EXPERT PAPER

Validating maximum network performance for modern warfare

COMPREHENSIVE TESTING FOR EFFICIENT CELLULAR MILITARY COMMUNICATIONS

ROHDE&SCHWARZ
Make ideas real

EXECUTIVE SUMMARY

Modern military operations increasingly depend on reliable mobile networks using cellular technologies for mission critical communications, data transmission and control of advanced systems. This expert paper outlines a comprehensive, phased approach to testing private 4G/5G networks deployed in fixed military installations – command centers, logistics hubs, training facilities, etc. – and explores the emerging challenges of testing cellular networks utilized during active operational deployments.

To successfully implement private networks, unique technical, operational and organizational challenges such as interference mitigation and interoperability must be addressed. This paper details best practice testing procedures, from initial spectrum verification to ongoing performance monitoring, and recommends key performance indicators (KPIs) tailored to specific military use cases such as autonomous systems and augmented reality.

Rohde & Schwarz offers a complete portfolio of testing solutions, including network scanners, spectrum analyzers and sophisticated software platforms to ensure these networks meet stringent performance, security and reliability requirements. By proactively validating network capabilities and continuously monitoring performance, military organizations can maximize operational effectiveness, safeguard sensitive information and maintain a decisive technological advantage. This expert paper provides a framework for military decision-makers, IT leadership and procurement agencies seeking to integrate network testing as an integral process for ensuring mission success in today's operational environments.

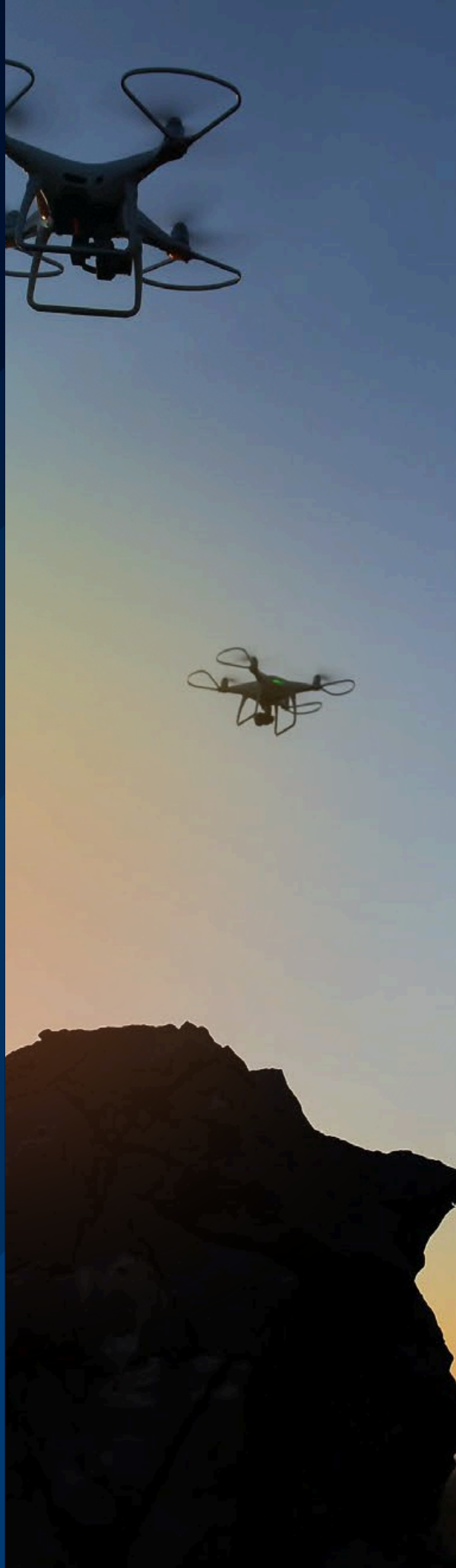


TABLE OF CONTENTS

HOW CELLULAR COMMUNICATIONS ARE EMPLOYED IN THE MILITARY DOMAIN

COMPREHENSIVE SENSOR NETWORK: INTRODUCING MMTC

Establishing comprehensive situational awareness requires a vast interconnected network of sensors for perimeter security, threat detection, environmental monitoring and logistical tracking. Massive machine type communications (mMTC) are designed to connect a large volume of devices simultaneously, making extensive sensor networks feasible. While integral to 5G, mMTC principles can also be applied to advanced 4G networks.

