2014 14th International Conference on Control, Automation and Systems (ICCAS 2014)
Oct. 22-25, 2014 in KINTEX, Gyeonggi-do, Korea

Development of CAD for Zone Dividing of Process Control Networks to Improve Cyber Security

Hiroki Moritani[1*], Shuichi Yogo, Takahito Morita, Midori Kojima, Kento Watanabe, Jing Sun, Ichiro Koshijima and Yoshihiro Hashimoto[2]

[1] Department of Civil and Management Engineering , Nagoya Institute of Technology, Nagoya, 466-0061, Japan (26418557@stn.nitech.ac.jp) *

[2] Department of Civil and Management Engineering, Nagoya Institute of Technology, Nagoya, 466-0061, Japan (hashimoto@nitech.ac.jp)

Abstract: Recently, cyber security becomes a serious problem for not only OA (Office Automation) systems but also PA (Process Automation) and FA (Factory Automation) systems. Even the controllers, which are not connected to Internet directly, have been attacked with malwares, such as Stuxnet and Quantum. When control system fails, it may lead to serious accidents such as explosion or leakage of poisonous and deleterious substances. For process control, cyber-attack is one of the causes to threaten safety. The authors of this paper had proposed zone division of process control networks to ensure cyber security and safety. To apply the method, it is necessary to build CE (Cause Effect) matrices which express the qualitative information of the plant and controllers. It is very troublesome for large-scale plants. CAD (Computer Aided Design) tool for zone dividing is proposed in this paper. CE matrices are generated by using DAE (Differential and Algebraic Equation) registered in equipment modules of plant CAD such as ASPEN or Pro II. The candidates of zone division of process control networks, which can assure the safety against concealment and remote operation by cyber attackers, can be proposed.

Keywords: Cyber Security, Process Control, Computer Aided Design, Process Safety

1. INTRODUCTION

For ICS (Industrial Control Systems), cyber security had not been a serious security problem for many years because they are isolated from internet and their operation systems are specific to the manufacturers. However, recently many ICS have already connected with internet to communicate many kinds of information such as production demands and performances. Remote maintenance becomes popular for ICS. Even to control system development, open systems such as Windows and Ethernet have been applied.

Stuxnet, which was a malware discovered in 2010, was epoch making. It succeeded to attack the PLC (Programmable Logic Controllers) of the centrifuges for uranium enrichment in Iran, even though they were isolated from internet and their operation system was maker's original. It had been spread via internet and USB. Because Stuxnet has zero-day attacks, any anti-virus could not work. It searched and found maintenance PC of the PLC. It invaded the PLC via maintenance PC, modified their codes and concealed the attack.

Although Stuxnet had the specified target, it can be tailored to attack any SCADA (Supervisory Control And Data Acquisition) systems and PLC systems. Therefore, indiscriminate cyber-attacks must be a serious threat for any ICS.

ICS has serious vulnerability. Anti-virus software is commonly applied to PC and its database is updated almost every day. Security patches are also provided from product developers. However, they are not applied to ICS because controller might become out of condition due to the increase of computer load.

In this situation, ICS require highly reliable security and safety services with urgent priority. It is necessary not only information network security measurements, but also essential ICS security measurements are necessary.

In this paper, automatic ICS zoning tool for safety improvement against cyber-attacks is proposed. It assumed that indiscriminate cyber-attacks are inevitable. If the protection measures of each zone are different from others, some zones can survive from cyber-attacks when another zone fell. If the attack could be detected immediately and countermeasures could be adopted in survivng zone, serious hazard could be avoided.

The design methods for zone dividing of the process control networks were already proposed [1, 2]. To apply it, it is necessary to build CE (Cause Effect) matrices which express the qualitative information of the plant and controllers. It is very troublesome if the plant is large-scale. In this paper, CAD (Computer Aided Design) tool for zone dividing is proposed. CE matrices are generated by using DAE (Differential and Algebraic Equation) which are registered in equipment modules of plant CAD such as ASPEN or Pro II. The zone division of process control networks, which can assure the safety against concealment and remote operation by cyber attackers, can be proposed.

2. SAFETY ANALYSIS CONSIDERING CYBER ATTACK

For safety analysis, **"cyber-attacks are malicious failures and malicious misoperations."** Failures and misoperations have been analyzed in safety assessment since long time ago. However, it was not considered that multiple troubles occur at the same time. Cyber terrorists combine the weapons to ensure their attacks. Whatever kinds of weapons would be utilized, the possible hazard

was already determined by the target plant. If only water is dealt in the plant, explosion cannot occur. If multiple failures are considered, safety analysis method can be effective to consider cyber-security measures [1, 2].

