A White Paper from the Experts
in Business-Critical Continuity™

# *Securely Deliver Remote Monitoring and Service to Critical Systems*

EMERSON™
Network Power

## Executive Summary

As a leading equipment manufacturer of critical infrastructure solutions for the data center, Emerson Network Power understands continued operation and availability of power and cooling components is crucial to enterprises' business-critical processes.

Enterprises seeking to improve the availability of business-critical systems can now utilize the Internet to dynamically control service access into their protected networks, while still shielding their assets from ongoing security threats.

Through a partnership with ILS Technology, Emerson Network Power has pioneered the use of Internet technology to create the Virtual Ntegrity Infrastructure (VNI).

VNI allows Emerson Network Power to deliver robust remote monitoring and maintenance services of critical systems in order to provide for early detection and faster response to problems that could affect the availability of business-critical systems.

This white paper describes how this service is delivered with particular focus on Network Security of VNI.

## Introduction

The Emerson Network Power VNI solution consists of three components that work together to create a unique, policy-based Secure Connection between the Emerson Network Power command center and customer location.

Virtual Ntegrity Gateway - Compact hardware appliance placed within the enterprise private network or within a DMZ that collects information from devices being monitored and provides remote access to devices being managed.

Virtual Ntegrity Administrator - Server located at the Emerson Network Power High Availability Response Center (HARC) that monitors information reported from the Virtual Ntegrity Gateways at enterprise locations, and dynamically applies rules and policies upon remote access requests (Figure 1).

Virtual Ntegrity Manager - Server located at Emerson Network Power High Availability Response Center accepts mutually consented Secure Connection between an Emerson Network Power device on the enterprise network and a specially trained Emerson Network Power Customer Engineer. Upon completion of remote access needs, all policies and rules are removed leaving no open path for security vulnerability.

## Secure Proactive Monitoring

**Figure 1. Customer engineers monitor information at the Emerson Network Power High Availability Response Center.**

VNI enables Emerson Network Power to utilize the Internet as an efficient service delivery transport infrastructure to perform advanced proactive monitoring and on-demand management access for remote critical infrastructure devices located on our customers' networks. From the end customer's perspective, VNI removes the cost, complexity, security, and compliance concerns associated with legacy remote connectivity methods such as Dial-up, Leased Lines or VPNs, while allowing our customers to receive critical infrastructure support services without any changes to their network security configurations and practices.

***VNI enables Emerson Network Power to utilize the Internet as an efficient service delivery transport infrastructure to perform advanced proactive monitoring and on-demand management access for remote critical infrastructure devices.***

As part of a VNI installation, a compact hardware appliance called the Virtual Ntegrity Gateway (VNG) is installed on the customer's network. The VNG can be placed on the private network or DMZ. The VNG (Figure 2) functions as the aggregation point for all data monitoring. It is also the local termination point for any on-demand remote device connection sessions initiated by Emerson Network Power's customer engineers.

The VNG provides a unique method to assure security to the enterprise network for both proactive monitoring and on-demand network device access. It does this by utilizing a "push" method where all communications are securely initiated and driven from the VNG and sent to its associated VNI collection application located in the Emerson Network Power HARC. This allows for remote monitoring without the concern of security

*For proactive remote monitoring, the VNG will continuously monitor the health of specific predefined devices on the enterprise network, and send its information via an encrypted outbound-initiated SSL heartbeat back to the HARC once a minute.*

vulnerability due to inbound holes placed in firewalls between the enterprise network and the Emerson Network Power HARC.

A VNG utilizes standard Secure Sockets Layer (SSL) technology as the connectivity component of its "push" functionality. Two SSL connections are established outbound from a VNG to the HARC.

- A periodic "heartbeat" used for the delivery of proactive monitoring information,
- A lightweight carrier tunnel called a VNIpathway used for the remote device connectivity transport.

For proactive remote monitoring, the VNG will continuously monitor the health of specific predefined devices on the enterprise network, and send its information via an encrypted outbound-initiated SSL heartbeat back to the HARC once a minute. Upon delivery confirmation of the heartbeat, the SSL session is completely removed until the next scheduled update.

Heartbeats contain managed device status information that the VNG collected such as a ping or port check. Heartbeats can also include SNMP traps that the VNG will relay from the managed device back to the Emerson Network Power Network Management System.

**Figure 2. Liebert Virtual Ntegrity Gateway (VNG) enables a set of services that will enhance the availability of mission-critical equipment infrastructure, while ensuring the security of the network.**

## Secure Remote Device Connectivity

In the event an authorized Emerson Network Power customer engineer needs to remotely access a monitored device to perform maintenance or repair, the remote device connectivity functionality of VNI allows the engineer to setup an on-demand and secure Internet Protocol security (IPsec)-based session to the target device from the HARC.

Similar to VNI's status heartbeats, remote device connections are initiated by the VNG, again requiring no open inbound holes in the firewall of the enterprise network, and traverse the SSL-based VNI pathway tunnel which provides an additional layer of encryption to each session.

Each remote device connection has unique dynamic routing policies and rules that lockdown the session between the target device and the authenticated engineer eliminating the access risk to unauthorized network devices on the enterprise network.

Upon completion of a remote device management connection session, closure of the connection will automatically remove these unique session rules and policies that were assigned from both end points, leaving no risk for reuse by man-in-the-middle attacks.

This closed architecture assures customers that visibility and access to their critical network elements is restricted only to authorized Emerson Network Power personnel.

## Traceability and Audit Trail

The Emerson Network Power VNI assists customers in meeting their regulatory compliance requirements. Every session is logged, providing for an audit trail of who, where, what, and when a remote session was performed. This assures that both the enterprise being monitored and Emerson

Network Power have information transfer traceability to meet customers internal and external audit requirements.

## Security Standards

VNI uses standard, proven protocols to ensure the highest level of end-to-end security and authentication. SSL is used to encrypt and transport the VNI heartbeats and IPsec-based remote device connections between the VNG and the HARC.

The utilization of IPsec over SSL provides for authentication and encryption at the IP level. Additionally, the dual channel closed system (SSL and IPsec) combination guarantees the authenticity of the connection and a higher level of security assurance.

*VNI incorporates the following security standards and policies:*

Encapsulating Security Payload (ESP) - The encryption in the ESP encapsulation protocol is done with block cipher. VNI's block cipher is 3DES.

Internet Key Exchange (IKE) - The IKE protocol sets up IPsec connections over the SSL VNI pathway after negotiating appropriate parameters. VNI distributes a unique key with each session, eliminating risk of reuse.

Two-Phase IKE Negotiations - VNI uses a custom matched pair system using 2192 bits per key.

## Firewall Provisioning

VNI only requires that TCP443 is open outbound from the customer location, and is typically pre-configured by customers for outbound access to support existing web services and applications. No inbound firewall ports are necessary for this solution.

## Conclusion

The Emerson Network Power Virtual Ntegrity Infrastructure provides a unique, secure, remote monitoring and access solution that utilizes the best of today's remote management technologies resulting in a higher level of customer service and satisfaction, while eliminating the security concerns of remote monitoring services.

**Emerson Network Power**
1050 Dearborn Drive
P.O. Box 29186
Columbus, Ohio 43229
800.877.9222 (U.S. & Canada Only)
614.888.0246 (Outside U.S.)
Fax: 614.841.6022

EmersonNetworkPower.com
Liebert.com

While every precaution has been taken to ensure accuracy and completeness in this literature, Liebert Corporation assumes no responsibility, and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Specifications subject to change without notice.