ENABLING REAL-TIME CONTROL: UNDERSTANDING URLLC

Precise, immediate control of drones, robots and automated defense systems – particularly in contested environments – demands exceptionally reliable, low-latency communications. Ultra-reliable low latency communications (URLLC) deliver this through advanced error correction and network prioritization. As a key feature within the 5G framework, URLLC ensures responsiveness where milliseconds matter.

HIGH-THROUGHPUT CONNECTIVITY: EXPLORING EMBB

The need for rapid intelligence dissemination – high-resolution video from drones and satellites, immersive training via virtual and augmented reality and swift access to maps and satellite imagery – requires substantial bandwidth. Enhanced mobile broadband (eMBB) meets this demand by providing significantly higher data rates than previous cellular technologies. Capabilities are further enhanced within the 5G framework.

UNDERSTANDING MISSION CRITICAL COMMUNICATIONS IN MILITARY ENVIRONMENTS

Mission critical communications (MCX) represents a key upgrade to existing military communications systems. It integrates advanced cellular capabilities – including 4G and 5G – and offers increased bandwidth and scalability, allowing for transmission of high-resolution video and large data files. MCX combines these advancements with established technologies like HF/VHF/UHF radio, satellite communications and existing cellular networks.

MCX is designed to operate seamlessly across environments, from command centers to remote field sites, prioritizing 5G where available and ensuring continued communications through existing systems when necessary.

MCX is the 3GPP-standardized feature set, built around the three components: mission critical push-to-talk (MCPTT), mission critical video (MCVideo) and mission critical data (MCData). These components provide the secure and immediate communications needed for effective operations in demanding environments.

Instant voice communications: MCPTT
Mission critical push-to-talk (MCPTT) provides immediate voice communications, mirroring the functionality of traditional walkie-talkies and group calls but leveraging the enhanced capabilities of a 4G/5G network. It enables rapid coordination between soldiers in the field, command elements and other key personnel and is particularly valuable during time-sensitive operations and for maintaining clear command and control.

Real-time video intelligence: MCVideo
MCVideo enables real-time transmission of high-resolution video over 5G networks, fundamentally transforming situational awareness. From reconnaissance to remote inspection, MCVideo provides commanders and personnel with the visual intelligence they need to make informed decisions.

Data connectivity: MCData
Mission critical data (MCData) enables reliable and secure transfer of vital information in real time. This is critical for controlling autonomous systems, transmitting sensor data and sharing tactical information, enabling a higher degree of coordination and control in complex military scenarios.

