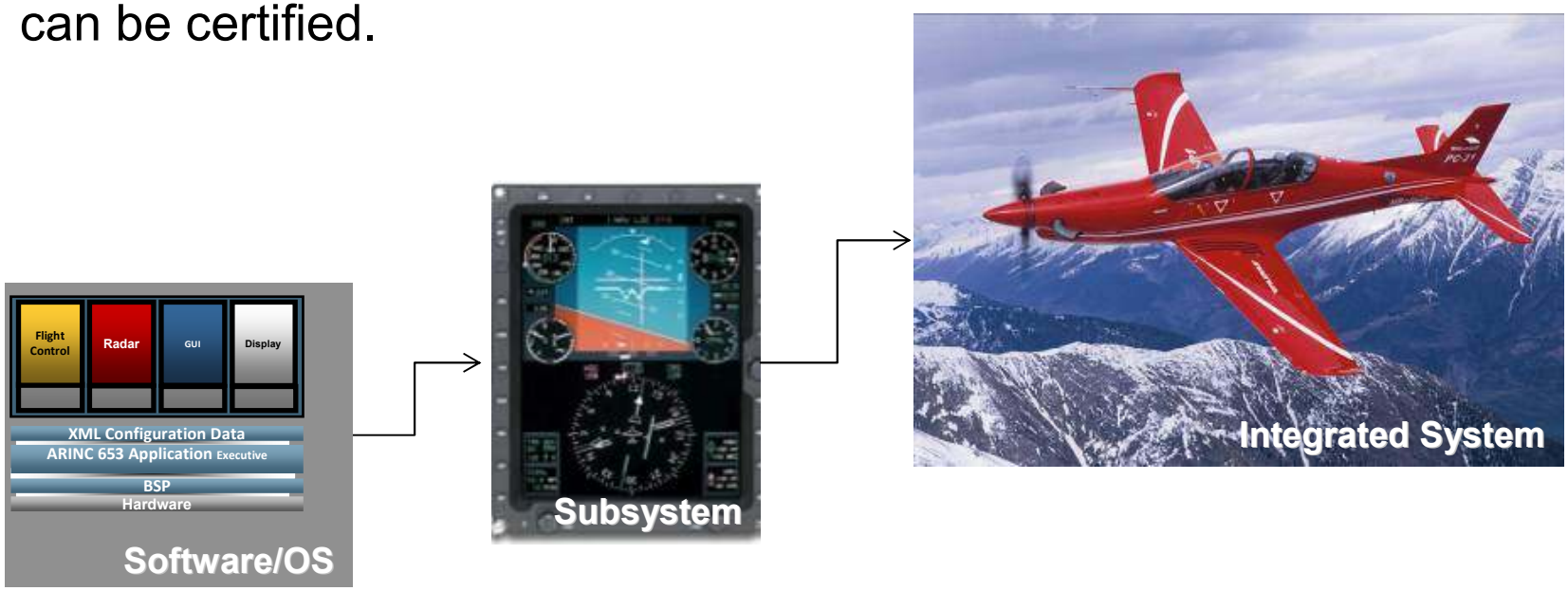
- Based on market-leading VxWorks 6 real-time operating system (RTOS)
- DO-178B certifiable: Certification evidence provided for system certification process
- IEC 61508 certification: Updated December 2010
- EN 50128 certification
- Broad processor/board support
  - PowerPC, Intel, ARM architecture
  - Comprehensive tools support
  - Wind River Workbench

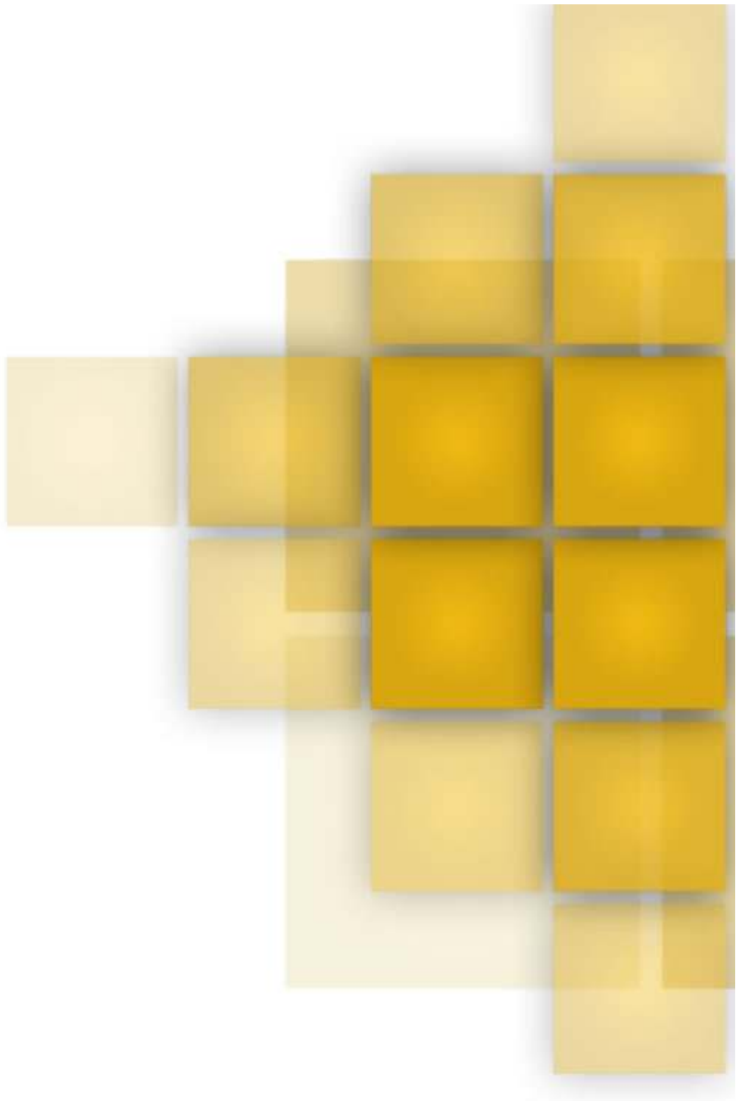
Raytheon Wide Area Augmentation System (WAAS)

Mitsubishi Power Plant Controller

Safety-Certified Systems

- A safety-certified system is an integration of separate hardware and software components, each of which may have separate safety requirements, levels, and criticality.
- Design, development, and production rigor is applied across the hardware and software components, but only an integrated system can be certified.

