WIND™

The RTOS as the Engine Powering IoT Critical Infrastructure

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Digital transformation offers industrial manufacturers the promise of business advantages and efficiencies through the use of data analytics and advanced control systems. To retain their market position and stay ahead of agile competitors, enterprises are embracing the era of Industrial IoT and investing in new capabilities. But realizing this vision of digital transformation is complex, with many challenges along the path to success. Adding network connectivity to your existing systems introduces more opportunity for cybersecurity threats, while opting to isolate your systems for safety and security reasons can mean missing out on some of the key benefits of IoT.

This paper examines how companies can establish a digital transformation strategy, realizing business value by creating data-enabled intelligent systems that are protected from cybersecurity threats while reducing total IoT critical infrastructure lifecycle cost and risk. We will look at the use of virtualization to consolidate core safety-certified applications and non-safe applications, separate IoT communications from legacy applications, and enable huge benefits in the use of advanced technologies to implement IoT capabilities. Finally, we will examine how virtualization can maximize product safety, using various types of partitioning in IoT design that lead to reductions in overall design cost and risk.

See how VxWorks® has evolved to be the real-time operating system (RTOS) for IoT, providing the reliability, safety, and security capabilities to successfully power IoT critical infrastructure systems into the future.

TABLE OF CONTENTS

As the ARC Advisory Group states, "The risk of being a late adopter now exceeds the risk of being an early adopter."

THE OPPORTUNITY

Across many industries, one common theme is digital business transformation. The rationale for implementing digital transformation is that it will lead to business goals of improved operations, profits, and competitiveness. A Tata Consultancy Services (TCS) 2015 report looking at the impact of IoT technologies, based on a survey of 795 executives from large multinational corporations who already had implemented IoT technologies or solutions, found that 19% of respondents from industrial manufacturing were already seeing more than 30% in revenue gains. Other key findings:

- In 2014, the average increase in revenue as a result of their IoT investment was 15.6%.
- Almost 1 in 10 (9%) saw a rise of at least 30% in revenue.
- The top 8% of respondents, based on ROI from IoT, reported a staggering 64% average revenue gain in 2014 as a direct result of these investments.

In the TCS 2015 survey looking at the impact of IoT technologies, executives in the industrial manufacturing sector are reporting the largest increase in revenue from IoT investments, with an average 28.5% ROI.

Let's take a look at three key areas of digital transformation enabled by IoT: new approaches to business strategy; increased efficiency, safety, and resource sustainability; and consideration of product lifecycles.

New Approaches to Business Strategy

As you investigate new and improved revenue streams, look to maximize your customers' experience by changing your strategy from a product-centric approach to a services approach. The idea is to ensure that you are resilient against digital competition and disruptive new competitors, while providing valuable services to your customers.

Increased Efficiency, Safety, and Resource Sustainability

The need to increase efficiency requires you to look at how you can continuously improve manufacturing processes and reduce energy and other resource usage, while at the same time ensuring safe manufacturing processes.

Consideration of Product Lifecycles

IoT is driving digital transformation by providing connected intelligent devices. For your company to be successful in connecting to the IoT, key decision makers like you must do more than recognize the general opportunity that is inherent in the digital transformation trend. You need to identify specific products, services, and business models that can drive "profitable outcomes"—for example, improving your customer engagement and experience, product or technology innovation, or business or product efficiency; or transforming your business entirely.

Part of this process is to determine what data must be gathered to drive these outcomes and enable better business decisions. In other words, the data being generated and the purposes it serves must add value to both you and your customers. Solutions that are simply intriguing without justifying their cost to your customers will not provide you long-term market traction, and implementations that are not profitable will not drive business success. Likewise, you need to look at how possible solutions fit into your overall company IoT strategy, and charting your IoT course requires defining offerings that are a suitable fit within the rest of your business.