TESTING AS LINE OF DEFENSE

WHY MEETING NETWORK PERFORMANCE KPIS SECURES MILITARY OPERATIONS

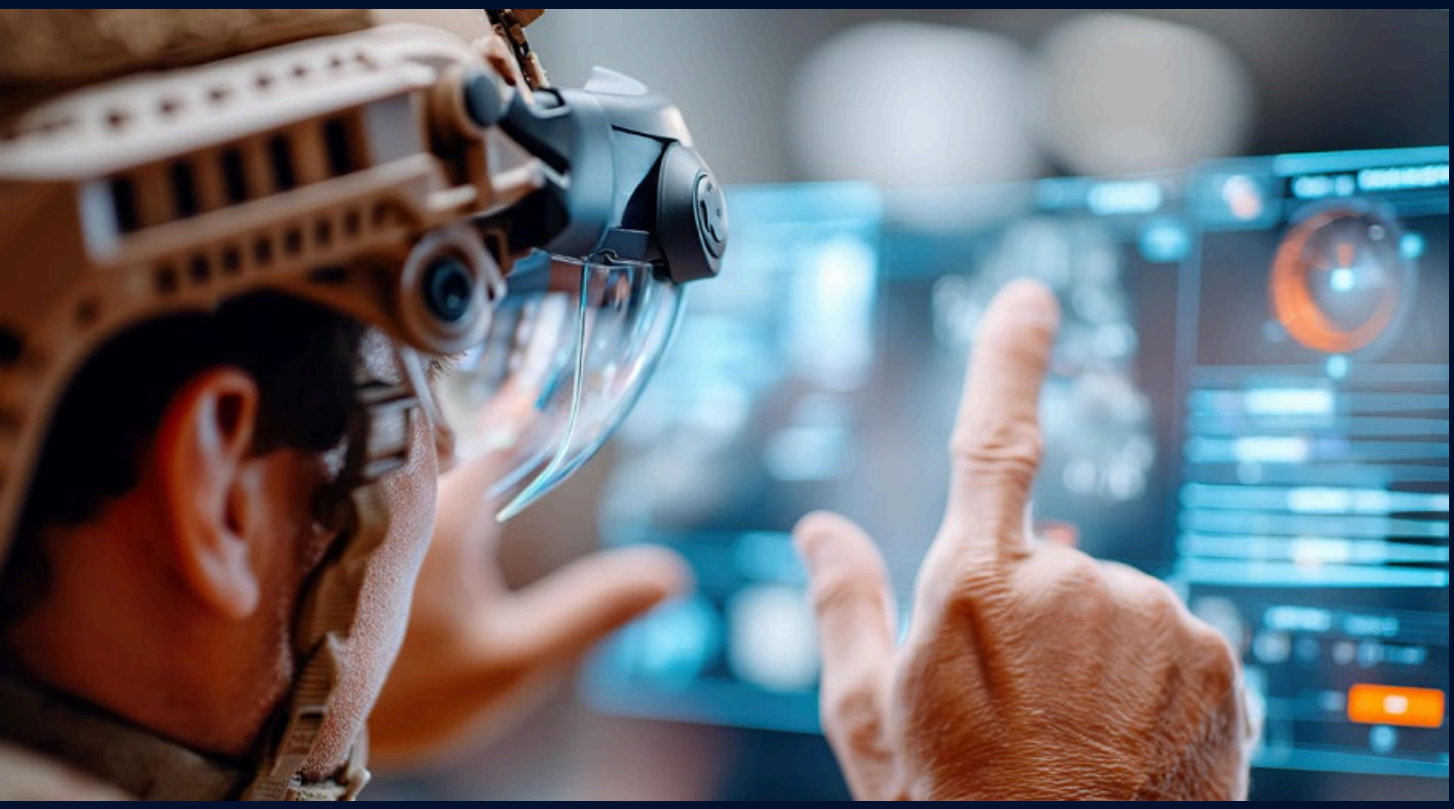
Comprehensive network testing is essential for mission effectiveness. **The network is the backbone for mission critical communications (MCX),** enabling real-time situational awareness as well as command and control. Beyond validating connectivity, rigorous testing safeguards critical information and ensures the capabilities needed in today's operating environment, which is why verifying network performance requires a proactive approach, especially in environments prone to interference.

Protecting sensitive information: Military installations and logistics hubs generate and rely on highly sensitive data – from strategic planning and supply chain coordination to personnel information. Thorough and regular network testing is essential, both to verify adherence to stringent security standards and to ensure networks meet sensitive data protection standards. Testing plays a vital role in identifying and mitigating vulnerability to interference, which is particularly crucial for maintaining operational effectiveness.

High network performance ensures operational capability: Maintaining consistent network performance under pressure is non-negotiable in the military domain. Network testing validates that KPIs – including latency and throughput – are met even under stress and that troubleshooting can detect link failures or configuration errors. Furthermore, comprehensive testing enables documentation and validation of failover, fallback and recovery procedures.

Supporting data-intensive operations: Modern military installations require reliable transmission of large data volumes to support critical operations. Prioritized private networks are essential for guaranteeing sufficient bandwidth and low latency, enabling capabilities such as real-time situational awareness via data transmission from sensors and surveillance systems. These networks also facilitate unit communications and coordination, advanced data analysis and reliable operation of automated logistics and security systems. Rigorous testing is crucial to confirming consistent, predictable network performance under load and ensuring mission success with diverse application use.

HOW PRIVATE 4G/5G NETWORKS POWER MODERN LOGISTICS AND CONTROL CENTERS



Optimized private networks are increasingly critical for enhancing situational awareness and enabling intelligent infrastructure. A performant network serves as the foundation for implementing integrated systems that provide real-time data and control functions.

