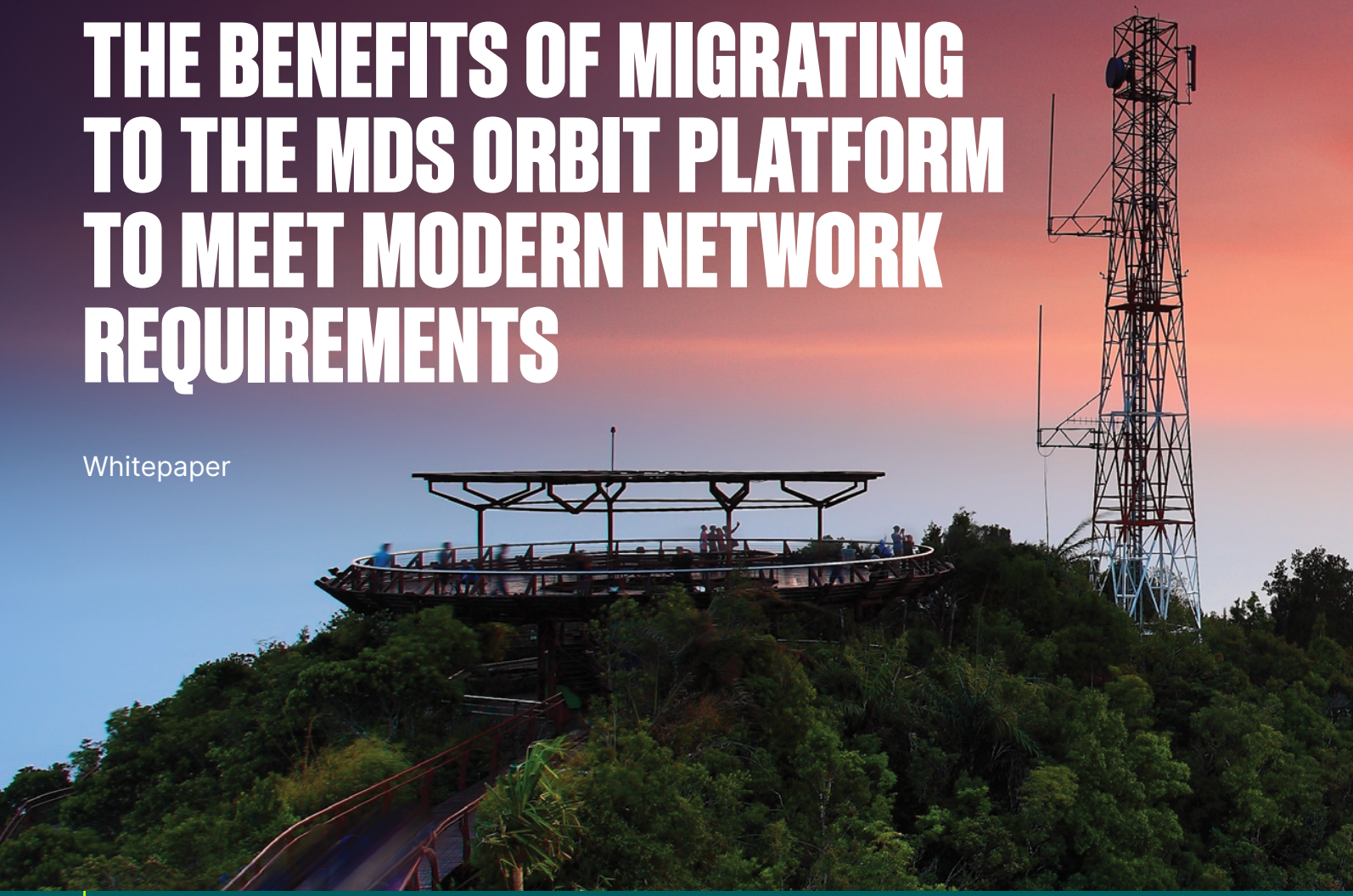
Grid Solutions

Evolution:
THE BENEFITS OF MIGRATING TO THE MDS ORBIT PLATFORM TO MEET MODERN NETWORK REQUIREMENTS

Whitepaper



As industrial wireless communication network performance and security requirements have advanced, technology has evolved with capabilities previously unimagined. This white paper is intended to assist MDS™ iNET II users in understanding the benefits of updating to the MDS Orbit Platform.

GE VERNOVA

INTRODUCTION

Wireless networks have provided reliable data transfer for critical industrial applications for nearly thirty years. As the technology ecosystem evolves into a digital world, wireless communications must also evolve.

Increased needs for application speed, various data sources, and comprehensive cybersecurity demand that the next generation of wireless technology performs to new standards.

