Computers and Chemical Engineering xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Computers and Chemical Engineering

journal homepage: www.elsevier.com/locate/compchemeng

Safety securing approach against cyber-attacks for process control system

Yoshihiro Hashimoto*, Takeshi Toyoshima, Shuichi Yogo, Masato Koike, Takashi Hamaguchi, Sun Jing, Ichiro Koshijima

Dept. of Civil and Management Engineering, Nagoya Institute of Technology, Nagoya 466-8555, Japan

ARTICLE INFO

Article history:
Received 16 September 2012
Received in revised form 1 February 2013
Accepted 25 April 2013
Available online xxx

Keywords:
Cyber security
Safety
Plant control
Design methodology

ABSTRACT

After the appearance of Stuxnet, the safety assurance against cyber-attacks has been a serious problem for process control. For safety assurance, not only information system securing approaches but also process control original measures are necessary. In this paper, a new protection approach is proposed. Application of an information system securing technique called “zones and conduits” to process control is discussed. By dividing the control system network into plural zones, higher possibility of detecting cyber-attacks and preventing operational accidents can be achieved. By defining detectability and reachability matrices, zone division for cyber-attack detection can be designed.

1. Introduction

Current Industrial Control Systems (ICS: from sensors to SCADA, MES) are connected to the Internet for many purposes such as information exchange for business oriented plant operations and remote maintenance. Although the open system movement shows great promise for certain benefits through COTS(commercial off the shelf) products, it also causes various risks as a result of open architectures and network technologies. Recently, a very specific threat for process plants has come in reality. Stuxnet is acknowledged as the first malware, which attacked continuously to a uranium enriching plant in Iran, targeting specific Programmable Logic Controllers (PLCs). This malware has been spread out all over the world to many process plants with and without Internet connection. After Stuxnet was discovered, many kinds of followers have been developed. Although Stuxnet had a specific target, indiscriminate attacks can be committed by them. In this situation, ICS requires highly reliable security and safety services with urgent priority.

In this paper, the authors discuss about a new protection approach for process plant that covers not only safety but also security. Under this approach, even if some invasion to the ICS is succeeded, plant operators might be able to handle the attacks. For improvement of safety against cyber-attacks, some examples of combination of intelligent and unintelligent systems are introduced. Design of dividing control network into plural zones is also discussed with an illustrative example. Zone division is effective for not only prevention of attackers' manipulation but also detection of cyber-attacks.

2. Characteristics of ICS security problem

Serious security holes of personal computer systems are frequently reported, and security patches are distributed almost every day. In some cases, the security patches make uncertain troubles from conflicts among installed applications. Full security patches, therefore, are rarely applied to ICS for keeping their availability. For the ICS security, particular approaches are necessary in addition to ones for information systems.

2.1. Standard schemes for enhancement of ICS security

Evaluation of security assurance level of ICS is discussed in ANSI/ISA99. Security zones and conduits shown in Fig. 1 are important concepts in ISA99 (Uehara, 2011). The security of the system is evaluated based on the zones and their interfaces. The firewalls between zones must not have the same vulnerability. In this standard, vulnerability of the network is considered, but safety, which is most important for ICSs, is not discussed at all. Because security incidents cause serious accidents, such as explosion, in ICSs, safety must be discussed with security. In this paper, cyber-security is regarded as a kind of cause for accidents.

* Corresponding author. Tel.: +81 52 735 5378; fax: +81 52 735 5595.
E-mail address: hashimoto@nitech.ac.jp (Y. Hashimoto).

0098-1354/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compchemeng.2013.04.019