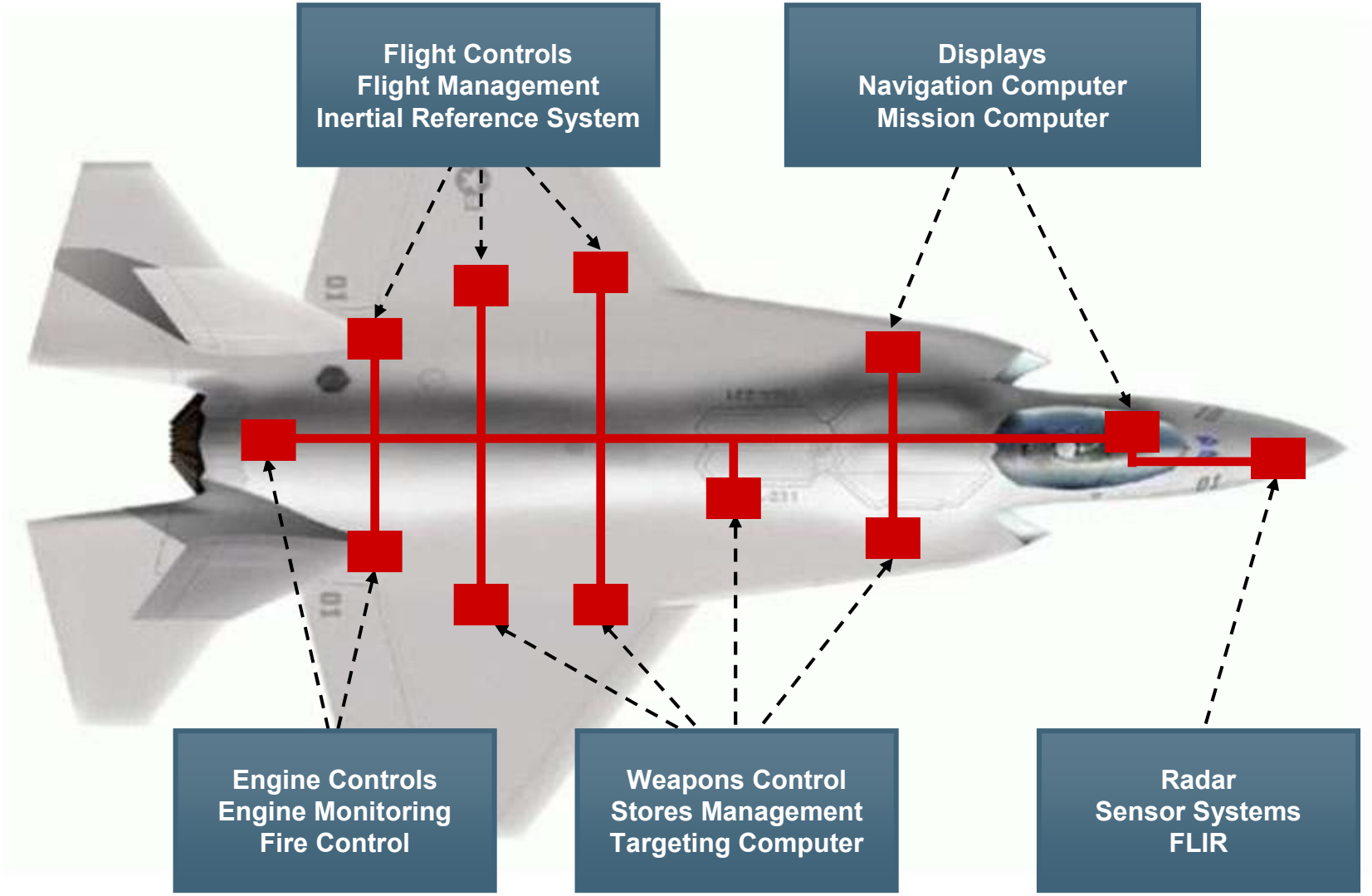




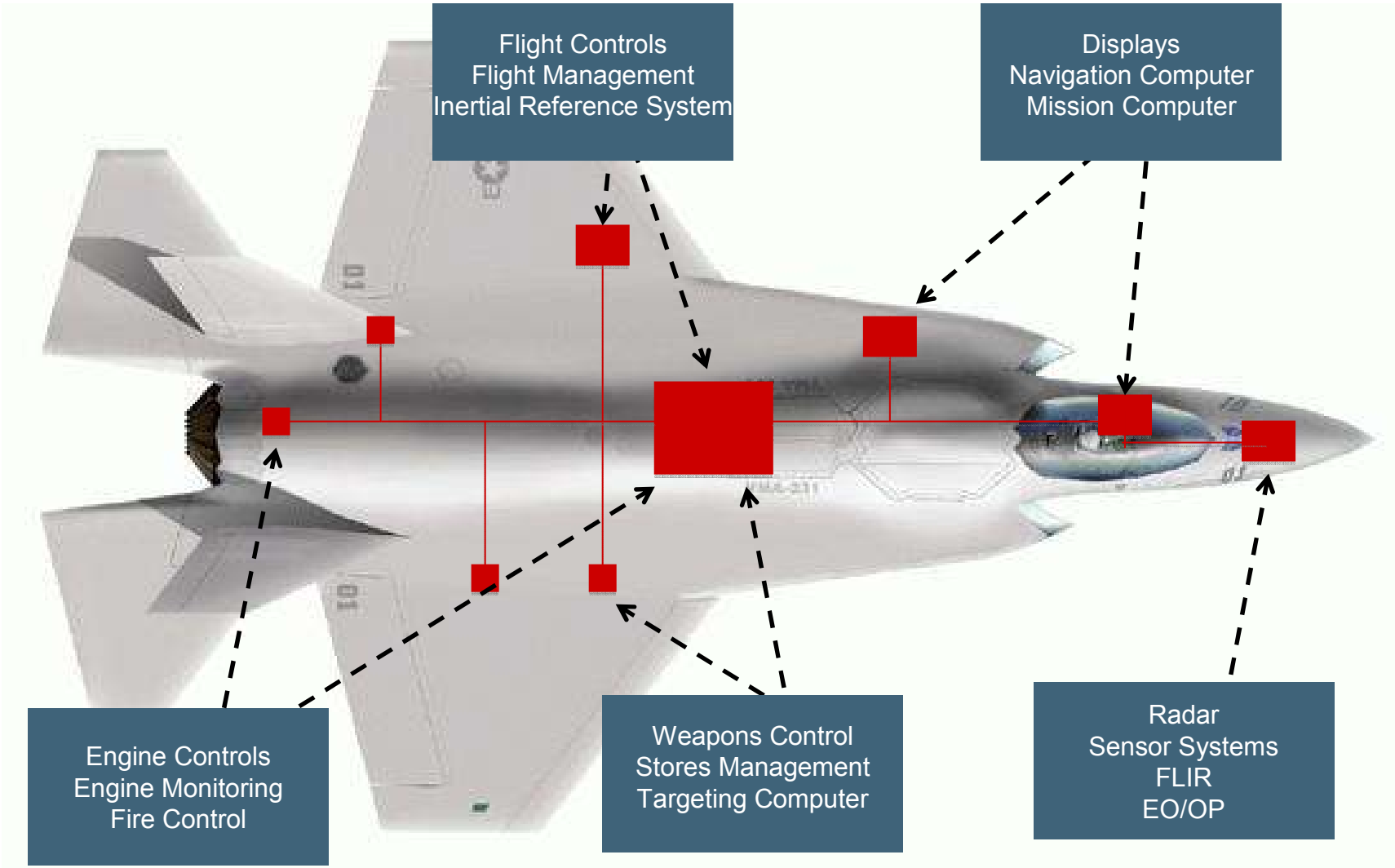
Avionics

DO-178B / ED-12B

Federated Avionics Systems



IMA Architecture (with Federated)



Federated and Integrated Modular Avionics

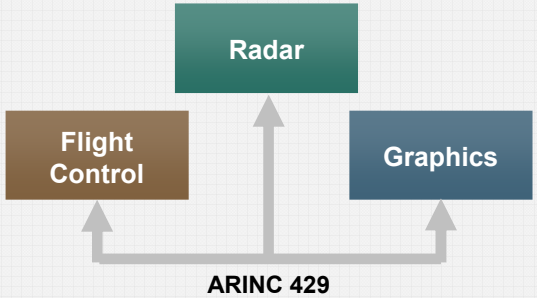
Federated

Usage and Advantages

- Single Level of Criticality
- Single Company Approach
- High performance
- Well-understood methodology
- Established supply chain

Challenges

- Greater size, weight, and power (SWaP) requirements
  - Each function is separate LRU
- Less software reuse
- Less portability, less modularity



