BY RICHARD DEDZINS, PFIZER BIOTECH, &
MATT JAMES, EMERSON PROCESS MANAGEMENT

# — CONTINUOUS SHM ASSURES —
# PFIZER'S AUTOMATION SYSTEM PERFORMANCE

## AUTOMATION SYSTEM HEALTH NEEDS TO BE CONTINUOUSLY TRANSPARENT; FORTUNATELY EMERSON HAS AN APP FOR THAT

**OVER THE** past 20 years, it has become an essential business requirement for process manufacturing plants to use digital automation systems to compete in a global economy. During this time period, the reliability of electronic equipment has also significantly improved. As a result, management has often redirected limited plant resources to perform higher value-added continuous improvement projects, with less time being allocated to manage the automation system. Today's lean manufacturing environment provides limited technical expertise and reduced staffing levels. In turn, some plant site's awareness and processes are not fully optimized for reacting to disruptive events or unexpected failure(s) in their automation system. Even when a plant is in full regulatory compliance, any loss in monitoring and control functionality while diagnosing a problem increases risk to the plant's overall site health, safety, product and the environment (HSE).

To address these challenges, many plant sites are investing in an affordable system health monitoring (SHM) solution that continuously monitors the health and fitness of the automation system, detects trends and uses diagnostic best practices to proactively notify plant staff to take corrective action and avoid unexpected failure(s). As a result, scarce plant resources can be directed to work on higher priority projects without having to worry about handling an unexpected system failure.

### WHY IS MONITORING A CHALLENGE?

Retaining experienced automation professionals to work at plant sites is often challenging for many reasons. Consistently finding the appropriate level of expertise in all plant locations around the world can be equally difficult. The task of managing an automation system is often delegated to a system administrator, who is responsible for the operation and maintenance of the system.

With continuous improvements in automation technology, it's often technically difficult and administratively challenging for a systems administrator to keep the hardware and software revision levels up to date and within allowable budget and production schedules. Obtaining around-the-clock, continuous coverage to monitor the automation system is not only tough, it's often cost prohibitive. Thus, with limited expertise and available time, the amount of resources available for monitoring the automation system are scarce and must be used wisely.

All automation systems offer maintenance and diagnostic displays to indicate operational status of the system and generate alarms in case of failures. However, the type of information provided by the automation system is typically after the fact, that is, after the failure event. Visibility to information leading up to the event(s) that caused the system failure is often not readily available. The response time to react to the system failure may be longer than desired since engineering staff must conduct an investigation to determine root cause and implement the necessary corrective action.

### INCREASING SYSTEM RELIABILITY, RELIABLY

Plant staff at Pfizer's Biopharma facility located in Sanford, North Carolina, faced a challenge of increasing automation system reliability, availability and production uptime, while reducing infrastructure support costs. To address these issues, the plant staff explored industry best practices for shifting monitoring activities from after-the-fact or reactive to implementing proactive processes that improve automation system availability and avoid unscheduled downtime. Secondly, the plant staff explored options for an affordable 24x7x365 system health monitoring solution that would centralize the data collection while providing maximum value for the investment.

## DEVELOPING SHM REQUIREMENTS

While there are many commercially available IT-related network health monitoring systems on the market, the SHM solution Pfizer adopted was tailored to specifically monitor a DeltaV distributed control system infrastructure. Requirements for the SHM solution included automatically checking health information of all automation system components including controllers, servers, workstations and safety controllers. Firewalls, cyber security protection devices, uninterruptible power systems and other non-automation system servers and workstations connected to the automation network were also included. The SHM solution had to provide trending and automated diagnostics to help leverage best practices and shift maintenance practices from a reactive to proactive stance. Pfizer expected the SHM solution to deliver a centralized, consolidated monitoring service for the entire plant. The SHM service also needed to integrate and be complementary to existing remote monitoring services.

