General Specifications

Network Healthiness Check Service
- Live Monitoring

GS 43D02T30-07EN

■ GENERAL DESCRIPTION

The Network Healthiness Check Service - Live Monitoring collects and analyzes the network traffic data without influencing the communication between the existing control systems, and detects any unusual traffic in the plant network and possible indications of potential cyber-attacks. This service provides support in maintaining the soundness of the control system throughout its lifecycle.

■ SERVICE MENU

Network Healthiness Check Service consists of a Reporting service (GS 43D02T30-06EN) and Live Monitoring service. This document describes the Live Monitoring service.

- Network Healthiness Check Service
  - Reporting (GS 43D02T30-06EN)
  - Live Monitoring ←

■ APPLICABLE NETWORKS

- Ethernet
- Vnet/IP

■ SERVICE CONTENTS

Network traffic data are collected by sensor PCs via mirror-ports located at specific switching hubs where they are recorded. The data of each sensor PC are gathered in a console PC and analyzed, viewed, and notifications send out to other systems.

Analyze: To detect unusual network packets, abnormal traffic, as well as indicate device status.

View: To visualize the live or playback network traffic data in the two- or three-dimensional modes.

Notify: To send event messages to CENTUM VP HIS, VPSRemote (GS 43D02H10-07EN), or other Network Management Systems if any unusual status is detected.

Figure 1 indicates an example of system configuration.

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

GS 43D02T30-07EN

2nd Edition Mar. 30, 2018

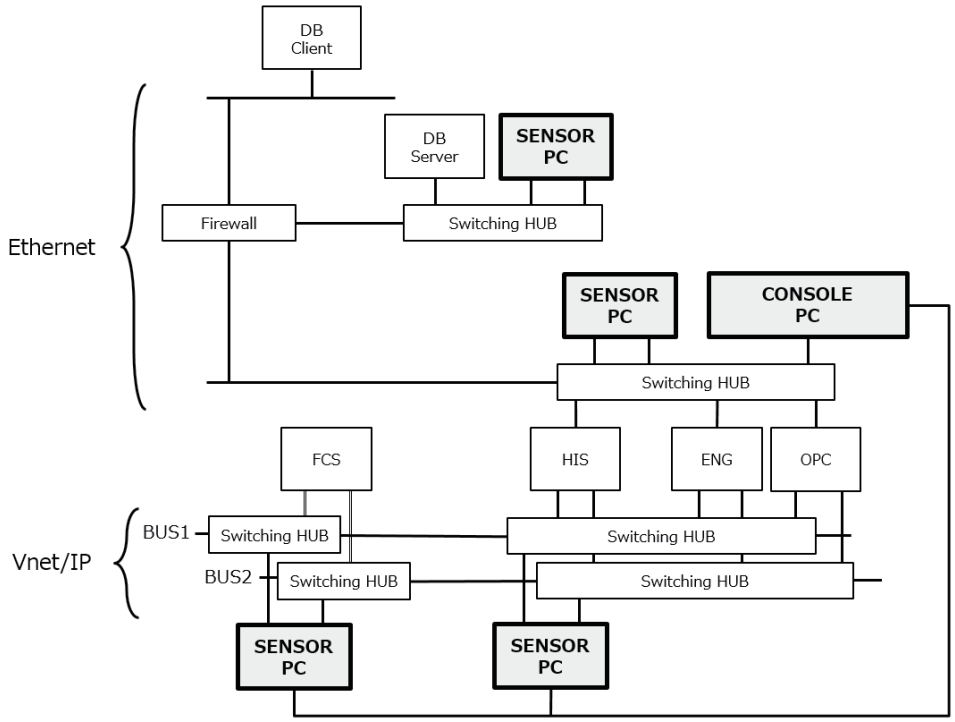

Figure1: Example of system configuration

Table 1 indicates a list of components to be installed at the site.

Table 1: System components

Name	Function	Quantity
Console PC	Analysis, Viewing, Notification	1 unit
Sensor PC	Collection, Recording	1 unit for each switching hub (Max. 32 units)

■ FUNCTIONS

This service has the following features.