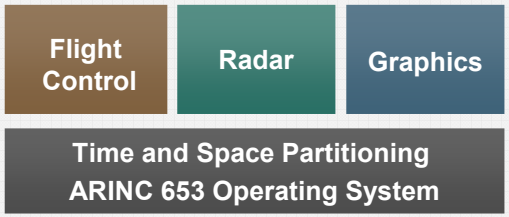
IMA

Usage and Advantages

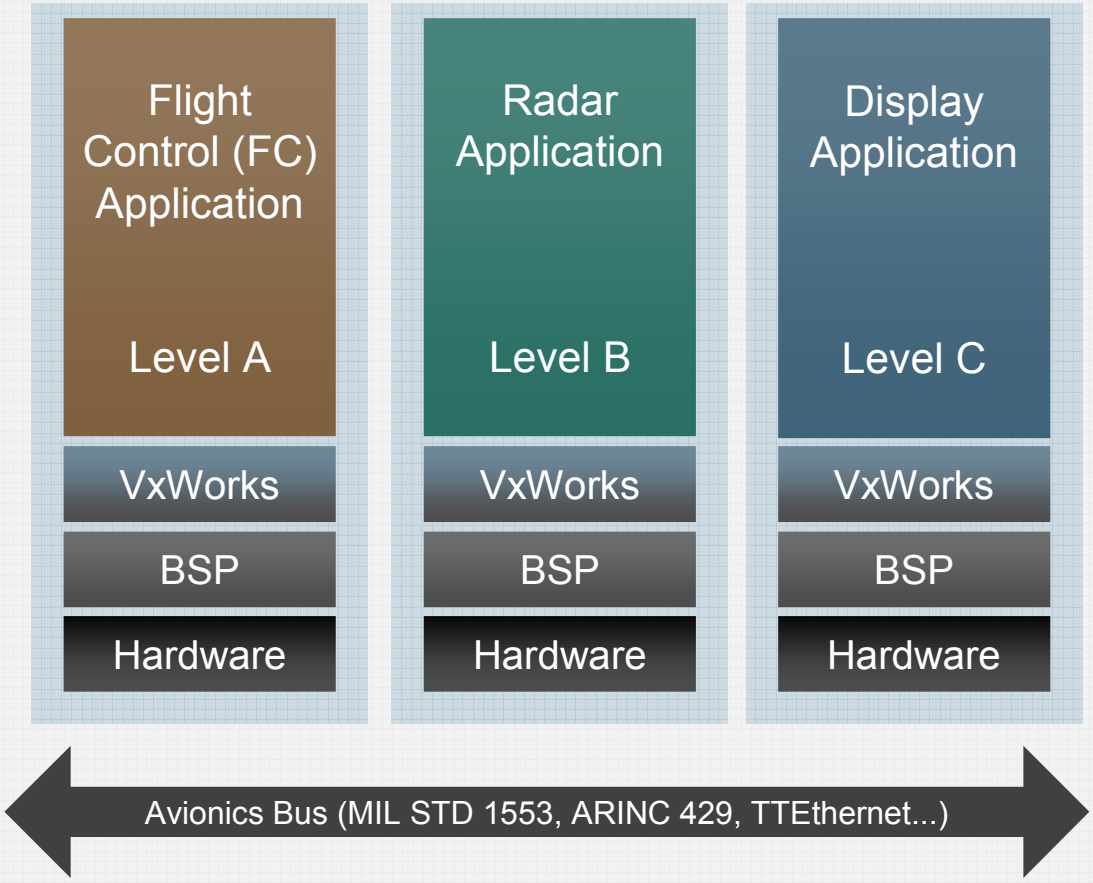
- Multiple Level of Criticality
- Multiple Companies involvement
  - Better software reuse, refresh
  - Better portability, modularity
- Can reduce Integration revalidation costs
  - More efficient platform certification
- Lower SWaP requirements
  - Multiple functions on single LRU

Challenges

- Greater complexity of system integration
- Greater complexity of design and certification
- Less experienced supply chain

