WNDRVR

VIRTUALIZATION FOR EMBEDDED SYSTEMS

A Bridge to the Future

Executive Summary

Burgeoning trends such as autonomous automobiles, the Internet of Things (IoT), and increasingly sophisticated industrial and manufacturing devices, machines, and systems are forcing change in the world of embedded systems. The old purpose-built, closed legacy architectures are giving way to a fluid, software-defined, and connected approach.

Virtualization has been a common practice in enterprise IT for years. Now it is evolving to become a natural solution for embedded systems. Wind River® Helix™ Virtualization Platform is designed specifically to enable this evolution, offering a single platform that will run essentially any embedded system, old or new. Helix Platform addresses the demanding security, safety, reliability, and certification requirements of modern embedded systems and critical infrastructure. In the process, it helps bridge the past with the future and enables innovation and IP reuse. Furthermore, the platform helps reduce both capital and operating expenses.

CONTENTS

INTRODUCTION

Embedded systems are undergoing a significant transition from purpose-built, closed legacy architectures to more fluid, software-defined, and connected systems. The emergence of IoT, along with ever more sophisticated and connected devices of all types, puts pressure on businesses to innovate more rapidly than legacy technology will allow. At the same time, the cost of supporting legacy embedded systems is growing to the point of unsustainability. It is time for a new approach to developing embedded systems.

Virtualization and the abstraction of software from hardware has been a common practice in enterprise IT for years. It is now practical for embedded systems as well.

Helix Platform is designed specifically to address the demanding security, safety, reliability, and certification requirements of modern embedded systems and critical infrastructure. It enables the consolidation of multiple embedded computing operating systems and applications onto a single device. Helix Platform is safety certifiable and supports many different industry-specific interoperability frameworks, such as ARINC 653, AUTOSAR Adaptive, and others. Helix Platform enables application consolidation and reuse while preserving security, safety, reliability, and certification investments. This enables significant reductions in both capital expenses (CapEx) and operating expenses (OpEx).

Avoid the friction inherent in legacy support with Helix Platform's path to future-proofing and innovation.

THE ONGOING EVOLUTION OF EMBEDDED SYSTEMS

Embedded systems are following enterprise systems in becoming more flexible and software-defined. Traditionally designed embedded systems are purpose built using closed architectures unique to each device. They run a real-time operating system (RTOS) such as VxWorks® in systems that have fixed time constraints, where predictability is key. The RTOS ensures that these systems do not fail. Alternatively, systems without real-time requirements can run customized versions of Linux, such as Wind River Linux.

Figure 1 shows a simplified example of embedded systems at work — in this case, in an automobile that runs multiple proprietary embedded systems in parallel. There's a system for telematics, one for braking and control, one for radar, and one for connectivity. Each has its own OS, dedicated silicon, and certification process.