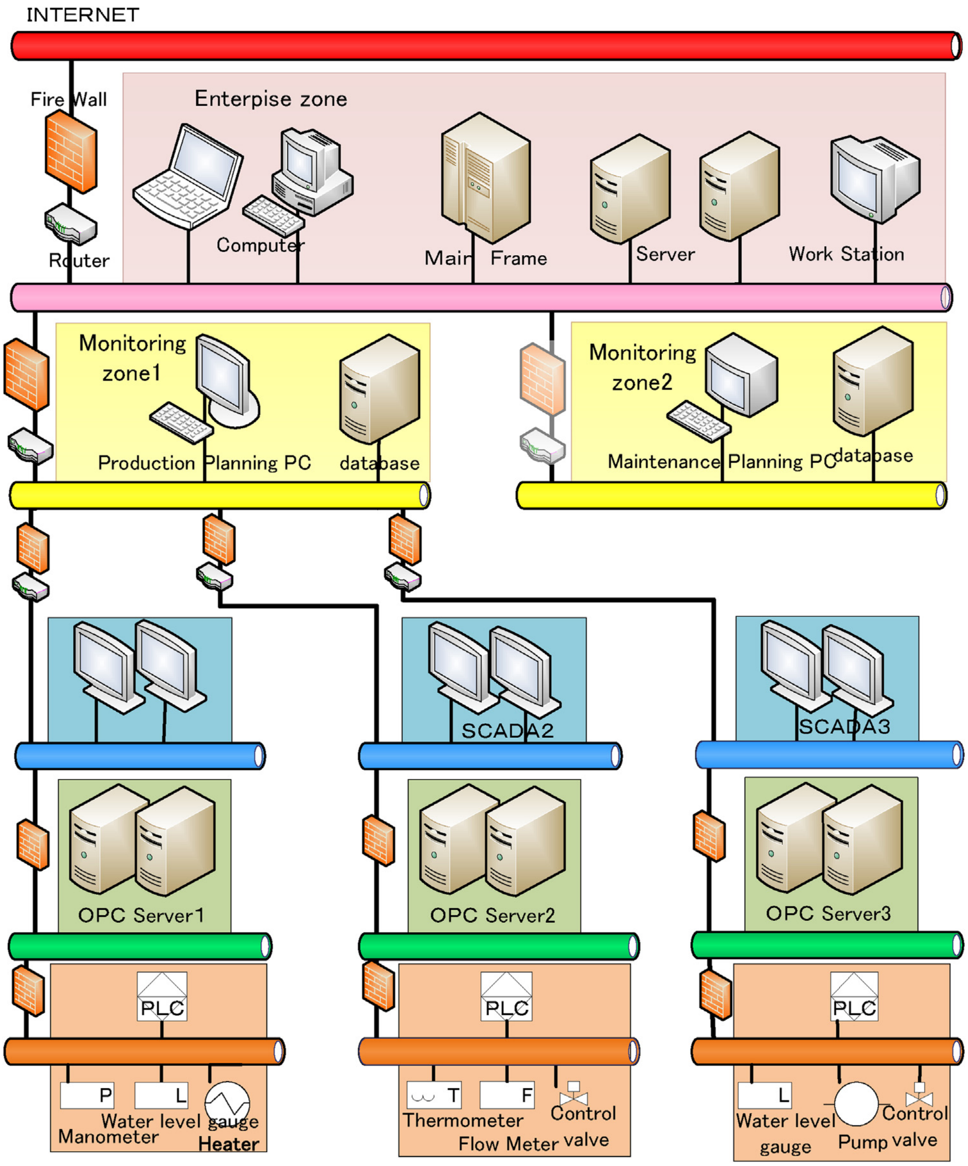


Fig. 1. Zones and conduits model.

2.2. Standard schemes for enhancement of ICS safety

The design approaches of Safety Instrument Systems (SIS) are described in IEC61508 (IEC61511 is the standard for process industry). Safety integrity and reliability are evaluated using hazard and operability studies (HAZOP), layers of protection analysis (LOPA), risk graphs, FTA and so on. However there are very few papers that consider the threats of the cyber attaches (NRC, 2010). Although the effects of a single failure are discussed in these approaches, attacks of cyber terrorists cause multiple failures. They invade the system via the Internet and/or malwares and steal, manipulate and conceal process and control information.

Cyber terrorists can attack plural layers in IPL (cf. 2, 3, 4, 6, 7 layers in Fig. 2) at the same time. Especially, when the emergency shutdown system in IPL4, which is constructed with PLC, is attacked, service of the plant can be stopped immediately.

