WIND™

AN INTEL COMPANY

THE INTERNET OF THINGS FOR DEFENSE

AGENTS OF CHANGE™

EXECUTIVE SUMMARY

The Internet of Things (IoT) is today's commercial effort to integrate a wide variety of technical and commercial information-generating components to provide new business opportunities based upon device and system intelligence. This technology is the large-scale commercialization of technology that has been developed and proven by the U.S. Department of Defense over the past fifteen years. In much the same way as NASA and the early space program in the 1960s spurred innovations in chip technology, automation, propulsion, and miniaturization that developed into innovative consumer products, solutions developed from the concept of network-centric warfare translate directly to the foundations of today's commercial IoT.

Given that IoT concepts originated in the defense sector, does the commercialization of IoT provide new opportunities for the defense sector? If so, how can vendors exploit them using commercial off-the-shelf (COTS) technologies from companies such as Wind River®? This paper will address these questions.

TABLE OF CONTENTS

NETWORK-CENTRIC CONCEPTS

Advanced situational awareness allows today's military commanders to make decisions based on real-time analysis generated by integrating information from unmanned sensors and reports from the field. These commanders benefit from a wide range of information supplied by sensors and cameras mounted on ground and manned or unmanned air vehicles—and on soldiers themselves. These devices survey the mission landscape and feed data to a forward base, some or all of which may be relayed to a command center, where it is analyzed and integrated with data from other sources to enable comprehensive battlefield situational awareness. Commanders then make decisions based on that data, which are delivered through the chain of command to be executed on the front lines.

The concept of network-centric warfare (Figure 1) transformed traditional approaches to military doctrine by (1) reversing the policy of expanded communication gateways, and (2) connecting battlefield assets back to HQ, sharing data between both legacy assets and new deployments to create a military advantage through force projection.

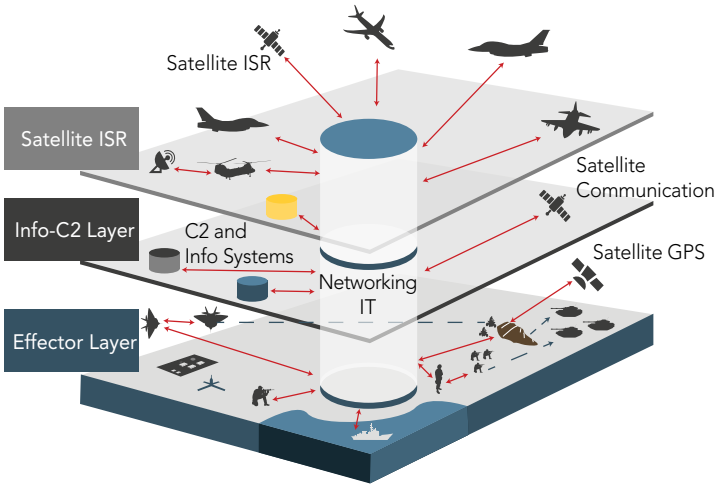

Figure 1: Network-centric warfare

Data and Decisions Drive the Value of IoT Information

This military scenario sets the stage for how today's commercial IoT works (Figure 2). Whether in critical infrastructure, industrial control, or consumer wearables, these IoT systems use similar data collection, distribution, feedback, and analytical technologies.