THE MODERN WIRELESS NETWORK

Today's environment requires network managers develop comprehensive communication networks to meet demanding and evolving user, geographic, and regulatory requirements. This ever-changing landscape often forces network managers to work with a variety of technologies to reach their infrastructure assets.

The modern wireless network must, at its core, include:

- Comprehensive cybersecurity
- Improved throughput
- Long-range flexibility
- Enhanced networking capability
- Traffic prioritization

GE Vernova has addressed this challenge with the MDS Orbit platform. This next generation wireless communication solution integrates a range of technologies, from cellular to private, and licensed to unlicensed, supporting customers' needs for secure private, public, and hybrid communication networks.

CYBERSECURITY

When the MDS iNET series was developed, it was the leader in encryption and authentication with security features including RADIUS authentication, VLAN traffic segregation, proprietary hopping patterns, and AES 128-bit encryption.

While these security features are still relevant, there has been an increase in cybersecurity requirements by the industry. And as technology has advanced over the years, the MDS Orbit platform was developed to incorporate advanced cybersecurity along with industry-recognized top performance, including embedded ruggedness that results in 65+ years of mean time between failure (MTBF).

Cybersecurity is at the forefront of technology evolution, and GE Vernova professionals have developed a thorough understanding of modern needs to meet the evolving and demanding communication network requirements. Whether complying with standards such as NERC CIP or mitigating business risk, Orbit offers many security features that are customizable to users' needs (refer to Figure 1).

Proper security involves assessing, planning, deploying, and monitoring cybersecurity controls. Orbit was designed with three levels of security: network, device, and user.

SECURING THE NETWORK

Securing the network ensures that only valid traffic and approved devices are permitted on the network.

- IPsec VPN Encryption: Standards-based IPsec VPN and Dynamic Multipoint VPN (DMVPN) functionality encrypts data paths among Orbit devices or between Orbit and third party VPN concentrators to ensure information travels between devices securely.
- Certificate Management: X.509 digital certificates, in DER (Distinguished Encoding Rules) and PEM (Privacy Enhanced Mail) format, are provisioned and automatically renewed through Simple Certificate Enrollment Protocol (SCEP). Orbit can integrate with multi-tier PKI (Public Key Infrastructure) structures.
- Over-the-Air Encryption: Enables the encryption of radio frequency (RF) paths between Orbit devices over proprietary licensed and unlicensed RF interfaces. Orbit supports 128-bit and 256-bit AES encryption using pre-shared keys or certificate-based public key.
- RADIUS Authentication: enables centralized authentication of users and devices on the network.
- Firewall: Stateful Packet Inspection (SPI) firewall can be configured to accept, drop, or reject traffic through each wireless network interface. Furthermore, Layer 2 MAC filtering can be used to block/permit traffic based on Layer 2 header information.
- 802.1x Authentication: Enables only approved devices to be admitted on the Ethernet and Wi-Fi access side of Orbit after a username/password challenge.
- VLAN Support: Network interfaces support IEEE 802.1Q VLAN trunk and access port modes to provide separation of traffic. In addition, Wi-Fi dual SSIDs map to separate VLANs.

SECURING THE DEVICE

Securing the device ensures that the device is not compromised by tampering or alterations.

- Logical and Physical Port Disable: Logical and physical interface ports can be individually enabled/disabled as needed.
- Firewall: A fully configurable firewall can be used to guard each network interface. Traffic can be classified by Layer 2, 3, and 4 protocol fields. Rules can cause traffic to be accepted, dropped, or rejected, and can be applied inbound or outbound on any network interface.
- Tamper Detect Magnetometer: Movement in any axis or rotation is detected by continuously measuring the electromagnetic field around Orbit.
- Digitally Signed Firmware: Firmware is cryptographically signed by GE Vernova and offers an additional customer signature option to ensure authenticity. Orbit checks the signature at power-on and on firmware updates.
- Secure Firmware Updates: Updates are loaded on to Orbit through SFTP to ensure secure transfer.

SECURING THE USER

Securing the user ensures only authorized users have access to device management, network configuration, and status entry.

- User Accounts: Username / password login is required for device management interfaces. Automatic lockout on five consecutive failed login attempts.
- Role Based Access Control (RBAC): Three user levels (operator, technician, admin) are available, with increasing levels of read, write, and execute privileges.
- Secure Interface Protocols: HTTPS, SSH, SNMPv3, and NETCONF provide secure access to device configuration and management.
- Radius/AAA: Centralized user authentication through RADIUS is offered with support for a secondary RADIUS server to provide high reliability. RADIUS user accounts can be mapped to specific RBAC roles.
- Configuration Files and Restore Points: Device configuration can be captured on device (as system restore points) or off device (as configuration files). Configuration files can be used to “clone” devices or quickly restore service in emergency situations.
- Audit and Logging: On-board event logging and alarm tracking are available including user login/logout, configuration changes, and network connections. Events can be forwarded to central system via SNMP traps, syslog messages including optional support for Syslog-over-TLS. Events can also be sent as NETCONF notifications, along with configurable support for mapping events to alarm states represented at the Power LED and/or as a pin on the COM1 serial connector.

