## GE VERNOVA

Cybersecurity in Mission Critical Licensed Networks

EVOLUTION OF INDUSTRIAL COMMUNICATIONS TECHNOLOGY

Whitepaper

This white paper is intended to assist users of GE Vernova's MDS x710, MDS SD series, and MDS Orbit Platform to understand the various industry security requirements and how the cybersecurity capabilities within each product platform support these new guidelines.

Grid Solutions
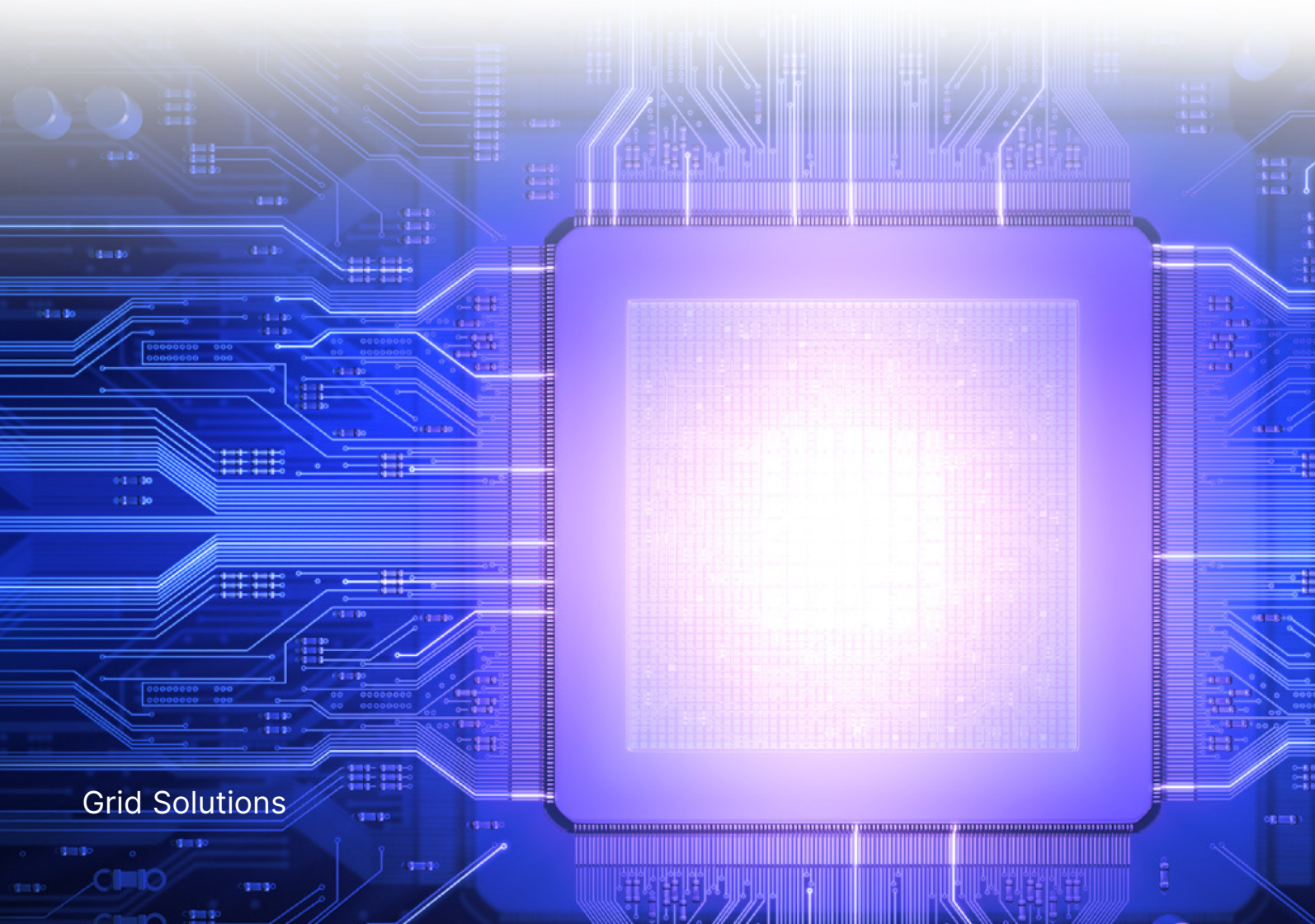
INTRODUCTION

Over the past few years, government regulation and information technology policy has increased cybersecurity requirements on mission critical wireless networks. New guidelines have been introduced which mandate modern security features that were previously non-existent. As security requirements have evolved, GE Vernova MDS has developed integrative platforms to deliver these modern security capabilities.