## IMPLEMENTATION TIME

Within a year of addressing the challenge and exploring options, the plant staff partnered with the digital automation systems supplier and its local service provider to implement the SHM solution at the site. Figure 1 reveals an architecture diagram of the SHM system. The SHM monitoring device is coupled to the control network and to the plant-wide information network behind a corpo-

rate firewall. An SHM monitoring device automatically checks health information of any network device connected to the control network.

Figure 2 illustrates the SHM monitoring device based centralized health monitoring of network devices. The SHM health monitoring solution centralizes the data collection function by monitoring network devices or nodes including DCS controllers, application servers and workstations, safety instrumented system (SIS) controllers, switches, firewalls, UPS's, and non-DCS PCs, servers and workstations (e.g., data historians, batch servers, operator stations, and similar devices).

Referring to Figures 1 and 2, the SHM monitoring device is configured to monitor detailed parameters indicative of the health, integrity and performance of the automation system. Server health checks may include monitoring of availability status, hard disk space utilization and performance, CPU and memory usage. Network switch health monitoring may include availability status, redundant power supply status, temperature, communications status, network communication error rates, and number of packets/second sent and received (See Figure 3). Controller health checks may include monitoring of availability status, CPU usage, availability of free memory, and controller redundancy status. Additional details of the device level parameters that offer a quick overview of the system health are shown in Figures 4 and 5.



Mail Server

Remote Monitoing Center

Plant LAN

SHM Monitoring Device

Application Station
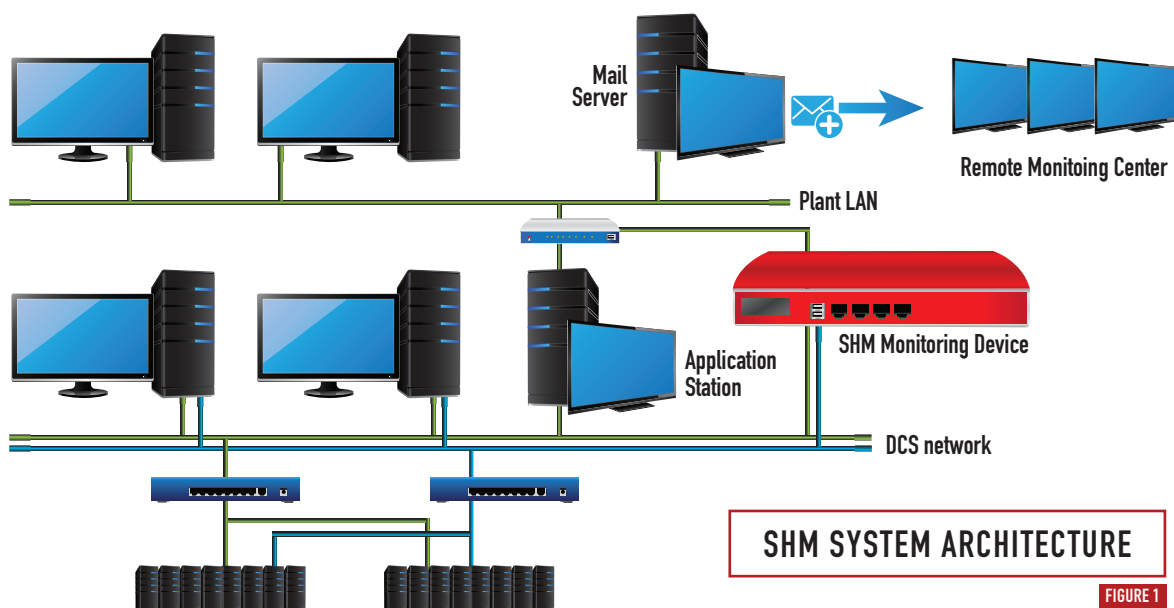
DCS network

## SHM SYSTEM ARCHITECTURE

FIGURE 1

## A PROACTIVE FUTURE

Parameters being monitored by SHM are typically useful in performing proactive analysis of future events. For example, repeated ping failures may indicate an insecure connection and may require re-termination of a cable to avoid a network failure. Since the SHM device is continuously monitoring health of the automated system on a continuous non-stop basis, it eliminates the need for site maintenance staff to perform periodic, manual health checks via internal system diagnostic tools. Any deviation conditions are automatically detected and reported.