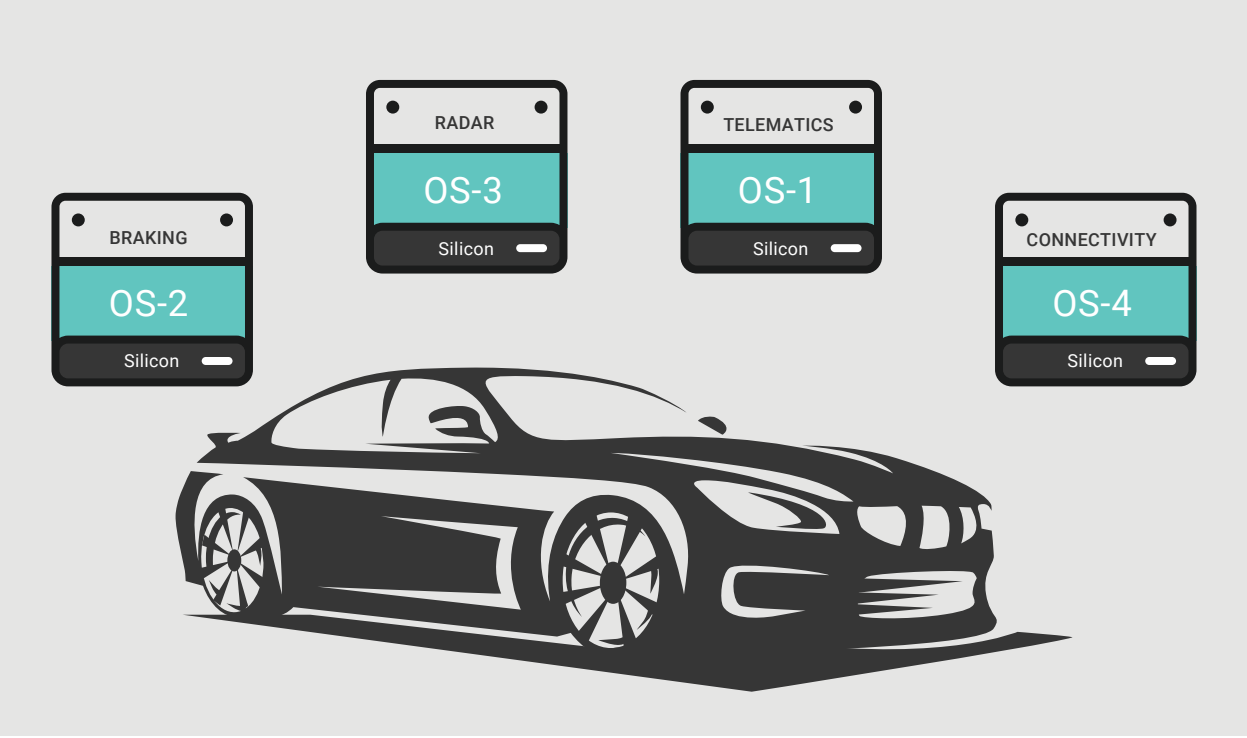


Figure 1. Examples of multiple, separate, and proprietary embedded systems running on a car

This traditional approach is now giving way to software-defined open architectures and consolidation. Using open standards, embedded systems can leverage commercial off-the-shelf (COTS) products. These include hardware-like certified or certifiable standardized board computers and PC platforms. This shift leads to dramatically reduced costs and faster time-to-market.

What were once isolated systems are also now increasingly connected. In the automotive example, the telematics, braking, and connectivity systems may work together to send vehicle data to the manufacturer, fleet owner, or autonomous driving system. As the telematics system is updated over time, the braking and connectivity systems will also likely need to be updated, even if they are built on different technology platforms and manufactured by different companies.

These automotive embedded systems, now connected to one another, need greater security countermeasures than when they were totally siloed. As many major recent data breaches have demonstrated, one system can provide the hacker's path into another. This was the case for a major retail chain whose point-of-sale (POS) systems were hacked because the attacker penetrated the store's unsecured but connected HVAC embedded system. This caused major damage to the retail store's brand and reputation.

A comparable change is occurring in the way manufacturers attain certification for embedded systems. There's a move to system-level certification versus certifying at the component level. This involves making sure that various separate embedded systems, each in a system component, can work together coherently.

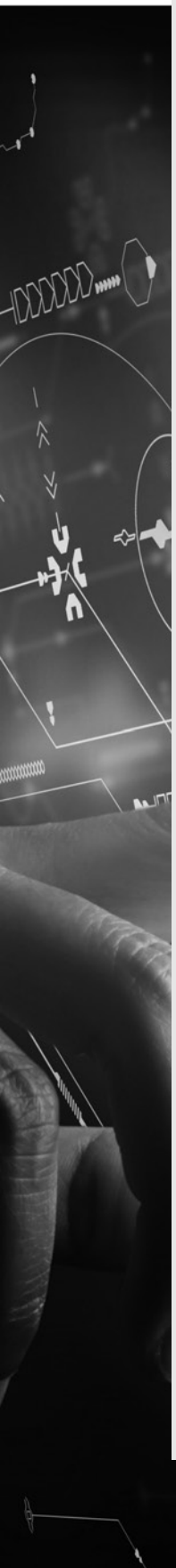
WHAT'S DRIVING CHANGES IN EMBEDDED SYSTEMS?

Drivers of changes in embedded systems design include improvements in hardware as well as the continuing evolution of software development methods.

At the hardware level, it's now possible to do more with a single CPU. Rather than host just one application, new multi-core systems-on-chip (SoCs) can support multiple applications on a single hardware platform, even while still maintaining modest power and cost requirements.

At the same time, advances in software development techniques point toward systems that are more software defined and fluid than their predecessors.

While many things have changed in the embedded systems world, the core requirements have not. Embedded systems have to be **secure, safe, reliable, and certifiable.**

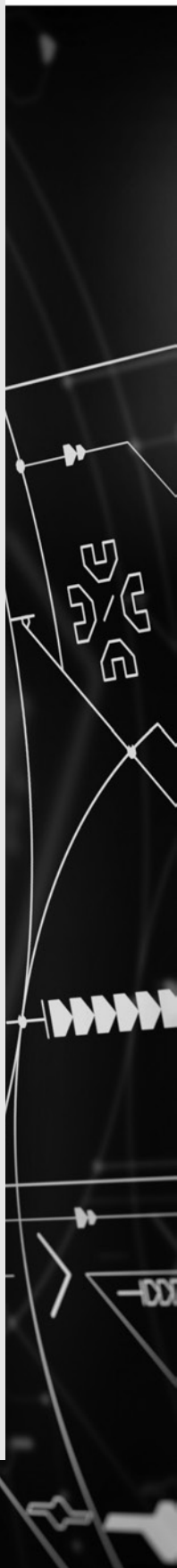


Security: Cyberattacks have become more common, while completely isolated systems are becoming more rare. Embedded engineers are taking security even more seriously than before.