Fault tree is a very popular method to evaluate risks. It can deal with multiple failures. Attacks of cyber terrorists are parts of causes of accidents. Fig. 1 shows the fault tree whose top event is "Fire or breakage of tank heater". To improve safety the condition of AND gates are important. If the prevention of one of the conditions is succeeded, the accident can be avoided. The tree structure in Fig. 1 is divided into time and state at the top. To succeed the cyber-attacks not only operation but also concealment must be considered.

To achieve fire or breakage of the heater, continuity of heating until temperature is increased to the dangerous point is necessary. It is necessary for cyber-attackers to prevent detection of overheat before fire or breakage of the heater. The left side of the fault tree in Fig. 1 analyzed the targets of concealment.

The right side shows the analysis of targets of remote operation. To achieve fire making the heater on and making the tank empty are necessary [2]. If the temperature controller or the level controller survives from cyber-attacks, the hazard cannot occur.

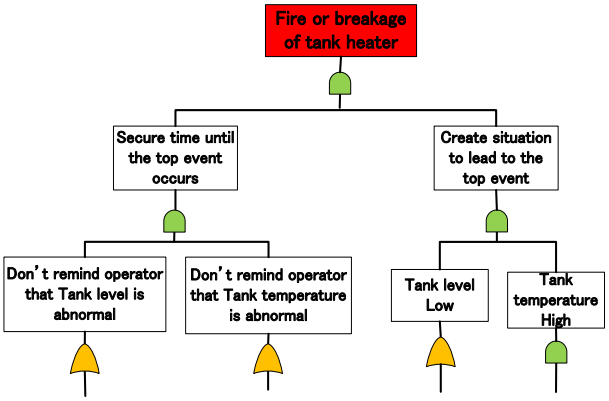

Fig. 1 Fault tree considering cyber-attack

3. ZONE DIVISION OF PROCESS CONTROL NETWORKS

As it is described in the previous section, cyber attackers need multiple operations to cause accidents. If the temperature controller and the level controller are divided into other zones and the both zones don't fall in cyber-attacks at the same time, the possibility of the hazard occurrence is decreased.

In Fig. 2 a sample structure of zone division is shown. In this example controllers and sensors in a plant are assigned into three zones. In each zone SCADA and an OPC (Object linking and embedding for Process

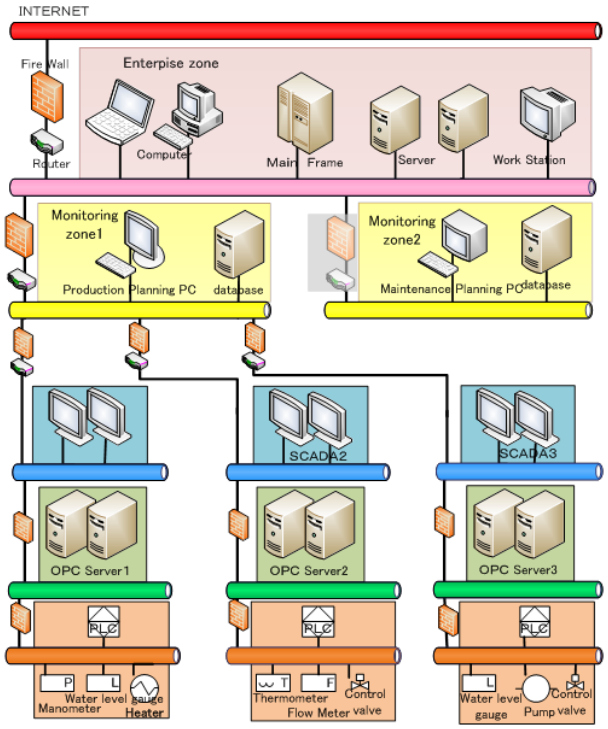

Fig. 2 Zone and conduit model [1]

geographically and functionally. Exchange of the controllers and sensors between zones is proposed in order to secure the control system. The operation of the three parts is executed normally. However, the information of the three parts is exchanged between OPC. By applying OPC-UA (Unified Architecture), the server OS, server machine, certification keys and so on can be different from other zones. By applying different security measures to zones, the vulnerability of the zones is made different [3].

