DeltaV™ System Health Monitoring Networking and Security

Introduction

Emerson's DeltaV™ System Health Monitoring service enables you to proactively maintain the health of your control system assets with continuous automated health monitoring. An on-site monitoring appliance powers the System Health Monitoring service, continuously checking critical health information of the integrated DeltaV distributed control system (DCS) 24x7x365. Detected alert conditions are sent via email to Emerson, quickly analyzed, and then communicated to the local Emerson service experts and site maintenance personnel with appropriate recommended mitigating actions.

When deploying the System Health Monitoring on-site monitoring appliance, there are some networking and security considerations that need to be accounted for. This document provides the detailed information to properly deploy the on-site monitoring appliance securely and ensure adherence to the best practices for DeltaV DCS cybersecurity.

Network Architecture

- The following diagram represents the architecture integration for the System Health Monitor (SHM) appliance. The architecture emphasizes a layered secure model and complies with Emerson's whitepaper "Best Practices for DeltaV Cybersecurity."
- The minimum connectivity requirements for the SHM appliance are a connection to the L2 & L2.5 LANs.
  - The SHM appliance contains four Network Interface connections supporting 10/100/1000 MB.

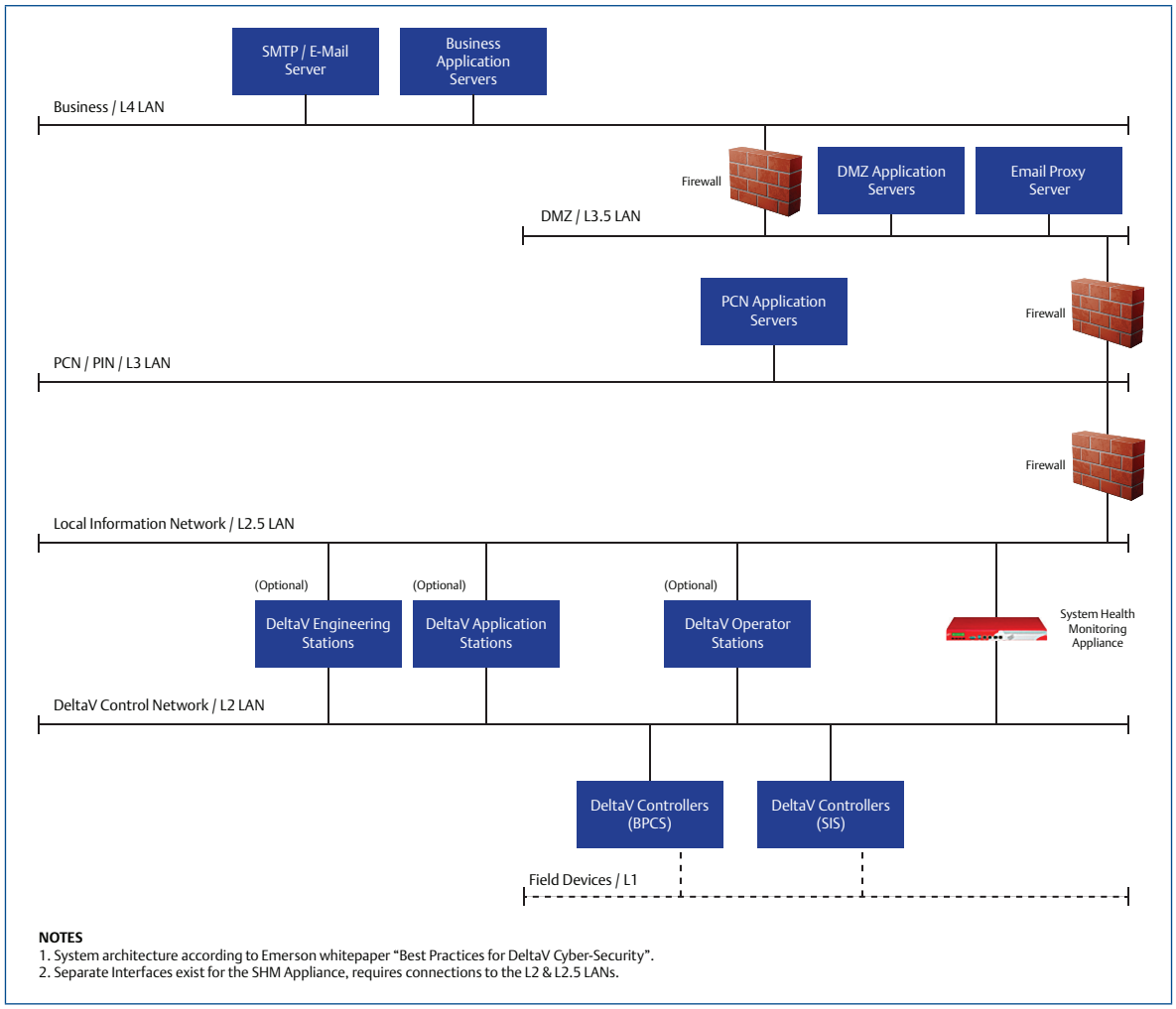

Figure 1 – Typical DeltaV Network Architecture with SHM.

Communication Services

3.1 Applications

There is only one application service on the SHM appliance which originates from the L2.5 LAN. This is the mail service notification, SMTP, which is programmed to send informational messages to the local site Mail Server.

3.2 Protocol Services

Mail notification protocol services are as follows:

- Application Layer Protocol = SMTP
- Version = Standard SMTP, non-binding
- Transport Layer Protocol = Transmission Control Protocol, TCP
- Transport Layer Port = 25

3.3 Directional Communication Requirements

All SMTP communications originate from the SHM appliance. Therefore, unidirectional communications can be assumed for Firewall security policy configurations. Because TCP is utilized for Transport Services, acknowledgement exchange messages are expected which require communication responses back to the SHM appliance. Such communications are standard and do not warrant additional firewall security policies.