Unmanned aerial and ground systems, for example, make a significant contribution to remote observation and reconnaissance. Operators leverage these platforms to receive live video feeds and sensor data, allowing them to assess areas such as maintenance zones, staging locations and critical access routes, thereby improving situational understanding and minimizing personnel risk. Simultaneously, augmented reality (AR) systems can support maintenance personnel. Technicians in maintenance facilities or control rooms can utilize AR-enabled devices for digital guidance, accelerating repairs and reducing downtime.

Beyond visual reconnaissance, **integrated sensor networks** deliver a continuous stream of critical environmental data. They continuously monitor variables such as temperature and fuel levels as well as chemical, biological, radiological and nuclear indicators. Strategically positioned sensors – for instance, in fuel depots or refrigerated storage for medical supplies – enable rapid responses to potential hazards. Advanced security camera systems with automatic alerting functions complement security protocols through proactive perimeter monitoring at checkpoints, loading/unloading areas and around storage facilities.

Effective asset management at these locations also relies on **precise tracking capabilities**. Systems utilizing tags and readers can provide real-time location and inventory level tracking in warehouses, distribution zones and loading/unloading bays. This ensures accountability and efficient resource allocation.

Beyond static monitoring and tracking, truly intelligent logistics relies on the dynamic orchestration of automated systems. Modern warehouses and distribution centers are increasingly deploying **automated guided vehicles (AGVs) and autonomous mobile robots (AMRs)** to streamline material handling. These robotic systems, navigating autonomously within high-bay storage facilities efficiently retrieve, sort and stage military supplies for shipment, drastically reducing manual labor and accelerating fulfillment times. A robust network with superior performance is paramount to the safe and reliable operation of these fleets – enabling real-time path planning, collision avoidance and coordinated task management

Furthermore, integration with warehouse management systems (WMS) via this network allows for predictive maintenance scheduling for the robots themselves, maximizing up-time and ensuring a consistently responsive supply chain.

By enabling faster decision-making, enhanced security and optimized resource utilization, high-performing networks are essential to improving readiness and responsiveness. But real-world, technical, operational and organizational challenges have to be addressed in order to maintain this high level of performance.

The following section outlines these challenges and offers an effective approach to overcoming them.

> **A PERFORMANT NETWORK IS THE INDISPENSABLE FOUNDATION FOR INTEGRATED SYSTEMS; WITHOUT THE DYNAMIC ORCHESTRATION OF REAL-TIME DATA, TRULY INTELLIGENT LOGISTICS AND ENHANCED SITUATIONAL AWARENESS CANNOT BE ACHIEVED.**

CHALLENGES FOR NETWORKS IN COMMAND CENTERS, LOGISTICS AND LARGER BASES

TECHNICAL CHALLENGES

Implementing 4G/5G networks in large military facilities such as command centers and logistics hubs presents several significant technical challenges. In particular, the **complex radio environment** and the resulting performance limitations pose a major hurdle. The use of a lot of metal construction and the multitude of devices within these facilities – including a growing number of IoT devices such as sensors and robots in logistics centers – can lead to coverage limitations and interference, causing diminished signal quality. This can make it harder to ensure sufficient network coverage, low latency and high data throughput, which negatively affects critical applications like real-time video surveillance, robot/drone control and transmission of sensor data.

Another key challenge is maintaining operational performance in the face of cyberattacks and electromagnetic warfare (EW). Command centers and logistics hubs are attractive targets for such attacks due to their strategic importance.

ORGANIZATIONAL CHALLENGES

Beyond the technical aspects, introducing new networks in the military domain presents several organizational challenges, among them is the **integration with existing systems** to ensure that the new network seamlessly interoperates with current logistics and communications software.

Another consideration is the tension between standardization and national customization.

Adherence to international standards must be reconciled with specific national security requirements.

Optimizing the use of available radio frequencies is also crucial. Efficient utilization of this limited resource is essential for network performance.

OPERATIONAL CHALLENGES

The question of network functionality must be answerable quickly and reliably to ensure smooth operational performance. However, the escalating complexity and sheer volume of network devices make manual oversight impractical. Consequently, **automated solutions for monitoring, configuration, and troubleshooting are essential to maintain performance and eliminate uncertainty regarding full operability.**

By relying on these automated systems and verified KPIs, military personnel can ensure decisive network management, supported by targeted training to master these technologies.