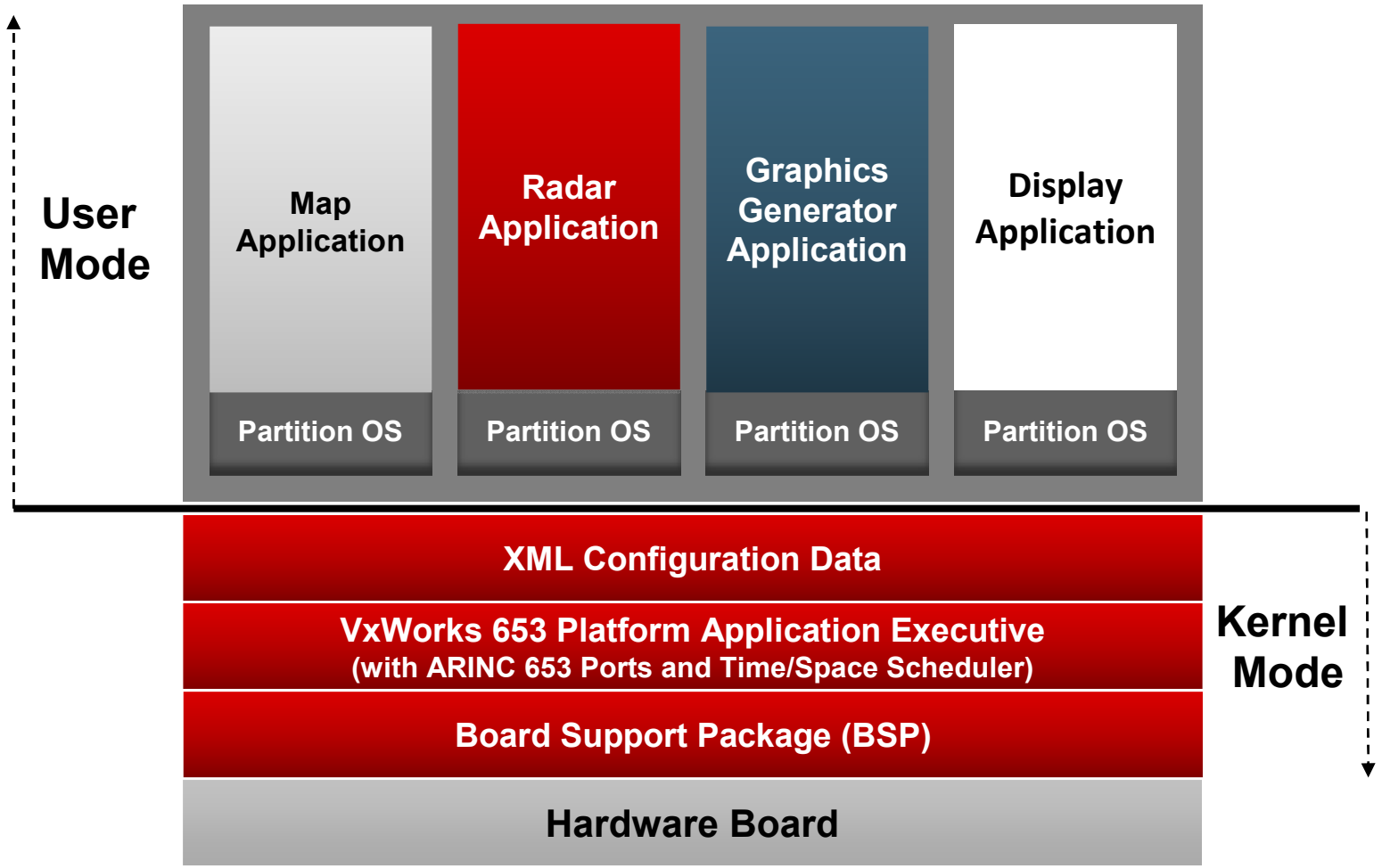


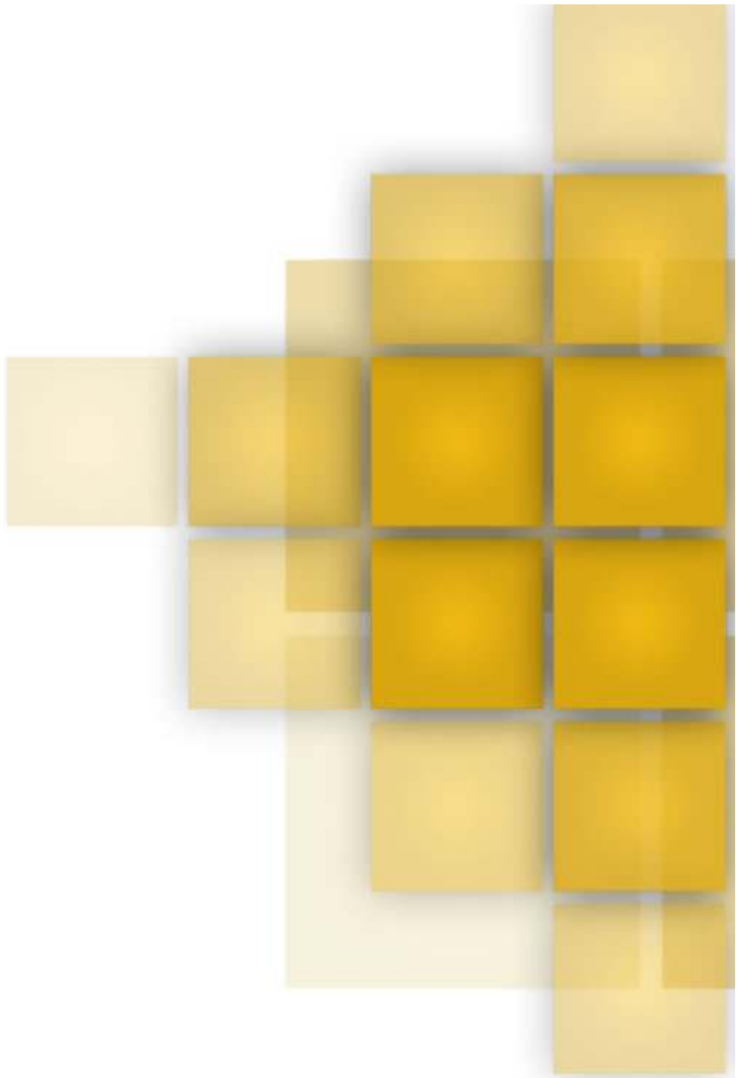
Federated using VxWorks Cert



- Each LRU certified separately
- Certification level specified by system requirements
- BSP, OS, and application typically certified together
- Wind River provides COTS Evidence for VxWorks
- Wind River can provide additional evidence for BSP

IMA Based on VxWorks 653 Platform





Industrial, Railways and Medical Systems

IEC 61508, EN50128 Railway, IEC 62304 Medical

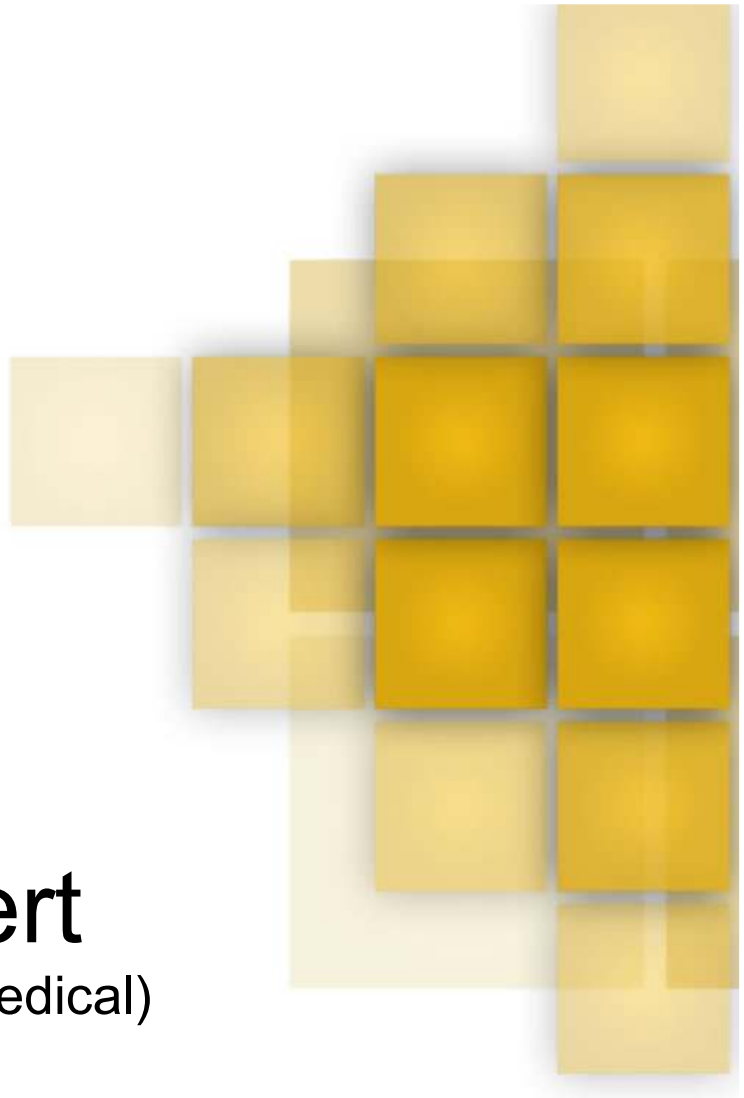
IEC 61508 Applications

- Applications areas
  - Industrial automation (process control, motion control, discrete manufacturing)
  - Transportation (e.g., railway)
  - Medical
  - Power generation and distribution
- Basis for other standards
  - EN 50128 railway
  - IEC 62304 medical

IEC 61508 is widely applicable because it is aligned with commercial off-the-shelf (COTS) vendors' interests where the market opportunity must be aligned with the development investment.

Focal Point: Safety Manual

- One of the most important documents
  - Detailed description of system states: startup, normal, shutdown, and emergency shutdown
  - Implementation guideline for safety-related techniques
  - Measures included in final version of safety manual
- Describes how Wind River VxWorks 61508 Platform has to be used to maintain safety; without it the end user may develop an “unsafe” application even when using the IEC 61508 API



Wind River VxWorks Cert

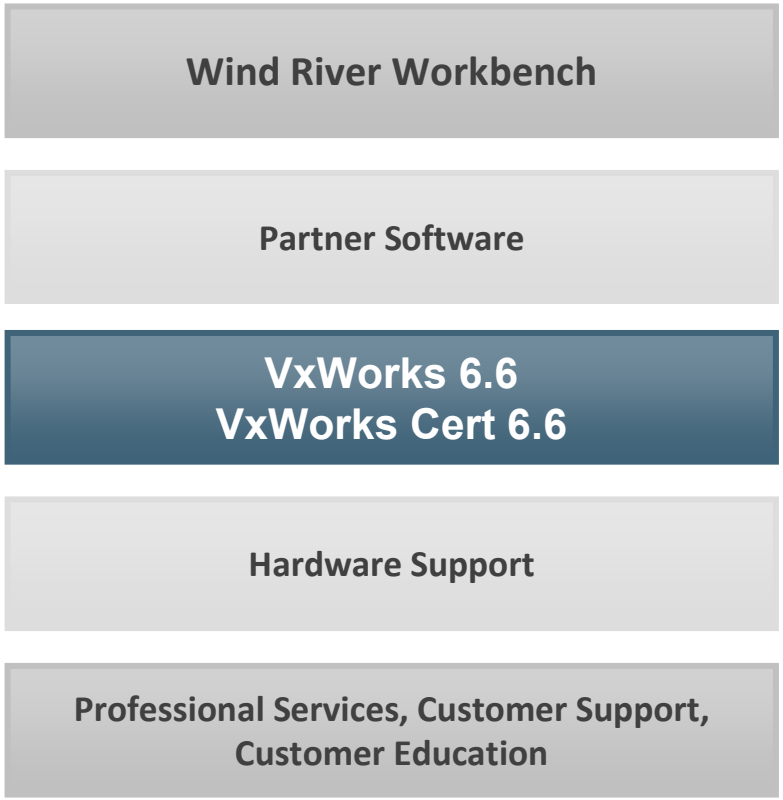
(Common for A&D, Industrial, Railway and Medical)