Data & Communication Security	Administrative Security	Manufacturing Security
Access control	Secure device management	Secure development
Authentication	Certificate management	Secure firmware
Data plane security	Audit and logging	Vulnerability tracking
• Username/ password login • RBAC • EAP-TLS authentication • IPsec VPN Encryption • Firewall & Stateful Packet Inspection • AES 128 & 256-bit encryption	• SSH, HTTPS, Netconf • Complete certificate services • Multi-tier PKI integration • Extensive event logging • Syslog-over TLS	• Secure coding practices • Third party testing • Digitally signed firmware • **100% designed and manufactured in Rochester, NY USA**

Figure 1: MDS Orbit’s Comprehensive Cybersecurity Framework

IMPROVED THROUGHPUT

When the iNET series was designed, it offered best-in-class throughput at 1024Kbps. The MDS Orbit Multi-Service Connected Router (MCR) with 900MHz licensed frequency option was designed and launched to exceed the iNET series’ high performance standard. Orbit MCR provides lower one-way latency at less than 5ms, higher packets per second and higher overall throughput than the iNET series at up to 1.25Mbps (refer to Figure 2). It is clearly the industry performance leader for Frequency Hopping Spread Spectrum 900Mhz radios.

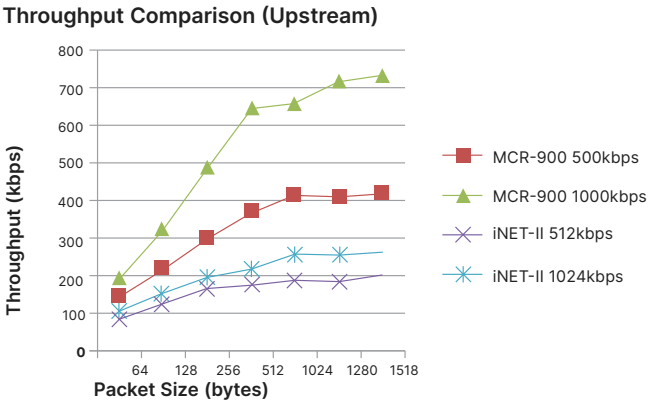


Figure 2: iNET II and Orbit MCR-900 Throughput Performance Comparison

LONG-RANGE FLEXIBILITY: STORE AND FORWARD

Store and Forward (SAF) offers a way to physically extend network range by enabling a "daisy chain" topology. It further allows users to overcome obstacles by routing the network around them.

As technology and capabilities have evolved, GE Vernova has built this capability into the Orbit platform, to meet this critical customer requirement.

SAF works by dividing the wireless network into a hierarchy of radio units. The highest level of the network consists of a single access point (AP), and the AP connects to either single or multiple units in the level below. The lower level units may also be connected to single or multiple units the next level down. Up to eight SAF levels are supported on Orbit. Multiple SAFs can be present on any given level to provide redundancy in the event of a single unit failure by enabling a self-healing topology.

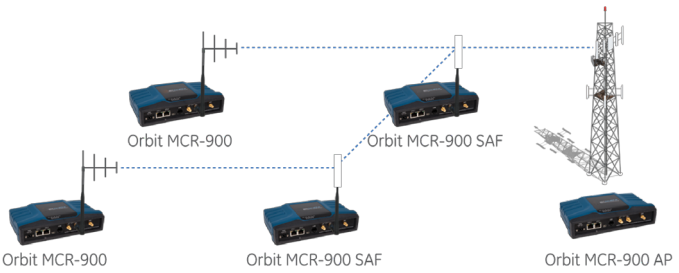


Figure 3: SAF physically extends the network range via a "daisy chain" topology

The advantages of Store and Forward are as follows:

- Range extension around obstacles
- Enabling a self-healing topology for network redundancy
- Network design flexibility with dynamic and static paths
- Optimized throughput with configurable dwell times
- Static or Dynamic automatic path discovery

ENHANCED NETWORKING CAPABILITY

Orbit brings added levels of network versatility over traditional radio devices. The support for dynamic routing protocols such as OSPF and RIP enable networks to grow and scale more quickly without the need of complex static configurations. Furthermore, dynamic routing helps networks adapt to changes in topology due to the addition of new devices or the failure of paths or networking devices.