INDUSTRY GUIDELINES

A range of cybersecurity guidelines are available for critical infrastructure and industrial control systems. These guidelines help users assess threats, plan their networks, and employ the right security controls. The most common guidelines are outlined below.

NERC CIP

The mission of the North American Electric Reliability Corporation (NERC) is to ensure the reliability of the bulk power system in North America. The NERC CIP (Critical Infrastructure Protection) standards specify a cybersecurity framework that includes incident reporting, management of security controls, training, and recovery planning that is applicable to electric utilities and energy providers. NERC CIP defines responsibilities, processes, policies, and activities that an entity must establish and maintain to manage the cybersecurity risks on its infrastructure.

NIST SP800-82

The National Institute of Science and Technology (NIST) has been heavily involved in setting guidelines and industry best practices for industrial control systems for many years. NIST publication SP800-82 Guide to Industrial Control Systems Security is applicable to any organization with a distributed control or SCADA system. SP800-82 provides guidance on the selection and application of security controls including configuration management, access control, identification and authentication, in addition to audit and accountability.

NISTIR 7628

NISTIR 7628 Guidelines for Smart Grid Cybersecurity is a publication from NIST that provides specific tailoring of NIST SP800-82 categories for smart grid deployments.

FIPS 140-2

The Federal Information Processing Standard (FIPS) 140-2 is directly applicable to federal entities but can provide additional assurance to non-federal entities such as electric and water/wastewater utilities. FIPS 140-2 defines requirements that must be satisfied by all cryptographic modules used by any Federal agency. In practice, this defines approved algorithms and implementations that can be included in equipment used in these applications.

SECURITY CONTROLS

Each of the standards listed above provide security guidelines or security controls that should be utilized in a critical infrastructure network. These security controls protect the components of the network and the processes and procedures used to create and maintain the overall network. Security controls can be divided into several categories including:

- Encryption and authentication mechanisms
- Configuration management including snapshots and restoration
- Secure access to management interfaces
- Control of unused logical and physical ports
- Prevention of execution of malicious software
- Auditing and logging

As standards have evolved, the depth and strength of the security controls in GE Vernova's MDS products has expanded and varies amongst product categories. This, in turn, offers tiered options based on users' detailed requirements.

LICENSED NETWORK PRODUCT OVERVIEW

GE Vernova's MDS licensed network products were developed at different times and have varying security features. The section below outlines an overview of the MDS x710, SD series, and MDS Orbit Platform security features.

MDS x710 Series

The MDS x710 series represents a set of digital radio transceivers designed to operate in a point-to-multipoint environment, as shown in Figure 1. Examples include electric utility Supervisory Control and Data Acquisition (SCADA) and Distribution Automation (DA), Water/Wastewater SCADA, Oil and Gas field automation, as well as online transaction processing applications. These products use a combination of simple microprocessor and Digital Signal Processing (DSP) technology to provide reliable communications under adverse conditions.
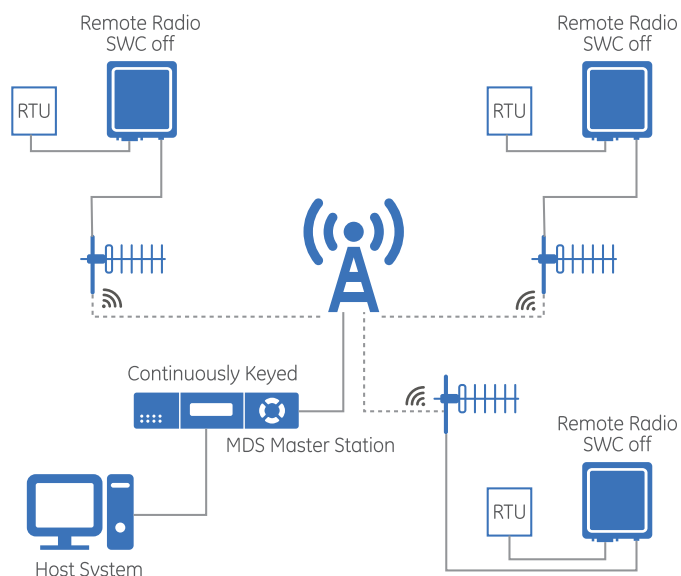
Figure 1: Typical MAS Point-to-Multipoint Network