Safety: This refers to the system's ability to ensure that it does not have an adverse effect on its environment. Industrial, transportation, aerospace, and automotive systems can cause death or environmental disaster if their embedded systems malfunction. Determinism, meaning the predictability and reliability of performance, is therefore of paramount importance. A failure in one zone should not trigger a failure of the entire system.

Reliability: Reliability in an embedded system means that it will always perform as expected. It should produce the same outcome, in the same time frame, the first or millionth time it is activated.

Certifiability: The certification process is a critical and costly part of development for many embedded systems. Certification in legacy systems must be maintained and leveraged, while ease of certification for future systems must be managed.



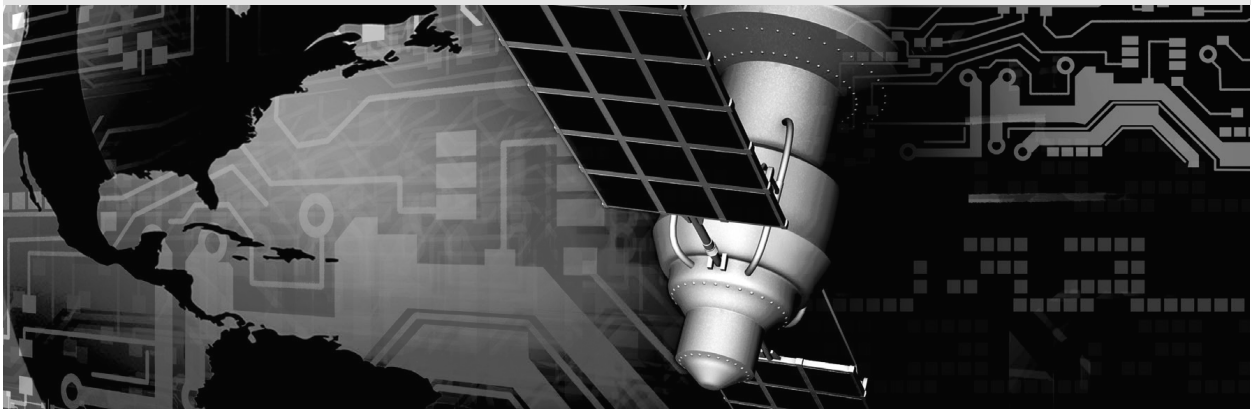
CHALLENGES IN SUPPORTING LEGACY EMBEDDED SYSTEMS

Right now, many manufacturers are facing end-of-life for their legacy embedded systems. Some components are decades old. They may be insecure, unsafe, or unable to meet new certification requirements. They need to be replaced, or at least upgraded, to fit with modern architectures and practices. This promises to be an expensive process — when it is even possible.

At the same time, the workforce is changing. The engineers who built the original designs are retiring, and the new workforce is trained to use a more mainstream approach.

An arguably even bigger problem is simply the rise of requirements for shortening development cycles. While it may once have been viable to take a year or more to create a fixed-function embedded system on a distinct piece of hardware, the market cycle now demands more rapid changes.

What can be done? Many legacy embedded systems are here for the long term — 35 to 45 years is not an uncommon lifecycle. They may not be modern, but the machines they run were built to last. Industrial control systems, for example, could have multi-decade lives, even if their digital components are hopelessly out of date. New solutions are emerging to address this dilemma.



ADVANTAGES OF VIRTUALIZATION IN EMBEDDED SYSTEMS

Fortunately, advances in hardware and virtualization have occurred in parallel with the changes besetting the world of embedded systems. It is now possible to overcome most of the difficulties inherent in having separate, purpose-built embedded systems running on separate proprietary hardware.

This is achieved by incorporating each separate embedded system, with all its applications and operating systems, into its own virtual machine, and then consolidating those on a single platform and hardware architecture.

