THE INTERNET OF THINGS FOR THE INTELLIGENCE COMMUNITY
EXECUTIVE SUMMARY

The Internet of Things (IoT) is today’s commercial initiative to integrate a wide variety of technical and commercial information-generating components to provide new business opportunities based on 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 and intelligence community (IC) over the past 15 years. In much the same way that NASA and the early space program in the 1960s spurred innovations in chip technology, automation, propulsion, and miniaturization, solutions developed from the concept of network-centric operations (NCO) translate directly to the foundations of today’s commercial IoT.

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

TABLE OF CONTENTS

Executive Summary ................................................................. 2
Network-Centric Concepts ..................................................... 3
   Data and Decisions Drive the Value of IoT Information .............. 3
Challenges Facing the Intelligence Community .......................... 3
Moving Forward with Combat and Tactical Clouds ...................... 5
Transforming Legacy Systems into the Combat Cloud ................. 5
Wind River: Driving IC Success in the IoT Era ........................... 6
Conclusion ............................................................................ 7
NETWORK-CENTRIC CONCEPTS

Advanced sensor-to-cloud intelligence gathering allows today’s security agencies to make decisions based on real-time analysis generated by integrating information from a wide range of sensors on a global basis. These systems provide a constant stream of data to agencies where it is analyzed and integrated with other data sources to enable comprehensive situational awareness of security-sensitive arenas.

Data and Decisions Drive the Value of IoT Information

This network-centric intelligence collection and analysis 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.

CHALLENGES FACING THE INTELLIGENCE COMMUNITY

The primary challenge for the military/IC sector is managing the ever-increasing volume of data generated by their systems, and open source systems, in an efficient and timely manner. Intelligence is based on a tasking, collection, processing, exploitation, and dissemination (TCPED) process, itself based primarily on a “send it back” model; unfortunately a large portion of the “collection” in this model goes to archive, unanalyzed. There has been a large growth in the use and adaptation of automated data processing and decision support tools to fix this TCPED logjam, but the growth of data-generating resources and the increasing demand for speed of action have shown the current architecture to be losing the battle for efficient and reliable information management.

Specific areas where advances based on IoT concepts and technology could positively affect the current system include:
• **TCPED architecture:** The centralized data processing systems currently relied on have proven to be incapable of keeping up with the growing sources of collection and data. “Virtualization” would allow the traditional sources and locations of networks, data fusion, and decision support to expand to include many if not all the sensors, systems, and devices deployed forward.

• **Beyond line-of-sight (BLOS) communication:** The TCPED and command and control (C2) process reliance on bandwidth/throughput-constrained satellites and other BLOS communications platforms is the Achilles’ heel of IC and military operations. A decentralized operational functionality needs to be implemented to diversify the risks of this communications chokepoint.

• **Multilevel Security (MLS) management:** Multiple services, agencies, coalition partners, and new operations partners need to be supported with automated connectivity, discovery, and security separation for multiple levels of IoT data and intelligence, at the user-specific access level without human intervention. This functionality needs to extend from commercial and government systems to private and personal systems, increasing the level of access and collaboration while maintaining data protection and access profile management.

If these challenges can be solved, there is an opportunity to multiply our force capabilities exponentially. Our global military and intelligence assets are now deployed in many global hot spots, and our technology has matured to the point where we can finally push data, data fusion, and decisions support forward into a new soldier-enabling architecture. NCO-enabled personnel can access a real-time common operating picture (COP) and command data immediately from a tactical cloud forward to solve immediate engagement challenges and identify and react to emerging opportunities faster—significantly accelerating the observe, orient, decide, and act (OODA) loop over today’s standards. Key elements of this new NCO architecture are:

• **Intelligence ubiquity:** Every device, sensor, and system contributing to and enabling the tactical cloud forward is available to the mission or operations commanders.

• **Multiple cloud availability:** Connections back to national and commercial cloud systems will be used when available, but a forward unit operationally capable subset of all the attributes and capabilities will provide a sustainable capability and allow for “graceful degradation,” regardless of area of responsibility (AOR) threat level.

• **Single cloud view:** Access to cloud services will appear as a single cloud architecture worldwide, with a fully functional cloud (“overcast cloud”) capable of gracefully breaking into “broken” and even “scattered” clouds but retaining basic multi-sensor or system fusion, data distribution, and access, adapting to the assets available at any given moment. Throughout the degradation of full overcast cloud access, whether caused by failure, denial, or corruption, operational functionality will be autonomously maintained through migrations of virtual network functions (VNFs) to scattered available clouds, maintaining the full flow of IoT data and commands to all systems forward—sensors, weapons, radios, and command consoles acting as a single living, breathing, self-repairing system-of-systems, in order to maintain soldier and mission awareness.