MDS x710 transceivers support the following features:

- Serial Data from EIA/RS-232
- 1200-19200 bps
- Frequencies of 330-512 MHz and 800-960 MHz
- Bandwidths of 12.5 kHz or 25 kHz

The most common application of the transceiver is to participate in a point-to-multipoint Multiple Address System (MAS) consisting of a central master radio and several associated remote units. The network provides communication between a central host computer and the remote terminal units (RTUs) or other data collection devices. The operation of the radio system is transparent to the connected computer equipment.

Security Overview

Although the MDS x710 series provided an alternative to using a physical link to access remote computing devices, security features found in more modern communications devices were not available at the time this product was designed and manufactured.

As a result, the devices require external mechanisms to provide the confidentiality and integrity provided by using cryptography to encrypt the data before it enters the communication channel. External mechanisms that provide confidentiality and integrity to the data include an upgraded PLC/RTU or an inline serial data encryptor, such as the SCADAcrypt. These external mechanisms include device authentication and data authentication through encryption.

MDS SD SERIES

The MDS SD Series is an industrial wireless solution that provides long distance communications over licensed radio bands, allowing users to interface both Ethernet and Serial devices such as PLCs, RTUs, and meters with host monitoring and control systems.

Key benefits include:

- High speed, up to 65 Kbps in 50 KHz channel in SD2 and SD9
- Operate IP/Ethernet and serial communication on a single network
- Implement push communication and report by exception from remote devices
- Simple, intuitive web based configuration and maintenance
- Easy migration path from serial to IP/Ethernet

MDS SD Series radios can be directly added to existing MDS x710 and x790 systems, providing both "drop-in" compatibility for expansions/replacements, and adding Ethernet support. Backward compatibility preserves your investment and allows a smooth transition from a serial based SCADA infrastructure to IP/Ethernet without disrupting day-to-day operations.

Security Features

The MDS SD Series contains security features that provide security controls enabling system administrators to partially meet requirements of modern security guidelines, however, the security features in the MDS SD Series are not sufficient to support NERC CIP, NIST SP800-82, NISTIR 7628, or FIPS 140-2 guidelines.

Key features include:

- 128-bit AES encryption to provide confidentiality of traffic on both the data and management channels
- User account passwords to limit access to modifying the device
- Logical data separation using VLANs to limit access to network traffic across the shared RF (radio frequency) network
- Redundant firmware images and firmware packages with CRCs to help mitigate corruption of data during a firmware update
- Management and console interfaces can be enabled/disabled as needed to limit access to modifying the device

When operating in transparent mode in an x710 network, the SD radio matches the security of the x710 device. Users who are utilizing SD radios in an x710 network that require data encryption must utilize an external device, such as an upgraded PLC/RTU or encryption device such as SCADAcrypt.

MDS ORBIT PLATFORM

The MDS Orbit Platform is a next generation wireless communications solution integrating a range of technologies, from public cellular to private licensed and unlicensed spectrum, supporting customers' needs for secure, private, public, and hybrid communications networks. Meeting the needs for functional and application flexibility and ease of use, the MDS Orbit Platform of products offers multiple interface options in a compact robust package, which adapts freely to indoor and outdoor environments.

Key features of the MDS Orbit Platform include:

- Optional secondary communication media: cellular, Wi-Fi, or unlicensed frequencies
- Radio failover for high availability networks
- Advanced networking with bi-directional adaptive modulation and quality of service

- Patented Media Access Control (MAC)
- Dynamic routing

Security Features

A foundational building block for the MDS Orbit Platform is security, a core competency area for GE Vernova and a critical consideration for evaluating wireless communications systems.