TECHNICAL CHALLENGES

ORGANIZATIONAL CHALLENGES

OPERATIONAL CHALLENGES

Rohde & Schwarz leverages extensive experience with industrial and private networks to support deployment and optimization of powerful networks for demanding military applications. Our testing solutions are crucial for validating network performance under realistic and complex RF conditions, ensuring functionality and compliance with national and international standards. We also facilitate seamless integration with existing systems and guarantee optimal frequency utilization, establishing reliable operation even under adverse circumstances. The standardized network testing procedure introduced in the next section proactively addresses technical, organizational and operational challenges to implementing new 4G/5G networks in a military context.

BEST PRACTICE PROCEDURE FOR MILITARY BASES AND INSTALLATIONS

1 PREPARATION FOR ROLLOUT

Objective: Interference-free use of the frequency spectrum reserved for the military base.

Procedure: Verification that the spectrum is free of interference from other radio signals before the private network is commissioned. This phase is typically conducted by the network planner (e.g. infrastructure provider, system integrator) and includes documentation of any identified interference and corresponding mitigation measures.

2 PERFORMANCE OPTIMIZATION AND ACCEPTANCE

Objective: Fine tuning of network performance following network deployment to meet defined KPIs for military requirements and final validation through an acceptance report.

Procedure: Validate network performance against established KPIs using passive radio measurements and active testing, enabling release for operational use. It includes the following steps:

- Coverage and signal quality verification: Validate radio coverage and signal strength (RSRP, SINR) across the operational area to ensure sufficient and reliable connectivity.
- Application performance testing: Emulate realistic military application scenarios with representative devices to test network responsiveness and ensure critical communications applications meet latency and real-time performance requirements.
- Data analysis and performance optimization: Analyze measurement results to identify potential bottlenecks and enable continuous performance optimization.

ENGINEERING (ONGOING):

Objective: Interoperability of mission critical communications with the aim of detailed analysis to optimize the network's radio and application performance. The emphasis of this phase is on the interaction between the network and devices (e.g. drones, tactical radios).

Procedure: Simulation of specific network scenarios (e.g. high device density, interference) by deliberately influencing devices and generating specific traffic patterns to understand network behavior under various conditions.

3 PERFORMANCE AND SERVICE LEVEL VERIFICATION

Objective: Long-term assurance of agreed-upon KPIs through continuous monitoring and proactive maintenance.

Procedure: Implement a tiered monitoring system to continuously verify network performance against pre-defined KPIs.
This includes:

- Manual verification: Conduct regular site surveys using mobile test equipment to validate performance and identify potential issues.
- Automated monitoring: Deploy network-distributed measurement probes for continuous performance monitoring and trend analysis.

4 TROUBLESHOOTING

Objective: Rapid identification and resolution of potential issues during ongoing operations, impacting network performance.

Procedure: When the performance and service level verification phase uncovers degrading service—such as a breach of the SLA or user reports of sub-optimal performance—swift and effective troubleshooting becomes essential.

A comprehensive root-cause analysis is then carried out using network traces and diagnostic data to pinpoint the source of the problem. This enables rapid remediation and guarantees that the network continues to deliver the high performance and reliability required by the SLA.

TESTING PRIVATE NETWORKS IN CONTROL CENTERS AND WAREHOUSES

PERFORMANCE STANDARDS DEVELOPED BY ROHDE & SCHWARZ

Private networks in control centers and warehouses need to be reliable and predictable. **KPIs offer a quantifiable way** to ensure this by validating network designs against application demands, proactively identifying and resolving bottlenecks before they impact operations and establishing performance baselines for ongoing monitoring and preventive maintenance.

We provide a set of KPIs based on best practice limits. These limits were established through detailed analysis of military use cases, including autonomous systems and augmented reality. This approach ensures a foundation for reliable, optimized network performance. The values are not arbitrary; they are derived from the specific latency and bandwidth requirements of each application. They should be considered starting points, adaptable to unique operational contexts and threat environments.

