DELL Technologies

Whitepaper

FPGA-Powered 5G: Securing Mission-Critical Connectivity

Revolutionizing Federal Networks with Agile, Secure, and Future-Ready Open RAN Solutions

Table of Contents

Executive Summary

Mission success in today's complex battlespace hinges on secure, resilient, and adaptable communications. Federal Private 5G (FP5G) offers dedicated capacity, control, and low-latency connectivity essential for mission-critical operations. Yet, the infrastructure supporting these networks must be equally robust, flexible, and secure to meet the unique demands of defense applications. This white paper explores how Field Programmable Gate Array (FPGA) technology serves as the optimal foundation for Open RAN Radio Units (O-RUs) in Department of War (DoW) and allied deployments, combining adaptability, security, and mission-critical performance.

Dell Technologies has developed an FPGA-based O-RU specifically designed to address the challenging requirements of the tactical edge, secure facilities, and forward-deployed missions. Leveraging FPGA technology, this solution offers key advantages:

- **Operational Agility:** Reconfigurable algorithms allow for quick adaptation to new waveforms, emerging electronic warfare threats, or mission requirements without replacing hardware. This agility ensures tactical units can respond in real time.
- **Federal-Grade Security:** With hardware-rooted trust and supply chain integrity, the platform enables Zero Trust architecture, ensuring secure operations even in highly contested environments.
- **Mission Sustainability:** An advanced radio architecture with design focused on energy efficiency minimizes logistical burdens, making it ideal for forward-deployed units that rely on limited power resources.
- **Future-Ready Architecture:** The FPGA-based platform is designed to support emerging technologies like AI and 6G, ensuring long-term investment protection and operational relevance.

Introduction: The Imperative for Resilient Communications

Enhancing Warfighter Readiness

In today's contested electromagnetic spectrum, secure, resilient, and adaptable communications are essential for mission success. Warfighters require reliable, low-latency networks to coordinate autonomous systems, enable sensor-to-shooter loops, and maintain situational awareness. Likewise, logistics hubs and command centers need dependable connectivity that can withstand disruptions, whether caused by adversaries or environmental challenges.

Dell federal Private 5G (FP5G) networks address these critical needs by delivering dedicated, secure connectivity independent of commercial carriers. However, the radio access layer—where digital systems interact with the spectrum—must be as flexible, secure, and agile as the mission demands.

Open RAN: Disaggregation for the Tactical Edge

The Open Radio Access Network (O-RAN) architecture eschews proprietary, monolithic hardware in favor of a disaggregated approach. This divides the base station into functional components: the Centralized Unit (O-CU), the Distributed Unit (O-DU), and the Radio Unit (O-RU). For federal deployments, O-RAN delivers several strategic advantages:

- **Vendor Diversity:** Avoid being locked into a single vendor by integrating best-of-breed technologies across components, ensuring operational flexibility.
- **Interoperability:** The standardized interfaces in O-RAN empower coalition operations, enabling seamless communication between allied forces.
- **Rapid Innovation:** New capabilities can be deployed quickly through software updates, eliminating the delays and costs associated with hardware replacement.

These attributes make O-RAN an ideal choice for defense applications, where adaptability and rapid response are paramount.

Why FPGA is Critical for the Mission

The Radio Unit (O-RU) is the critical interface between digital processing and RF transmission. While many commercial networks rely on Application-Specific Integrated Circuits (ASICs), these fixed-function processors lack the flexibility needed for defense operations since they can't be easily updated. In contrast, FPGAs provide a reconfigurable logic fabric, enabling mission-specific customization and in-field updates.

