Solution Brief

End-to-End Private 5G: Simple, Open and Secure for Critical Implementations

Trenton's Integrated Edge Solution for 5G (IES.5G) streamlines deployment of private 5G networks for battlespaces, emergency services and beyond.

As the volume, velocity and variety of operational data grow without limit, critical communications for military and emergency-services organizations must keep pace. Next-generation networks must be developed not only in permanent facilities such as military bases and public safety access points (PSAPs), but also for field installations such as battlespaces and disaster response. The high speed, security, low latency and high reliability of private 5G networks make them ideal for these usages.

Accelerating adoption in the military, the National Defense Authorization Act (NDAA) signed into law by President Biden in December 2023 calls for the Department of Defense (DoD) to install private 5G networks on military bases.[1] Strategically, this development contributes to the DoD's goal of a more disaggregated and distributed force structure. Tactically, it requires deployment of novel technologies in an efficient, effective, secure manner. A similar vision guides the need for rapid deployment of private 5G wherever it is needed, from conflict zones to natural disasters.

To address those needs, Trenton Systems — in partnership with Intel — offers its Integrated Edge Solution for 5G (IES.5G), a private 5G Core coupled with centralized unit (CU) and distributed unit (DU) that can be deployed in minutes. Based on a ruggedized, field-ready hardware system and open-standards-based software, IES.5G provides integrated radio access network (RAN), 5G Core and zero-trust network security in an ultra-reliable, modular architecture.

Trenton Systems IES.5G private 5G solution.

Trends and factors for advanced private 5G

The requirements that shape the future of military and emergency-services private 5G deployments draw on broader industry trends. These critical communications epitomize the need for high-speed data access and security. Improvements in throughput, latency and reliability make 5G networks increasingly attractive for applications such as command and control, surveillance and emergency response.

Real-time data transmission and analysis can enhance situational awareness and operational effectiveness based on critical communications. In addition, the following factors embraced across industries are helping drive implementation requirements specific to these critical public-sector usages:

- **Edge computing** moves processing power closer to where data is produced and consumed, reducing latency especially for critical communications and other real-time usages at scale.
- **Ruggedized, ready-to-deploy solutions** are needed for fast time-to-activation and reliability, particularly in field deployments. Harsh, remote environments often make traditional infrastructure impractical and require ruggedized equipment to ensure continuous operation.
- **Interoperability and standardization** based on vendor-neutral components are increasingly desirable as the industry moves away from monolithic hardware-defined requirements. Open architectures enabled by 5G facilitate seamless collaboration among agencies and jurisdictions.

Trenton IES.5G helps drive this spectrum of trends and factors in the broader telecommunications ecosystem, with enablement for enhanced cybersecurity and emerging requirements including AI. This solution augments that generalized industry expertise with domain-specific expertise for critical military and emergency services implementations.

Challenges to overcome for 5G deployments

The virtualized, software-defined nature of 5G networks often makes forklift upgrades using stand-alone architectures desirable. This is especially true in the case of field-deployable private 5G, which tends to be a more greenfield scenario than public mobile networks, for example. The resulting comprehensive nature of these implementations tends to intensify the challenges described in this section.

Cost

A primary consideration for organizations making decisions about private 5G networks is to ensure the cost-effectiveness of their projects. These factors include both the initial investment in hardware, software, licensing and deployment as well as ongoing costs such as maintenance and upgrades. Many look to turnkey solutions such as IES.5G for predictable cost-effectiveness and to avoid the need for 5G network teams attached to every distributed site.

Complexity

Integrating private 5G networks into existing infrastructure and workflows tends to be a complex and time-consuming process. Organizations commonly face challenges ensuring compatibility with legacy systems, migrating to the new system and training staff. Associated challenges with cross-vendor compatibility and vendor lock-in are also important considerations.

Security

Cloud-based security based on zero-trust network access (ZTNA) is as complex as it is critical, especially given the sensitive nature of the data and applications involved in military and emergency services operations. Cross-domain security is particularly germane for moving defense information (classified or otherwise) to destinations across appropriately trusted environments.