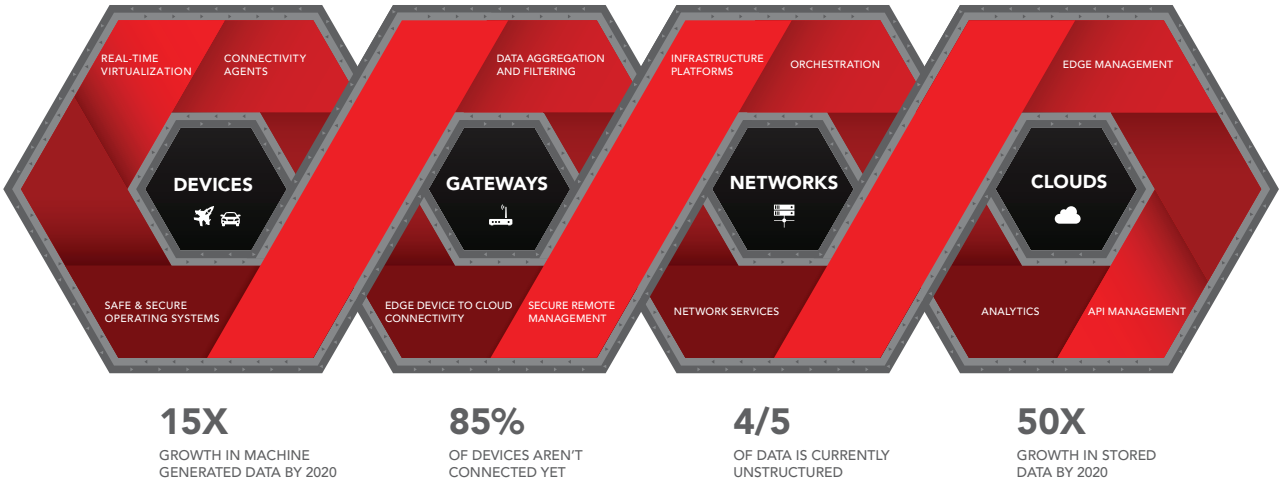

Figure 2: Wind River Internet of Things topology

The strict control and ownership by government and services of real-time IoT data limits the commercial opportunity by defense contractors to sell derived intelligence from this data. But creating affordable, high-value systems that deliver enhanced situational awareness for military and homeland security agencies has a proven business value. Complementing this intelligence with integrated commercial IoT data is also a compelling business model for innovative defense contractors and systems integrators.

A good example of IoT in the military is soldier healthcare. Because most military bases and deployments are 100% controlled by the military service, and have a well-defined and controlled perimeter with a fixed health system, it is easier to administer health programs, both preventive (in the home or barracks) and on demand (in the hospital), than in civilian environments. Today, both soldier facilities and soldier equipment (including wearables) contain a wide range of health and security monitoring systems, enabling an effective, end-to-end soldier health system. These systems can readily alert the soldier and, if necessary, a medical response team in a base hospital, to changes in a soldier's medical condition that require a re-provisioning of health services.

One area of the military where the IoT business model is similar to commercial aerospace is in predictive maintenance of equipment, which uses the real-time IoT data of military systems to determine when repairs should take place before breakage occurs. Although the volume of aircraft and other military vehicles tends to be much smaller in number than commercial aircraft, the diversity, density remoteness and time criticality on the military aircraft maintenance and logistics system creates similar benefits of a highly connected support system. These systems can also enhance mission reliability and security, saving both lives and resources.

SECURING THE BATTLEFIELD

While the defense sector has been a reliable proving ground for technologies that comprise IoT, it is also one of the primary beneficiaries of the increasing sophistication of those technologies, such as security.

Today, security remains a paramount issue that needs to be addressed at every level of IoT, from cloud-based control systems through network infrastructure to the thousands of endpoint devices that gather data and execute tasks. And because interference, intrusions, and ownership of weapons, guidance, intelligence, surveillance, and targeting systems have obvious mission- and life-threatening consequences, security is also the key differentiating factor for companies that develop and implement defense solutions using IoT technology.

Next-generation processors include many new hardware features aimed at providing a highly trusted compute platform. For example, Intel® processors include an implementation of the Trusted Platform Module (TPM), designed to secure hardware through cryptography and other security techniques. In addition, technologies such as ARM® TrustZone®, Freescale Trust Architecture, and Intel Trusted Execution enable the integration of both software and hardware security features to create a platform that endures over the lifetime of the deployment with a wide range of software builds.

HANDLING THE VOLUME OF DATA

As the connectivity of sensors increases and they start supplying data, the system can become overwhelmed with the huge volume of data in transit. This increase in data may force an upgrade to a system's network infrastructure to increase bandwidth, or, alternatively, the performance of intelligent data filtering and throttling by edge devices.