An increased level of system security is also a feature of Pfizer's SHM. Continuous monitoring of control system servers, smart firewalls and smart switches supports effective cybersecurity protection measures by assuring these devices are online and operational. SHM is integrated with Emerson's Guardian Support service to improve decision making. The support service requires up-to-date system information in order to provide the site staff with current system-specific actionable information. The SHM enables frequent and automatic collection of automation system related profile data and securely emails it to Guardian. Any changes made to the system content are automatically checked against previously published critical KBAs for potential conflicts. The integration between SHM and s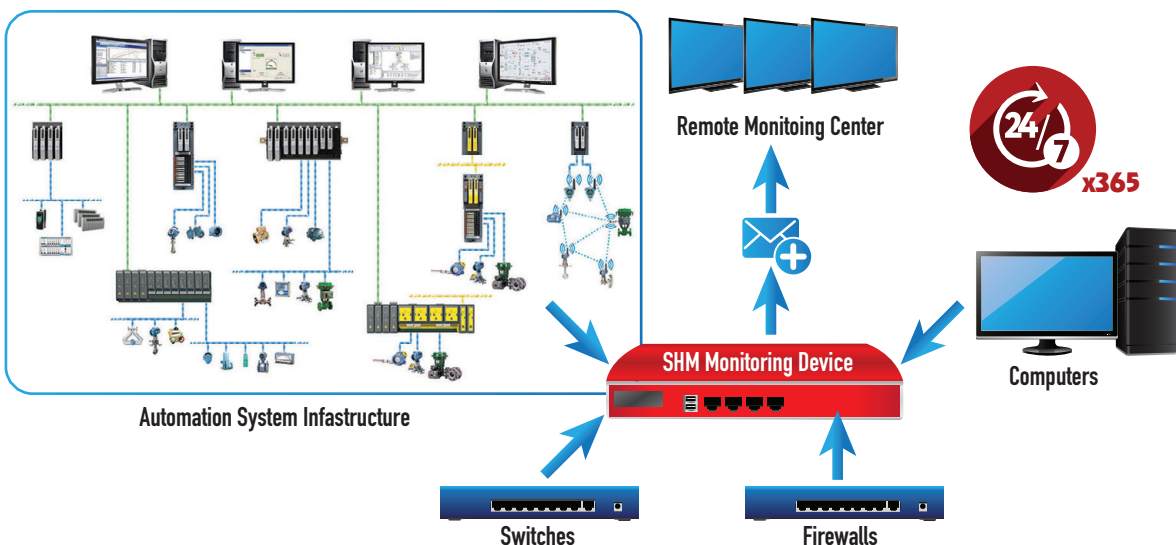upport service ensures the latest safety and security updates for the automation system, and applicable operating systems are always readily available to the site staff for download.

Figure 3 illustrates a SHM solution workflow from an initial health alert detection, to analysis and diagnosis of root cause, to resolution of the problem. The SHM solution sends notifications and alerts via email to the automation system supplier's Remote Monitoring Center (RMC) that operates continuously. The notifications are automatically sent by the SHM device when any observed health parameter exceeds expected or normal operating values. The automation supplier provides pre-defined templates with recommended limits rooted in best practices. These limits can also be configured as needed for site-specific conditions. The SHM device sends a periodic heartbeat message to the RMC to indicate that it is operating normally. The RMC staff includes dedicated resources and subject matter experts that use software tools to monitor and analyze real-time alerts from the plant.

Diagnostic data related to the initial alert message is analyzed by the experts at the RMC to determine the root cause(s) of the problem and identify a potential solution. After that, RMC staff collaborates with local service experts and site engineering personnel to recommend an action plan and ensure any required corrective actions are taken. Thus, SHM proactively notifies plant staff to

## CENTRALIZED, CONTINUOUS SYSTEM HEALTH MONITORING

FIGURE 2



Automation System Infastructure

Remote Monitoing Center

24/7 x365

SHM Monitoring Device

Computers

Switches

Firewalls

make corrective changes well before the initial alert notification escalates into a system failure. The RMC staff can monitor multiple plant sites from a central location on a continuous and concurrent basis.

