A Hot-Backup System for Backup and Restore of ICS to Recover from Cyber-Attacks

A hot-backup system for backup and restore of ICS to recover from cyber-attacks

Shinya Yamamoto[1,*], Takashi Hamaguchi[1], Sun Jing[1], Ichiro Koshijima[1] and Yoshihiro Hashimoto[1]

[1] Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan

Corresponding Author's E-mail: cjh17092@nitech.jp

Abstract. Because the techniques of cyber-attacks are developed every day, it is impossible to defend the cyber-attacks completely. Therefore, it is necessary to discuss how to defend proper control against cyber-attacks when the attackers intrude in the ICS. We focus on new ICS structure without stopping the plant operation under the situation, and aim to improve detection, security and restoration abilities of ICS on the continuous process. In this paper, a virtualization technology is used to realize the three purposes. Using the feature of virtualization technology, we propose a hot-backup system for backup and restore of ICS to protect from cyber-attacks.

Keywords: Cyber-Attacks · Industrial Control System · Security

1 Introduction

Strengthening of cyber security is not a problem only for the IT field. By an appearance of Stuxnet, even the controller of ICS (Industrial Control System) becomes the target of the cyber-attacks [1]. The conventional ICS uses vendor original OS and communication protocol. Additionally it is hardly that the conventional ICS network connected to the IT network. Therefore, cyber-attack to ICS was arduous.

However, the present ICS is connected to IT network to increase production efficiency including the optimization of operation conditions and the acceleration of managerial decisions. In addition, the present ICS is introduced inexpensive or free open source application such as consumer OS, PC terminal and Ethernet-TCP/IP to reduce cost. They have many vulnerabilities. In consequence, these cause the vulnerability of ICS itself.

The cyber-attacks to ICS is not only cause adverse effects for the plant operations, but also cause severe accident such as the explosion of facilities. When IT system restores, the system is generally rebooted. However, ICS of continuous process must be always driven to continue plant operation. Therefore, we must consider that the system is restored without stopping of plant operation. The ICS must maintain the control function even if the sub system is stopped and restored to recover against cyber-attacks.

Because the techniques of cyber-attacks are developed every day, it is impossible to defend the cyber-attacks completely. Therefore, it is necessary to discuss how to defend proper control against cyber-attacks when the attackers intrude in the ICS. Takagi *et al.* discuss a systematic approach to design robust protection systems against cyber-attacks for ICS [2]. We focus on new ICS structure without stopping the plant operation under the situation, and aim to improve detection, security and restoration abilities of ICS on the continuous process. In this paper, a virtualization technology is used to realize the three purposes. By the virtualization technology, not only independent plural virtual machines can be built on one machine, but also virtual network structure can be changed freely. Using the feature of virtualization technology, we propose a secure ICS with "Dualization of the controller" and "Security Patch update system" and so on.

2 Secure ICS structure against cyber-attack

Fig.1 shows a structure of ICS. ERP (Enterprise Resources Planning) exists in the enterprise zone, which is used by head office and business functions as the highest layer system. It is necessary to unify the management information such as production schedule, quality control of products, ordering, and stock to plan optimization of the whole company.