Against cyber-attacks, the layers in IPL cannot be independent. The order of the layers has no sense against cyber-attacks. In our approach, causes of the accidents are reviewed considering malicious attacks of cyber-terrorists. Although IPL against cyber-attacks

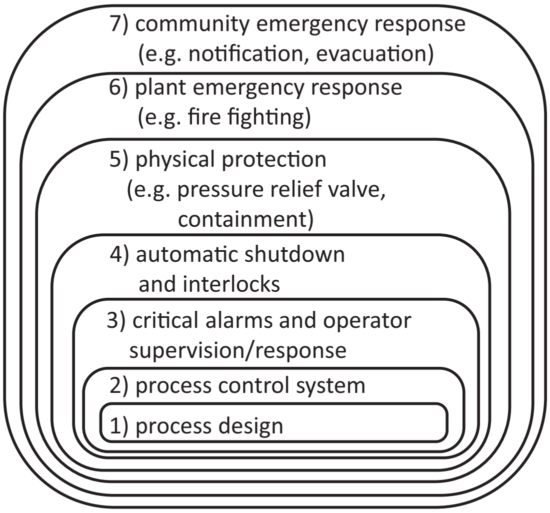

7) community emergency response
(e.g. notification, evacuation)
6) plant emergency response
(e.g. fire fighting)
5) physical protection
(e.g. pressure relief valve,
containment)
4) automatic shutdown
and interlocks
3) critical alarms and operator
supervision/response
2) process control system
1) process design

Fig. 2. Independent protection layers.

Please cite this article in press as: Hashimoto, Y., et al. Safety securing approach against cyber-attacks for process control system. *Computers and Chemical Engineering* (2013), http://dx.doi.org/10.1016/j.compchemeng.2013.04.019

is not introduced in this paper, it must be different from previous IPL and it will be designed using our securing approach.

3. Fault tree analysis for threats of cyber attacks

Fault tree is a very popular method to evaluate risks. Because it can deal with multiple failures, it can be applied to evaluate the threats of cyber terrorism. Attacks of cyber terrorists are parts of causes of accidents. Manipulation sequences by terrorists are similar to sets of mal-operation. Concealment of their manipulation is similar to a set of sensor malfunctions. In safety assessment, they have been evaluated based on human factors and equipment failures. In security problems, the probability of their occurrence is not independent. Cyber terrorists combine the causes to ensure their attacks. The possibility to successfully execute cyber terrorism can be evaluated with FTA.

Because the scenarios of cyber-attacks are combination of the causes, the countermeasures against cyber-terrorists are also combination of the countermeasures to the causes. The possibility of each cause's occurrence is evaluated considering the vulnerability and its countermeasure application.

In the discussion of cyber-security, concealment must be considered. Even if a countermeasure is already planned to a cause of an accident, it cannot be activated when the cause cannot be detected. Concealment is a cyber-attack, which prevent to detect the trigger information of the measure.

In safety assessment, sensor location is discussed to detect ill conditions. However, concealment of sensor information is not discussed. The effects of concealment must be considered as well as manipulation by cyber-attackers.

How to construct fault trees for evaluation of security threats were discussed in our previous papers (Shindo, Yamazaki, Toki, Koshijima, & Umeda, 2000; Toyoshima, Sun, Koshijima, & Hashimoto, 2011; Yogo, Toyoshima, Sun, Koshijima, & Hashimoto, 2011). In this paper, a systematic, qualitative and quantitative scheme is proposed to evaluate the effects of manipulation and concealment by cyber terrorists. The efficiency of the scheme to divide the plant instrumentation network into plural zones is evaluated on the view of invalidation of cyber-attacks.

4. The effects of manipulation and concealment by cyber-attackers

The threats of cyber terrorists are all sorts of accidents (i.e. explosion and contamination of drinking water) and/or sabotage against service continuity (i.e. power outage and water outage). In industrial plants, they are caused by manipulations of valves and/or switches. In many cases, it takes time until accidents occur after terrorists' intentional manipulation because the process dynamics has delays. If actual process data can be observed by operators, they can detect the manipulation and prevent accidents. Terrorists, therefore, conceal their manipulations to disable countermeasures.

The effects of the manipulation and concealment by cyber-attackers are discussed considering secure network zones separated by fire-walls.