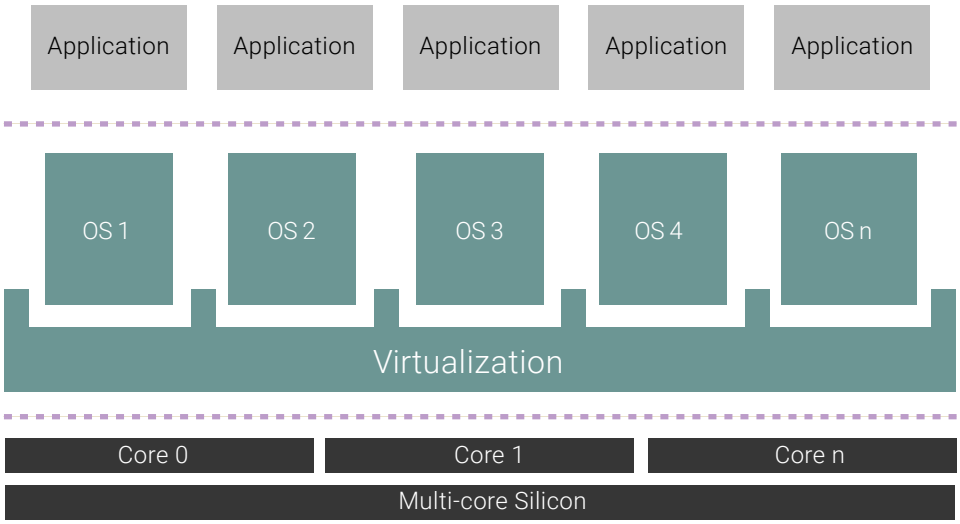


Figure 2. Reference architecture for multiple embedded systems running on a single processor using virtualization

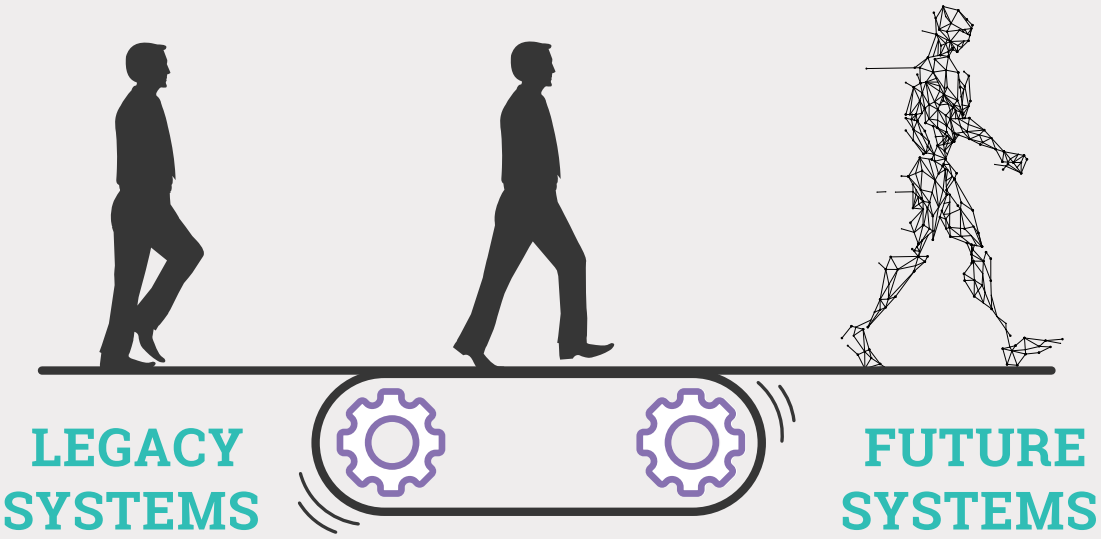
As depicted in Figure 2, virtualization can place multiple embedded systems, each running its own OS, on one piece of multi-core silicon hardware. Advances in silicon design, processing power, and virtualization technology make this possible. The same silicon can host more than one version of Linux, along with multiple RTOSes and other common legacy operating systems.

Virtualization abstracts the embedded system application and its OS from the underlying hardware. As a result of this innovation, it becomes possible to overcome many of the most serious challenges arising from legacy embedded systems.

Engineers gain:

- A significant increase in scalability and extensibility
- Support for open frameworks and reuse of IP across devices
- The ability to build solutions on open, standardized hardware that offers more powerful processing capabilities
- Simplification of design and accompanying acceleration in time-to-market
- Application consolidation within the device, which reduces the hardware footprint and costs related to the bill of materials (BOM) that comes with the development of a piece of hardware
- A gradual learning curve, using the OS and programming languages they are are comfortable with, deployed in a virtualized system
- The ability to run multiple operating systems and applications side by side
- Isolation of each operating system and application instance, providing additional security and allowing both safety-certified operating environments and “unsafe” applications
- Easier upgrades via new methodologies such as DevOps, which simplifies the quick extension of new features
- Faster response to security threats

VIRTUALIZATION BRIDGES LEGACY AND FUTURE SYSTEMS



- Closed
- Purpose-built
- Aging, requiring maintenance
- Isolated
- Component certified

- Open, safe, secure
- Software defined, flexible
- Intelligent
- Connected
- System certified

Helix Platform brings your legacy systems into the software-defined era of increased flexibility, code reuse, certifiability, and security.