Wind River VxWorks Cert Platform 6.6.x

Wind River Workbench 3.3.2

- Eclipse framework
- C, C++, Ada*, Java*
- Wind River GNU Compiler
- Wind River Compiler
- VxWorks Simulator
- Uncertified projects
  - All Workbench tools
- Certified projects with Workbench debugger
  - Agent-based debugging
  - Host shell (subset)
  - On-chip debugging
  - Source-code browsing; other editor capabilities
- Certified projects without Workbench debugger
  - On-chip debugging
  - Editor capabilities
- Host OS support
  - Microsoft Windows XP Professional, Windows 7
  - Solaris 10
  - Red Hat Enterprise Linux, Workstation 4, 5, and 6
  - Red Hat Fedora 13
  - OpenSUSE Linux 11.2
  - Novell SUSE Desktop 10 SP2, 11
  - Ubuntu Desktop 10.04

**Partner integration*



Partner Support

- Ada run-time (AdaCore, Aonix)
- Java Virtual Machine (Aicas, Aonix)
- OpenGL (Presagis)
- SCADE Suite (Esterel)
- VAPS (Presagis)
- Other VxWorks 6 partners

VxWorks 6.6/VxWorks Cert 6.6

- Standard VxWorks 6.6
- VxWorks Cert 6.6
  - Cert API subset, C, C++
  - Kernel modules and RTPs
  - No SMP, VxBus, or TrueFFS
- Network stack optional
  - IPv4/UDP/TC stack with multicast
  - Optional file system
  - Fail-safe, 16GB+ files, 2TB disks
  - Multiple transaction commit policies

Hardware Support

- MPC8349E, MPC7447, PPC750GX
- Intel Core 2, Intel Atom
- ARM Cortex A-9, TI OMAP3530 (Cortex A-8)

 |

What's New

VxWorks Cert 6.6.4
Release Date: December 2011

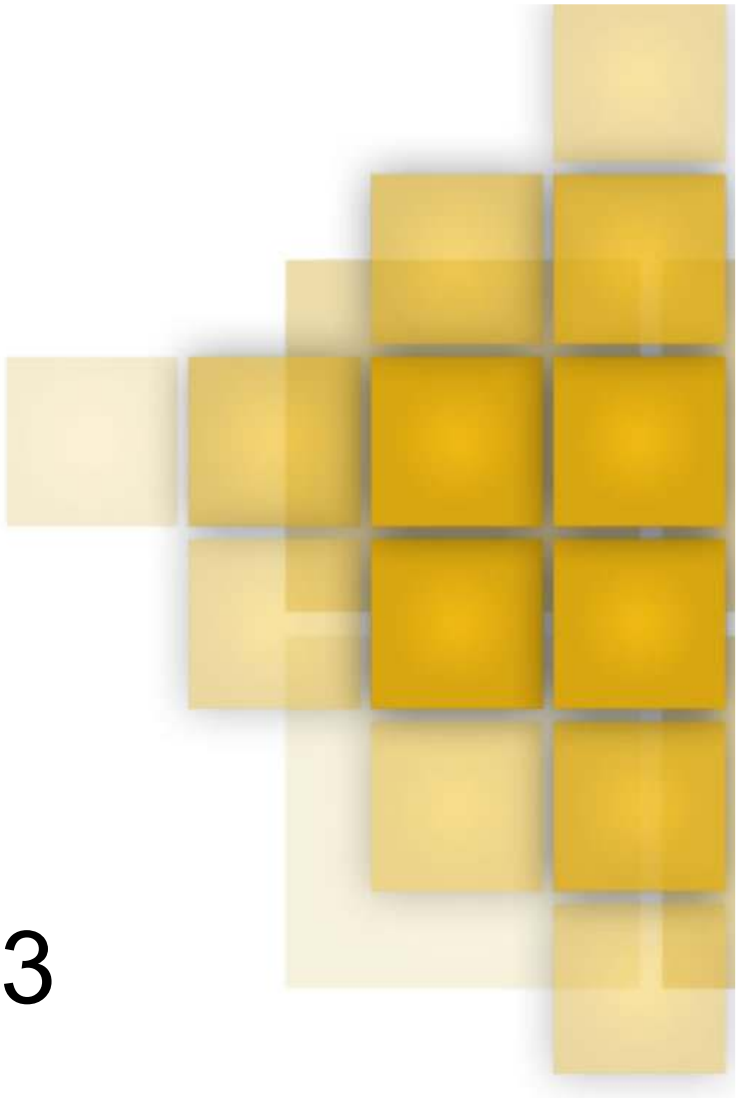
- ARM architecture support
  - ARM Cortex A-9 (Coretile Express A9x4) single-core support
  - TI OMAP3530 (Mistral OMAP3530 EVB)
- Expanded PowerPC support
  - PPC750GX support (Wind River SBC750GX board)

VxWorks Cert 6.6.3.1
Release Date: October 2011

- DO-178B and IEC 61508 certification packages for new features
  - Cert HRFS on Intel architecture
  - C++ functionality
  - Intel Atom

Differences from VxWorks 6.x

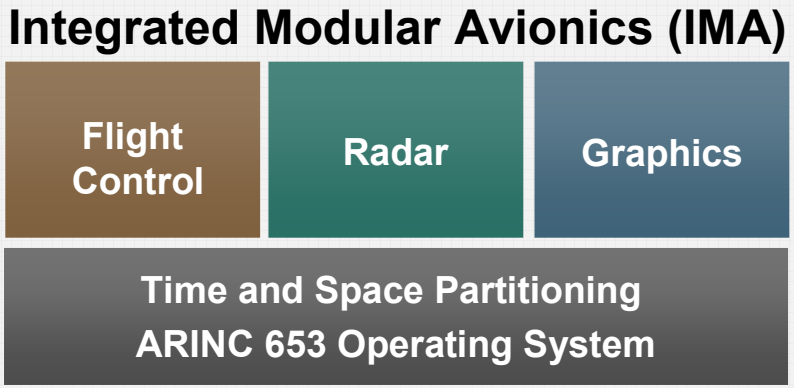
- Reduced set of kernel APIs
  - No support for SMP, TrueFFS, or VxBus
- C++ feature subset
  - No exception handling, RTTI, run-time library support
- RTP support
  - Overlapped memory model, statically invoked
  - No user-level devices, no direct access to network
- Links explicit objects, not binary archives
  - Prevents unintended binaries from getting pulled into the build
- Reboot alternative
  - lastRites(): routine to handle fatal errors
- memNoMoreAllocations() and rtpMemAllocDisable()
  - Disables mallocs after application initialization
- cert_ioDevLib
  - Provides simple I/O through serial channels



