MASTERING THE CHALLENGES OF THE
INTERNET OF THINGS

A Holistic Approach to Addressing the System-Level Requirements of IoT
EXECUTIVE SUMMARY

The Internet of Things (IoT) has begun to deliver on its promise of bringing revolutionary benefits to businesses and society. It now represents a watershed opportunity for the makers of embedded software products that are building IoT to its full potential.

But creating the infrastructure for IoT also comes with challenges. To tap into this multi-trillion dollar market, embedded device and systems manufacturers need to update their thinking about how they create their products, moving toward a more holistic design approach that accounts for the intrinsic demands of IoT.

TABLE OF CONTENTS

Executive Summary ............................................................... 2
Vision and Reality in IoT ..................................................... 3
Bridging from the Past ......................................................... 3
What It Takes: The Key Capabilities Required Today .................... 3
  Ensuring Security ............................................................. 3
  Achieving End-to-End Integration ........................................ 4
  Managing Lifecycles ......................................................... 4
  Driving System Intelligence ............................................... 4
Toward a Holistic Approach ................................................ 4
  Moving Embedded Development to the Cloud ....................... 5
Conclusion ................................................................. 5
VISION AND REALITY IN IOT

By now, the promise of IoT is becoming a reality for many businesses and consumers.

Industrial enterprises are seeing enormous productivity gains through smarter automation of factories. Managers are gaining more operational insight based on data generated by connected machines. Engineers are remotely monitoring equipment in the field. Ubiquitous sensors are helping building owners reduce energy consumption. And intelligent vehicles with driver assistance systems are saving lives.

IoT, however, is not only improving how things work, it is also driving the creation of entirely new business models.

Product companies are now leveraging data from their equipment to roll out new services. Healthcare providers are moving medical services out of hospitals and into homes. And auto insurance companies are personalizing coverage based on individual driver behavior.

All these changes are just the beginning of the transformation that IoT is bringing to businesses and society. At the heart of this transformation sits embedded software. It serves as the operating system and intelligence for the sensors, devices, and systems that form the connection between the physical and digital worlds.

But creating devices, systems, and applications for IoT brings a new set of performance and design challenges related to security, integration, lifecycle management, and system-based intelligence.

Engineers and software developers need to address these challenges early in the planning and design stage in order to create products that best support the unique requirements of IoT.

No single technology can address all of these needs, nor can any one challenge be addressed in isolation from the others. Building secure and reliable IoT systems and devices requires a holistic approach, taking into account all the elements in play in such a complex system-of-systems that reaches from the edge of the physical world into the enterprise and back again.

BRIDGING FROM THE PAST

Traditionally, embedded devices have had very different requirements from the devices that now make up the IoT world:

- **Isolated:** Security for pre-IoT embedded devices was not designed with the Internet in mind, relying on the controlled environments and isolated nature of most systems to limit threats.
- **Proprietary:** For the most part, devices running embedded software were built for proprietary, closed-loop systems without any native ability to connect with the Internet.
- **Fixed-function:** Traditional embedded devices were mostly designed for a single, fixed-function task, with extremely limited processing capacity or other capabilities to interact with diverse systems or networks.
- **One-way:** To the extent that devices provided data to upstream systems, it was typically via a one-way channel with little capability for dynamic networking communications.

In contrast, IoT presents a new set of requirements:

- **Comprehensive security:** Intrinsically, IoT requires embedded devices to connect to larger, IP-based IoT networks, creating far greater security exposure and demanding integrated, layered, coordinated security at device, network, and system levels.
- **Flexible connectivity:** Developers must design software for networked connections and interoperability, both planned and unplanned—not only for the application’s known connectivity needs, but also for any that may arise in the future.
- **Open interoperability:** Almost any IoT embedded device or system will need to be able to work with a diverse set of systems and networks, requiring support for a common standard or set of standards beyond its specific task.
- **Round-trip communications:** For an IoT application to be effective, the flow of data must be two-way. Edge devices, for example, need to transmit data to a cloud-based controller that analyzes the data and sends instructions back to the devices.

WHAT IT TAKES: THE KEY CAPABILITIES REQUIRED TODAY

While an IoT system or application is uniquely designed to meet a specific business or operational requirement, embedded software organizations need to consider each of the foundational capabilities required by IoT.

In addition, businesses often have a substantial investment in existing infrastructure and may be resistant to new IoT concepts if they require a “rip and replace” investment. Developers need to find ways to help enterprise customers protect their investment while building key IoT capabilities into their existing brownfield or their new greenfield systems.

