Security Engineering for Control System

Masaki Kawasumi [*1] *Ichiro Ochiai* [*1] *Kenichi Yokoyama* [*1]

High availability is required in control systems that support critical infrastructures. Therefore, they must be protected from a growing number of cyber-attacks. However, without appropriate consideration of the requirements and operational conditions specific to control systems, engineering for security countermeasures may cause system failures. Meanwhile, Yokogawa has established its own best practices for security countermeasures based on its wealth of experience in providing control systems to customers over many years and through knowledge obtained through its involvement in international and governmental standardization. Yokogawa can offer proper security engineering based on these best practices. This paper introduces Yokogawa's security concept for control systems and the related engineering.

INTRODUCTION

Various security countermeasures are available for information systems. However, these countermeasures cannot be directly applied to control systems that require high availability. Appropriate countermeasures must be selected and proper engineering for them is also necessary. Yokogawa has studied such countermeasures and selected security countermeasures best suited for control systems. Furthermore, Yokogawa has established best practices for implementing the security countermeasures and provides security engineering based on them. This paper outlines Yokogawa's security engineering.

NETWORK ARCHITECTURE PROPOSED BY YOKOGAWA

Yokogawa is proposing a policy of "defense in depth" that protects lower layer assets such as workstations even when defense at a higher layer is broken. To achieve the defense in depth, a proper network architecture that can serve as the basis for security countermeasures is essential. In order to reduce risks, costs and failures and build a robust, secure and cost-effective system, the ISA99 standards for security in control systems recommend dividing a system into areas corresponding to functions. This is called the Purdue model [(1)]. Yokogawa provides an architecture based on this model shown in Figure 1. The functions of each level area are explained below.

- Level 3.5 – Demilitarized zone (DMZ) area
  This area controls the data traffic to and from the Level-4 business area to protect the control systems in the Level-3 or lower areas.
- Level 3 – Site manufacturing operations control area
  This is an area responsible for a site manufacturing operation control area, which cooperates with systems such as an enterprise resource planning (ERP) system in the business area.
- Level 2 – Area supervisory control area
  This area monitors and controls production processes of products.
- Level 1 – Local or basic control area
  This area obtains data from field devices and executes production processing of products following control algorithms.

SECURITY COUNTERMEASURES

Management of Anti-virus Software

System protection by anti-virus software is an endpoint security countermeasure, a countermeasure at the last defense line of the defense in depth. Virus pattern files and virus search engines are continually updated to respond to ever-increasing malware. Such information is periodically verified in Yokogawa, and it is recommended to timely apply such information.

The endpoint security (EPS) service provided by Yokogawa offers a means in which service engineers manually update those files and engines for each client. For details on the EPS service, see another paper "Endpoint Security for Industrial Control Systems" in this issue. In this paper, integrated management by an anti-virus software management server (hereafter, referred to as an AV server) is introduced as an additional security countermeasure.

The integrated management by using AV servers reduces work for updating settings. Without AV servers, operators need to manually update settings on each PC. This manual update is effective as long as the number of target devices is limited and they are closely located. However, if a large