Orbit's operation as a Layer 3 router as well as a Layer 2 managed switch with full VLAN and 802.1Q support, allow a variety of flexible topologies to be implemented, including pure Layer 2, pure Layer 3, in addition to an integrated Layer 2/3 topology.

Orbit's DMVPN is a standards-based implementation and allows the simplification of complex multipoint VPN topologies as well as integration with third party VPN concentrators.

Additionally, the Orbit MCR form factor can be packaged with a 900Mhz radio as well as a cellular radio for backup. The cellular radio can also be used as a primary connection with the 900Mhz radio as a downstream multipoint radio for network extension purposes.

Finally, the Orbit MCR and ECR form factors can support a 900MHz radio along with Wi-Fi.

TRAFFIC PRIORITIZATION: QUALITY OF SERVICE

Orbit provides advanced quality of service (QoS) capabilities to ensure proper traffic management during times of network congestion. QoS becomes a critical capability in converged networks where more than one application is being transported simultaneously and provides tools to ensure that critical traffic is transported first with minimal latency and performance impact.

Orbit supports classification of incoming traffic based on Layer 2, 3 and 4 header information. This provides more granularity over traditional 802.1p/DSCP prioritization mechanisms and allows Orbit to natively identify and classify applications based on such header information. This is completed without the dependence of third party RTU/Relays/PLCs to mark their traffic, as is the case with most radio products available on the market.

After applications are classified, they are then queued into 1 of 16 available priority queues. On the egress interface, Orbit supports three mechanisms of traffic queuing:

- **Priority Queuing:** ensures traffic lined-up in the priority Queue 1 is always addressed on the expense of all other traffic waiting on the remaining queues.
- **Fair Queuing:** an alternative mechanism that acts similarly to priority queuing while allowing some transmit time for lower priority traffic.
- **Traffic Shaping:** the first queueing mechanism which allows the user to "carve" a specific bandwidth on a per-application basis (e.g., DNP3/SCADA may be allocated 20Kbps, VoIP 15Kbps, Network Management 10Kbps, etc.). The network operator not only ensures priority for critical traffic, but also a more deterministic minimum throughput allocation.

Orbit's QoS set of tools empower the user to enable multiple applications simultaneously on the network, while ensuring critical traffic receives adequate attention during times of congestion, minimizing the impact of congestion on latency and throughput.

PERFORMANCE EVOLUTION

The table below outlines key security, performance, networking, and attributes of the iNET II and Orbit in a side-by-side table for comparison.

FEATURE	ORBIT MCR/ECR 900MHz	INET II 900MHz
Data Rate	125, 250, 500, 1000, 1250 kbps	512, 1024 kbps
Media Access	Proprietary, efficient, collision free data	CSMA/CA
Dwell Time	Variable: 10-400 msec	4 Discrete Steps: 16-131 msec
Beacon Interval Time	Variable: 10-300 msec	5 Discrete Steps: 10-260 msec
One Way Latency	As low as < 5 msec	As low as < 10 msec
Adaptive Data Rate	Yes (as of Orbit OS firmware 3.0.3)	Yes
Store and Forward	Yes up to 8 hops	No
Advanced QoS	Yes	No
Propagation Delay	Variable: 20, 40, 60 miles	Fixed
Fragmentation	Yes	Yes
Dynamic Fragmentation	Yes	No
Payload Compression	Yes	Yes
IP Header Compression	Yes	No
AP: Remote Ratio	1:500	1:128
Multi-hop Wireless Routing	Static, Automatic (optimal path analysis)	No
Self-healing	Yes, when using Store & Forward	No
Input Voltage Range	10V-60V	10V-30V
Serial Port	RS-232/485/422	RS-232 Only
Ethernet Port	10/100 Mbps w/ Auto Cross-Over	10Mbps Fixed
Temperature Range	-40 to +70C	-30 to +60C

CONCLUSION

The MDS team and our partners around the world truly appreciate the loyalty and commitment our customers have shown over the last 30 years. In turn, it is our ongoing commitment to ensure we provide a broad range of technical features and capabilities to support our customers' evolving network requirements.

Our global sales, application engineering and partner organization worldwide are available at any time to discuss the features covered in this whitepaper in greater detail. They are also available to consult with you on developing the best technology selection and migration strategy possible to align with your evolving network.

For more information on the MDS Orbit platform, visit:
https://www.gevernova.com/grid-solutions/automation/critical-infrastructure-communications/industrial-wireless/mds-orbit-platform

View and interact with our Interactive MDS Orbit platform explorer online:
https://library.grid.gevernova.com/interactive-product-explorers/mds-orbit-explorer

For more information, visit
gevernova.com/grid-solutions

GEA-31956 (E)
English
251007

GE VERNOVA