3.4 Communication End-Point

The only End-Point the SHM appliance communicates with is the site Email Server (or the site Email Proxy server if one is deployed). The intended SMTP message is ultimately relayed to Emerson's Remote Monitoring Center via the site Email Server.

3.5 Communication Frequency and Loading

By design, the SHM monitor polls diagnostic data on the L2 network at specified intervals for each node to balance overall loading. If an alert condition is present, the SHM appliance generates an SMTP message for each alert. The following loading characteristics are considered:

- 1 System Alert = 1 SMTP message
- Messages are generated by exception
- Maximum messages per second = 2
- Persistent abnormal conditions do not generate repeated SMTP messages. i.e. 1 every 24hrs.
- Message content, payload for network packets, are generally less than 1k in size and will be less than the maximum frame size, 1514 bytes.
- If filtering or throttling is required for SMTP messages, Emerson anticipates the site Mail Server configurations would facilitate such actions. However, we do not anticipate this as a fundamental configuration requirement.

3.6 Security

The following security features apply to the SHM appliance:

- SMTP message content contains diagnostic data, exclusively, for the control system.
- SMTP messages, by default, do not require encryption services.
  - As required, SMTP encryption can be enforced from the site Mail Server to Emerson's Remote Monitoring Center.

- Outgoing email sent to Emerson's Remote Monitoring Center does not include:
  - Server IP Address
  - Domain Name
- SMTP User Account requirements can be configured with either of the following options:
  - Anonymous
  - User Account Enforcement
- An L2 Domain Service Account is required to facilitate application services for the SHM appliance.
  - This account only applies to the L2 Domain.
- Network Management access to the SHM appliance is via HTTPS with configurable user account access.
  - Accessible via L2 & L2.5 LANs
- Remote Access, RDP or otherwise, is not possible to the SHM appliance. Therefore, Emerson does not require remote access to the appliance.
- Firewall security policy is INSIDE to OUTSIDE to facilitate SMTP, TCP port 25
  - There are no OUTSIDE to INSIDE Firewall security policies required to be configured for the SHM appliance.

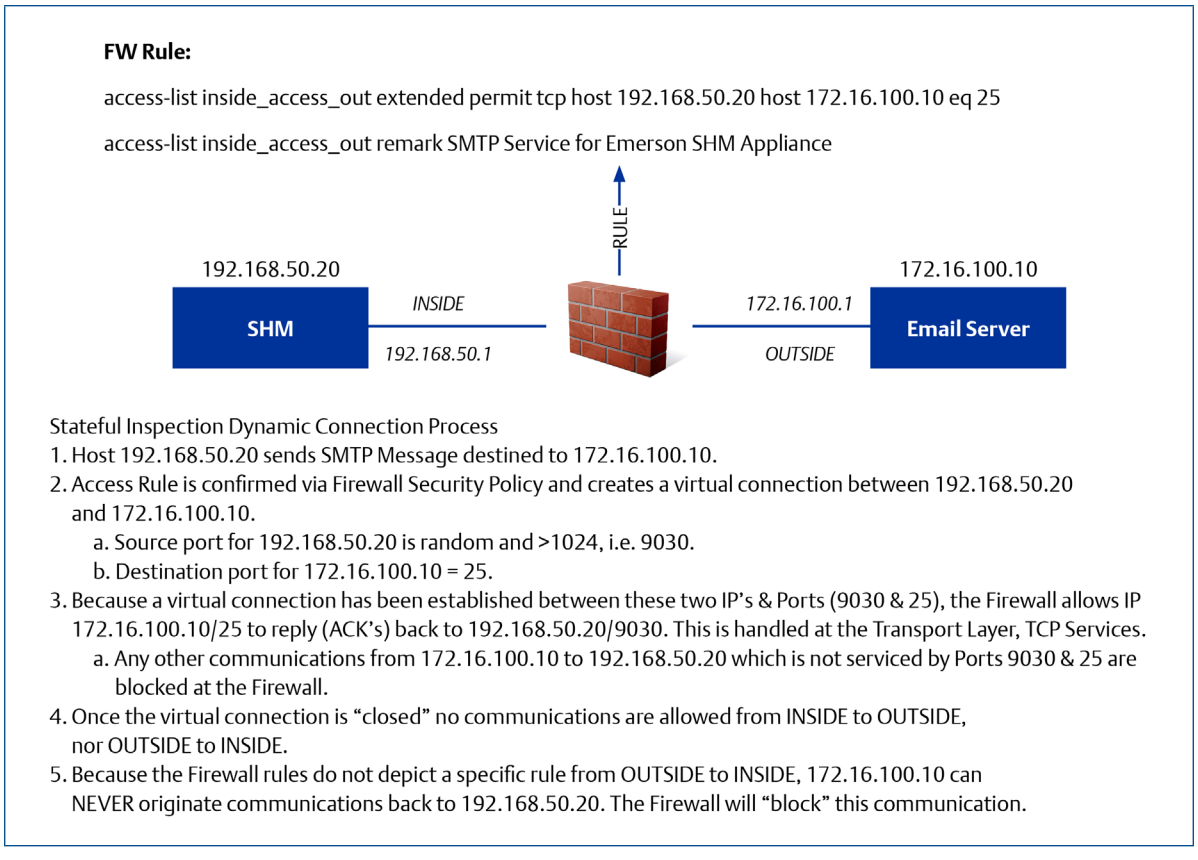

Figure 2 – Communication details for SHM.

DeltaV System Health Monitoring Networking and Security

White Paper
May 2018

This page intentionally left blank.

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
+65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/shm