

# Managed Service Enhanced with ITIL Best Practices

Chooi LaiKong \*1

---

*To improve the operational flexibility and efficiency of on-site production work, manufacturers have introduced open-standard networks for their industrial automation and process control systems. Such a network allows plant managers to remotely access the systems and share plant data, applications, and resources with engineering personnel and external partners. Since the shrinking number of skilled workers is making it difficult to share information and quickly respond to troubles in plants, remote support services by automation vendors are increasingly needed. In response, Yokogawa has launched the Managed Service based on the best practices of the information technology infrastructure library (ITIL) approach. This paper introduces how the Managed Service improves operational efficiency.*

---

## INTRODUCTION

To increase the operational flexibility and efficiency of on-site production work, manufacturers have introduced open network standards for industrial automation (IA) and control systems.

Open networks have the advantage of allowing plant managers to remotely access the control system regardless of its physical location and to share accurate information, applications, and resources of plant operations with engineers and other plant personnel. On the other hand, security management tends to be difficult and complex because plant control systems and equipment come from different suppliers. Therefore, it is necessary to establish and operate an integrated security management system.

In addition, due to the decrease in skilled workers as a result of population aging and other factors, it is increasingly difficult to manage plant equipment and respond quickly to emergencies. Plant managers expect their suppliers to provide

support in the operational technology (OT) domain to ensure stable operation of the control systems via remote access and other means. If the managers can also entrust IT support, including security management in open networks, to suppliers, they can concentrate on their main production tasks. Thus, there is an increasing need for managed services for integrated IT and OT services, from introduction to management and operation.

In the IA industry, the concept of IT/OT convergence is now widely accepted. In 2013, when the term was still unfamiliar even within the industry, Yokogawa had an opportunity to provide such services. Shell, a British multinational oil and gas company, planned to deploy the Shell SecurePlant solution project at its plants around the world, and chose Cisco Systems, which is an IT industry solutions leader, and Yokogawa as partners. Yokogawa had already established a long-standing partnership with Shell and provided advanced solutions in process control. In addition, Yokogawa had extensive experience in building control systems for OT in the IA field. The three companies jointly developed a comprehensive cybersecurity management solution, with Yokogawa providing its operational services. The background of the development is explained in the following sections.

---

\*1 Service CoE Department, Lifecycle Services Business Division, Digital Solutions Headquarters

This paper explains how Yokogawa established an operational structure, which led to the foundation of the OpreX Managed Service and developed new services by making full use of its experience and expertise gained through the SecurePlant project and various best practices from the information technology infrastructure library (ITIL). The paper also describes the establishment of the organization commissioned in this project, the internal control required for the project, and how this new service organization will lead to new business.

This paper is organized as follows:

- (1) Background of the development of Shell SecurePlant
- (2) Creating the solution and services
- (3) Internal control in accordance with SSAE16
- (4) Benefits brought by the new service and future issues
- (5) Future development

### BACKGROUND OF THE DEVELOPMENT OF SHELL SECUREPLANT

Among the various reasons why Shell decided to develop and implement the SecurePlant solution, there was an urgent need to establish thorough security management to address the threat of cyberattacks.

At that time, each regional office and plant of Shell chose OS security updates and antivirus software at their discretion for control systems and their component PCs. Many plants also independently managed the updating of virus definition files. As a result, security operation and management varied, and no one knew whether security measures were implemented on a timely basis.

Shell delegated the management to its own IT service desk. However, it was not easy for a single section to handle the complicated security management because each region and equipment had different suppliers of their control systems. A service provider was needed that could support everything related to security, including establishment, management and operation.

Therefore, Shell, Cisco, and Yokogawa worked together to design, develop, and operate SecurePlant, a comprehensive cybersecurity management solution that strengthens and standardizes security management in control systems.