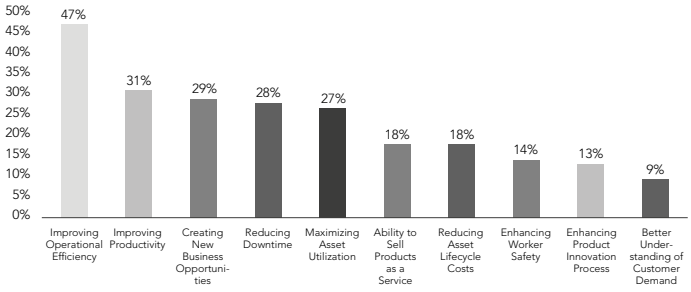
Until this point, the discussion has focused on designing new critical infrastructure systems and services to fulfill a business need. But sometimes you need consider how to migrate and manage your legacy critical infrastructure systems to connect to the IoT, since these systems may not have been designed for the IoT era due to their traditionally long product lifecycle. And it is just too expensive to build from scratch an entirely new IoT critical infrastructure system. As Table 1 shows, businesses planning to connect to IoT must consider the longer lifecycles for critical infrastructure, future system obsolescence, and the ability to periodically update both the software application and the underlying hardware platforms.

Table 1. Typical lifecycle of devices

Device	Typical Lifecycle (Years)
Smartphone	<2 years
Mission/Avionics platform	3–5 years
Auto/Car	8–10 years
Programmable logic controller (PLC)	10–15 years
Train	30–50 years
Aircraft	40–50 years

THE BUSINESS DRIVERS

Improving operational efficiency and productivity are the most critical business drivers among manufacturers moving into the IoT. In order to implement systems that fulfill these requirements and provide positive business outcomes, you need data-enabled intelligent systems that are protected from cybersecurity threats and are more affordable.

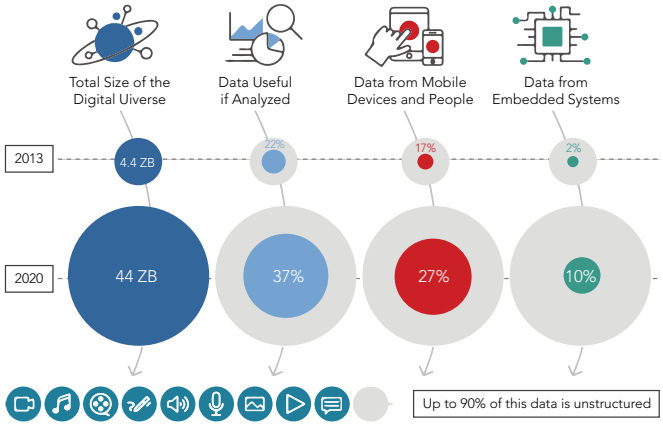


Sources: Morgan Stanley – Automation World Industrial Automation Survey, AlphaWise

Figure 1. Benefits of IIoT: Industrial Internet of Things drivers

Data-Enabled Intelligent Systems

Your ultimate goal is to have all systems connected to the overall IoT environment, so that you can make business decisions based on the big-picture analysis of that data. Although this sounds simple, it is usually slower to implement than originally predicted,[1] and there are other consequences that you need to consider as well. First, the data volume involved is substantial, so it is useful to do some preprocessing of data before the transition. This allows you to choose which data to transmit and preformat if needed. Second, you are now connecting systems to the network, and that exposes you to cybersecurity threats.



Source: EMC Digital Universe with research and analysis by IDC, "The digital universe of opportunities: Rich data and the increasing value of the Internet of Things," April 2014; International Data Corporation, "IDC iView: Extracting value from chaos," 2011.
www.emc.com/collateral/analyst/idc-extracting-value-from-chaos-ar.pdf, accessed December 29, 2016.

Deloitte University Press | dupress.deloitte.com

Figure 2. The expanding digital universe, 2013–2020

As our goal is to collect data from all systems, those that have a functional safety requirement are included. These systems control machines that could cause injury or death in the event of a software or hardware failure. In these cases, government regulations mandate certain requirements. A good example of these can be found in IEC 61508, which defines "functional safety of electrical/electronic/programmable electronic safety-related systems." Any additional code added to these systems to data-enable them could be costly due to the test and validation requirements of these regulations.

> Functional safety is the part of overall safety that depends on a system or equipment operating correctly in response to its inputs. It includes the detection of a potentially dangerous condition, resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or to provide mitigation to reduce the consequence of the hazardous event.