WIND RIVER HELIX VIRTUALIZATION PLATFORM

To realize the potential of virtualization in embedded systems, Wind River has developed Helix Platform. As shown in Figure 3, Helix Platform supports operating systems as varied as VxWorks, Wind River Linux, Microsoft® Windows®, Android, and other guest operating systems, including unmodified bring-your-own (BYO) guests. Hardware decoupling lets any mix of operating systems run on either Intel® or Arm® architectures. The Helix Platform Type 1 hypervisor operates at the level of the processor cores, facilitating the smooth, safe, and concurrent operation of each application.

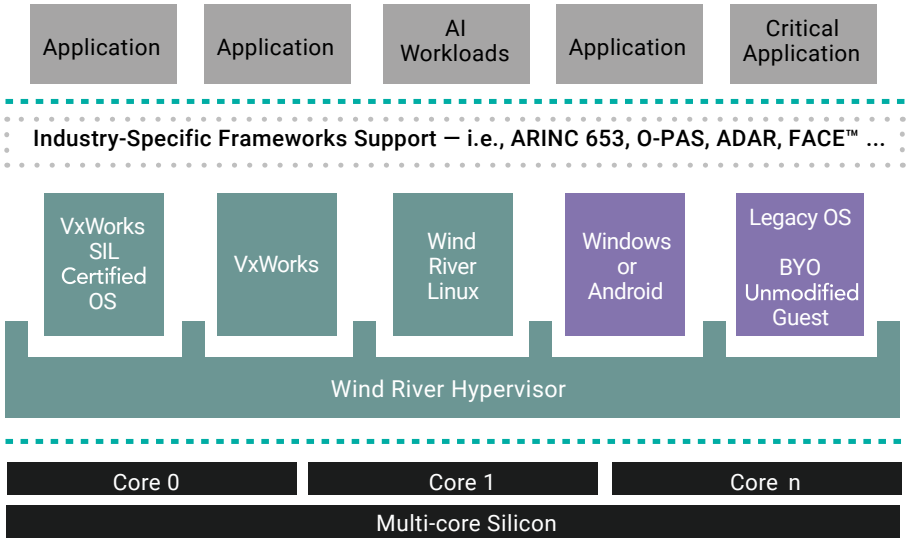


Figure 3. Reference architecture for the Helix Platform Type 1 hypervisor, which enables multiple embedded systems to run on a single piece of silicon

Helix Platform supports many different industry frameworks, such as ARINC 653 software specification for RTOS space and time partitioning in safety-critical avionics, O-PAS industrial automation standards, and ADAR for automotive. Helix Platform is also easily certifiable for DO-178C airborne system safety, IEC 61508 industrial functional safety, and ISO 26262 automotive safety.

