# Accelerating Avionics Safety Certification

Using Wind River Certifiable IP Blocks

## SHORTENING THE RUNWAY TO DO-178C CERTIFICATION

Ever since the tale of Icarus, human beings have recognized the importance of aviation safety. Today's commercial and military aircraft are subject to some of the most rigorous safety standards of any industry, and rightfully so. One of the most critical components of avionics safety focuses on the embedded software systems that operate modern aircraft, which are governed in the United States, Europe, and Canada by DO-178C, the certification standard for Software Considerations in Airborne Systems and Equipment.

DO-178C specifies five design assurance levels (DALs) that correspond to the impact that a component's design failure would have on the aircraft. Failure of components designated as DAL A, for example, would result in a catastrophic failure, while a DAL E component's failure would have no material impact on the aircraft's operations. To achieve DO-178C certification for a single component, aircraft manufacturers need to complete four stages of involvement (SOI): planning (SOI1), implementation (SOI2), verification and validation (SOI3), and final certification (SOI4). This is a very time-consuming and cost-intensive process for aircraft manufacturers, requiring thousands of hours of testing, hundreds of pages of detailed documentation, and gigabytes of metadata. It is not at all unusual for the DO-178C certification process of a single software component to take 18–36 months at a cost of several million dollars.

## MORE TURBULENCE LIES AHEAD

Beyond the inherent challenges of the DO-178C certification process itself, aviation manufacturers now face additional challenges due to the increasing complexity of avionics software systems (including an industrywide shift from single-core to multi-core processors), global supply chain issues that have delayed the implementation and testing processes, and the diminishing pool and rising cost of testing engineers in the workforce.

Aerospace manufacturers need to deliver safety certification artifacts for a variety of software components that typically include a real-time operating system running on architectures popular in aerospace and defense, board support packages (BSPs) of multiple device drivers that collectively represent thousands of effective lines of code (ELOCs), real-time network stacks, and security hardening. Completing DO-178C certification for all these components could take five or more years and, for more complex systems, easily cost in excess of $25 million.

## REUSING CERTIFIABLE INTELLECTUAL PROPERTY IS THE INTELLIGENT APPROACH

For avionics software safety certification, the key to reducing time, cost, and risk is reusability. There are no shortcuts in DO-178C certification, but there is also no need to recreate the wheel — or, in this case, the wing — each time the same component is certified. For example, once you've completed the planning, implementation, verification, and attendant documentation for the DO-178C certification of an Arm® Cortex-A72 multi-core processor, you can reuse all that information to pre-certify future applications that use the same processor chip.

Wind River® provides commercial software, such as Wind River Helix™ Virtualization Platform, and professional services to many commercial and military programs that have airworthiness requirements. We have a substantial worldwide team of services experts who spend thousands of hours developing software and safety artifacts to meet rigid commercial and military safety standards. By repackaging this intellectual property (software and artifacts) into reusable, pre-built modules — known as certifiable IP blocks — we can dramatically reduce the time, cost, and risk associated with airworthiness certification.

Wind River certifiable IP blocks represent a set of key software components that have been tested and documented from SOI1 through SOI3 of the DO-178C certification process. Recently, one of the world's leading aerospace engine and systems manufacturers engaged with Wind River to streamline its DO-178C certification activities for an unmanned aerial vehicle (UAV) in an effort to reduce costs, accelerate time-to-market, and address both supply chain and skillset shortages. They were able to leverage many of our IP certifiable blocks for a system that included a 16-core Arm-A72 processor, virtualization platform with the VxWorks® real-time operating system, real-time network communications stack, security framework, high-reliability file system, and a board support package (BSP) with driver support for a variety of connected devices. Once the IP blocks were delivered, we worked with our aerospace customer to make some adjustments to the software to meet their unique use case requirements. Once those adjustments were made, we performed a final delta certification (SOI4), saving them a significant amount of time versus starting the certification from scratch.

The specific certifiable IP blocks of software and artifacts used in this engagement were:

- VxWorks real-time operating system
- Helix Platform hypervisor
- A custom BSP featuring pre-certified drivers and APIs for the customer's I2C bus, general-purpose input/output (GPIO), serial input-output, PCI, clock, and interrupt handler designed to support their choice of Arm Cortex-A72 multi-core processor
- Wind River RTnet real-time network protocol stack with support for a wide variety of network protocols including TCP, UDP, IPv4, ARP, and ICMP
- Wind River information assurance foundation security framework featuring full encryption and specialized software code
- Certified, power fail-safe highly reliable file system (HRFS) designed to meet DO-178C DAL A safety requirements

By leveraging the existing intellectual property and testing tools that Wind River had created, the aerospace manufacturer hoped to complete all DO-178C DAL C safety certification testing (SOI1–SOI4) in just over a year while saving millions of dollars and reducing project risk.