This challenge is similar to what the commercial networking infrastructure is facing with the proliferation of smart, "video-enabled" phones and tablets. In the commercial world, network bandwidth and quality-of-service challenges are being addressed with the use of high-bandwidth carrier grade network infrastructure. This infrastructure is based on open standards–based network devices, using, for example, COTS hardware combined with open virtualization platforms to dynamically manage network demands.

These advanced network servers provide both high availability and also new approaches to controlling and provisioning network systems by delivering a path to Network Function Virtualization (NFV). NFV offers the operator the ability to dynamically configure the network infrastructure through sophisticated management protocols such as OpenStack, which enables operators to optimize for different network situations and demands, such as giving priority to certain data flows, or protecting parts of the network from certain attacks.

These commercial solutions can be adapted to the control and management of data as it passes through the various military networks to get to the combat cloud. NFV empowers military commanders to quickly configure data feeds for changing operational requirements, and to manage device and data security throughout the system.

IS THERE ANY SUCH THING AS A COMBAT CLOUD?

Can we truly implement a military IoT system with network-enabled capability (see Figure 3)? Currently each military force has its own infrastructure, both for connectivity and for the back office systems. Transitioning to a combat cloud infrastructure would offer huge operational advantages, with greater ability to export both data and assets in the field for joint operations. When implemented, a combat cloud would allow information and control to move farther forward when appropriate, providing the operational flexibility to deal with a near peer targeting the national data systems.

TRANSFORMING LEGACY SYSTEMS

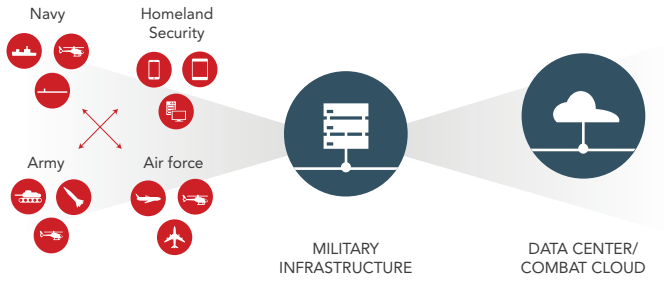

Figure 3: The military Internet of Things

INTO THE COMBAT CLOUD

The complexity and high cost of defense systems means these systems must remain in service for many years. This longevity creates operational challenges for enhancing their capability and attaching them to the combat cloud. For example, how do you share data between a stealth unmanned vehicle and a legacy F-16 aircraft, or between the unmanned vehicle and ground forces?

New technologies such as multi-core silicon and virtualization can help create affordable solutions to these challenges. Virtualized systems enable the continued use of legacy software applications while combining them with new capabilities on new operating environments. On legacy single-core processors, this virtualization would have a direct impact on platform performance, with the processor having to run both legacy and new code while maintaining strict separation for safety and security reasons. But with the advent of modern multi-core technology, the performance and separation risks can be mitigated in silicon, separating legacy and new environments on separate cores and networks to achieve the goals of affordability, performance, and mission capability enhancement.

For example, Lockheed Martin demonstrated how an open systems architecture can enable improved interoperability between next-generation and legacy fighter aircraft. According to the press release, the flight tests of an F-22 and the F-35 Cooperative Avionics Test Bed (CAT-B) were flown to assess the capability to share information—in real time—among varied platforms. The effort demonstrated:

- Ability to transmit and receive Link-16 communications on the F-22
- Software reuse and reduction of the aircraft system integration timelines
- Employing Air Force UCI messaging standards

This is clearly the first step in providing access to the combat cloud from legacy aircraft not originally designed for this capability.

WIND RIVER: DRIVING SUCCESS IN THE IOT ERA

As a worldwide leader in embedded solutions, Wind River is uniquely positioned to help the defense industry take advantage of the efficiencies created by the commercial IoT business transformation. Unique capabilities invented by defense industries can now be purchased as COTS components, reducing size, weight, power, and costs (SWaP-C) in order to create affordable solutions to enable the combat cloud.