Protection from Cybersecurity Threats

Given the goals of digital transformation, you know your organization will use data to make business decisions, so any impact on the validity of that data could lead to unwanted circumstances. Data becomes the most important part of your system and so must be protected from cyberattacks, as with any other asset. This leads to the second requirement: cybersecurity.

Connecting devices to the Internet, or to systems that connect to the Internet, will expose them to threats and vulnerabilities that they originally were not designed to cope with. However, cybersecurity is now vital throughout the life of the system, and therefore mechanisms should be provided to address cybersecurity throughout the life of the device, including remote monitoring and updates for already-deployed devices.

Greater Affordability

Managing costs for software development projects has always been challenging, mainly because the capability or feature required tends to expand during the development process. For IoT systems, this challenge expands to include devices that have been out in the field for many years. This is because your goal is to generate revenue from these devices through a service-based model, so you must consider lifecycle costs, including how to diagnose, fix, and update their software.

This drives new technologies and software architecture changes to allow for these updates and to maintain security protection. Typically, embedded systems are developed for a single purpose: to control a machine, for example, or operate a safety feature. Often this is handled by a single block of code, fully integrated into the system's hardware. This can be difficult to maintain, update, and enhance with new capabilities without a complete rewrite of the software.

Given the need to improve efficiencies, there is a trend toward consolidation of these systems onto a single, more powerful platform—running a virtual machine to host "applications." These platforms support use of virtualization and multi-core processors to provide flexible, high-performance systems that can lower lifecycle costs and improve operational expenses by allowing easy maintenance, updating, and management of software applications.

The data collected and analyzed can also change throughout the device lifecycle (this often occurs following analysis of the overall system data), requiring additional data to be collected or requiring the frequency of collection to change. This depends on the ability to rapidly adapt or expand existing applications, through adaptable applications or update services. These advanced services and updates can also be used to maintain device security.

Virtualization of safety functions also allows a consolidation strategy to isolate them from the connectivity and control of IoT. This means you can maintain functional safety aspects while simultaneously providing the back-office connectivity needed to fulfill your IoT requirements.

SOLUTIONS FOR IMPLEMENTING IOT SYSTEMS

In order to solve these challenging requirements, businesses need to consider new approaches to system level architecture and use the latest technology. Systems must not only meet the data-enabled intelligent systems requirement for IoT but also provide reduced lifecycle costs, while remaining safe and secure. Add in the existing requirements of scalability and modularity to cover the broad range of devices and sensors needed across systems—as well as the continuing need for absolute reliability—and the need for a new approach is clear.

VxWorks supports the broadest spectrum of 32-bit, 64-bit, and multi-core processors, including Arm®, Intel®, and Power® architectures. Its portfolio of additional middleware and advanced technology components, as well as a large ecosystem of validated complementary third-party hardware and software solutions, enables you to differentiate your platforms with best-of-breed capabilities, and provide systems that can meet the demands of the Internet of Things.

The Foundation of Data-Enabled Intelligent Systems

The operating system is the foundation for enabling intelligent systems and has to provide real-time performance because it is controlling expensive, long lifecycle equipment (often with human life dependencies) and cannot afford to miss any deadlines. VxWorks is a fully deterministic real-time operating system that has been deployed in the industry controlling embedded systems for nearly 40 years.

To provide value, you need connectivity to ensure that the data from such systems is transmitted reliably over a variety of protocols to where it's needed. With VxWorks, right out of the box you have the support of industry-leading connectivity standards and networking protocols such as CAN and Ethernet, the MQTT IoT connectivity middleware protocol, and high-performance networking capabilities such as Precision Time Protocol (PTP) and Time-Sensitive Networking (TSN). Through the vast VxWorks partner ecosystem, you can add additional protocols such as Bluetooth,

NASA MARS EXPLORATION ROVERS

Figure 3. NASA's Mars Science Laboratory rover Curiosity running Wind River VxWorks RTOS

Launched: 2003

Original mission: 90 days

Current status:

- Still returning scientific data in 2019
- Holds the record for the longest distance driven by any off-Earth wheeled vehicle

Interesting facts:

- Featured in the 2011 science fiction novel The Martian by Andrew Weir and in the film adaptation directed by Ridley Scott and starring Matt Damon, released in October 2015
- One of seven Wind River Mars missions with NASA/JPL, which most recently landed the InSight lander safely on Mars in November 2018
- For more information about Wind River in space, visit Over 20 Years in Space

Features:

- Running the VxWorks RTOS
- Remote operations
- Data collection
- Communications
- Software updates

ZigBee, Wi-Fi, DDS, and CoAP, among others. The modular nature of VxWorks also allows you to add connectivity and networking capabilities after the fact, so you can bring many previously disconnected devices online without reworking the core of your embedded software.