In industrial plants, many controllers are utilized and communicate with SCADA systems. If the controller network is divided into plural secure zones and if the different cyber-attack schemes are necessary to invade the zones, some zones might be able to survive against cyber-attacks. As a result, possible manipulations are limited in the invaded zones. If plural manipulation in different zones is necessary to activate an accident, the probability of accident can be reduced with zone division. For example, in order to cause overheat of a tank, increasing heating power and stopping the liquid feed are necessary. If one of them cannot be executed, the accident is difficult to occur. When the actuators for heating and feeding are located in different network zones, the possibility that the both are manipulated by cyber-attackers becomes low.

Dividing the control network into plural zones is also effective for the detection of cyber-attacks. Even if the effects of cyber-attack are concealed in the invaded zone, there is possibility that physical effects of the attack appear in the survived zone. If heating rate is manipulated and the temperature changes are concealed by cyber-attackers, the detection of the attack is difficult. But, if temperature sensors in the survived zone can detect the temperature change, the cyber-attack can be detected.

Cyber-attack consists of both physical manipulation and information manipulation. If the sensor signal for control is disguised, controller action or operator's manipulation can be caused. As a result, the plant might be stopped unnecessarily.

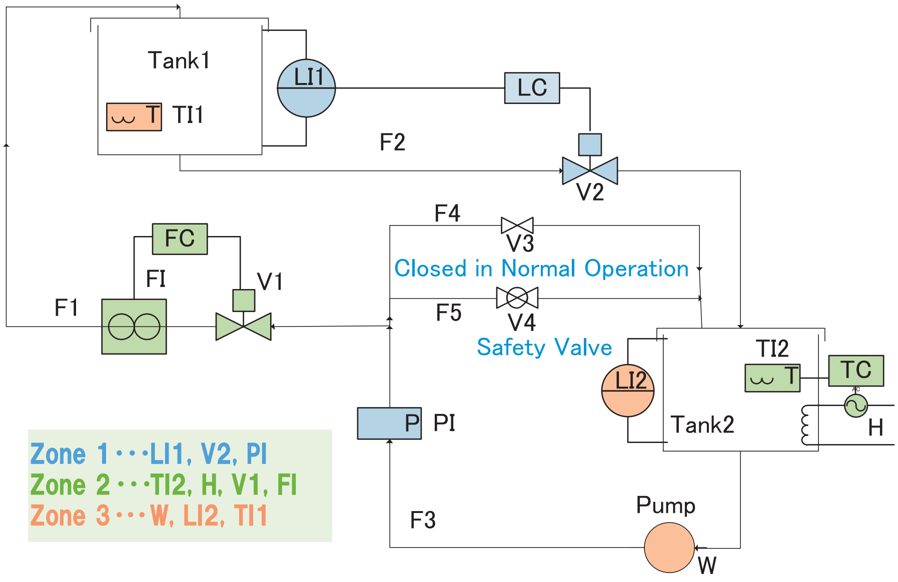
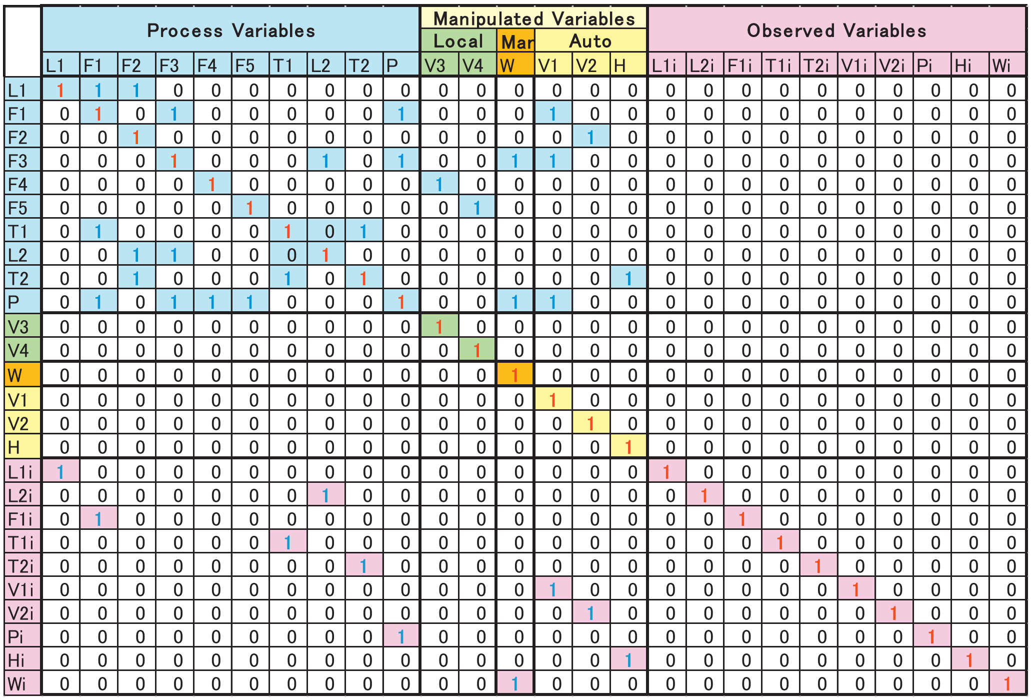