A FOCUS ON SPECIFIC USE CASES

Autonomous systems (AGV/UAS/robots)
Autonomous systems operating at the edge require responsive control links. Although control data throughput is relatively low, even brief interruptions or packet loss can lead to mission failure or put lives at risk. High bandwidth is also crucial for processing sensor data such as laser scans and high-resolution video, which enables informed decision-making and autonomous navigation. Recommended KPIs include:

Data throughput:
- Control: > 0.2 Mbit/s
- Video transmission: > 10 to 15 Mbit/s
- Laser scans/high-resolution video: > 100 Mbit/s

Latency:
- Control: < 10 ms
- Drones: < 40 ms
- Cooperative robots: < 60 ms

Packet loss: < 0.0001 %

Augmented reality (AR)
Augmented reality (AR) applications offer significant advantages in areas like remote expert assistance for equipment repair or enhanced training simulations. To deliver these capabilities, AR demands consistent high bandwidth and low latency to deliver immersive and useful experiences. Testing focuses on image quality, smooth rendering, low latency for user interactions and consistent connection stability during movement. Recommended KPIs include:

Data throughput: > 15 Mbit/s (uplink and downlink)

Latency:
- Application layer: < 50 ms
- Transport layer: < 20 ms

Packet loss: < 0.1 %

The importance of continuous KPI refinement
The field of military communications is constantly evolving. Continuous research and testing are vital to refining these KPI values and expanding the library of application-specific performance metrics. Prioritizing network performance through consistent monitoring and adaptation is essential for ensuring mission success in an increasingly complex operational landscape.

UTILIZATION OF CELLULAR NETWORKS IN OPERATIONAL DEPLOYMENT

This part focuses on the utilization of networks in the field. Successful integration demands a robust and adaptable testing approach, acknowledging that military requirements are dynamic and frequently evolving. While many specific testing details are still under definition in coordination with relevant military committees, key international initiatives – including the US Department of War (DoW) 5G Strategy, the European Defense Fund (EDF), and the NATO Emerging and Disruptive Technologies Strategy (EDT) – are driving adoption. These initiatives recognize the significant advantages of 5G for enhancing operational effectiveness and security through higher data speeds, lower latency and massive connectivity.

Examples of networked applications in the field

Modern military field operations increasingly rely on networked capabilities across a diverse range of applications. Autonomous systems, including drones or self-driving vehicles, are deployed for reconnaissance, surveillance, mine clearance and transport, and all these systems are reliant on network control links.

Connected sensors, such as motion detectors, acoustic sensors and chemical/biological detectors, enhance awareness through continuous monitoring and threat detection. Underpinning all of this is a fast and verified communications network enabling mission critical voice communications, data transmission and video feeds throughout the operational area.

Challenges of operational private network deployment

Deploying and maintaining cellular networks in military environments presents a unique set of challenges. Achieving reliable network coverage under extreme conditions is a primary concern. Military operations frequently occur in remote areas, mountainous terrain, deserts and urban canyons, environments that demand comprehensive coverage even during adverse weather. Providing this coverage requires a substantial deployment of base stations and relay stations. Powering these stations can prove particularly difficult in remote locations. Maintaining interoperability with existing systems and allied partners is a critical consideration. Integrating established infrastructure with modern 5G networks and ensuring seamless communications during joint operations require careful planning and adherence to agreed-upon standards and protocols.

BEST PRACTICE KPIS FOR FIELD OPERATIONS

To support operational military applications reliably, we have defined best practice network performance requirements. These values, derived from 3GPP standards and tailored to the specific needs of the defense sector, serve as guidelines for ensuring dependable operation in challenging environments. A strong understanding of these requirements and their underlying rationale is therefore critical. We've established these best practice limits for two critical application areas: tactical system monitoring and military machine/process control.

The first area, **tactical system monitoring,** centers on real-time awareness of deployed assets, monitoring the condition of vehicles, systems and personnel and tracking parameters like temperature, position and overall operational status. Testing in this scenario prioritizes maintaining connection stability despite challenging environmental conditions such as dense foliage, urban canyons, or adverse weather – e.g. heavy rain or snow – and ensuring the energy efficiency of deployed sensors and communications devices. Key performance metrics for this application are:

Data throughput:

- > 0.016 Mbit/s. This provides sustainable bandwidth for transmitting basic status data.

Latency:

- < 10 to 20 ms (critical for safety)/< 200 ms (for regular measurements). Rapid response is vital for addressing critical events such as impending failures or threats.

Packet loss:

- < 0.01 %. This ensures critical information is not lost during transmission.

Interruption duration:

- < 30 to 300 ms can be tolerated.