*1 YEI System Integration Technology Center

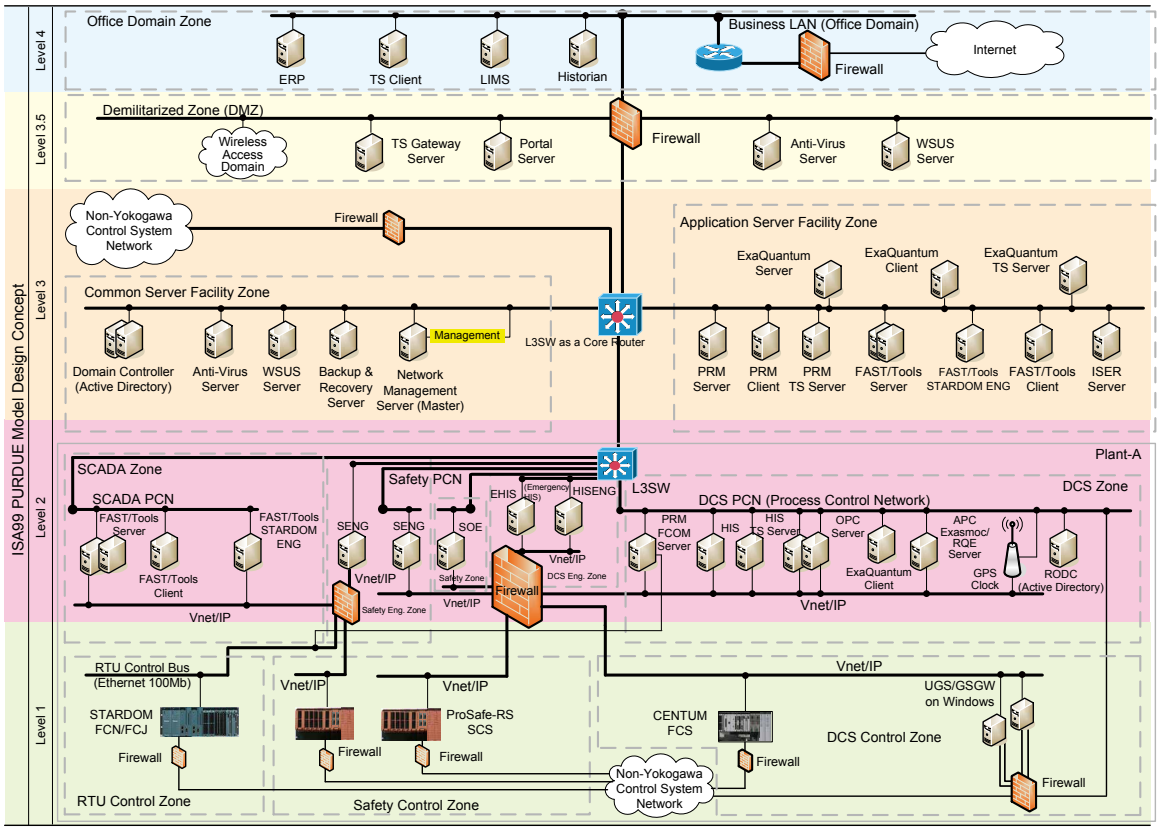

Figure 1 Network Architecture Proposed By Yokogawa

number of devices are involved or they are distributed in a wide area, AV servers must be introduced. Whether to choose AV servers or a manual update by the EPS service is finally decided depending on discussions with customers considering the number and locations of target devices and the running cost of the AV servers.

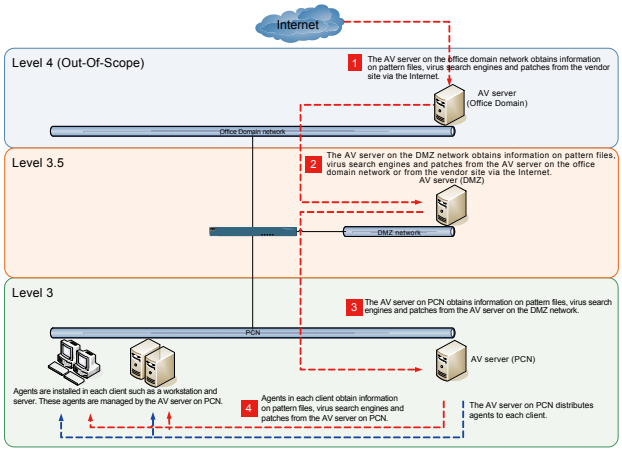

Figure 2 Typical system configuration using AV servers

Figure 2 shows a typical system configuration using AV servers. AV servers are located in each layer of the system. This is to keep the security of the Level- 3 AV server in the process control system area by preventing it from being connected directly to the Internet.

The Level-3.5 AV server pulls the information from the Level-4 AV server or pulls it directly from the vendor site via the Internet. The Level-3 AV server pulls the same information from the Level-3.5 AV server and distributes it to each workstation and server.

Management of Microsoft Security Update Programs

Microsoft Corporation provides security update programs (MS patches) every month or as needed to fix security holes. Their proper application is also an endpoint security countermeasure, a countermeasure at the last defense line of the defense in depth.

The EPS service offers a means in which service engineers manually apply MS patches for each client. As an additional means, this paper introduces an integrated management method using a Windows server update service (WSUS) server. The WSUS server can obtain MS patches from the Microsoft website or the upper level WSUS server and distribute them to target devices.

The integrated management using WSUS servers reduces the workload for applying MS patches. As with AV servers, the effectiveness of introducing WSUS servers depends on the number and locations of target devices. Whether to choose WSUS servers or manual updates by the EPS service is finally decided by discussions with customers considering the number and locations of target devices and the running cost of WSUS servers.

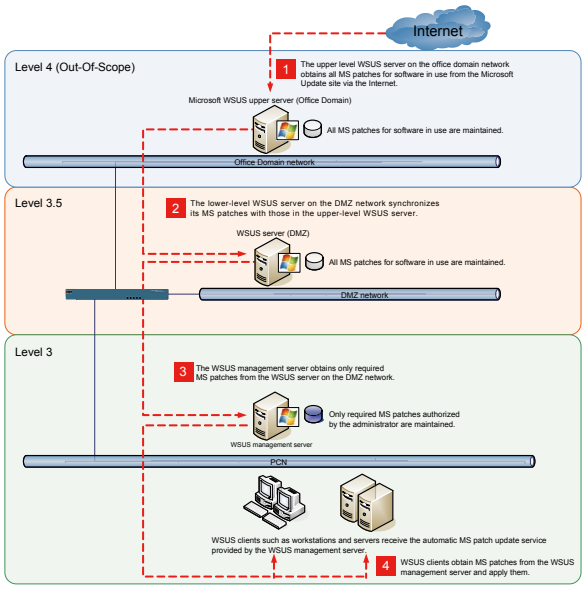

Figure 3 Typical system configuration for applying and managing MS patches

Figure 3 shows a typical system configuration for applying and managing MS patches. WSUS servers are located in each layer of the system. As in the case of the AV server described above, this configuration aims to prevent the Level-3 WSUS server from connecting directly to the Internet. The Level-3 WSUS server pulls MS patches only necessary for Yokogawa products from the upper level WSUS server.