Figures 4 and 5 are illustrative display screens available at the monitored site for real-time monitoring of current health, integrity and performance of the automation system. SHM displays can provide information about the automation system at an overview level, an individual network device level, or at an individual parameter level within each device.

With a simple observation of the colors displayed on a screen, any authorized user can intuitively and instantly ascertain the operational status of the automation system. A green indicates normal operation, a yellow implies caution or warning, a blue indicates a communication link problem that may require reconfiguration between a sender and receiver device, and a red indicates a critical alert condition. All displays contain hyperlinks that may be used to call up other displays for further detail.
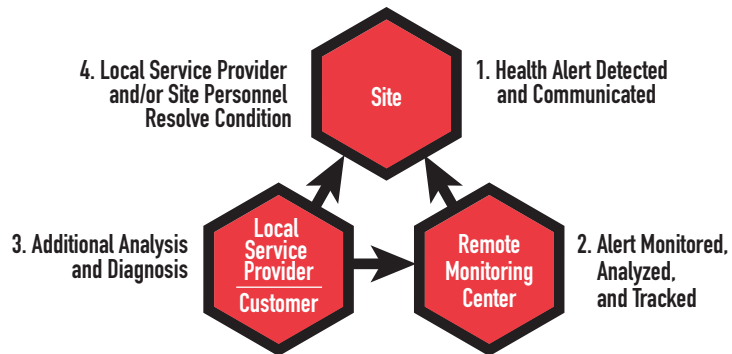
Figure 6 illustrates trend data collected on any analog variable in the system. Historical data related to performance of each network device and analog parameters within each device connected to the control network may be collected and trended without utilizing data historian tags and incurring additional data historian license fees. The site engineering staff and/or the local service provider often use the trend data to perform root cause analysis that can link an alert event with a root cause, such as a controller running on low memory.

## CHALLENGES ENCOUNTERED AT THE SANFORD SITE DURING IMPLEMENTATION

Similar to configuring an automation system, a first step in configuring the SHM system is to identify all network devices connected to the control network. The SHM solution provides a utility to read configuration files of the automation system and convert them to text. The text file is then modified by the system administrator and imported into the SHM device. The SHM device can monitor any device or node on the control network that has an IP address and has a communication protocol



### SYSTEM HEALTH MONITORING SERVICE WORKFLOW

FIGURE 3

4. Local Service Provider and/or Site Personnel Resolve Condition

Site

1. Health Alert Detected and Communicated

3. Additional Analysis and Diagnosis

Local Service Provider / Customer

Remote Monitoring Center
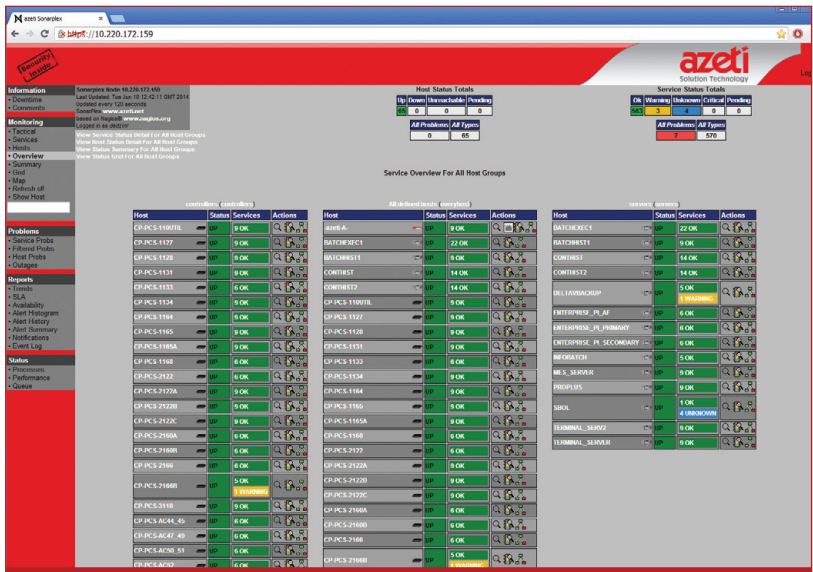
2. Alert Monitored, Analyzed, and Tracked

supported by the SHM device.

