WIND™

Affordability by Design for Aerospace and Defense Systems

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

There is one challenge that every business executive in the aerospace and defense industries is deeply concerned about today: affordability. Given the large investments companies need to make in developing, testing, certifying, deploying, and maintaining critical systems in our software-defined world, affordability underpins every product and engineering decision.

How can we make our systems more affordable? This paper presents five factors and recommended design decisions that drive greater affordability in aerospace and defense platforms.

TABLE OF CONTENTS

FACTORS IMPACTING SYSTEM AFFORDABILITY

Five steps will have the most significant impact on platform affordability in the aerospace and defense industries:

1. **Choose the system architecture:** There are two prevailing system architecture designs in today's critical systems—federated and integrated modular avionics (IMA). Federated systems offer the simplest design and the best separation for incremental addition of capabilities, but they have a significant impact on increasing size, weight, and power (SWaP). IMA consolidated platforms have a lower impact on SWaP but a much more complex architecture, especially when multiple suppliers and multiple levels of safety and security are required. The table below summarizes these architecture trade-offs.

Federated Systems Architecture	Integrated Modular Avionics (IMA) Architecture
+ Simpler architecture	+ Lower SWaP requirements
+ Design independence	+ More efficient use of multi-core hardware
+ Certification independence	+ Common hardware architecture
+ Standard supply chain flow	+ Ease of cross-platform soft ware portability
- Increase in size, weight, and power (SWaP)	+ Integrated redundancy/ failover
- Greater tendency for hardware uniqueness	+ Ability to support multiple levels of safety and security
- Multiple supported hardware platforms	+ Ability to support multiple OS environments
- Hardware-specific redundancy	- Higher complexity of design
- Single level of safety and/or security	- Greater challenges in support ing multiple suppliers
- Poor utilization/optimization of hardware	- Greater complexity of systems integration
- Single OS support	- More complex test and integration

With the proliferation of powerful single core processors with memory management units (MMUs) and multi-core processors with hardware virtualization assist, the trend over the last 10 years is toward IMA consolidated platforms. Wind River® is seeing a strong shift toward this trend: Of the 550 certification programs executed by Wind River over the last 15 years, 440—about 80%—use Wind River VxWorks® 653 Platform, an IMA-conformant consolidation platform. We expect this upward trend to persist as multi-core processors continue to increase their power, performance, and core count. This added capability allows support of "virtual federated systems" on multiple hardware cores.

2. **Design for change:** Coupled with a strong systems architecture, a new platform must be designed for a lifetime of change. Systems must be ready to accept updated application components at any point in their operation. They must also support a structured method of integrating these changes, to minimize the impact on the entire system. Specifically, system designs should endeavor to minimize the scope of retesting to the scope of the change. This characteristic is often overlooked by development teams, with the result that they need to retest 100% of the platform before release. Confining retesting to the scope of future changes can save millions of dollars in testing costs while also accelerating the platform back into service.
3. **Design for test with model-based engineering (MBE) design tools:** The days of designing and developing software systems "from scratch" and "by hand" are over. Our industry now has a rich collection of design tools that are based on formal methods and other technologies, such as Ansys SCADE and Presagis VAPS XT. These tools allow designers to create complex critical systems using an advanced GUI environment. Auto-generation of code that is correct by construction provides code that does not need white-box testing. This generated code can be immediately integrated with other software and data structures to accelerate time-to-deployment.
4. **Design for safety and security:** In our Internet of Things (IoT) world, we have evolved from disparate, disconnected embedded devices to a world of highly connected, always-on systems of embedded platforms that have a safety and security impact. In addition, these systems will always be under attack by an ever more sophisticated army of networked security threats. This is the most important aspect of your platform design. Creating a robust, resilient, and dynamic environment for protecting and enforcing the safety and security of any solution can significantly impact affordability. Certified systems that are not designed to minimize the cost of change over the life of the product can cost many millions of dollars more to support. Applications with requirements for high levels of safety and security are the most expensive parts of any platform, and therefore they need the most attention for minimizing the cost of certification and recertification.