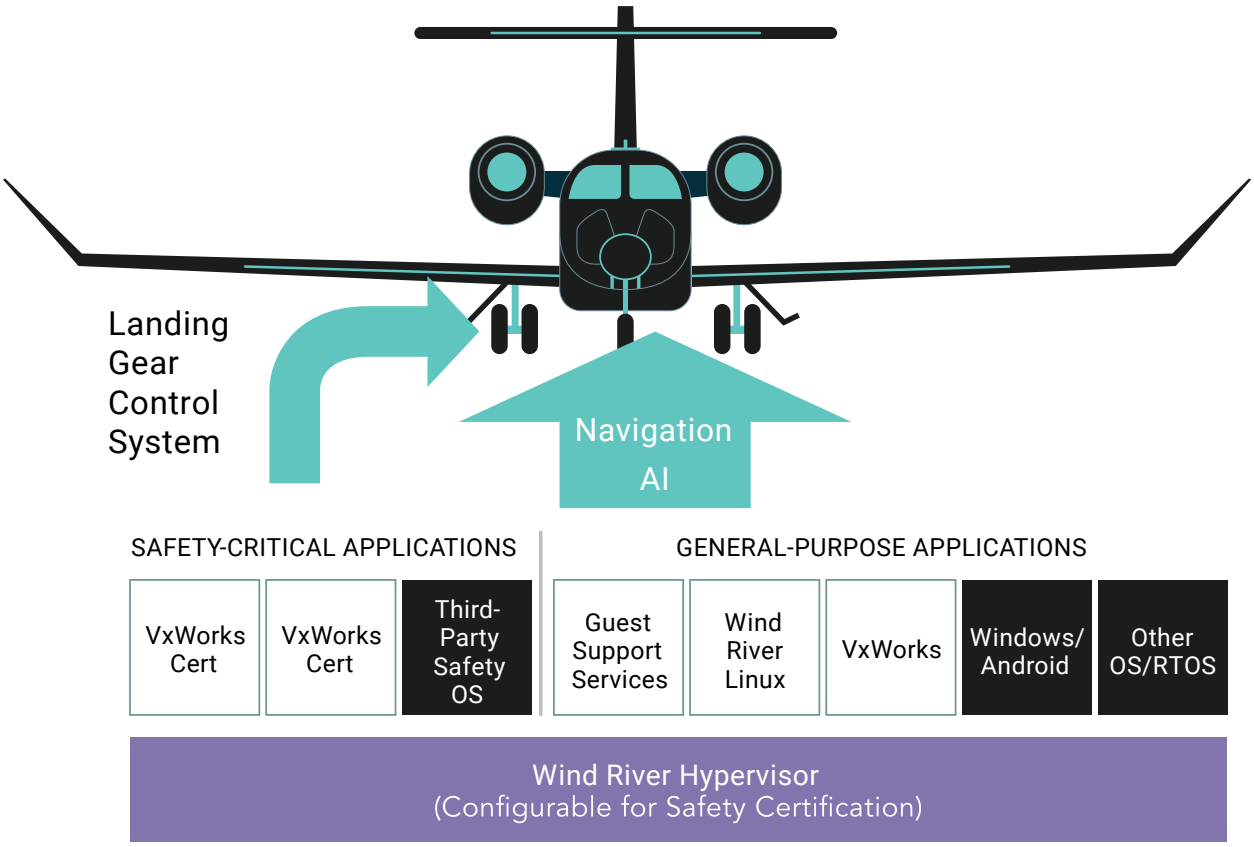


Figure 4. Helix Platform enables static, locked, or dynamic flexible configurations to run simultaneously on the same hardware

For example, Figure 4 depicts how an aircraft can use Helix Platform to run a combination of safety-critical applications for RTOS-based systems and other general-purpose applications, such as a user interface, but it can also run AI and machine learning apps.

The singular Helix Platform architecture would generally be considered more secure than the alternative of running each embedded system independently. More systems mean more surface area is exposed to potential attack. Cybersecurity best practices suggest that multiple endpoints are harder to protect than a single endpoint. It's easier and more secure to apply a security policy such as zero trust on a single hypervisor than it would be to apply it to multiple embedded systems on multiple devices.

It's also theoretically easier to test for vulnerabilities. In the example shown in Figure 3, a security tester would only have to test one path from the hypervisor to the internet, rather than five. And, given that deficient patch management practices are a known source of cyber risk exposure,[1] it's far more secure to have a single hypervisor to patch rather than an assortment of (potentially unpatchable) legacy systems. This assumes isolation of the embedded systems, which Helix Platform provides.

Robust partitioning within Helix Platform restricts access to critical embedded system elements. If a malicious actor, bad call error, or problematic application can penetrate one embedded system, then he, she, or it cannot easily attack any of the others on the platform. This is a core countermeasure in most cybersecurity frameworks. The platform also controls resource allocation, which protects the integrity of the system.

1. *Roger A. Grimes, "Zero-Days Aren't the Problem – Patches Are," CSO Online, June 1, 2016*

A BRIDGE TO FUTURE APPLICATIONS

Of course, the journey from legacy systems to the future never happens overnight. Helix Platform can serve as a critical bridge that enables developers to deploy existing applications (and their relevant certifications) until end-of-life alongside new applications. This mixture of new and legacy applications can also run on a mixture of new and old operating systems.

Think about an avionics controller. It must run on an RTOS for safety and certification reasons, but it may also connect with a Linux-based artificial intelligence (AI)-driven route optimization solution. This solution is itself part of a larger flight management system. The whole system is subject to rapid product release cycles and rigorous cybersecurity requirements. Helix Platform provides the combined stability and flexibility you need to run legacy and newly emerging applications on a single hardware-independent platform.

Helix Platform can bridge your investment in legacy applications to a software-defined future.