**Ensuring Security**

Security is the cornerstone of the IoT infrastructure. Clouds and enterprise systems need to be able to trust the data they are
receiving from devices on the edge of the network. And devices need to be secured from hackers looking to steal information or hijack system controls.

Measures to detect and prevent unauthorized intrusions or malicious code should be built in at the design stage and at every level, from the device to the gateway to the cloud. Specific capabilities to consider include:

- Secure boot
- Provisioning for access control and device authentication
- Application whitelisting
- Secure partitioning
- Firewalls and intrusion prevention systems
- End-of-life management for taking compromised devices offline

Addressing security issues earlier in the solution lifecycle is more cost effective; once a solution is in the field, deficiencies may be difficult or impossible to correct.

The challenge is identifying just the right level of security for the application's business requirements. It must be robust enough to address all foreseeable threats and sufficiently flexible to respond to emerging ones, yet open enough to allow for integration and interoperability with other systems.

Achieving End-to-End Integration

In a typical IoT topology or structure, data flows across a number of elements:

- Sensors and actuators that control edge devices
- Edge devices that perform specific tasks and generate data
- Networks that connect the devices
- Gateways that connect the network to the cloud
- Cloud platforms that collect the data from the devices and manage the system

The more easily these elements integrate with each other, the less time developers have to spend resolving integration issues. Ease of integration is also key to building scalability and flexibility into the system by allowing for customization and the introduction of additional connectivity.

Managing Lifecycles

The initial design of an IoT system must take into account the anticipated operating life of the system or devices. Equipment in industrial and enterprise applications will be expected to last and perform for years or even decades. The system will require constant updating, both to avoid performance degradation and to take advantage of software improvements that will bring greater processing speed, capacity, and efficiency. Developers need to build in the ability to do the following:

- Provision and upgrade devices remotely, often thousands at a time
- Change network configurations without affecting devices in the field
- Customize devices and systems in the field
- Remotely debug devices before deploying applications
- Disable devices that are no longer needed, compromised, or malfunctioning

System simulation is a useful tool for lifecycle management. Developers can model various system scenarios at scale, both pre- and post-deployment, and anticipate risks that may occur at different points in the system lifecycle.

Driving System Intelligence

The value of an IoT solution lies not only in its ability to collect and aggregate data from edge devices, but also in its ability to make decisions and take action based on that data. Considering the enormous volume of device-generated data flowing through a system, and taking into account bandwidth constraints, this requires intelligence throughout the system to prevent data logjams. Specifically that means:

- At the cloud level: Big-data analytics and modeling to drive control strategies
- At the gateway level: Data aggregation and filtering capabilities to properly route data
- At the device level: The intelligence to identify the specific data to be transmitted to the cloud

TOWARD A HOLISTIC APPROACH

As noted earlier, addressing these challenges calls for a holistic approach. Understanding that these are common issues for IoT devices and systems, developers stand to benefit from building on a technology infrastructure in which these common capabilities are well supported. Without having to spend time and resources solving fundamental IoT issues, developers can focus on pioneering new applications and refining functions for specific tasks.

To that end, the Wind River® Helix™ portfolio of software, technologies, tools, and services is designed to help meet the system-level challenges of IoT. The components of Helix are designed to work together to provide an end-to-end, integrated solution for creating IoT infrastructure. With robust support for the
development, implementation, and management of IoT devices and systems, the Helix portfolio gives developers ready-made software platforms and tools to help them more quickly and easily design, build, and manage new products for IoT infrastructure.

Moving Embedded Development to the Cloud

To further extend the ability of Helix to help embedded software makers build for IoT, Wind River is introducing new tools for cloud-based development and management, allowing organizations far greater flexibility in where and how they build software for IoT devices and systems.

- **Wind River Helix Lab Cloud**: Provides instant, on-demand access to virtual hardware systems in the cloud for anywhere, anytime access to the development environment by any project member
- **Wind River Helix Device Cloud**: Makes it possible to connect IoT devices to a centralized console that controls, manages, and collects data from edge devices; Device Cloud can integrate with enterprise systems that utilize or analyze data from IoT networks
- **Wind River Helix App Cloud**: Provides a hosted development environment in which developers can create, debug, test, and deploy IoT applications, making it possible for teams of developers working in different locations to collaborate in a single space

CONCLUSION

The Internet of Things is no longer hype. It’s here, delivering benefits to businesses and society in the form of higher productivity, more efficient use of existing resources, and new revenue potential.

Realizing those benefits, however, requires recognizing and addressing the fundamental technical challenges to development and implementation. Working closely with application designers and system architects, Wind River is delivering the technology and expertise to support a holistic, end-to-end approach for creating IoT products, helping embedded software developers master the challenges and seize the opportunities in this new era of the digital age.