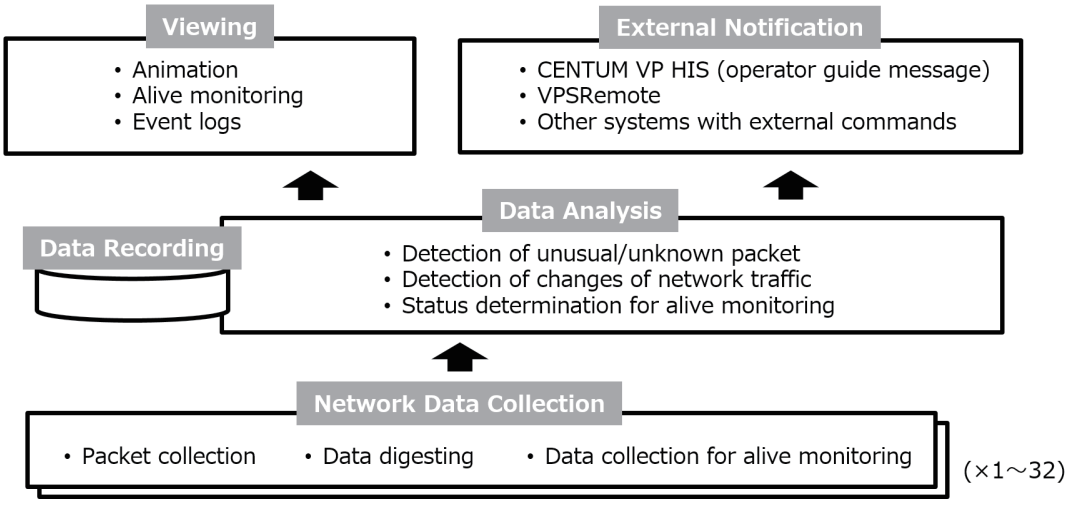

Figure 2: Functional overview

1. Functions

(1) Network Data Collection
This function collects network packet data and network information for monitoring.

- Packet collection
  Packet data are collected via a mirror-port located at a switching hub.
- Data digesting
  Network data are digested for traffic analysis and animation.
- Data collection for alive monitoring
  Response packets from target devices are collected.

(2) Data Analysis
This function detects abnormal statuses by analyzing traffic data.

- Unusual/unknown packet
  Detects network packets that are not defined in a whitelist, list of legitimate IP addresses as well as product-specific communications.
- Changes of network traffic
  Detects network traffic across pre-defined thresholds.
- Status determination for alive monitoring
  Statues (online/offline) of each device are determined based on the responses from the devices.

(3) Data Recording
This function records the data that is collected and analyzed by the Network Data Collection and Data Analysis functions.

(4) Viewing
This function displays the monitoring statuses.

- Animation
  Network packet data are represented with arcs, and every arc is drawn from a source to a destination. Each arc is given a different color based on the type of packet data. The rates of data transmission and reception are represented with color bars. The live/playback animation is available in both the two- and three-dimensional modes.
- Alive monitoring
  The status summary of monitoring devices is displayed.
- Event logs
  Statuses of each function and detected events are displayed.

(5) External Notification
This function notifies the following external systems of the detected events:

- CENTUM VP HIS (with operator guide message)
  Note: VP6H2411 Exaopc OPC Interface Package (for HIS) is required for CENTUM VP HIS.
- VPSRemote
- Other systems with external commands

2. Functional limitations

A software license in which the number of sensor PCs and license period are embedded is required to use all of the functions. If the number of sensor PCs in the network is different from the value embedded in the license or the license expires, the following functions are disabled.

- Number of sensor PCs : All functions except the Network Data Collection function
- License expiration : Viewing and External Notification functions

■ SECURITY MEASURES

The following security measures are available for the components of this service.

● IT Security Configuration

Security measures for the IT environment are implemented to defend and counter current and future security threats such as cyber terrorism.

● Implementation of Microsoft Security Updates (option)

Microsoft Security Updates required for Yokogawa products are installed to protect against intrusion or infection by malware such as a computer virus.