FINANCIAL PAYBACK FROM THE VIRTUALIZATION OF EMBEDDED SYSTEMS

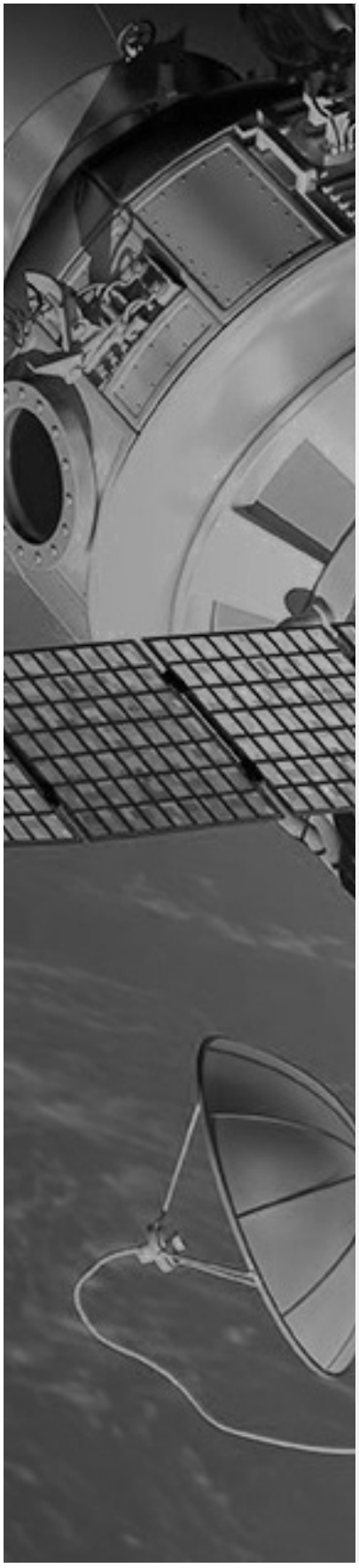
Makers of devices and solutions that rely on embedded systems should be able to see a return on investment (ROI) from the move to virtualization. From a CapEx perspective, Helix Platform reduces the need to acquire specialized hardware for development, testing, and production of embedded systems.

In terms of OpEx, virtualization drives ROI through savings in more than one cost category. Everything moves faster in the product development cycle, so there should be reductions in development spend. Testing and QA are similarly truncated, leading to savings in that area. The need to hire and retain developers with increasingly rare skill sets falls off with the hypervisor approach. Also, the notorious "long tail" of supporting earlier generations of embedded systems shrinks as application consolidation increases.

Revenue should also increase as a result of embedded system virtualization. The acceleration of the product development cycle will increase sales. Increased extensibility and integration can also lead to revenue growth. What might have been a standalone device can now easily become part of an expanded system, with more potential customers who want to buy it. Cuts in CapEx and OpEx, coupled with increased revenue, mean strong ROI for the virtualization of embedded systems.

Reuse of intellectual property (IP) also contributes to the ROI from virtualization. With a single platform that's forward-compatible with existing embedded system software, it becomes easier to repurpose existing code bases and guest operating systems for new embedded system innovations.

Helix Platform simplifies, secures, and future-proofs designs in the aerospace and defense market. These capabilities apply to both legacy and new applications, based on industry standards such as ARINC 653, POSIX®, or FACE™. Applications can run on operating systems such as Linux, VxWorks, and others.



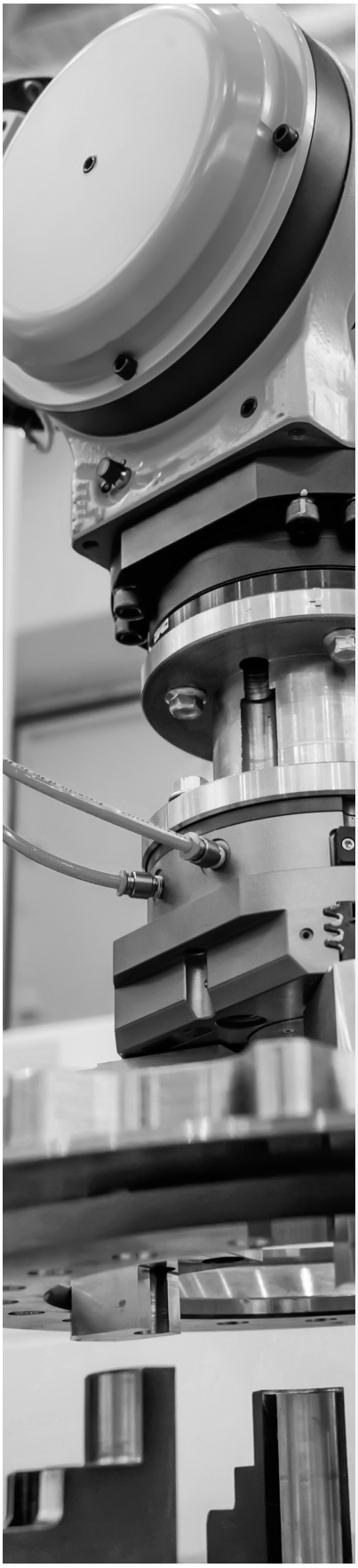
Aerospace and Defense Market

Wind River has proven market excellence in aerospace and defense. Helix Platform evolved from VxWorks, the market-leading RTOS from Wind River, leveraging a successful track record of more than 30 years of software innovation deployed in over 2 billion devices and more than 90 civilian and military aircraft. VxWorks is trusted by more than 9,000 companies. It was chosen as the RTOS to go to Mars with NASA for nearly 25 years. VxWorks supports C11 and C++17 programming language standards as well as standards-based virtualization of common devices, including serial, networking, and storage.