Compatible Software and Hardware Ecosystem

In addition to delivering rock-solid real-time performance and other cutting-edge features, an RTOS for IoT must support a broad ecosystem of tested and verified complementary hardware and software solutions. This broad feature set delivered by VxWorks and its ecosystem of compatible third-party applications is essential to enabling you to create a differentiated product offering and secure a sustainable competitive advantage. VxWorks delivers the most exhaustive library of off-the-shelf board support packages, allowing you to begin development immediately, with your project leveraging significant COTS technology. This means you can focus on differentiating your product offering with leading-edge features and capabilities, accelerate your time-to-market through rapid, lower-risk integration using best-in-class third-party technology, and cut costs by deploying systems integrated and validated out of the box.

The edge devices in IoT are also likely to be very small scale, due to cost and power constraints. But these devices still require the security and connectivity offered by VxWorks in order to satisfy IoT requirements.

Cybersecurity Protection

As described, data-enabled intelligent systems must be designed, built, and deployed with security in mind, as pervasive IoT connectivity exposes them to increasingly numerous and complex threats. The software platform for IoT provides the flexibility to design embedded systems to the necessary level of security by leveraging a comprehensive set of built-in features covering all areas where IoT data is touched:

- Design
- Boot
- Data in use
- Data in transit
- Data at rest

Table 2. VxWorks RTOS IoT security

Design	Boot	Data in Use	Data in Transit	Data at Rest
• Secure development processes • Signed binary delivery • IEC 62443 • IEC 27034	• Secure boot/load • Measured boot/load • Signed binary application authentication • Digital certificates/PKI • Remote attestation	• Secure partitioning • Cryptography • User authentication and management • Auditing and logging	• Network security • SSL/SSH • IPsec/IKE • Firewall	• Encrypted storage • Sanitization

VxWorks supports these security features not only to protect against malware and unwanted or rogue applications but also to deliver secure data storage, data transmission, and tamper-proof designs. OS-level support for these features is critical, since adding them at the user or application level is ineffective, expensive, and risky. Security threats and vulnerabilities evolve and become more complex over time. VxWorks adapts to this complex threat scenario and supports the secure upgrade, download, and authentication of applications to help keep your devices secure throughout their lifecycle.

Creating More Affordable Systems

Over the years, VxWorks has driven many systems that have a long lifecycle, usually in fixed static roles, running single functions or driving single devices. In an IoT environment, you need to be able to update and manage these systems as well as support your legacy applications already deployed. A gateway can act as an interface between legacy and IoT systems, protecting the earlier investment; or you can consider a partial migration through the use of virtualization technology and new multi-core processors.

Virtualization allows creation of virtual machines that can efficiently isolate and duplicate the computing requirements of legacy and new applications. This can support migration of legacy applications and also future-proof your platform by providing the ability to upgrade applications. This capability provides a method of isolating applications, which enables the following:

- Support for legacy applications
- Isolation of functional safety code
- Isolation of data for security
- Application sandbox for future capabilities

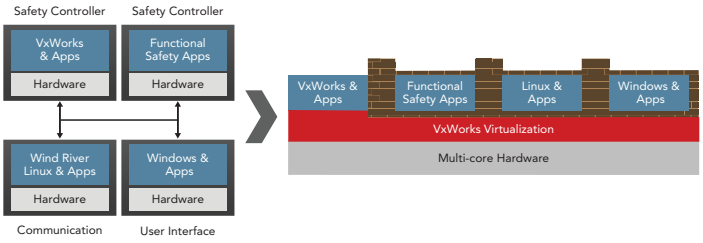


Figure 4. Migrating your legacy system to IoT securely with virtualization

When combined with modern multi-core processors, this capability also provides the performance necessary to run both new capabilities and legacy applications, without loss of performance.