The MDS Orbit Platform contains sufficient security controls that enable a system administrator to meet their obligations under NERC CIP, NIST SP800-82, NISTIR 7628, and FIPS 140-2. The next few sections provide details of the MDS Orbit Platform security controls and are discussed in three categories: securing the network, the device, and user access.

Securing the network

Securing the network ensures that only approved devices are permitted on the network, that only valid traffic flows over the network, that the integrity of transmitted data is maintained, and that the transmitted data is kept confidential.

SECURITY FEATURE	DESCRIPTION
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 (refer to Figure 2). The MDS Orbit Platform's VPN client has been successfully integrated with Juniper, Palo Alto, and Cisco VPN servers. Fig. 2: An example of the use of VPN tunnels to separate and secure multiple traffic streams IPsec VPN
Device Authentication	To ensure only legitimate devices connect and use the network, the MDS Orbit Platform uses device authentication through X.509 digital certificates during EAP-TLS authentication to prove identity.
Certificate Management	Orbit supports X.509 digital certificates in Distinguished Encoding Rules (DER) and Privacy Enhanced Mail (PEM) format that are provisioned and automatically renewed through Simple Certificate Enrollment Protocol (SCEP). Additionally, Orbit supports certificates generated by a multi-tier Public Key Infrastructure (PKI) that may include Root, Intermediate, and Issuing CAs. The use of digital certificates provides cryptographically strong identification of devices while the use of SCEP automates the provisioning process and reduces human error.
Over-the-Air Encryption	Enables the encryption of 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 so that there is a single repository of user accounts to manage.
Firewall	The MDS Orbit Platform's on-board firewall is highly configurable by the user and employs Stateful Packet Inspection (SPI). SPI allows for dynamic Transmission Control Protocol or TCP-based connections that are used in many applications.
802.1x Authentication	Enables only approved devices to be admitted on the Ethernet and Wi-Fi access side of the MDS Orbit Platform after a username/password challenge. Use of 802.1x authentication prevents unwanted devices from being connected to the edge of the network to gain access.
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. The use of VLANs allows for network traffic to be kept separated, to minimize broadcast domains, and allow for various policies to be applied to each traffic flow.

Securing the device

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

SECURITY FEATURE	DESCRIPTION
Secure Device Management	The MDS Orbit Platform provides multiple options for secure device management including Secure web / HTTPS, SNMP v3, SSH command line interface (CLI), and NETCONF with YANG models. Device management features include: • System restore points for configuration rollback • Local event logging and event forwarding via syslog client, SNMP traps, and NETCONF notifications • Secure event reporting for syslog-over-TLS (Transport Layer Security) • User-defined configuration via scripts • Time synchronization via Network Time Protocol (NTP) client
Logical & Physical Port Disable	Logical and physical interface ports can be individually enabled/disabled as needed. This can be done through any of the device's user interfaces such as web or SSH, and can be done locally or remotely.
Tamper Detect Magnetometer	Movement in any axis or rotation is detected by continuously measuring the electromagnetic field around the MDS Orbit Platform. When movement is detected, the device moves to an alarm state and sends out an alert message via SNMP trap and syslog.
Digitally Signed Firmware	The MDS Orbit Platform employs a boot security mechanism to ensure that it only executes authentic firmware. This mechanism ensures that the device only runs firmware that has been created and distributed by GE Vernova.
Secure Firmware Updates	The MDS Orbit Platform supports two firmware images to ensure a device does not go offline due to a failed download.