Usability

For personnel responding to critical circumstances on the ground, usability is central to the 5G solution's success or failure. Ensuring the performance and reliability of the solution in production is essential to the missions it supports. The infrastructure deployed must provide deterministic results in overcoming network congestion, latency, downtime and service degradations.

Streamlining success with the Trenton IES.5G solution

As an integrated, ready-to-deploy private 5G solution, Trenton Systems' IES.5G offers seamless, efficient end-to-end deployment. It is designed as a comprehensive, scalable platform with advanced features to match predictable high performance in the field with robust back-end and operational quality, including integration with DevOps and other modern organizational practices.

The solution is based on international industry standards and protocols for ease of integration and interoperability with existing infrastructure and systems. This standards-based approach helps ensure extensibility in the future with best-in-class solutions and functions from a broad ecosystem. The solution as a whole includes the components and capabilities described in this section.

Hardware

Trenton Systems delivers IES.5G using ruggedized systems based on an Intel technology stack. These systems help ensure performance, efficiency and security, even in extreme, unpredictable conditions. As a Titanium Intel® Partner Alliance member, Trenton Systems has early access to upcoming Intel processor generations, helping drive deployment of the latest features and capabilities to its customers as soon as possible.

Software

The software components of the IES.5G solution provide the intelligence and network functionality needed to operate, manage and control the private 5G infrastructure. Networking and management software components provide powerful configuration and optimization for network settings, and security functions protect against cyberthreats and unauthorized access. The solution can also draw on the open ecosystem of 5G components.

Networking

IES.5G incorporates advanced networking technologies and protocols for high-speed, low-latency communication among devices and applications. This includes support for network slicing, quality of service (QoS) management, traffic prioritization and seamless handover between different network cells. These networking capabilities enable organizations to deliver reliable and responsive connectivity for critical applications and services.

Security

Cyber protection of communications and data is fundamental to the IES.5G solution, to protect against threats as well as to ensure the integrity and confidentiality of transmissions. Pre-configured true ZTNA protection enforces continuous authentication and authorization for all users, devices and applications that access services on the network. This functionality is supported by security functions such as encryption, access control and intrusion detection to safeguard sensitive data and critical infrastructure.

Orchestration and management

To help streamline deployment, configuration, monitoring and maintenance, IES.5G provides centralized orchestration and management. These capabilities can include automated provisioning of network resources, real-time performance monitoring, fault detection/remediation and policy-based management of network configurations. The solution's orchestration and management capabilities help increase operational efficiency and maximize uptime.

Intel building blocks that underlie the solution

Trenton Systems uses 3rd Gen Intel® Xeon® Scalable Processors today and is working on integrating the latest 5th Gen Intel® Xeon® Processors. To optimize the handling of exponentially rising amounts of data, Intel architecture delivers performance, efficiency and security with standards-based technologies. The stack enables network virtualization to converge 5G network functions on IES.5G's hyperconverged infrastructure. Highly optimized for workloads at the edge and in the cloud, Intel components employ a secure supply chain manufacturing process that helps ensure sound, authentic parts for the solution.

5th Gen Intel® Xeon® processors

Network-optimized 5th Gen Intel Xeon Processors provide the state-of-the-art engine for the IES.5G solution, designed specifically for virtualized data plane and signaling workloads. With high throughput and performance per watt, the processor provides power-efficient results that anchor its leading size, weight and power (SWaP) characteristics. To provide a balanced platform, 5th Gen Intel Xeon Scalable processors incorporate advances across execution, memory and I/O:

- **High-throughput, high-efficiency execution resources**. Improved per-core performance and up to 64 cores per socket, with the industry's most built-in accelerators and energy savings with Optimized Power Mode.
- **Enhanced memory subsystem**. Up to 16% increased DDR5 memory speed and up to 3x total last level cache compared to its predecessor,[2] to hold more user plane data close to the processor for enhanced throughput.
- **Expanded I/O speed and capacity**. Up to 80 lanes of PCIe Gen 5.0 per socket, with Intel Ultra Path Interconnect (Intel UPI) 2.0 speeds up to 20 GT/s and support for Compute Express Link (CXL) Types 1, 2 and 3.