The solution designed and developed jointly by the three companies was rolled out at dedicated Shell plants. It provides security updates for target control systems and virus definition files for antivirus software in one package. Yokogawa was responsible for operating a service desk, which monitors the operation and health of this solution and manages the plants in a centralized manner. This made it possible to grasp information on equipment delivered to each site in real time, and to periodically check the delivery and application status of security update programs and virus definition files. Yokogawa’s service desk operated 24/7 to respond immediately to any events at Shell’s sites all over the globe. Figure 1 shows the architecture and operational flow of the SecurePlant solution.

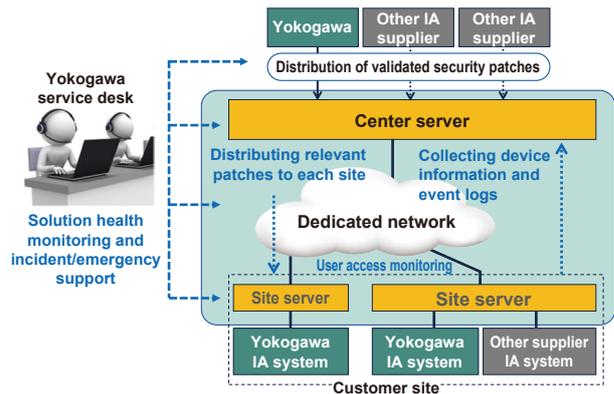


Figure 1 Architecture and operational flow of the SecurePlant solution

### CREATING THE SOLUTION AND SERVICES

To quickly roll out the SecurePlant solution at respective Shell sites, Shell requested Yokogawa to train engineers and set up a support system. In this case, engineers were categorized in two groups: those who manage the delivery and commissioning of the system at each site and those who work at the service desk. In response, all Yokogawa personnel involved in the project worked together. Specifically, we used various ITIL best practices to efficiently build an organization that satisfies the IT service management framework and helped each engineer hone their skills. As a result, we were able to establish an operation that provides advanced services to all Shell plants.

In the area of IT service management, the maturity of IT solutions management is determined by the balance of three factors: people, processes, and technology. As shown in Figure 2, it is important to combine these three elements in a well-balanced manner.

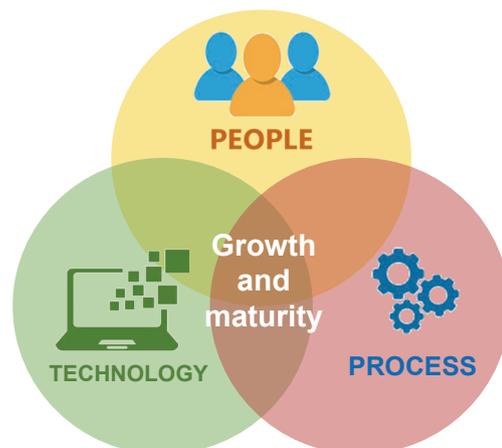


Figure 2 Good balance among people, processes, and technology

First, from the perspective of people, establish a system with clearly defined roles and responsibilities. From the

viewpoint of processes, clarify the processes and documents to execute tasks. Then, from the viewpoint of technology, introduce tools and systems necessary for managing organizations and executing tasks.

At the start of the SecurePlant project, we established three working groups as shown in Figure 3 by determining the scale of workforce and different skills required for each group.



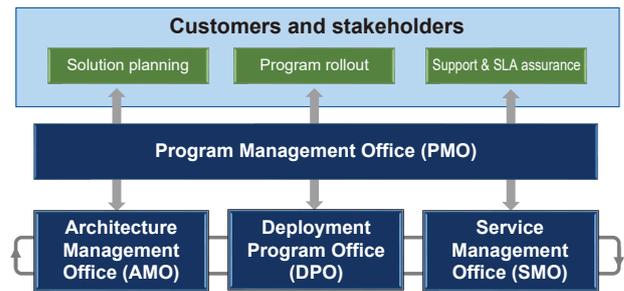
**Figure 3** Three groups for implementing the SecurePlant project

The Architecture Management Office (AMO) is responsible for designing and developing the architecture of the SecurePlant solution, managing its release, and drawing up a roadmap. It is also involved in deploying the solution and improving the operation of the service, for example, by developing tools for effective operations.