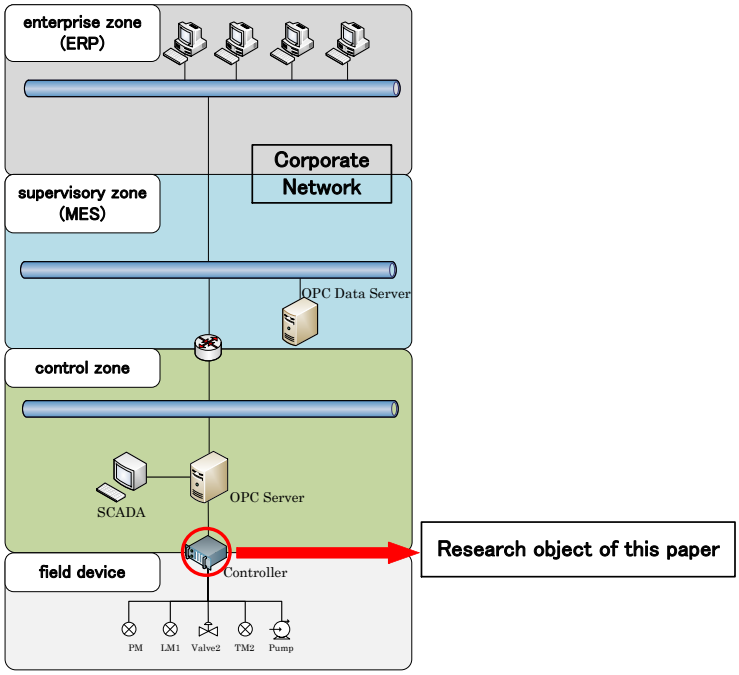

Fig. 1. Structure of ICS.

Production optimization of the whole factory is performed in MES (Manufacturing Execution System). As shown in Fig.1, it is located in the middle of enterprise zone and

control zone. Generally, MES performs production support and management such as process control, quality control, manufacturing management and point of production (POP) information management. In this research, we call a network above from MES Corporate Network.

Recently, SCADA (Supervisory Control and Data Acquisition) system is adopted for ICS. The function of SCADA system is monitoring of the plant and collection of control data. The SCADA is used to manage the system distributed to the wide area remotely. Generally, the operator supervises the control system through terminals. In the SCADA system, the general-purpose products such as PCs and standardized network protocol are used. Thereby, they have the vulnerability of security for the cyber-attacks by attackers.

ICS has controllers called PLC (Programmable Logic Controller) and DCS (Distributed Control System). The controller reads PV (Process Variable; measurement signals such as flow rate and temperature, the pressure) from Field Device. It does control operation based on PV it reads. It out-puts MV (Manipulative Variable) which is quantity of control to the operation apparatuses such as actuators.

The OPC (OLE for Process Control) is an important standard to connect between SCADA and PLC. Even if the apparatuses such as client applications or the controller adopt different communication protocol, they can be connected by a function of OPC. The OPC server accumulates data of PVs, which are sent from controllers. The operator monitor the plant operation through terminals. Fig. 2 shows the general structure of ICS's controller. A controller communicates with "Plant" and "Monitoring System" through "Data I/O". The controller generate MV to operate the actuator from a deviation of SV and PV.

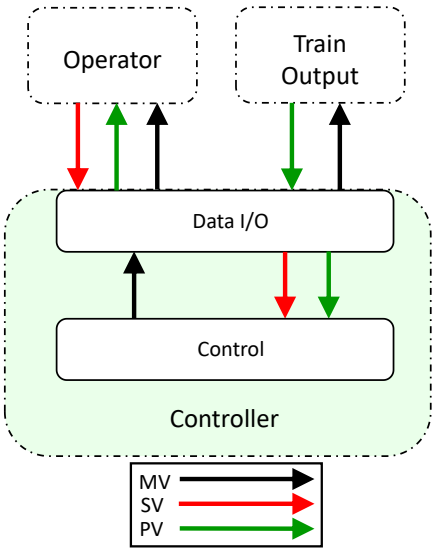

Fig. 2. The general structure of ICS's controller.

To ensure that the reproduction of your illustrations is of a reasonable quality, we advise against the use of shading. The contrast should be as pronounced as possible. If

screenshots are necessary, please make sure that you are happy with the print quality before you send the files.

In this paper, we assume that attackers try to make the falsification of SV to controller and to rewrite control program in the controller. We propose a hot-backup system for backup and restore of ICS to recover from cyber-attacks, as shown in Fig. 3. The "Corporate Network" and "Monitoring System" are connected directly. The "Monitoring System" and controller are connected through a SV check system. The SV check system is explained in section 3. The controller has "Dualization Controller System" and "Backup & Restore System", too. Each system is explained in section 4 and 5. Moreover, we explain "Security Patch update System" to reduce the vulnerability in ICS is explain in section 6.