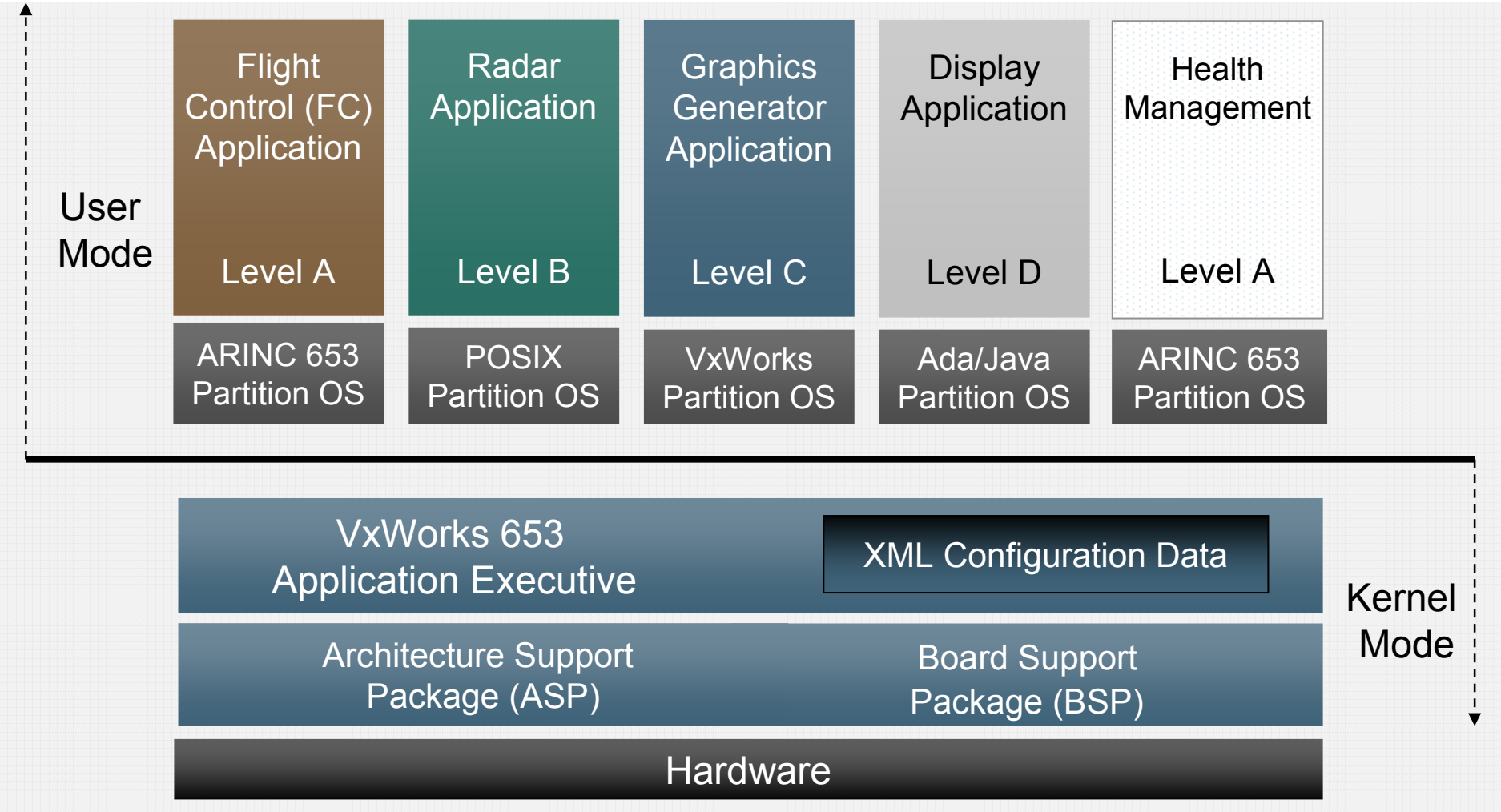
Wind River VxWorks 653

ARINC 653 for Integrated Modular Avionics

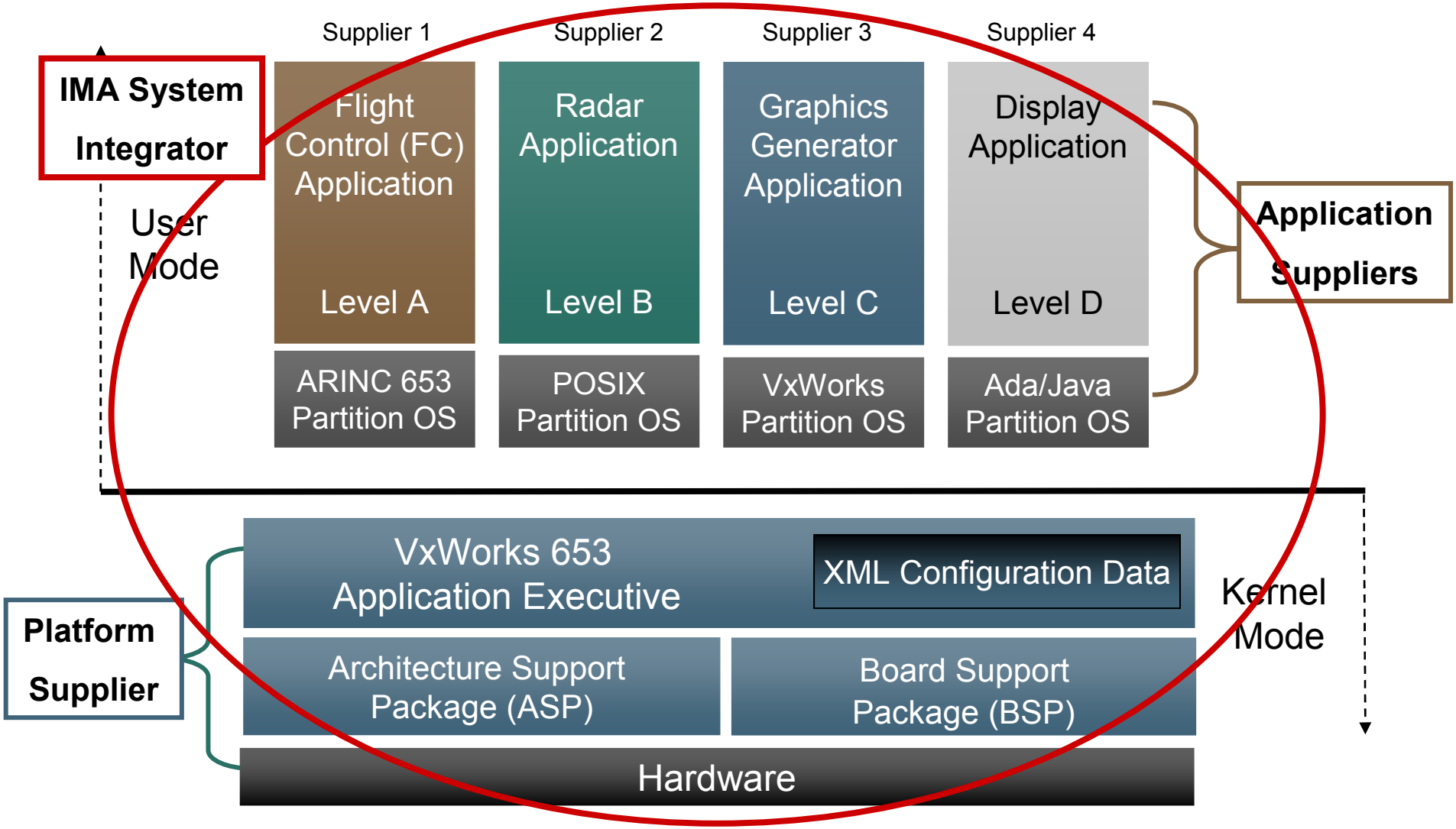
- Goal: Reduce size, weight, and power (SWaP) requirements
- ARINC 653: Industry specification for Integrated Modular Avionics (IMA)
- Includes API of 56 routines
  - Time and space partitioning
  - Inter- and intra-partition communications (IPC)
  - Health monitoring (error detection and reporting)
- **IBLL**: Independent Build Link and Load for Modularity, including Certification