The processors incorporate built-in Intel® QuickAssist Technology (Intel® QAT) for accelerated crypto on the fly, which directly benefits 5G throughput for the pervasive encryption required by 5G and ZTNA. Offloading these tasks from the CPU cores to the Intel QAT engine frees processor resources for other work, further benefiting the solution as a whole.

Hardware for vRAN enablement

Intel has helped drive the evolution of RANs from a closed ecosystem of monolithic approaches to open solutions for cloud-native deployment on general-purpose servers. Intel® Ethernet Controllers make a substantial contribution to this progress with products that offer hardware-enhanced timing and synchronization. They enable the phase accuracy required by virtualized RANs (vRANs) without the added cost and complexity of dedicated timing devices, incorporating precise timing information into data streams on a per-packet basis.

The Intel® vRAN Dedicated Accelerator ACC100 SoC reduces the time needed to perform RAN Layer 1 (L1) forward error correction (FEC), which resolves data-transmission errors to help ensure the fidelity and integrity of communications. This common function is one of the most compute-intensive of all 5G workloads, so accelerating it can substantially improve network performance. The Intel® vRAN Dedicated Accelerator ACC100 SoC supports an open source software stack built to integrate with open RAN architectures including Intel FlexRAN™ (discussed below) while reducing requirements for power, space and computing resources.

Intel FlexRAN™

To optimize resource use by 5G vRANs, IES.5G implements Intel FlexRAN™, which separates network functions from the underlying hardware. A key aspect of this architecture is control and user plane separation (CUPS), which enables the two to scale independently of each other, for improved efficiency. It also increases the openness of the solution, allowing for software components from multiple control-pane and user-plane vendors to interoperate more smoothly. FlexRAN™ incorporates the Open RAN (O-RAN) architecture called for in emerging DoD directives for private 5G deployments mentioned earlier in this paper.

Target field use cases

The Trenton IES.5G solution is built for general-purpose deployment in addition to critical usages for military forces and emergency services teams. The domain-specific intellectual property and expertise built into the solution is highlighted in the use cases described in this section.

Mobile command centers and vehicles

IES.5G is ideally suited to the critical nature of secure, resilient communications needed for mobile operations, field deployments and disaster response:

- **Military communications and command apparatus**. The IES.5G solution can rapidly establish secure and reliable mobile communications, providing real-time data transmission for command and control capabilities in the shifting battlespace.
- **Emergency response and disaster management**. In emergency situations such as natural disasters or humanitarian crises, IES.5G can support first responders and emergency management teams by enabling fast and resilient communication networks for coordination, resource allocation and situational awareness.

Surveillance and monitoring

Perimeter protection and monitoring/surveillance of critical infrastructure and resources are enabled by the portability and low latency of the IES.5G solution. These implementations provide the real-time (or near-real-time) data processing and analysis needed to detect and respond to threats, including denial of physical access by unauthorized parties. The agility with which such capabilities can be deployed highlights the flexibility and robustness of the solution.

Conclusion

Emerging requirements for high-throughput, low-latency, secure communications are particularly resonant in critical implementations by military and emergency-services organizations. Trenton Systems draws on its domain expertise in this area to offer the IES.5G private solution. Built for rapid deployment with leading-edge Intel technologies, these networks provide crucial infrastructure for the work of personnel dedicated to protecting life.

Learn More

Trenton Systems IES.5G

Intel Federal and Aerospace

Intel-powered private networks

Solution provided by:

intel + TRENTON SYSTEMS®

[1] Federal News Network, December 22, 2023. "Military installations will soon get private wireless networks." https://federalnewsnetwork.com/defense-main/2023/12/military-installations-could-soon-get-private-wireless-networks.

[2] On select SKUs. Results have been estimated or simulated comparing theoretical performance of DDR5-4800 to DDR5-5600. Performance varies by use, configuration and other factors. Performance varies by use, configuration and other factors. Learn more at intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for configuration details.

No product or component can be absolutely secure.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a nonexclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

0324/DP/MESH/PDF 356877-001US