● Implementation and updating of antivirus software (option)

Antivirus Software for Endpoint Security Service (AV11000: GS 30A15A20-01E) is installed and its virus definition files and engine are updated periodically to protect against intrusion or infection by malware such as a computer virus.

● Virus check (option)

A dedicated software tool is used to detect whether the system has been infected by malware. The PC is removed

from the network in advance, and then the virus scan software is executed from the USB port of the PC.

* Should the system be infected by malware, the software will not automatically eliminate the malware. Instead, Yokogawa will provide consultation or propose a countermeasure.

● Software backup (option)

On the condition that the PC proves to be sound by running a virus scan, a full system backup is made and stored in a pre-arranged medium. (The backup includes the configuration information of the hard disk(s) and the OS stored on them.) Should a hard disk failure or malware infection occur, the backup will significantly reduce the recovery time.

* Yokogawa recommends that a backup be made on a periodic basis.
* A third-party backup tool and a backup medium are separately prepared by Yokogawa.

■ SYSTEM SPECIFICATIONS

Hardware and software specifications/requirements of system components are as follows.

● Console PC

Table 2: Hardware/software specifications of Console PC

Item		Details
Hardware	Selected	PC: Yokogawa Global PC YG1T5810 + Option(/N01) Display: FHD (1920 x 1080)
	Recommended	CPU: Intel Xeon Processor E5-1620 v3 Quad Core 3.50 GHz or faster Memory: 8GB or higher HDD: 1TB or larger Graphic: NVIDIA Quadro K620 or greater LAN port: 10BASE-T/100BASE-TX/1000BASE-T x 2 Display: FHD (1920 x 1080) or larger Keyboard: English or Japanese Mouse: Scroll wheel is required
OS		Windows 10 Enterprise 2016 LTSB (64bit)
Software		Yokogawa Live Monitoring Software Microsoft Visual C++ 2015 Redistributable (x64) Microsoft Visual C++ 2015 Redistributable (x86) Microsoft Visual C++ 2012 Redistributable (x86) Yokogawa OPC Client Software SnmpSharpNet

● Sensor PC

Table 3: Hardware/software specifications of Sensor PC

Item		Details
Hardware	Selected	PC: Yokogawa Global PC YG1XE2 + Option(/N01) Display: FHD (1920 x 1080) USB-HDD: 1TB/USB3.0 or larger
	Recommended	CPU: Intel Core i3-4330 Dual Core, 3.50 GHz or faster Memory: 8GB or higher HDD: 500GB or larger LAN port: 10BASE-T/100BASE-TX/1000BASE-T x 2~3 Display: FHD (1920 x 1080) or larger Keyboard: English or Japanese Mouse: Scroll wheel is required USB-HDD: 1TB/USB3.0 or larger
OS		Windows 10 Enterprise 2016 LTSB (64bit)
Software		Yokogawa Live Monitoring Software Microsoft Visual C++ 2015 Redistributable (x64) Microsoft Visual C++ 2015 Redistributable (x86) Microsoft Visual C++ 2012 Redistributable (x86) Win10pcap

●Switching HUB (for Vnet/IP)

[Model GRVSW Network Switch for Vnet/IP (GS 30A10B10-01EN)] The latest firmware and setting change are required.

■ PRECAUTIONS

Please note the following precautions regarding this service.

(1) This service is aimed at reducing potential cyber-attacks and/or any risk of unauthorized access and does not guarantee the complete detection of such attacks or risks.

(2) The software license is not provided separately from this service.

(3) We cannot provide this service if the switching hub does not have a port-mirroring function or 2 or more vacant ports. In such a case, we will replace the switching hub with another switching hub that includes the port-mirroring function at an additional cost on a timely basis according to the plant's operation plan.

(4) The customer will need to prepare adequate space for installation of the sensor PCs and the console PC and to provide power outlets for them.

■ TRADEMARKS

- All brand or product names of Yokogawa Electric Corporation in this document are trademarks or registered trademarks of Yokogawa Electric Corporation. All other company brand or product names in this document are trademarks or registered trademarks of their respective holders.