Success Story

Control System Cyber Security Service Enables Chemical Plant to Take Preventive Measures to Guard against Cyber-Attacks

Location: **Japan**
Order date: **2015**
Completion: **2015**
Industry: **Chemical**

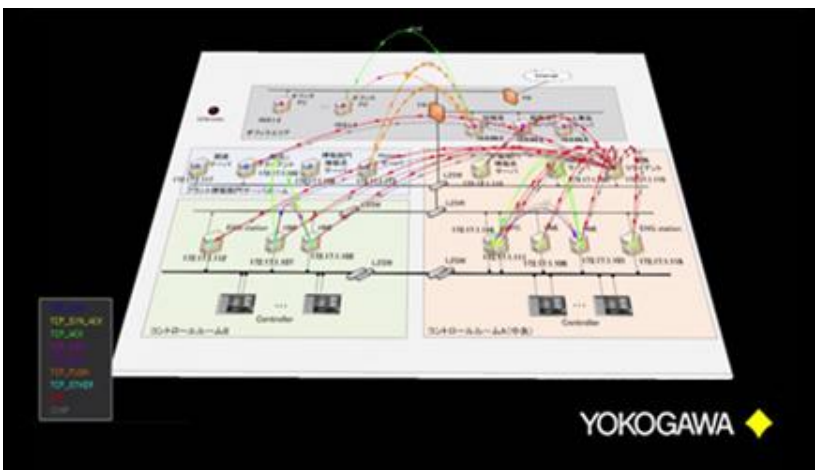
Executive Summary

This solution was provided to a chemical company that is a subsidiary of a major Japanese enterprise that does business globally. The chemical company produces a diverse range of innovative products, and its works in west Japan produces mainly styrene monomer, polyethylene, and acrylonitrile.

Cyber-attacks involving the use of malware and other means have become one of the most pressing concerns in recent years, and there is an urgent need for reliable security measures with control systems, particularly those used in critically important facilities such as power stations, gas plants, and petrochemical plants. The techniques employed in such attacks are growing increasingly sophisticated, however, and it is often no longer sufficient to rely solely on general security measures such as the use of antivirus software. Companies such as this customer in the chemical industry are aware that even minor attacks can have a major impact on their operations, and are keen to correct weaknesses in their defenses.

Using the NICTER* real-network visual analyzer (NIRVANA) that it jointly developed with the National Institute of Information and Communications Technology (NICT) and Kyoto University, Yokogawa provided this chemical company a fit-for-purpose network healthiness check service solution that helps identify deviations from normal network behaviors so that it can take appropriate preventive measures.

*NICTER: Network Incident Analysis Center for Tactical Emergency Response



Visualization of network traffic

The Challenges and the Solutions

A cyber-attack is a deliberate exploitation of a computer system or network that involves the use of malware and other means to disrupt or gain control over essential processes and access sensitive data. All critically important infrastructure like power grids, gas facilities, and water supply systems continually face the risk of cyber-attacks on web servers that can cause the shutdown or malfunction of essential systems and the theft of key information. Industrial facilities such as the chemical plant operated by our customer are also vulnerable to such attacks, and this can lead to uncertainty about a company's operations and even damage its reputation and finances. The latest tools are needed to stay one step ahead of criminals.

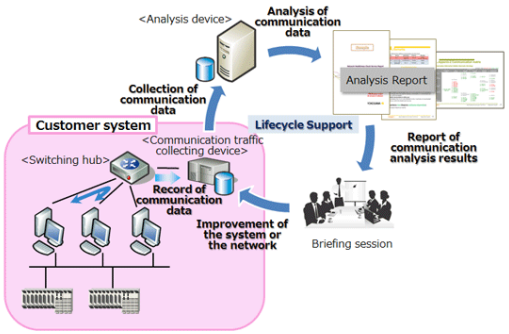
Up till now, there has been no quick way to verify whether communications between any of the elements that make up a control system as well as communications with field instruments have been compromised. One had no choice but to analyze all communications traffic, which, in addition to being very time consuming and costly, leads to disruptions that can undermine plant performance and availability.

Yokogawa has taken another tack, focusing instead on the characteristics of control system networks. Compared to general information systems, it is easier with control networks to identify when a normal state exists in communications traffic because these systems are designed and used for a specific purpose. By singling out and excluding all normal control system communications traffic, it is much easier to spot packet transfer and other network communication activities that originate from outside the system and deviate from normal traffic patterns. What makes this possible is a new technology for visualizing and analyzing control system traffic that was jointly developed by NICT, Yokogawa, and Kyoto University. This can quickly verify the integrity of communications and detect security incidents by visualizing communications traffic, collecting data on this, and analyzing it.