A second key area, **military machine and process control**, encompasses the real-time control of vital military assets, including tanks, aircraft or autonomous platforms. Testing here focuses on verifying the real-time capability of control mechanisms, the precision of command execution and the network's resilience to interference. Key performance metrics for this application are:

Latency

- < 20 to 100 ms. Critical response time is essential for safe and effective control of these systems.

Packet loss:

- < 0.0001 %. Data loss must be minimized to avoid any impairment of control functionality.

Interruption duration:

- < 10 to 50 ms. Minimizing downtime during interruptions is crucial for maintaining operational control.

These areas represent a starting point for developing best practice KPIs. Rohde & Schwarz is committed to further investigation and analysis, including dedicated research and testing, to define KPIs for other potential applications and ensure optimal network performance across a broader range of military scenarios.

EXPLORE OUR TESTING SOLUTIONS

See also:
rohde-schwarz.com/mnt

CONCLUSIONS AND RECOMMENDATIONS

KEY FINDINGS

The adoption of private 4G and 5G networks is a major step toward more efficient military communications. To get the most out of these systems, it is helpful to look beyond the initial setup. Ensuring that your network performs reliably in different environments—whether in a logistics hub or the field—is the best way to support modern applications.

THE VALUE OF TESTING

A clear testing process helps you confirm that the network actually delivers the performance you expect. By verifying the radio environment and monitoring key metrics, you can ensure a smooth experience for all users. This proactive approach helps you maintain high standards of connectivity and simplifies the management of complex communication systems.

RECOMMENDATIONS

To maximize the effectiveness of your communications infrastructure, we recommend these focused actions:

- **Standardize the testing lifecycle:** Implement a phased procedure from spectrum clearance to troubleshooting to ensure your cellular networks are stable and predictable from day one.
- **Align metrics with reality:** Use application-specific KPIs to ensure your network meets the exact latency and throughput requirements of your specific military use cases.
- **Leverage our expertise:** Utilize the comprehensive Rohde & Schwarz testing portfolio to simplify complex network audits. Our industry-leading scanners and software provide the precision needed to validate performance and secure your digital backbone.
- **Commit to continuous optimization:** Partner with us for ongoing performance monitoring, ensuring your systems stay future-proof and optimized as operational demands evolve.

TRUE SPECTRUM DOMINANCE IN ALL DOMAINS

NON-TERRESTRIAL MONITORING

MONITORING SOLUTIONS

COUNTERING DRONES

ELINT / RESM

COMINT / CESM

CYBERSECURITY

MOBILE NETWORK TESTING

NAVAL COMMUNICATIONS SYSTEMS

CELLULAR NETWORK AND IP ANALYTICS

TEST & MEASUREMENT

TACTICAL COMMUNICATIONS

AIRBORNE COMMUNICATIONS

Today's military missions increasingly rely on information superiority and advanced command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems. Control over the electromagnetic spectrum has become essential in achieving strategic military dominance.

Rohde & Schwarz develops, designs, manufactures and implements turnkey end-to-end solutions for secure communications, SIGINT / EW, intelligence, test & measurement and security in modern warfare. Our solutions contribute to effective C4ISR, enabling customers to achieve dominance in the electromagnetic spectrum for a decisive edge in modern warfare.

SIGNAL MASTERY

Signal testing and generation, secure communications, encryption, signal detection, location, analysis and interception from a single source.

VERTICAL INTEGRATION

Rohde & Schwarz maintains a high degree of vertical integration with nearly its entire value chain inside the company. All products are developed and manufactured in its own factories.

ONE-STOP SHOP

Rohde & Schwarz provides a one-stop shop with the full range of turnkey solutions, from sensors and analysis to effectors across the electromagnetic spectrum.

TRUSTED PARTNERSHIP

As an independent, privately-owned company, Rohde & Schwarz finances its growth with its own resources. The company is not beholden to capital markets or stock market expectations.

Service at Rohde & Schwarz
You're in great hands

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

Rohde & Schwarz

The Rohde & Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test&measurement, technology systems and networks & cybersecurity. Founded 90 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.
www.rohde-schwarz.com

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

Rohde & Schwarz training
www.training.rohde-schwarz.com

Rohde & Schwarz customer support
www.rohde-schwarz.com/support