Wind River Helix™ is our portfolio of software, technologies, tools, and services for addressing the system-level challenges and opportunities created by IoT (Figure 4). It offers the following points of value:

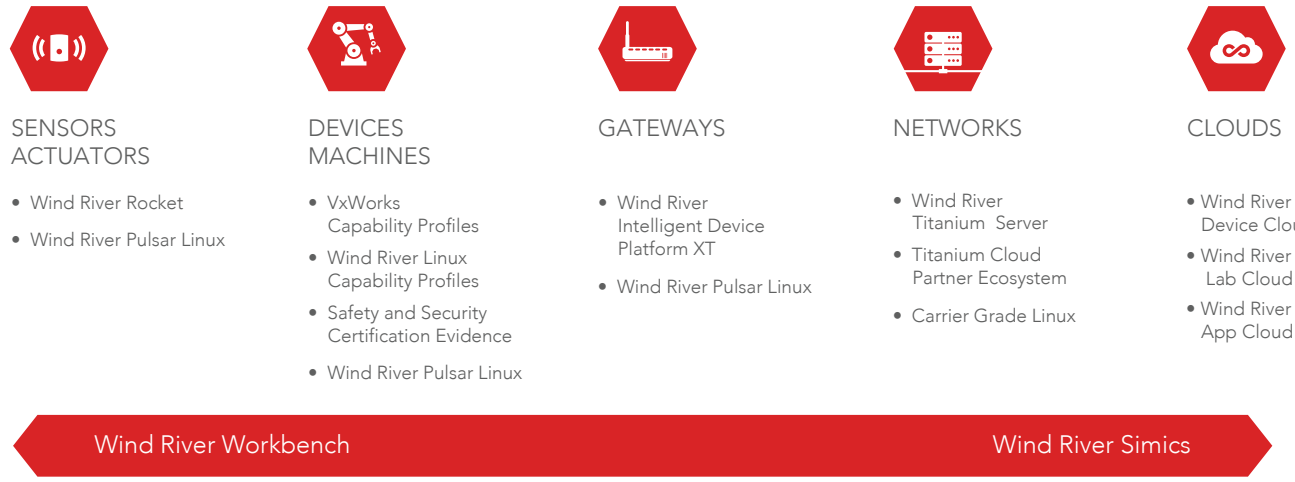

Figure 4: Wind River Helix portfolio applied to IoT topology

- Building safe and secure systems is the hallmark of Wind River. For the past 30 years Wind River technology has been tested and proven for safety, security, and reliability, without compromising performance.
- We're now harnessing our decades of field experience to deploy advanced technologies such as software agents and microkernels to more fully integrate our ultra-reliable operating systems into IoT.
- Wind River Intelligent Device Platform XT offers crucial software support for the development, integration, and deployment of IoT gateways, providing front-line data fusion capabilities.
- Wind River Titanium Server enables an NFV infrastructure to achieve the high reliability and high performance mandated for network-enabled systems of systems and combat clouds.
- Wind River Helix Device Cloud is a cloud-based platform that helps sensors, devices, and machines connect securely to your network infrastructure.
- Our commitment to open standards leads the industry, with a wide range of solutions using ARINC 653, Carrier Grade Linux, Eclipse, FACE™, POSIX®, and the Yocto Project.
- Wind River platform consolidation solutions enable developers to deliver powerful integrated IoT solutions quickly, while driving down SWaP and system deployment and operational costs.
- Wind River Simics® simulates systems—from the smallest to the most complex—so you can adopt new development techniques that are simply not possible with physical hardware. These new development techniques accelerate every phase of your development lifecycle, dramatically reducing the risk of shipping late, overrunning budget, and sacrificing quality.
- The global Wind River Professional Services and Wind River Education Services teams help customers gain a competitive edge by providing design support from concept through implementation.

CONCLUSION

In the IoT era, consumers are realizing the benefits—and businesses are monetizing the intelligence—gained from technologies tested and proven in the defense sector. This commercial investment is driving huge cost savings for next-generation defense IoT systems. With Wind River as its business partner, the defense industry can now reap the benefits of transforming its systems into the next generation of high-value network-enabled solutions, enabling an affordable Internet of Things for defense.

WIND
AN INTEL COMPANY

Wind River is a world leader in embedded software for intelligent connected systems. The company has been pioneering computing inside embedded devices since 1981, and its technology is found in nearly 2 billion products. To learn more, visit Wind River at www.windriver.com.