The Deployment Program Office (DPO) has two roles. One is to determine a standardized roll-out process in deploying the solution at each Shell plant, work with each Shell site to draw up an action plan based on the process, and train and dispatch engineers to each site for deploying the solution according to the plan. The other is to provide training for customers at each Shell site after delivery of the system. Yokogawa Europe B.V. (YEF) in the Netherlands led the task of preparing necessary knowledge and resources. In addition, Yokogawa trained personnel at its service sites which cover major Shell sites and facilitated the deployment.

The Service Management Office (SMO) has an around-the-clock service desk that monitors the health of the solution at each Shell site in real time and handles incidents reported from each site while following the processes defined in ITIL. Yokogawa set up this 24/7 service desk at YEF Romania. We also set up the Center of Excellence (COE) team for escalation at YEF Netherlands, defined the necessary processes, and drew up manuals. In addition, we created the necessary tools for systemization to reduce manual work and perform the tasks efficiently and effectively. In this way, we have struck a good balance of three elements: securing personnel with the required skills, establishing clear processes, and utilizing technology and tools to improve efficiency.

While maintaining a good relationship with Shell and Cisco, we used the governance scheme (engagement model) to conduct regular reviews and discussions with upper management to ensure that there are no problems in delivering the solutions and services. Figure 4 shows the scheme.



**Figure 4** Governance scheme for implementing the solutions and services

Figure 4 shows the horizontal and vertical collaboration among the organizations. Horizontally, the AMO develops and releases a solution, the DPO rolls it out at each site, and the SMO manages and supports its operation. Through day-to-day support, the SMO's service desk obtains feedback and provides it to the AMO. This collaboration leads to the next development.

Vertically, the Project Management Office (PMO) governs the activities of the AMO, DPO, and SMO, conducts regular reviews with customers, checks comments there and feedback from the sites, and reflects customer needs in the activities of the AMO, DPO, and SMO.

Based on this engagement model, communications are well established and information is shared vertically and horizontally among all the organizations and teams, thus raising the competence of all staff.

### INTERNAL CONTROL IN ACCORDANCE WITH SSAE16

Being commissioned by Shell and Cisco to operate the service desk, Yokogawa is required in the contract to submit SAS certification reports. This means that Yokogawa needs to be audited by an independent auditing firm for its internal control and process related to the service and meet the requirements of SSAE16 (later revised to SSAE18). SSAE16<sup>(1)</sup> stands for "Statement on Standards for Attestation Engagements No. 16," which is a set of auditing standards published by the American Institute of Certified Public Accountants (AICPA). Auditors use SSAE16 as a guide to verify the effectiveness of the internal control of a company that performs outsourced services. The audit ends with two specific reports.

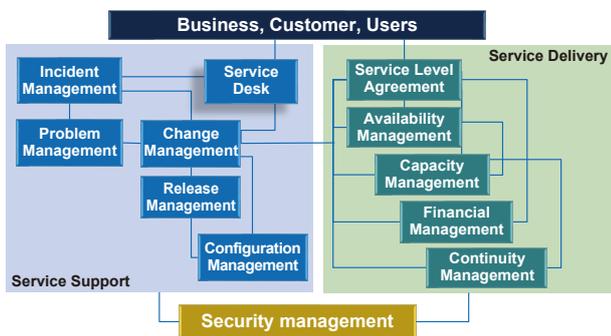
Type 1: Verifies that the internal control framework (rules and workflows) of a service provider has been clearly defined.

Type 2: Combines the Type 1 audit with verified implementation and effectiveness of the controls for a period of 6 months to 1 year.