Fig. 3. Two tank system for Example.



	Process Variables										Manipulated Variables						Observed Variables									
											Local		Mar	Auto												
	L1	F1	F2	F3	F4	F5	T1	L2	T2	P	V3	V4	W	V1	V2	H	L1i	L2i	F1i	T1i	T2i	V1i	V2i	Pi	Hi	Wi
L1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
F2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
F3	0	0	0	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
F4	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F5	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L2	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T2	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
P	0	1	0	1	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
V3	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V4	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
V1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
V2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
H	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
L1i	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
L2i	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
F1i	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
T1i	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
T2i	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
V1i	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
V2i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
Pi	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Hi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
Wi	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1

Fig. 4. Cause effect matrix of process dynamic [P] (26 × 26).

5. Cause–effect matrix for evaluation of cyber-attack effects

We proposed to divide the control network into plural zones in order to improve security and safety. Even for such a small plant shown in Fig. 3, there are many possible patterns of zone division. To select effective zone division pattern, automatic evaluation method of security level of each zone division pattern is necessary.

In this section, the evaluation method of the influence of cyber-attacks using cause-effect matrices. For illustration of the scheme, a simple plant shown in Fig. 3 is utilized.

Fig. 4 shows plant matrix P. It is a square matrix and the rows and columns are corresponding to the plant variables, which are 10 process variables, 6 manipulated variables and 10 sensed variables. Process variables are variables necessary to express the dynamics of the plant. Manipulated variables are classified into three groups. The first group corresponds to the manipulated variables which cannot be operated by cyber attackers. It contains two local valves V3 and V4. The second one contains remote operable variables, which are not connected to a controller. In this example, the pump power switch is included in this group. The last one is a group of actuators of controllers. Two valves V1 and V2 and heater power H are included in this group. Observed variables are the ones whose values can be changed by cyber-attackers. Controlled variables and manipulated variables and other sensor signal are included. The plant dynamics is expressed as one in the matrix P, where all diagonal elements are ones.

Fig. 5 shows a part of control matrix C. The size of the control matrix C is the same as plant matrix P. Fig. 5 shows V1 is manipulated based on observed value of F1. Matrix C expresses not only controller but also manual operations based on the observation.

These two matrices do not depend on zone division.

The following four matrices M_x, A_x, S_x and O_x are arranged according to zone division. The subscripts of these matrices indicate invaded zones

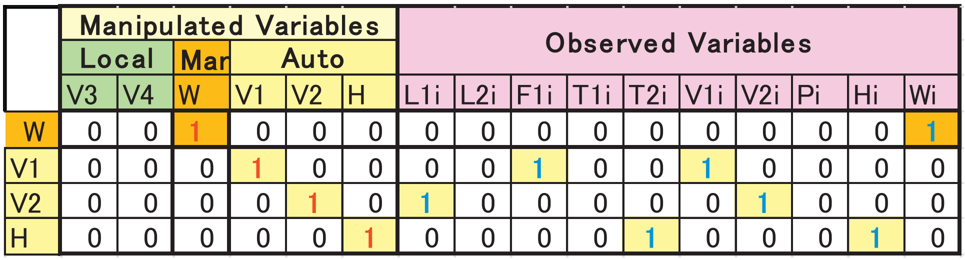
For illustration of the arrangement of these matrices, the zones are assumed to be set as shown in Fig. 3. The control network is divided into three zones. Even when zone division is determined, it is not determined which zones are invaded by cyber-attackers.