Table 1: Strategic Advantages of FPGA vs. ASIC for Defense

Capability	ASIC (Commercial Standard)	FPGA (Defense Optimized)
Adaptability	Fixed at manufacturing	Reconfigurable in the field to meet new threats
Algorithm Updates	Requires new hardware	Software update only
Supply Chain	Long lead times, often OCONUS	Flexible supply chain, rapid prototyping
Security	Static security features	Updatable security logic to counter new threats
Lifespan	Driven by commercial cycles	Extended support for long-lifecycle programs

For the DoW, the ability to update radios post-deployment offers a mission-critical advantage. For example, if adversar-ies deploy new jamming techniques, engineers can develop and deploy updated filtering algorithms remotely, ensuring operational continuity without requiring hardware replacement.

Technical Architecture and Scalability

Dell O-RU Platform Overview

Dell Technologies, in collaboration with Altera, has developed an FPGA-based O-RU tailored for federal use. Built on the Altera Agilex 7 SoC FPGA, this platform combines dedicated high-performance blocks with programmable logic, offering a balance of efficiency, flexibility, and scalability.

Key Technical Specifications:

- **Antenna Configuration:** 4T4R (FPGA scalable from 2T2R to massive MIMO for diverse mission needs).
- **Bandwidth Support:** Each component carrier supports 100 MHz bandwidth with carrier aggregation for broader coverage.
- **Synchronization:** Precision timing support via PTP ensures seamless coordination across deployments.
- **Processing:** Integrated Hard Processor System (HPS) enables efficient management and control.

Scalability for Multi-Domain Operations

The modular architecture supports a wide range of mission types:

- **Expeditionary Deployments:** Compact designs enable rapid deployment in austere environments with limited infrastructure.
- **Base Operations:** High-density deployments, ideal for smart warehouses, airfields, and command hubs, provide reliable coverage and operational functionality.
- **Secure Facilities:** Custom configurations tailored to SCIFs ensure compliance with strict security protocols.

6G and AI Readiness

The future of defense communications will increasingly leverage AI for cognitive radio capabilities and 6G for enhanced connectivity. The FPGA-based architecture is inherently adaptable to these advancements:

- **AI/ML Integration:** Neural network inference engines can be implemented on FPGA fabric for intelligent spectrum management and adaptive beamforming.
- **Mixed Numerology:** Support for diverse subcarrier spacings ensures compatibility with emerging traffic types, critical for future 6G networks.

Operational Agility: The Power of Field Updates

Adapting to the Threat Environment

In contested environments, adaptability is a force multiplier. Adversaries evolve electronic warfare strategies constantly, requiring communication systems to adjust in real time. Traditional radios, dependent on fixed hardware, are ill-suited to this dynamic landscape. FPGA-based O-RUs, with their ability to be reprogrammed in the field, provide a significant advantage.

Example Scenario: Electronic Warfare Response

If an adversary introduces a new jamming technique, an FPGA-based radio can be updated with a secure algorithm patch within hours, rather than waiting months for hardware replacement. This enables commanders to maintain communication superiority in active theaters.

Accelerating Development Cycles

The use of Altera's proven IP ecosystem accelerates prototyping and deployment. By building on a validated O-RAN baseline, defense teams can layer mission-specific enhancements—like proprietary waveforms or advanced encryption—without redesigning the entire system. This streamlined process reduces development time for critical upgrades.

Power Saving Features

Energy Efficiency Through Intelligent IP

Network energy consumption is a critical concern for operators as well as the military as it leads to smaller, more nimble communication packages. RAN sites account for 70-80% of mobile network energy consumption, with RUs consuming up to 75% of that total. The FPGA-based architecture enables sophisticated power-saving features.

Dell's O-RU implements multiple Energy Saving Features (ESFs) enabled by Dell's and Altera's flexible IP:

Symbol TRx Shutdown and User Packing

During TDD operation, transmit and receive chains can be shut down during unused symbol periods. Advanced Sleep Modes (ASM) enable cross-layer optimization, proactively shutting down the power amplifier when no downlink symbols are scheduled. This innovative approach can achieve up to 25% energy savings.

RF Channel Reconfiguration

The MIMO configuration can be dynamically adjusted based on traffic demand. When full spatial multiplexing is not required, the O-RU can reduce from 4x4 MIMO to 3x3, 2x2, or even SISO operation, shutting down unused antenna paths. Depending on traffic patterns, this can deliver 11-86% energy savings.