• **MLS:** Access to all cloud and system services will have a natural, embedded MLS method to autonomously filter data to warfighters and mission personnel, with automatic discovery and control to provide the most complete COP.

• **Self-repairing systems:** The flow of data must be self-repairing—able to reconfigure automatically and adapt to new sensor and systems availability, maintaining and updating prioritization processing as information channels morph into new improved or degraded scenarios.

• **Open standards and architectures:** All components of this architecture must be based on open standards and open architectures to enable the rapid insertion of new capabilities and the modification or adaptation of existing ones to support new and modified mission scenarios.

• **Platform consolidation:** The use of consolidation platforms using common core processing platforms with rapid, dynamic insertion capabilities is mandatory.

• **Secure remote management:** Edge management systems and control systems must have secure remote management for reconfiguration to new environments and response to changes in the threat landscape. The ability to update and reconfigure software packages on the fly makes it easier to adapt to areas of operations and threat responses.
• **End-to-end security:** An end-to-end security architecture must be designed, deployed, and maintained. This security architecture must include both hardware and software as a combined, complementary solution, and include both legacy (brownfield) and new system (greenfield) platforms. This security starts with a trusted boot mechanism and extends through virtualization environments and layered intrusion protection and detection, as well as the capability to dynamically configure any aspect of any platform as required to maintain both platform and system health.

• **Platform simulation:** A system simulation or virtualization model of each hardware element will enable exhaustive testing—including scenario, reconfiguration, and degradation testing—on the overall system at any time. These simulation models can be made available prior to the availability of the actual hardware, allowing for security and robustness testing and design changes in advance of hardware readiness, accelerating time to deployment and overall security robustness.

**MOVING FORWARD WITH COMBAT AND TACTICAL CLOUDS**

A fully functional, fully virtualized, self-repairing combat or tactical cloud is the foundation of next-generation intelligence systems (see Figure 3). Currently each military service or coalition partner 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, providing all connected entities a real-time COP. It would also offer an enhanced environment for dynamically enabling coalition operations.

**TRANSFORMING LEGACY SYSTEMS INTO THE COMBAT CLOUD**

Next-generation TCPED and tactical cloud forward systems must be based on advanced network servers to provide both high availability and also new approaches to controlling and provisioning network systems by delivering full Network Functions 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 cyberattacks.

While designed to adapt to changing telecommunications network system requirements and provide cost benefits, these COTS components can be utilized for developing ad-hoc self-organizing network-forward systems-of-systems that can solve the challenges of future defense networks.

These COTS-based 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.
Along with NFV capabilities, 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 in new operating environments. On legacy single core processors, this virtualization would have a direct impact on platform performance, with the processor running both legacy and new code while maintaining strict separation for safety and security functionality requirements. But with the advent of modern multi-core technology, the performance and separation risks can be further mitigated in silicon, separating legacy and new environments on separate cores and networks to achieve the goals of affordability, performance, and mission capability enhancement well beyond legacy single core processors.

Network Functions Virtualization

NFV is the telecommunications industry's version of IT virtualization, achieved by augmenting the latter with the carrier grade capabilities required for high availability, security, and performance, as well as for more efficient network management. Key benefits of NFV for the telecommunications industry include faster time-to-market, enabling new services quickly, rapidly scaling resources up and down, and lowering costs.

In NFV, software-based VNFs run on one or more virtual machines and are chained together to create communications services. NFV solutions consist of three layers: a VNF layer running on an NFV infrastructure (NFVI) layer, and an NFV management and orchestration layer that manages the VNF and NFVI layers. The NFV server, the basic building block for NFV carrier grade solutions, consists of NFV software running on industry-standard hardware.

Implementation of NFV in network elements requires a range of critical elements, including:

- Carrier Grade Linux (or other operating system)
- High-performance virtualization
- Data plane acceleration, including high-performance vSwitch support
- Integration with OpenStack
- Management and orchestration layer with strong links to existing OSS/BSS systems

Wind River Titanium Server is the industry's first fully integrated, open source–based, feature-complete NFV server. It supports a wide range of redundancy types and fault management features to achieve better than six-nines availability at minimal redundancy costs.

Wind River: Driving IC Success in the IoT Era

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

Wind River Helix™ is our portfolio of software, technologies, tools, and services for addressing the system-level challenges and opportunities created by IoT in IC environments. Helix offers the following features:

- 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.

Figure 4: Virtual functions and networks creating the “Tactical Cloud”
• 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-C 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 intelligence community. This commercial investment is driving huge cost savings for next-generation security agency systems. With Wind River as its business partner, the intelligence community can now reap the benefits of transforming its systems into the next generation of high-value network-enabled solutions, increasing the knowledge, speed, and utility of future security agency systems.