The influence of cyber-attacks should be estimated for every combination of zones.

Fig. 6 shows a part of manipulation matrix M_{23}. Its columns correspond to the manipulation in the invaded zones. M_{23} means zones 2 and 3 are invaded. When zone division is determined, M_1, M_2, M_3, M_{12} and M_{13} can be also generated automatically.

Fig. 7 shows a part of deception matrix A_{23}. Its columns correspond to observed variables which can be changed by cyber-attackers.

Fig. 8 shows a part of conceal matrix S_{23}. Its diagonal elements corresponding to the observed variables in invaded zones are zeros.



	Manipulated Variables						Observed Variables									
	Local		Mar	Auto												
	V3	V4	W	V1	V2	H	L1i	L2i	F1i	T1i	T2i	V1i	V2i	Pi	Hi	Wi
W	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
V1	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0
V2	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0
H	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0

Fig. 5. Controller matrix [C] (26 × 26).

	V1	H	W
W	0	0	1
V1	1	0	0
V2	0	0	0
H	0	1	0

Fig. 6. Manipulation matrix [M_{23}] (26 × 3).

	F1i	T2i	V1i	Hi	L2i	T1i	Wi
L1i	0	0	0	0	0	0	0
L2i	0	0	0	0	0	0	0
F1i	1	0	0	0	0	0	0
T1i	0	0	0	0	0	0	0
T2i	0	1	0	0	0	0	0
V1i	0	0	1	0	0	0	0
V2i	0	0	0	0	0	0	0
Pi	0	0	0	0	0	0	0
Hi	0	0	0	1	0	0	0
Wi	0	0	0	0	0	0	0

Fig. 7. Attack matrix [A_{23}] (26 × 7).

Fig. 9 shows a part of observation matrix O_{23}. Its rows correspond to surviving sensors.

These matrices can be generated when invaded zones are determined.

Detectability matrix is defined by Eq. (1).

$$D_{23}(n) = \sum_{k=1}^{n} O_{23}(S_{23} \cdot P \cdot C)^{k-1} S_{23} \cdot P \cdot M_{23} \tag{1}$$

If non-zero elements appear in each column of the detectability matrix, it can be judged that the effects of the manipulation can be detected under concealment by cyber attackers. If manipulation cannot be detected, all elements of the column corresponding to it remain zero even when the order of detectability matrix (i.e. n in Eq. (1)) is larger than the number of columns of P.

	L1i	L2i	F1i	T1i	T2i	V1i	V2i	Pi	Hi	Wi
L1i	1	0	0	0	0	0	0	0	0	0
L2i	0	0	0	0	0	0	0	0	0	0
F1i	0	0	0	0	0	0	0	0	0	0
T1i	0	0	0	0	0	0	0	0	0	0
T2i	0	0	0	0	0	0	0	0	0	0
V1i	0	0	0	0	0	0	0	0	0	0
V2i	0	0	0	0	0	0	1	0	0	0
Pi	0	0	0	0	0	0	0	1	0	0
Hi	0	0	0	0	0	0	0	0	0	0
Wi	0	0	0	0	0	0	0	0	0	0

Fig. 8. Concealment matrix [S_{23}] (26 × 26).

	L1i	L2i	F1i	T1i	T2i	V1i	V2i	Pi	Hi	Wi
L1i	1	0	0	0	0	0	0	0	0	0
V2i	0	0	0	0	0	0	1	0	0	0
Pi	0	0	0	0	0	0	0	1	0	0

Fig. 9. Survivor matrix [O_{23}] (3 × 26).

	W	V1	H
L1i	1	1	0
V2i	1	1	0
Pi	1	1	0

Fig. 10. Detectability matrix [$D_{23}(26)$] (3 × 3).

	V1	H
L1i	1	0
L2i	1	0
T1i	0	1
V2i	1	0
Pi	1	0
Wi	0	0

Fig. 11. Detectability matrix [$D_2(3)$] (3 × 3).