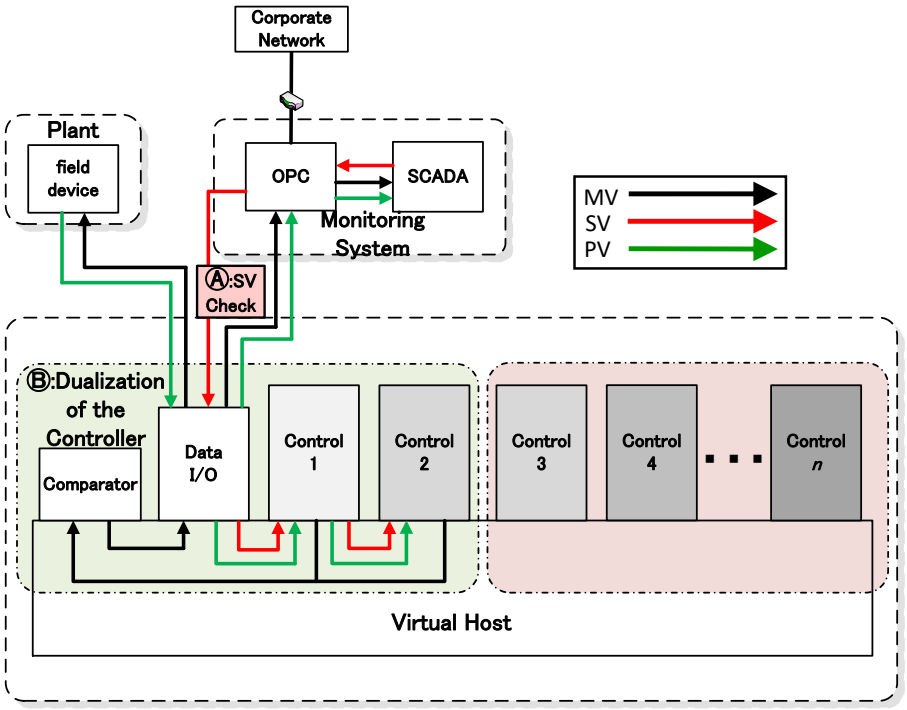

Fig. 3. A hot-backup system for backup and restore of ICS to recover from cyber-attacks.

3 SV Check System

To damage the plant, attacker may change the SV into the inappropriate SV region. The purpose of SV check system is to protect the plant safety from the inappropriate input of SV change. The flow chart is shown in Fig. 4. When the desired new SV is bigger or smaller than permitted SV region, then the SV change must confirm by the physical permission such as pushing button or turning a physical key by operator. If the SV change cannot permit operator, it may be cyber-attacks. It the SV change permit the operator and the SV change cannot reflect the terminals, it may be cyber-attacks, too. This system can be used as a detection system for cyber-attacks.

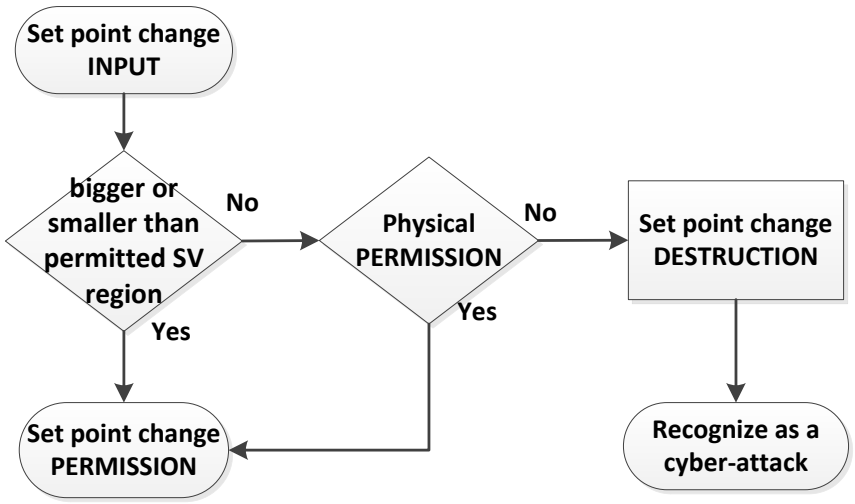

Fig. 4. Flow chart of SV Check.