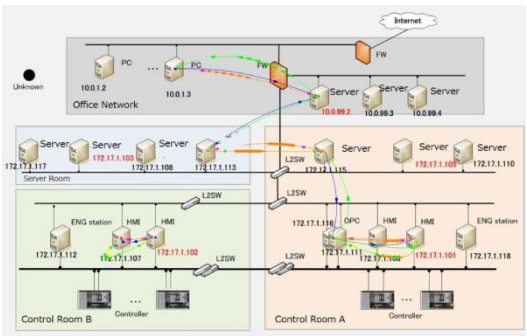
Based on this network visualization technology, Yokogawa has developed a network healthiness check service that is dedicated for use with plant control systems, an industry first* . This service eases the task of identifying abnormalities in control network communications by using a Yokogawa-prepared visualization & analysis PC to gather network data via a switching HUB mirroring function.

* Based on a September 28, 2015 Yokogawa survey

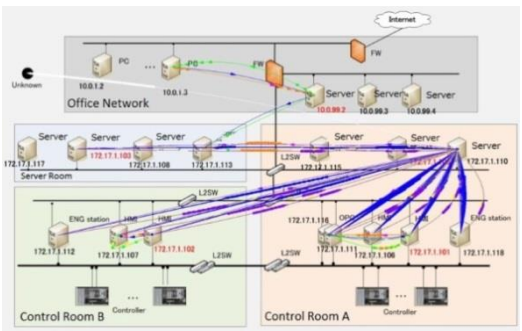
As there is no need to install detection software on each control system host (or server), this technology is easy to be introduced and does not impact control system availability. Data from the visualization & analysis PC is regularly compiled and analyzed to prepare an analysis report. With this information, measures can then be taken to counter detected risks.



The network healthiness check cycle



Normal control network communications

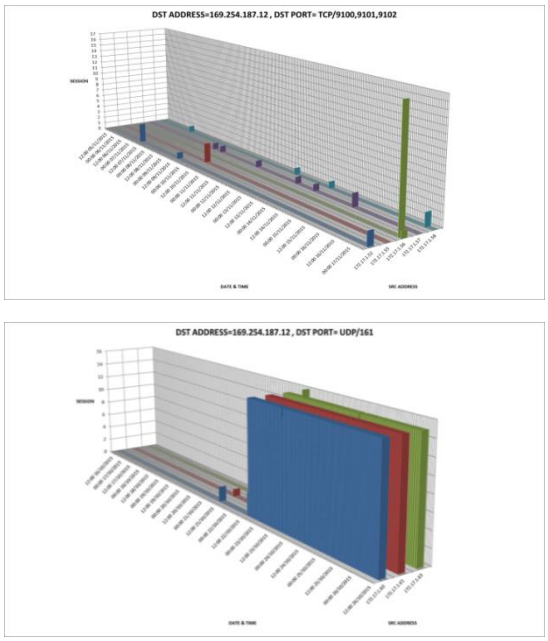


A compromised control network

In the above case, there is a surge in network traffic originating at a server in control room A that has been infected with malware.

Note: The above images are provided for general explanation purposes only and are not representative of the type of information provided with Yokogawa's analytical reports.

After introducing Yokogawa's network healthiness check service, this customer has been able to obtain analysis reports that visualize incoming communications traffic originating from unknown IP addresses, traffic using unspecified protocols and/or ports, unauthorized data transmissions, and other potential hazards.



Examples of detection of network communication from unknown source

The customer was surprised at the data in these analysis reports. Working together with Yokogawa, they analyzed where this communications traffic was coming from and sought to identify its source. With this information, it was then possible to take appropriate preventive measures.

With this Yokogawa service, one can intuitively visualize and grasp the status of a control system's communications traffic so that preventive measures can be taken in response to any potential issue. In the case of cyber-attacks, the sooner the response the better.

Customer Satisfaction

Our customer has attested to the quality of this service, saying that the analytical reports that they receive from Yokogawa have made clear to them the extent of their issues with unauthorized communications traffic and allowed them to identify its sources . Thanks to these reports, they have been able to take preventive measures. They would like this service to be soon expanded to include real-time monitoring, automatic inspection, and notification.

Note: As the subject of this success story is a cyber security solution, the name of this customer is being kept confidential.

For more Information and Contact

Plant Security Consulting Services

www.yokogawa.com/pr/news/2015/pr-news-2015-0916-en.htm

YOKOGAWA ELECTRIC CORPORATION
World Headquarters
9-32, Nakacho 2-chome, Musashino-shi, Tokyo
180-8750, Japan
www.yokogawa.com

Contact Us
kenzen-support@ml.jp.yokogawa.com