In addition, the customer utilized the Wind River Simics® platform to help accelerate system testing using a software-based hardware simulation environment. With Simics, the customer created a digital twin of hardware

instances (specifically, NXP's LX2160A processor) to stand up thousands of virtual CPUs for application testing and development, saving the company millions of dollars in hardware costs. By using the Simics platform, the customer also eliminated the need to procure and then wait for hardware to be shipped to them, cutting critical months from the project's schedule time.

## A SECURE PATH TO FASTER INNOVATION

By using Wind River IP certifiable blocks, this aerospace customer was able to cut years from project development, save millions of dollars in costs, and significantly reduce risk with proven software that was already validated, verified, and fully documented upon arrival. From that point, Wind River Professional Services worked closely with the customer to customize the pre-certified software around specific use case requirements and complete the delta certification to conclude the final stage (SOI4) of the DO-178C certification process.

Streamlining the software certification process will allow the aerospace customer to bring its solutions to market faster, making it more competitive and increasing its time-to-revenue. With IP certifiable blocks that support both Arm-A72 and -A53 processors, Wind River provides a flexible path to multi-core processing that will allow its customers to standardize on a future-friendly platform that accelerates the avionics innovations of tomorrow.

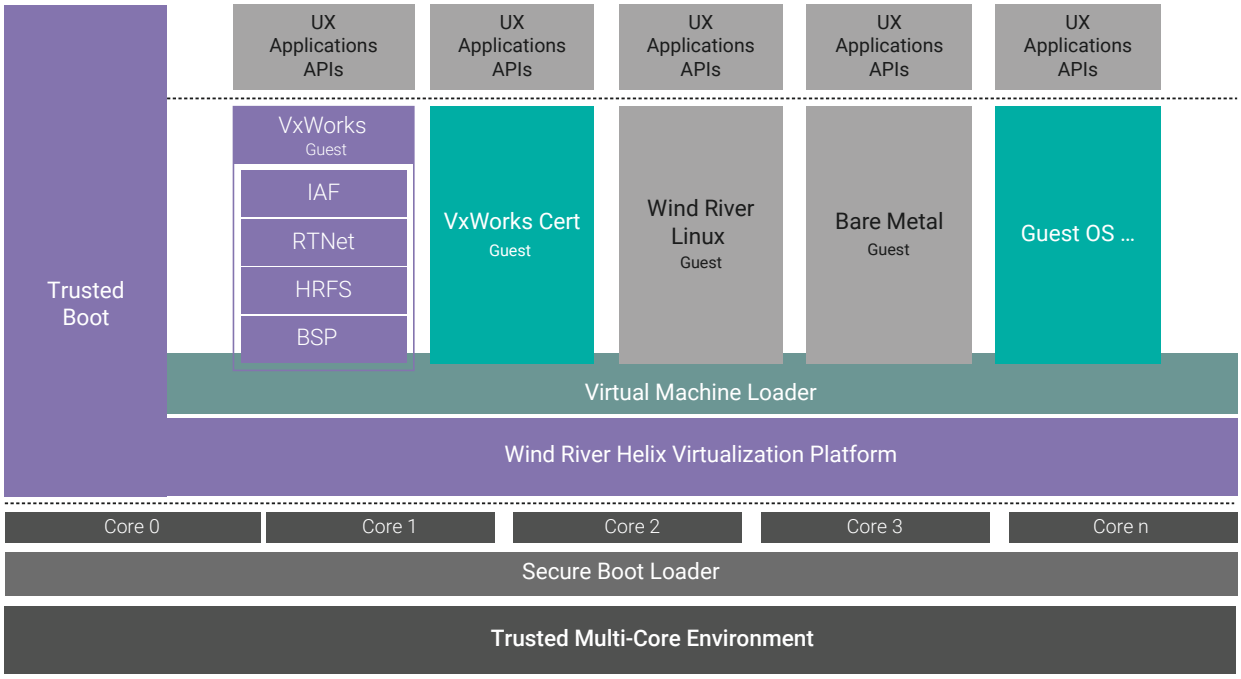


*Figure 1. Certifiable software stack for multiple operating systems and mixed levels of criticality*

WNDRVR