Initial challenges at the Sanford site included limited SHM device installation and configuration documentation, along with limited local expertise on technical issues related to the SHM solution. This partially stemmed from early Pfizer adoption of the initial SHM release. The most recent SHM release now addresses these challenges, and installation manuals and overall guidance documents have significantly streamlined the deployment process. The SHM monitoring appliance is configured to send SMTP messages to the mail server (through the control system layer firewall) at the plant site. The plant site mail server then sends out health alerts by exception via email to the Remote Monitoring Center.

Once the initial SHM system was up and running, the next challenge was to better manage the large quantity of email alerts originally being generated. Similar to the need for better management of the operator alarming function in an automation system, a tuning effort is needed to focus on allowable tolerance levels for each SHM measurement and eliminate nuisance alarms. Today, assessing the health of the automation system is very simple — no email alerts received from SHM means there is a high degree of confidence that everything is functioning normally. This allows plant staff to focus on more value added activities that have a direct impact on the business.

### SHM SOLUTION DELIVERS RESULTS

The system health monitoring service adds value by continuously monitoring performance data used
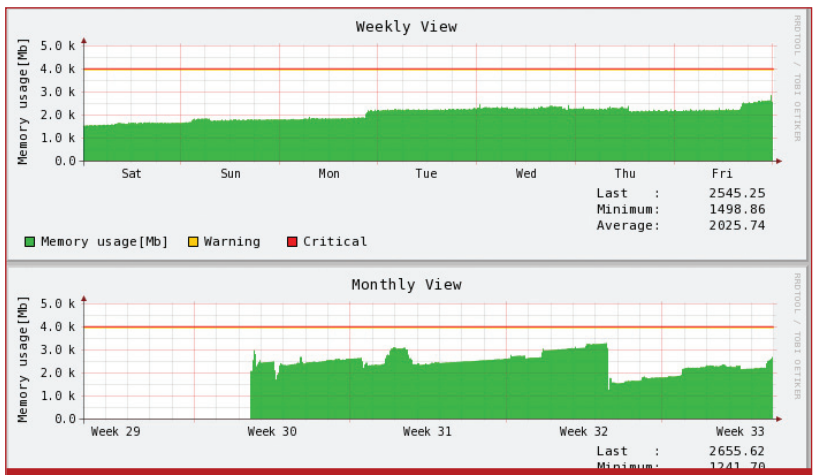
**SYSTEM OVERVIEW DISPLAY**  FIGURE 4



**NETWORK DEVICE DETAIL DISPLAY**  FIGURE 5



**TREND DISPLAY**  FIGURE 6

as an indicator of the health of the automation system. The SHM solution includes a proactive monitoring service that alerts plant and local service provider staff to take corrective action that preempts the occurrence of a potential failure and avoids unexpected downtime. For example, since initial installation, the SHM monitoring device has already identified several significant conditions at Pfizer including ping failure(s) due to a loose connector, low controller memory during specific production operations, network time protocol offset drifts during backup operations and an unsecured primary switch fiber connection. SHM's proactive monitoring and alert notifications enabled site personnel to address these conditions before they became major issues, which resulted in optimal system availability.

The SHM service supports centralized operations as well as the affordable monitoring and managing of all automation systems at the Sanford site without a large upfront investment in capital and staff resources necessary to build and maintain a site-specific operations monitoring center. Thus, the remote monitoring center's centralized operations increased control system availability while reducing plant staff resources for continuously monitoring the health and performance of all automation systems at the site. SHM's early detection of events and proactive alert notifications also resulted in an overall process improvement and personnel efficiency gain at Sanford, which were two of the primary objectives for Pfizer for deploying SHM. Ⓟ