Automotive Market

Wind River worked with a manufacturer in the automotive market to build a secure gateway that connects multiple components of an advanced driver assist system (ADAS). ADAS is designed to help drivers increase road safety. The challenge, in this case, was to deliver a single box/gateway that would consolidate communications among the ADAS-related components. It had to have the functionality of up to three distinct control modules in one platform. The whole solution had to be certifiable according to ISO 26262 (the Automotive Safety Integrity Level, or ASIL), which is the industry standard certification for computerized components of cars.

Helix Platform enabled the manufacturer to consolidate the communication controls, security, and device management. Thus the main engineering goal was met, with faster software development delivery for all components. From a revenue perspective, Helix Platform gave the manufacturer a common solution to target to multiple auto manufacturers.



Industrial Market

Makers of industrial systems are benefiting greatly from embedded system virtualization. They're putting the architecture to work in process automation, robotics safety systems, energy protection systems, monitoring solutions, and AI-driven industrial analytics solutions. Predictive maintenance is an example of the latter. Like other businesses, industrial system companies also want faster time-to-market and IP reuse. Virtualization serves these needs as well.

A maker of control systems approached Wind River with a project to expand the functionality in its next-generation control platform. The challenge was to reuse as much of the existing code base as possible, avoiding the costs of recoding what the developers knew already worked. And, of course, the maker wanted to maintain safety certification.

Helix Platform solved the problem by standardizing the control platform's legacy operating systems (which included roll-your-own Linux) on a software platform. This way, the development team could evolve an expanded portfolio of products at a reduced cost compared to earlier generations. Helix Platform gave the team the ability to produce the new-generation system with full Safety Integrity Level (SIL) 3 certification, which included the hypervisor.

Medical Market

In the medical market, hosting multiple embedded systems on Helix Platform enables medical device manufacturers to consolidate applications while meeting the industry's high standards for safety, security, reliability, and certification. Examples include CAT scanners, MRI machines, X-ray machines, pacemakers, precision surgical systems, surgical robots, and infusion pumps.

A piece of medical equipment may house more than one embedded system. An MRI machine, for example, could easily have separate embedded systems for its diagnostic electronics, the motors that move the internal parts, the magnetic charging components, and more. Being able to consolidate these embedded systems on one piece of hardware — and run them on a flexible, software-defined basis — gives the device maker much more agility while also streamlining the certification process. Helix Platform also simplifies connections with electronic health records (EHR) and cloud-based medical data storage repositories.

CONCLUSION

The days of building closed, purpose-built products are coming to an end. The practice is simply too slow and expensive. What's more, it strips the resulting systems of the much-needed extensibility and integration capabilities that are expected in the modern world of embedded devices.

Helix Platform offers a solution. Designed to address a host of demanding security, safety, reliability, and certification requirements, it presents a single platform that will form a bridge to the future of embedded systems. It's one virtualization platform that runs on the leading hardware architectures and reduces certification challenges for the aerospace and defense, automotive, industrial, and medical markets.

Helix Platform makes it possible for embedded system makers to avoid the legacy-support trap. In just about all industries, it drives ROI through faster time-to-market and IP reuse, along with reductions in CapEx and OpEx. Helix Platform provides a way forward for embedded systems developers who need to evolve with the times, while preserving their legacy investments.

ABOUT WIND RIVER

Wind River is a global leader in delivering software for mission-critical intelligent systems. For 40 years, the company has been an innovator and pioneer, powering billions of devices and systems that require the highest levels of security, safety, and reliability. Wind River software and expertise are accelerating digital transformation of critical infrastructure systems, including automotive, aerospace, defense, industrial, medical, and telecommunications. The company offers a comprehensive portfolio supported by world-class global professional services and support and a broad partner ecosystem.

90+
Civilian and military aircraft

2B+
Deployed devices in critical infrastructure

50+
Space deployments

20+
Years' experience in safety certification software products

350+
Customers on safety platforms

560+
Safety certification programs

PROVEN, TESTED, DEPLOYED

WHEN CUSTOMERS NEED IT TO WORK AND WORK RIGHT,

THEY CHOOSE WIND RIVER.

EMERSON · SIEMENS · IAI · Rockwell Automation

Schneider Electric · Collins Aerospace · MAGNETI MARELLI · TOSHIBA Leading Innovation

OLYMPUS Your Vision, Our Future · KUKA

Wind River virtualization technology allows us to drive time-to-market [and] get newer and faster hardware solutions out, while reusing a lot of that same investment that we put into our software development.

Scot Tutkovics, Vice President of Engineering, Rockwell Automation