Security, availability, processing integrity, confidentiality, and privacy are the five criteria, and one or more of which are selected for verification.

Yokogawa was checked by a Dutch auditing firm and received Type 1 and Type 2 certification reports for the operations of the service desks in YEF Romania and YEF

Netherlands. Yokogawa also submitted regular reports describing the evidence of the systems and processes in operation to Cisco and Shell.



**Figure 5** Scope of the audit

Figure 5 shows the scope of this audit. The operation has two aspects defined in ITIL: service support and service delivery. Service support refers to the daily tasks performed by the service desk (management of incidents, problems, and others) in operating information systems. These tasks ensure that Shell, the customer, can easily access and use the IT services of the service desk. Service support is assessed on whether it is managed systematically based on ITIL operation standards. Meanwhile, service delivery is assessed in terms of five management processes: service level agreement (SLA), financial management, availability management, continuity management, and capacity management.

Having internal controls audited and reporting the certification are beneficial to both outsourcers and service providers. Shell and Cisco can be sure that Yokogawa is in compliance with laws and regulations, while Yokogawa can establish and operate effective internal controls to protect the security and privacy of its customers and provide reports to other stakeholders. This control also allowed Yokogawa to conduct organizational operations based on clear rules.

**BENEFITS BROUGHT BY THE NEW SERVICE AND FUTURE ISSUES**

It was not easy for Shell’s section alone to standardize an IT/OT solution and roll it out as the Shell SecurePlant solution; it was not Shell’s core business. Therefore, Shell decided to work with two companies having strengths in their respective fields; Cisco is the solution leader in the IT industry, and Yokogawa has extensive knowledge of building and operating OT control systems in the IA field. As a result, the three companies were able to design a solution with standardized hardware and software, which is used for security measures in both the IT and OT domains. The service desks set up by Cisco and Yokogawa provided both IT and OT support to Shell sites. In addition, Yokogawa sent engineers with both IT and

OT knowledge to Shell sites. They reassured workers on site at the time of roll-out and troubleshooting in cooperation with Cisco support and greatly helped Shell’s operation.

While establishing and operating such an organization in the SecurePlant project, the persons in charge of the service business in Yokogawa became aware of the importance of combining the three elements of people, processes, and technology in a carefully balanced manner and continuously improving each element. In terms of “people,” an appropriate workforce must be maintained for the service desk. This requires training to make sure that IT engineers can gain more OT knowledge while OT engineers absorb IT knowledge. In recent years, there is a great need for engineers who can make full use of both IT and OT knowledge; their recruitment and training must be taken into account.

In addition, continuous improvement in processes and technology is essential. It is necessary to actively introduce processes, documents, and useful tools that improve the efficiency of operation without only relying on the skills of individual workers. We also need to develop an operation model based on a well-balanced combination of people, processes, and technology.

**FUTURE DEVELOPMENT**

Through the Shell SecurePlant project, Yokogawa was able to transform its services into a new field of managed services by making full use of various best practices in ITIL. This is the foundation of the OpreX Managed Service.

The OpreX Managed Service will continue developing and growing toward 2030. Its operational model will not only inherit the workforce developed and the knowledge and experience gained through the Shell SecurePlant project but also evolve to meet the market needs of customers in the IA industry. This is a crucial element for Yokogawa’s service business to take a new step forward.

**CONCLUSION**

According to Shell’s decision, Cisco and Yokogawa terminated the SecurePlant service in September 2021 and handed it over to Shell. Since the launch of this project, Yokogawa had accumulated valuable experience over the years. We would like to express our gratitude to all those involved, including the pioneering staff who were involved in the launch of the project and their successors.

**REFERENCES**

(1) SSAE-16 website, <https://www.ssae-16.com>

\* OpreX is a registered trademark of Yokogawa Electric Corporation.  
 \* All other company names, organization names, product names and logos that appear in this paper are either registered trademarks or trademarks of their respective holders.