4 Dualization Controller System

Some controllers for train have dualization structure for machine trouble as shown in Fig. 5. In the system, comparator compare the MVs from Control 1 and 2. When the Control 1 and 2 are normal, the MVs match and the MV is transmitted to a plant. If the MVs do not match because the Control 1 and/or Control 2 have machine trouble, then the controller must output the suitable MV to stop the train for safety [3].

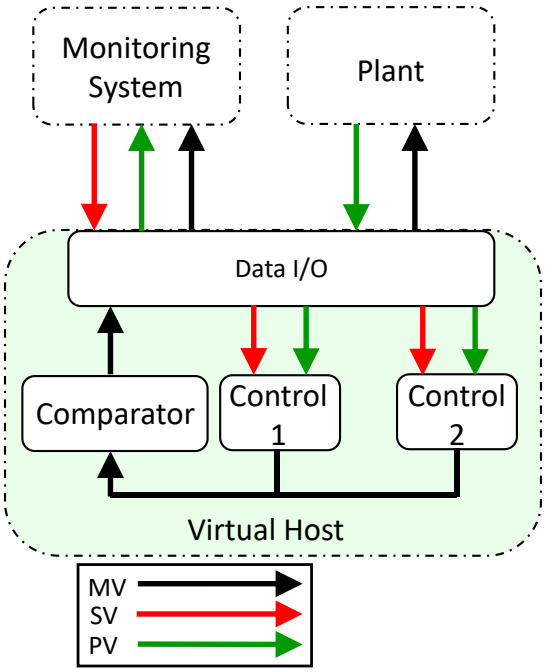

Fig. 5. A dualization of the controller for machine trouble.

In this paper, we assume that attackers try to make to rewrite control program in the Controller. In the structure of Fig. 5, attackers may re-write both Control 1 and 2. If attackers rewrite either Control 1 or 2, it is desirable to product by another Control without stopping the plant operation. We propose a dualization of the controller for the cyber-attacks on the continuous plant based on the dualization of the controller for machine trouble as shown in Fig. 6.

The difference between the structures in Fig. 5 and in Fig. 6, Control 2 does not connect directly to Data I/O, but connect to through Control 1. The structure is adopted to prevent rewriting program of Control 2 by attacker. We consider the Control 2 can get SV and MV through Control 1, even if attackers rewrite the program of Control 1.

At first, a change procedure of the program of Controller is explained. The behavior of this system is determined by combination of the state of Control 1 and 2. In this example, each Control 1 and 2 has following four states.

P1: program 1 is running.
P1(P2): program 1 is running, but program 2 is downloading, too.
P1=>P2: program 1 is stopping, and program 2 is installing to change from program 1.
P2: program 2 is running.

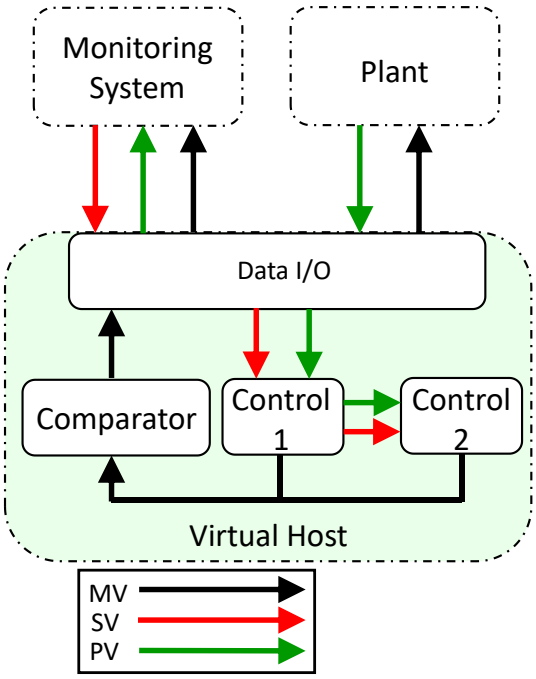

Fig. 6. Dualization of the controller for the cyber-attacks.

In this paper, the combination of the state of Control 1 and 2 is explained by brackets such as [state of Control1, state of Control2]. The * means the wild card for state. The state transition of rewriting program of Control is shown in Table 1. The Comparator outputs are summarized followings.