Deep Sleep and RU Hibernation

When traffic can be steered to adjacent cells, an entire O-RU can enter deep sleep mode, reducing power consumption by 97-100% while maintaining the ability to wake rapidly when needed.

Quantified Savings

Based on Dell's analysis using daily average usage traffic models is quantified in Table 2:

Traffic Load	Hours/Day	Percentage of Day
Full (100%)	2	8%
Busy (50%)	6	25%
Medium (30%)	10	42%
Low/Idle	6	25%

Table 2: Traffic vs. Utilization % of Day

Implementing Symbol TRx Shutdown ESF with this traffic profile yields approximately **$920 in energy cost savings per O-RU over a 5-year period** (at $0.15/kWh). Across a deployment of hundreds of radio units, these savings become substantial.

The FPGA Advantage: Because these power-saving algorithms are implemented in reconfigurable logic, they can be **optimized and updated after deployment.** As Dell engineers develop more sophisticated power management techniques, these improvements can be pushed to fielded units – continuously improving efficiency throughout the deployment lifecycle.

Security Architecture: Trust at the Edge

Security is paramount for federal networks. Dell's FPGA-based platform aligns with Zero Trust principles and DoW cyber guidelines, ensuring hardened protections and supply chain transparency.

Hardened Hardware Security

The Altera Agilex 7 FPGA incorporates a Secure Device Manager (SDM) that establishes hardware-rooted trust:

- **Secure Boot:** Protects against unauthorized software by verifying all code at startup.
- **Anti-Tamper Mechanisms:** Detect attempts to compromise the hardware and respond proactively.
- **Bitstream Encryption:** Safeguards intellectual property loaded onto the FPGA, reducing exposure to reverse engineering.

Supply Chain Integrity and Sovereignty

Supply chain risk management is critical for mission assurance. Dell's O-RU platform is manufactured in TAA-compliant facilities and comes with comprehensive Software and Hardware Bills of Materials (SBOM/HBOM), ensuring full transparency. This rigorous oversight ensures operational sovereignty, allowing sensitive missions to remain independent of external infrastructure.

Air-Gapped Operations

For government agencies managing sensitive or classified data, air-gapped systems deliver unmatched security by isolating critical systems from untrusted networks. This eliminates external cyber threats and safeguards mission-critical data.

The Dell O-RU supports deployments where:

- No connectivity to public internet is required
- All management occurs through secure, isolated channels
- Data never traverses third-party infrastructure
- Full operational sovereignty is maintained

Conclusion

The choice of radio unit architecture has lasting implications for Federal Private 5G deployments. While ASIC-based solutions may offer cost advantages at very high volumes, FPGA-based O-RUs deliver compelling and strategic benefits for federal and defense deployments.

Flexibility: The ability to update algorithms after deployment eliminates the traditional trade-off between time-to-market and feature completeness. Organizations can deploy with confidence, knowing that improvements and new capabilities can be added throughout the system lifecycle.

Security: Hardware-rooted security features, combined with Made in USA FPGA manufacturing options and TAA compliance, address the stringent requirements of federal deployments. The FPGA's reconfigurability also enables rapid response to emerging security threats.

Efficiency: Sophisticated power-saving features enabled by Dell's and Altera's flexible IP deliver measurable reductions in energy consumption and operating costs and packaging size and weight. These algorithms can be continuously improved and updated in fielded units.

Future-Proofing: As 3GPP standards evolve and O-RAN specifications mature, FPGA-based O-RUs can adapt without hardware replacement. This protects the deployed investment and ensures continued compliance with emerging requirements.

Dell Technologies and Altera have combined their expertise to deliver an FPGA-based O-RU platform that addresses the unique requirements of Federal Private 5G networks. This solution provides flexibility, security, and performance that mission-critical federal deployments demand.

For more details, contact our Federal Team or visit dell.com/federal.