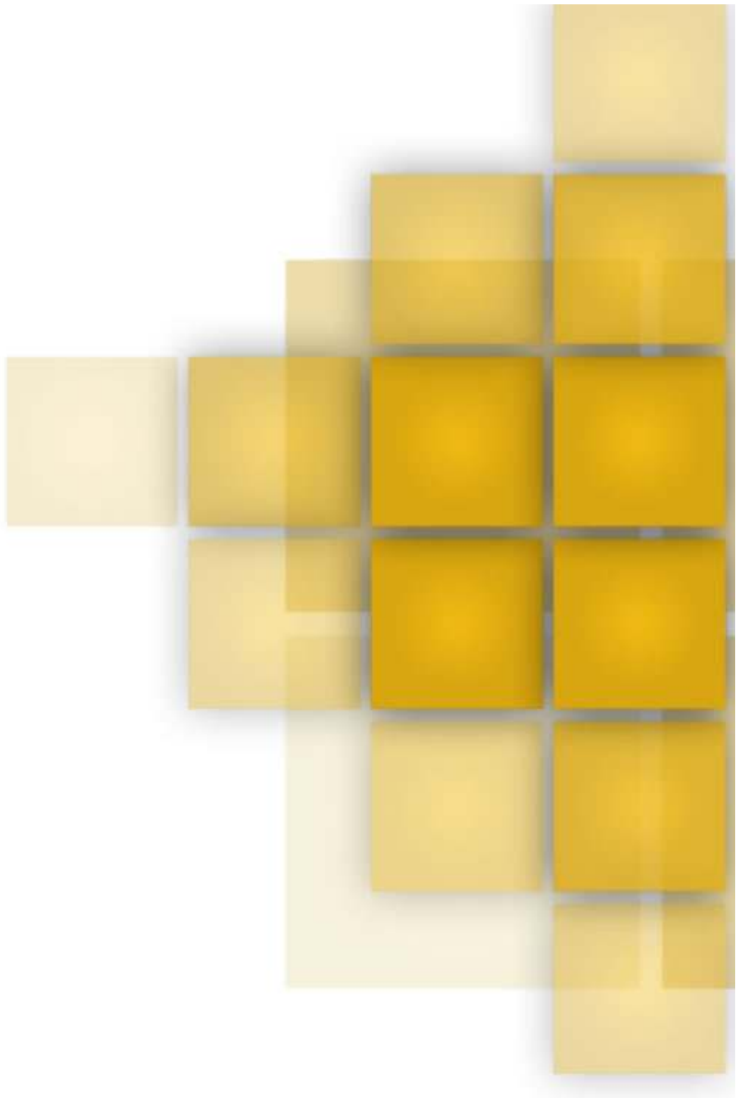
IMA using VxWorks 653



Independent software delivery / DO-297



 |



VxWorks Cert / 653 Common Features

Application Development

- C, C++ language
  - Wind River GNU Compiler
  - Wind River Compiler (VxWorks-Cert only)
- Ada
  - AdaCore GNAT Pro High-Integrity Edition
  - Atego ObjectAda
- Java
  - Aicas Jamaica VM
  - Atego PERC VM

Certifiable Network Stack (optional)

- Developed using DO-178B Level A and IEC 61508 SIL 3 guidelines
- Configuration support for combination of UDP/TCP/IPv4/IGMPv4, multicast
- BSD style sockets in the following domains
  - IPv4, Internet communications domain (AF_INET)
- Broadcast, subnet, and multicast support
  - RFC919, RFC922, RFC950
- Architecture for IP address allocation with classless inter-domain routing (CIDR)
  - RFC1518, RFC1519
- Source Example: TFTPv1-remote access support (server and client)
  - RFC783, RFC1350
- Source Example: Simple Network Time Protocol (SNTP) version 2
  - For IPv4 and OSI: RFC2030

Certifiable File System (optional)

- Several possibilities depending on the need: HRFS of FS2
- HRFS
  - Optimized for SATA usage
  - Shares code base with VxWorks HRFS
  - 64 bits File System: 2TB disk sizes, 16GB file sizes
  - Power-safe and fail-safe: file system integrity maintained
  - Transactional with three commit policy options and capabilties
    - Automatic commit policy (default)
    - High-speed commit policy
    - Programmatic initiation of commits
  - POSIX-style file permissions and file linking available
  - Disk partitioning and formatting executed on VxWorks (non-cert mode)
  - Accessible via low-level I/O calls
- FS2
  - Optimized for Flash usage
  - 32 bits File System, Power fail-safe

Certifiable Graphics (thru partners)

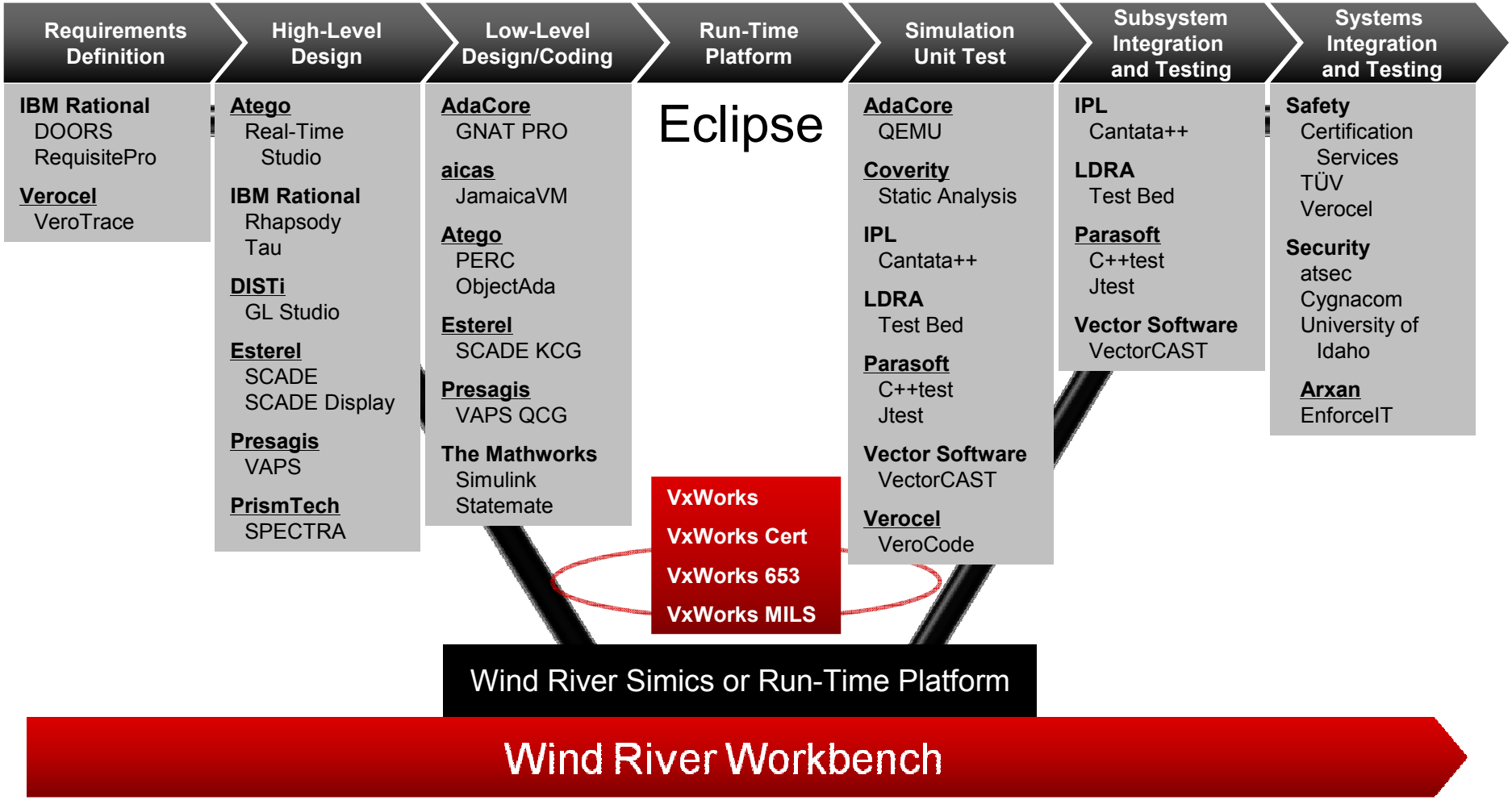
- Industry leading design tools for certified graphics
  - Esterel SCADE Display
  - Presagis VAPS XT
- Certified OpenGL drivers
  - ALT Software
  - Presagis / SeaWind
- Leading hardware vendor support
  - Curtiss-Wright
  - GE Intelligent Platforms