CS1: [*, P1 or P1(P2)] ; Comparator outputs P1.
CS2: [*,P1=>P2] ; Comparator outputs maintain a former MV of Control 2.
CS3: [*,P2] ; Comparator outputs P2.

Table 1. State transition of rewriting program of Control.

State	Activity (Control 1)	Control 1	Activity (Control 2)	Control 2	Activity (Comparator)
1	Steady-state	P1	Steady-state	P1	P1 out
2	Download P2	P1(P2)	〃	P1	P1 out
3	Input P2	P1⇒P2	〃	P1	<A>P1 out
4	Steady-state	P2	〃	P1	<A>P1 out
5	〃	P2	Receive P2	P1(P2)	<A>P1 out
6	〃	P2	Input P2	P1⇒P2	<B>
7	〃	P2	Steady-state	P2	P2 out

The <A> and <B> in Table 1 means reasons of Comparator outputs.

<A> To continue operating without stopping the operation of the plant, MV of Control 2 is transmitted to Field Device.
<B> To continue operating without stopping the operation of the plant, a last MV of Control 2 based on P1 is maintained and transmitted to Field Device.

Next, let's consider that Control 1 is rewritten from P1 to P2' by attackers. An appreciate output P1 can be maintained until state 4, [P2', P1], by Control 2. Therefore, the detection method of state 2, 3, and 4 by cyber-attacks and the protection method to stop the progress from state 4 to state 5 must be considered.

The detection method can be realized by the monitoring the Comparator's judgement. If the comparator outputs the <A> without operator's command, then it means the possibility of cyber-attacks. The protection method without operator's command can be realized by the physical action as same as SV Check.

5 Security Patch update system

Structure of security patch update system is shown in Fig. 7. Update Security Patch is required that the operation is not adversely affected by Security Patch. Thereby, the Security Patch must be checked whether it is suitable for ICS.

This system uses the structure like a foregoing chapter. Some virtual ma-chines that are the same structure as Control 2 is prepared. Control 2' is held as the same state. The other control group is hit with various Security Patches. The purpose is a behavior investigation when a Security Patch is applied. These machines are not used real plant operation. Thus, these machines are not outputted for Comparator. However, MV of all Control group is outputted for Management that is the machine of the third party to determine whether each Security Patch is applied to ICS. To create MV, SV and PV is given to the Control group from Management as an identification signal. The difference of behavior Control 2' and the other Control group can be checked from Management.

The Security Patch evaluated that it does not adversely affect ICS assume Control X. In changing virtual networks, Control X use as Control 2. During this substitution, MV is maintained a former value illustrated by a foregoing chapter. Finally, Control 1 is replaced to Control X. In this method, the ability for security of the ICS controller can be improved with bumpless.

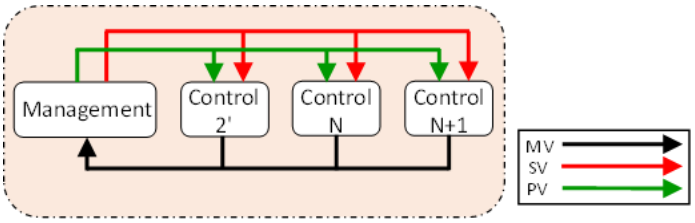

Fig. 7. The structure of Security Patch update system.

6 Conclusion

In this paper, we proposed a hot-backup system for backup and restore of ICS to recover from cyber-attacks. As prospects for the future, we will implement the proposal system and develop function more. The proposal system is considered for continuous process. It is important to consider others manufacturing processes such as lot production and batch production.

References

1. Macaulay, T., Singer, B.: Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, CRC Press, Boca Raton, Florida (2011)
2. Takagi, H., Morita, H., Matta, M., Moritani, H., Hamaguchi, T., Jing, S., Koshijima, I., Hashimoto, Y. : Strategic Security Protection for Industrial Control System. Proc. of SICE Annual Conference 2015, 1215--1221 (2015)
3. Hirao, Y.: Anzen system to software (in Japanese). Anzen anshin shakai kenkyu vol.2, pp. 61--73. (2012) http://safety.nagaokaut.ac.jp/~safety/wp-content/uploads/2013/12/anzen_02-07.pdf