These patches are periodically verified by Yokogawa in its test environment.

Management of Windows Domain and Account

As control systems are becoming larger and more complex, the number of endpoints in plants such as workstations is increasing, making it more difficult than ever to set and manage passwords, security policies and the like at each endpoint. Thus, more users are investigating whether to introduce Microsoft active directory (AD) for resource management and centralized collective security setting.

By defining resources and user accounts in plants in its directory as a logical structure, the AD can manage them separately from the actual physical structure. The AD also offers a setting management satisfying sophisticated security requirements such as settings of role-based access control.

To introduce the AD into a control system, the following items must be set properly.

a) Forest and domain models
b) Locations of domain controllers
c) Domain name service (DNS) configurations
d) Function levels of forests and domains
e) Flexible single master operation (FSMO) and global catalogs (GC)
f) Site configurations
g) Time synchronization

Yokogawa provides proper engineering depending on the size and requirements of control systems.

System Hardening

The settings for system hardening are recommended as protective countermeasures against cyber-attacks, unauthorized operation of terminals, stealing of information and so on. Yokogawa provides an IT security tool that can collectively execute the following settings.

- Restrict software execution
- Disable autoruns
- Disable NetBIOS over TCP/IP
- Set audit policies
- Disable removable media access

In addition to the collective settings above, Yokogawa engineers perform the following settings for system hardening.

a) Changing an administrator account

Because the built-in account generated at the installation of the Windows OS is vulnerable to password cracking, it is recommended to change the name of the administrator or invalidate it.

b) Turning off unnecessary services

Many services in the Windows OS are enabled by default. Attackers may, in the worst case scenario, take over administrative authorization for the domain through attacks aiming at the vulnerabilities of these services. To reduce such risks, Yokogawa recommends turning off unnecessary services. Note that services should be turned off so as not to affect other installed applications.

Management for Backup and Recovery

If a system fails to cause business interruption, the company will lose not only revenue during suspension but also reliance in the market. In the worst case scenario, this may endanger the company's existence. Therefore, a backup and recovery management system needs to be designed considering both aspects of data and system protection so that the system can promptly recover from the failure.

Yokogawa provides a wide range of comprehensive solutions including those for selecting optimum backup media and software, and for establishing backup plans and recovery methods taking business and operation aspects into consideration.

The latest backup and recovery technologies have the advantage of a shorter time required for recovery. It does not require several days or even several hours. Although it is necessary to verify software licenses, backup data can be recovered in a different hardware environment. The latest technologies provide a flexible recovery means.

Improved Protection of Safety Instrumented System (SIS)

The safety instrumented system (SIS) plays a significant role for securing plant safety, and thus its availability should be secured with the highest priority.

Usually, control network of SIS is connected to the control network of distributed control system (DCS) for optimizing the configuration of the whole control system and

improving the efficiency of engineering and plant operation. In this network configuration, even if the DCS is infected with viruses, the SIS must not be affected. Thus, Yokogawa is offering engineering in which a SIS is connected with a DCS network via protective devices such as a firewall.

SECURITY TRAINING

For implementing security countermeasures for control systems, engineers need to apply security solutions based on information system technology on the premise of a good understanding of the control system itself and availability and safety of the plant.

For this purpose, Yokogawa provides its control system engineers with training that enables them to understand the security system based on the best practices and suitable for control systems, and enables them to perform actual engineering.

The training consists of the following three steps. Engineers who have passed the qualifying examination after the course are enrolled and treated as Yokogawa security-certified engineers.

- Total system architecture
- Advanced module for each security solution
- Practical module for each security solution

In 2013, the global industrial cyber security professional (GICSP) certification program was established. The GICSP is a professional qualification for security staff in critical infrastructures and one of the certifications awarded by Global Information Assurance Certification (GIAC), a certification organization that provides many other certification programs in the fields related to cyber security. The GICSP certification requires comprehensive knowledge not only on the design and implementation of security countermeasure systems but also on the entire lifecycle from the initial stage of developing security policies and introduction plans to emergency procedures on incidents during actual operation.

Regarding the GICSP as important, Yokogawa has developed a dedicated training module for engineers to acquire this qualification and started the training at each global office to promote companywide acquisition of this qualification.

CONCLUSION

This paper has introduced Yokogawa's security concept for control systems and related engineering. Regarding security countermeasures, Yokogawa studied those in general information systems, selected solutions best suited for control systems, and formulated their architecture, implementation and operation as best practices. Control systems for critical infrastructures must be protected from cyber-attacks. Yokogawa provides proper security engineering based on the best practices to reduce security risks, and will continue to support secure and stable operation of plants.

REFERENCES

(1) ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, ISA, 2007, pp. 69-73