ADVANCED REAL-TIME CAPABILITIES

In the previous section, we discussed how VxWorks can help satisfy the basic requirements of IoT systems, meeting the demands of digital transformation to provide business value. But is this enough? You need to consider that these devices will be deployed in the field for many years, and requirements could change. To help with your IoT needs going forward, VxWorks provides advanced real-time capabilities that can help future-proof your designs.

Safety While Enabling Connectivity to the IoT

Safety is paramount in many embedded operating systems, because they control machines that can endanger life, or whose malfunction can cause injury or death. Although well established in aerospace, medical, and industrial markets, regulators are now applying safety standards to new markets, such as the automobile and energy industries. Additionally, better applications of existing standards are being sought for such systems as smart grid meters and medical devices. As standards evolve, manufacturers increasingly look to Wind River to deliver the appropriate capabilities to more easily obtain required safety and security certifications for their end products.

Of course, these safety features and requirements also have to be evaluated against the required benefits of IoT, and against increased security threats. Safety must remain the highest-priority requirement, as these systems could endanger human lives.

For manufacturers of industrial control and automation systems that require IEC 61508 functional safety certification, auto manufacturers that require ISO 26262 ASIL D hazard and risk assessment, or avionics manufacturers that require DO-178C DAL A safety certification, VxWorks Cert Edition and its optional certification evidence packages deliver a rich real-time operating environment that enables flexible system design options and reduces cost, risk, and lead time for full system certification.

Multi-core

As embedded systems grow in complexity and capability, and as the need increases for cost-reducing consolidation, multi-core processors are becoming the platform of choice. VxWorks delivers comprehensive multi-core processor support, including asymmetric multiprocessing (AMP) and symmetric multiprocessing (SMP) OS configurations and hardware-optimized multi-core acceleration.

The VxWorks 653 Multi-core Edition COTS platform enables even greater flexibility in harnessing the power of multi-core, as well as additional consolidation options to reduce size, weight, and power (SWaP) consumption.

64-bit Processing

Many embedded systems today have already reached the limitations of 32-bit processors, especially when implementing a strategy of consolidation using virtualization, and so the 64-bit processor era is emerging. VxWorks supports the broadest spectrum of 64-bit and multi-core silicon architectures, including Arm, Power, and Intel architectures.

CONCLUSION

Digital transformation and the Internet of Things require you to build data-enabled intelligent systems, but also to provide reduced lifecycle cost and risk while retaining safety and security. Reliability, scalability, and modularity are also vital for an IoT RTOS to cover the broad range of devices and sensors that you require across your IoT systems.

The VxWorks RTOS product family supports the broadest spectrum of processors. Its portfolio of additional middleware and advanced technology components, as well as a large ecosystem of validated complementary third-party hardware and software solutions, enables you to differentiate your platforms with best-of-breed capabilities and provide systems that meet the demands of the Internet of Things.The RTOS of the future is here now: VxWorks gives you, as a manufacturer of embedded systems, a competitive edge in the world of IoT by enabling you to bring industry-leading devices to market faster, while reducing development and maintenance costs and project risk.

REFERENCE

1. www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things

SOURCES

1. ARC Advisory Group, www.arcweb.com/advisory-services/industrial-iot-and-digital-transformation.
2. Tata Consultancy Services (TCS), www.tcs.com/iot-tcs-global trend-study-2015.
3. Wind River Going Green, www.windriver.com/announces/greener-with-wind-river.
4. McKinsey, Benefits of IIoT—The Industrial Internet of Things Drivers, www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things.
5. Unlocking the Potential of the Internet of Things, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.
6. EMC Digital Universe with Research and Analysis by IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, April 2014, www.emc.com/leadership/digital-universe/2014iview/index.htm.
7. Over 20 Years in Space, www.windriver.com/inspace.

WIND

Wind River is a global leader in delivering software for IoT. Its technology is found in more than 2 billion devices and is backed by world-class professional services and customer support. Wind River is accelerating digital transformation of critical infrastructure systems that demand the highest levels of safety, security, performance, and reliability.