Fig. 10 shows the detectability matrix $D_{23}(26)$. All elements of the column corresponding to heater power H are zeros. It shows that manipulation of heater cannot be detected when zones 2 and 3 are invaded. The plant shown in Fig. 3 has only two temperature sensors and they are included in zones 2 and 3. The temperature change caused by heater power manipulation cannot be detected when zones 2 and 3 are invaded. This fact can be recognized automatically through Boolean matrix calculation.

Fig. 11 shows the detectability matrix $D_2(3)$. It shows every manipulation in zone 2 can be detected in three steps of propagation. The value of n in Eq. (1) can be a performance index for detection. In this case, the manipulation of heater can be detected with the temperature sensor at the other tank, T1i.

It is easy to calculate the detectability matrices for all cases of invasion by cyber attackers. It can be confirmed that only the case in which zone 2 and zone 3 are invaded and heater is manipulated is undetectable. Needless to describe, if all zones are invaded, any manipulation under concealment cannot be detected from sensed information.

To enable the detection of the heater manipulation by cyber-attackers, temperature sensor signal is necessary in zone 1. It can be

	F1i	T2i	V1i	Hi	L2i	T1i	Wi
L1	1	0	1	0	0	0	1
F1	1	0	1	0	0	0	1
F2	1	0	1	0	0	0	1
F3	1	0	1	0	0	0	1
F4	0	0	0	0	0	0	0
F5	0	0	0	0	0	0	0
T1	1	1	1	1	0	0	1
L2	1	0	1	0	0	0	1
T2	1	1	1	1	0	0	1
P	1	0	1	0	0	0	1
V3	0	0	0	0	0	0	0
V4	0	0	0	0	0	0	0
W	0	0	0	0	0	0	1
V1	1	0	1	0	0	0	1
V2	1	0	1	0	0	0	1
H	1	1	1	1	0	0	1

Fig. 12. Reachability matrix [$R_{23}(3)$] (26 × 7).

Please cite this article in press as: Hashimoto, Y., et al. Safety securing approach against cyber-attacks for process control system. *Computers and Chemical Engineering* (2013), http://dx.doi.org/10.1016/j.compchemeng.2013.04.019

realized without addition of a temperature sensor if analog signal from the temperature sensor is duplicated and transferred to zone 1. Another method is to limit the number of zones two.

The risk of deception can be estimated with the following calculation.

$$R_{23}(n) = \sum_{k=1}^{n} (P \cdot C)^{k-1} P \cdot A_{23} \tag{2}$$

Fig. 12 shows reachability matrix $R_{23}(26)$. It shows the effects of deception in invaded zones. While deception of T1i does not affect others, the change of T2i can cause heater manipulation by its controller.

By computing detectability matrices and reachability matrices, influence of manipulation, concealment and deception can be estimated. The security levels of different zone division patterns can be compared numerically.

6. Conclusion

Evaluation method of security zoning for Industrial Control Systems is proposed by defining detectability matrix and reachability matrix. This approach shows an example of the cooperation of information engineers and process engineers for security improvement of control systems.

Acknowledgment

The authors wish to express sincere appreciation to the METI's Task Force on ICS security for their valuable feedback.

References

National Research Council. (2010). *Review the Department of Homeland Security's Approach to Risk Analysis*. National Academy of Sciences.

Shindo, A., Yamazaki, H., Toki, A., Koshijima, I., & Umeda, T. (2000). An approach to potential risk analysis of networked chemical plants. *Computers & Chemical Engineering*, *24*(2), 721–727 (7).

Toyoshima, T., Sun, J., Koshijima, I., & Hashimoto, Y. (2011). Risk analysis and countermeasure planning against cyber-attacks. *Journal of Human Factors in Japan*, *15*(2), 4–9.

Uehara, T. (2011). SCADA system and cyber security. *Journal of Human Factors in Japan*, *15*(2), 10–13.

Yogo, S., Toyoshima, T., Sun, J., Koshijima, I., & Hashimoto, Y. (2011). Design of safe plants considering cyber security. In *Proceedings of 43rd Autumn Meeting of S. Chem. Engr* Japan, Q101, 2011.

Please cite this article in press as: Hashimoto, Y., et al. Safety securing approach against cyber-attacks for process control system. *Computers and Chemical Engineering* (2013), http://dx.doi.org/10.1016/j.compchemeng.2013.04.019