5. **Design in trust:** Complex software-defined multi-core open virtualization platforms are tough to build, tough to test, and tough to maintain over a product's lifecycle. One must create trusted architectures, design components, build and test processes, and proven commercial off-the-shelf (COTS) software components to form a foundation of trust that will allow focus on new, highly competitive aspects that do not have proven safety, security, and operational credentials. Using trusted components drives down program risk and accelerates time-to-market and deployment.

DESIGN DECISIONS THAT INCREASE AFFORDABILITY

With the above design criteria in hand, how does one build a platform that enables better affordability? Here are a few suggestions:

- **Maximize the capability of your design tools:** Too often, one team will use a small feature of a design tool, but this tends to minimize the development impact of using the tool. Design and development teams need to embrace the use of tools across the enterprise for the full value of the tool to become available to reduce development costs, reduce testing costs, accelerate development, and therefore increase affordability across the enterprise.
- **Use industry standards:** Historically it was advantageous to create highly proprietary solutions that were difficult for competitors to penetrate. In our new virtualized, software-defined world, this is no longer a successful product strategy. Next-generation platforms need to provide an open standards-based system that is capable and ready to adapt to any modern or legacy operating system and application environment. Proven open software standards that span both commercial and military usage, such as POSIX® and ARINC 653, have an available market and therefore can allow development costs to be amortized across many customer environments.
- **Create common, virtualized platforms that are used across multiple product lines:** Due to increased costs of both personnel and platform maintenance, we are nearing the end of the era when each segment of a company's product portfolio developed its own proprietary and unique hardware and software platform. Companies need to create common virtualization platforms that enable the use of any guest operating system, embedded or enterprise, to be deployed in any segment or application area across the enterprise. This platform needs to support open architectures and multiple guest OS virtual machines, such as POSIX, ARINC 653, Linux, and possibly VxWorks. Investing in one powerful platform that all product segments can use with ease eliminates the wasted design, development, and support costs of many single-use, proprietary internal platforms that no longer drive a competitive advantage.
- **Use digital twins and system simulation tools:** Using MBE coupled with system simulation tools through the product lifecycle designs in quality up front, tests and verifies quality over the useful life of a platform, and lowers TCO from power on to power off in an embedded platform.
- **Use COTS components:** Today there is a rich and competitive software components ecosystem serving the global aerospace and defense industries. Most of these software packages not only have well-defined test/quality credentials but may also have high technology readiness levels (TRLs) that will accelerate time-to-deployment and program acceptance.
- **Use COTS safety and security evidence:** In addition to having high TRLs, many COTS software suppliers have robust safety and security certification evidence available as a COTS offering. These packages can drive test/acceptance and airworthiness costs down, while accelerating time-to-market and time-to-deployment. These characteristics drive up affordability and advance time-to-revenue.
- **Enable your integrated supply chain with independence:** As platform consolidation and IMA systems on multi-core processors become the norm, your supply chain needs to be able to design, develop, test, and ship components to your systems integration center with minimal dependencies. Capabilities such as Wind River VxWorks 653 independent build, link, and load (IBLL) enable the supply chain to ship only tested binaries and XML configuration to systems integrators, with minimal disruption to other suppliers' activities and system integration efforts.
- **Insist on robust partitioning across the platform:** Robust partitioning eliminates the requirement to retest your entire platform when any change is made. Robust partitioning is a hard requirement for any complex integrated system, and it enables a drastic reduction of the total cost of ownership (TCO). Integrated systems without robust partitioning are untenable for long-lifespan products and exponentially increase lifecycle costs.

- **Focus on the total cost of ownership (TCO):** It is easy and appealing to have one team in a design flow make decisions—but such decisions may negatively impact TCO in ways that do not show up until after a product or platform is deployed. These self-centered decisions make your overall system less affordable and less competitive. They are also more difficult and costly for both the supplier and customer to maintain. Never lose focus on TCO.

CONCLUSION

Wind River is the global leader in helping customers build trusted and affordable systems. Our VxWorks and VxWorks 653 products are now used in more than 550 safety and security programs by over 350 customers in more than 90 aircraft. All of our COTS products based on open standards have high TRLs and are ready for use in your next critical platform development. Wind River has the products, partners, and software quality credentials to enable your team to integrate enduring platforms that are both highly competitive and affordable over the entire product life cycle.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.