Securing user access

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

| SECURITY FEATURE	DESCRIPTION
User Accounts	Username / password login is required for device management interfaces. An automatic lockout occurs after a user-defined number of consecutive failed login attempts.
Role Based Access Control	Three user levels (operator, technician, admin) are available, with increasing levels of read, write, and execute privileges.
Radius/AAA	In order to integrate with enterprise account control, 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 Role-Based Access Control (RBAC) roles to limit user access to only what they require to perform their function.
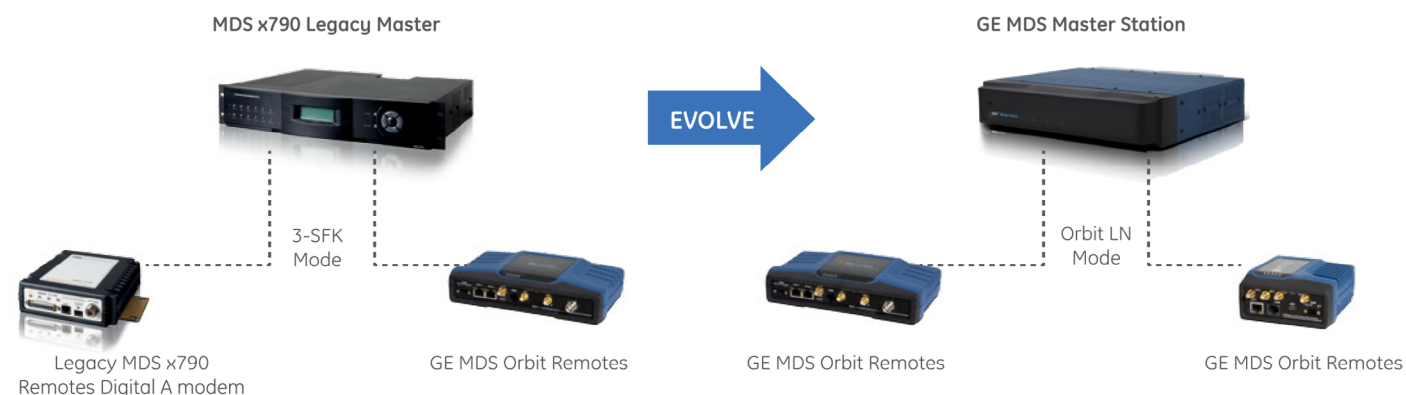
Figure 3: Backwards compatibility firmware in the GE Vernova MDS Orbit remote, allowing x710 networks to migrate to the MDS Orbit Platform through the legacy Master Station.
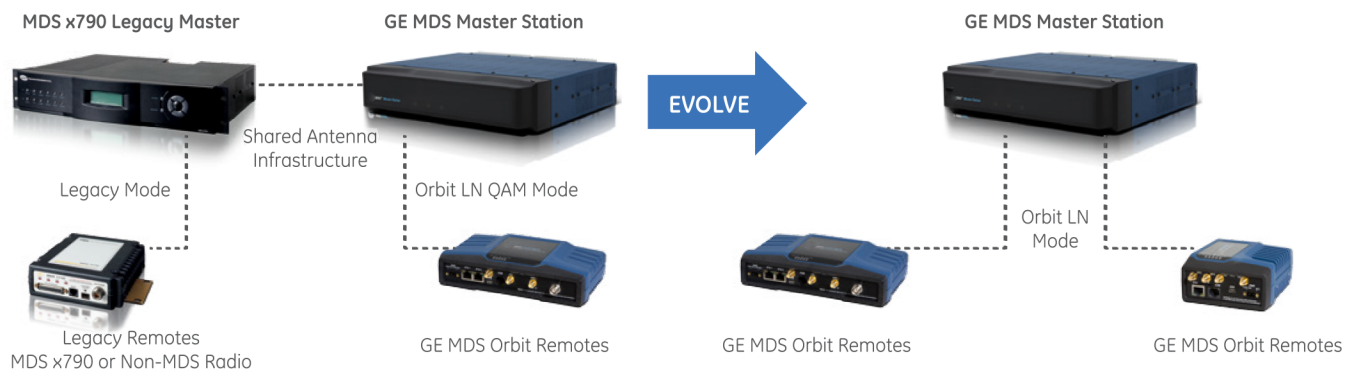
Figure 4: Co-Existence through the GE Vernova MDS Master Station with evolution technology allowing x710, SD, or other licensed frequency equipment to immediately co-exist with the MDS Orbit Platform remotes.

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:
www.gegridsolutions.com/Communications/catalog/MDSOrbit.htm

View and interact with our Interactive MDS Orbit Platform explorer online:
https://library.grid.gevernova.com/industrial-wireless/mds-orbit-explorer

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

GE VERNOVA