Complete COTS graphics stacks – ready to use

Proven in multiple DO-178B Level A programs

 |

Tools Choice Across the Life Cycle

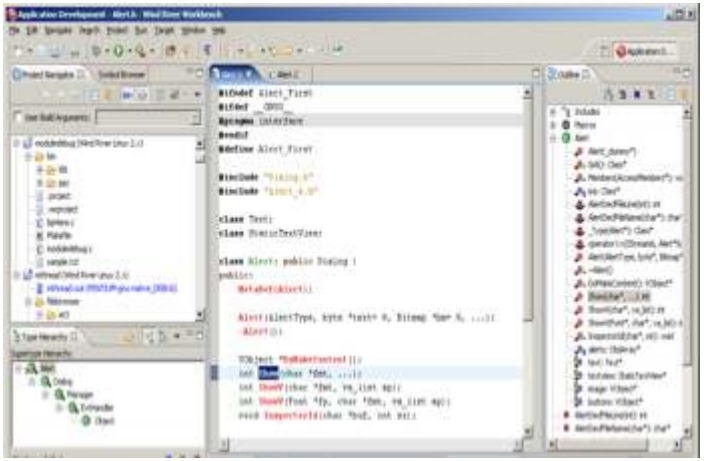


Wind River On-Chip Debugging Solutions

Wind River Probe

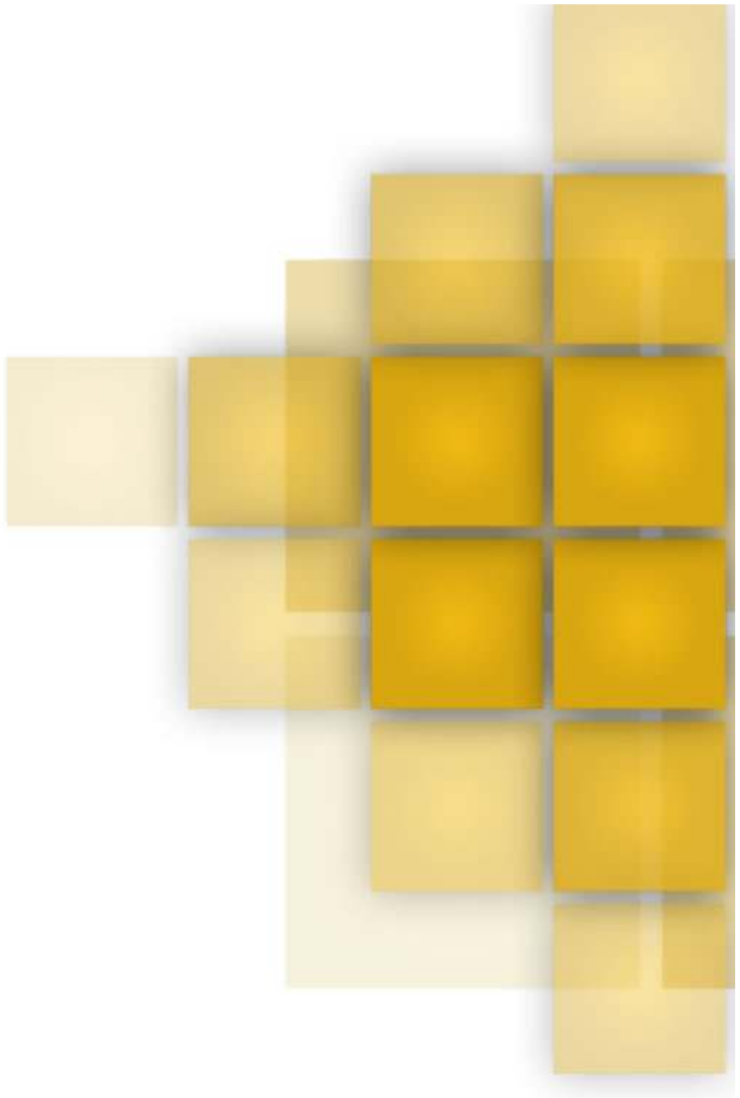
- 100MHz JTAG clock
- USB 1.x and 2.0 compliant
- Auto-voltage
- Bus powered

Wind River Workbench On-Chip Debugging



Wind River ICE 2

- 20MHz JTAG clock
- Multi-core
- Multisession



Certification Evidences

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE

No. Z10 10 11 75658 001

Holder of Certificate: **Wind River Systems, Inc.**
500 Wind River Way
Alameda CA 94501
USA

Factory(ies): 75661

Certification Mark:

Product: **Software, Operating Systems**
Real time Operating System

Model(s): **VxWorks Cert 6.6.1.x**

Parameters: The current Annex and the report no. WA83446C are mandatory parts of the certificate. Only together with the currently valid versions of the Annex and the test report, the product complies with the listed standards.

Tested according to: IEC 61508:2010 part 1, 3, 4 (SIL3)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: WA83446C

Date, 2010-12-01

(Günter Greil)

365442

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

VxWorks Cert DO-178B-178C / ED-12B Level A Certification Evidence Package

- VxWorks DO-178B Platform kernel
  - Source and binary code
- Plan for Software Aspects of Certification (PSAC)
- Software Quality Assurance Plan
- Software Configuration Management Plan (SCMP)
- Software Development Plan (SDP)
  - Software requirements standards
  - Software design standards
  - Software coding standards
- Software Verification Plan (SVP)
- Software Requirements Specification (SRS)

- Software Design Document (SDD)
- Version Description Document (VDD)
- Traceability matrix
- Software development folder
  - Design reviews
  - Code reviews
  - Test reviews
  - Functional test coverage results (object level)
- Tool qualification documentation
  - Test Harness for VxWorks Cert
  - VerOcode, VerOLink, VeroSource-A, VeroTrace
- Software Accomplishment Summary (SAS)
- Software Vulnerability Analysis

Sealed DVD with Certification Artifacts

 |

VxWorks 653 DO-178B-178C / ED-12B Level A Certification Evidence Package

- VxWorks DO-178B Platform kernel
  - Source and binary code
- Plan for Software Aspects of Certification (PSAC)
- Software Quality Assurance Plan
- Software Configuration Management Plan (SCMP)
- Software Development Plan (SDP)
  - Software requirements standards
  - Software design standards
  - Software coding standards
- Software Verification Plan (SVP)
- Software Requirements Specification (SRS) (7,000 Requirements)

- Software Design Document (SDD)
- Version Description Document (VDD)
- Traceability matrix
- Software development folder
  - Design reviews
  - Code reviews (40,000 LOC)
  - Test reviews (7,500 Tests)
  - Functional test (270,000 LOC)
  - Functional test coverage results (object level)
- Tool qualification documentation
  - Test Harness for VxWorks Cert
  - VerOcode, VerOLink, VeroSource-A, VeroTrace
- Software Accomplishment Summary (SAS)
- Software Vulnerability Analysis
- ***Robust Partitioning Analysis***

Sealed DVD with Certification Artifacts
(70,000 hyperlinked files)

 |