4. ZONE DESIGN FOR CYBER-ATTACK DETECTION

If there are zones which survive from cyber-attacks, there is possibility to detect the effects of remote operation in the zones which fell in attacks. Even if the changes were concealed in the zones fell in cyber-attacks, the physical changes might propagate to the zones which survived.

The possibility of cyber-attack detection depends on the division of the controller zones. A method based on CE matrices has been already proposed [2]. If assignment of sensors and controllers into zones is assumed, the detectability of the remote operation and concealment can be assessed.

CE matrices express the relationships between variables of the plant and control system with Boolean. They express behavior related to operation and disturbance of the plant qualitatively.

Although the structure of CE matrices is very simple, generation of the CE matrices of the whole equipment of large scale plants are very troublesome.

For process design and simulation, there are many

Table 2 DAE structure of the example plant

	dx/dt	x(t)	z(t)			u(t)			
	dL/dt	L	F1	F2	P2	V1	V2	P1	P0
0	1	0	1	1	0	0	0	0	0
0	0	1	0	0	1	0	0	0	1
0	0	0	1	0	0	1	0	1	1
0	0	0	0	1	1	0	1	0	1

Table 3 Matrix from system equations using random number

	dx/dt	x(t)	z(t)			u(t)			
	dL/dt	L	F1	F2	P2	V1	V2	P1	P0
0	0.709	0	1	−1	0	0	0	0	0
0	0	1.078	0	0	1	0	0	0	1
0	0	0	0.695	0	0	1.013	0	1	−1
0	0	0	0	1.944	1	0	1.849	0	−1

Table 4 Result of sweeping out calculation

	dx/dt	x(t)	z(t)			u(t)			
	dL/dt	L	F1	F2	P2	V1	V2	P1	P0
0	0.709	−0.5545	0	0	0	−1.4576	0.95113	−1.4388	0.41004
0	0	0	1	0	0	1.45755	0	1.43885	−1.4388
0	0	−0.5545	0	1	0	0	0.95113	0	−1.0288
0	0	1.078	0	0	1	0	0	0	1

Table 5 CE Matrix expressing process of example plant

P		x(t)	z(t)			u(t)			
		L	F1	F2	P2	V1	V2	P1	P0
x(t+⊿t)	L	1	0	0	0	1	1	1	1
z(t)	F1	0	0	0	0	1	0	1	1
	F2	1	0	0	0	0	1	0	1
	P2	1	0	0	0	0	0	0	1
u(t)	V1	0	0	0	0	1	0	0	0
	V2	0	0	0	0	0	1	0	0
	P1	0	0	0	0	0	0	1	0
	P0	0	0	0	0	0	0	0	1

Table 6 Simplified CE matrix when only L is the controlled variable.

P		x(t)	u(t)			
		L	V1	V2	P1	P0
x(t+⊿t)	L	1	1	1	1	1
u(t)	V1	0	1	0	0	0
	V2	0	0	1	0	0
	P1	0	0	0	1	0
	P0	0	0	0	0	1

determined according to the valve openings V1 and V2. V1, V2, P0 and P1 are the causes and F1 and F2 are the effects.

There is possibility to have other boundary conditions. In some case, F1 is determined by the upstream equipment. In this case F1 and V1 are the causes and P1 is the effect. It can be changed according to the boundary conditions, which are causes or effects.

Therefore, registration of CE matrix is difficult to equipment module in CAD.

In this paper, it is proposed that CE matrices for whole plant are generated using DAE.

For each equipment module, DAE as shown in Table1 are registered in the CAD tools. At first, the DAE for each module are combined according to the connection of the equipment icons on graphical display.

Based on the combined DAE, the Boolean matrix of the whole plant is generated as shown in Table 2. “1”s in the matrix express the existence of the term of the variables in each equation of DAE.

Next, the dependency between the process variables must be considered. The manipulated variables and the

When only L is the controlled variable, the CE matrix can be simplified as shown in Table 6.

Because this procedure solves linear equations numerically, even to large-scale plants, it is applicable for generation of their CE matrices.

4.2 Cyber-Attack Detectability Check using CE Matrices

In this section, the method to assess the detectability of cyber-attacks using CE matrices is illustrated by using the plant shown in Fig. 4. Controllers and sensors are divided into two zones.

The CE matrices in this procedure contain two entries for each variable to distinguish real and tricked values as shown in Tables 7-12. For example, L1{1}indicates the real value and L1{1}i does the observed value.

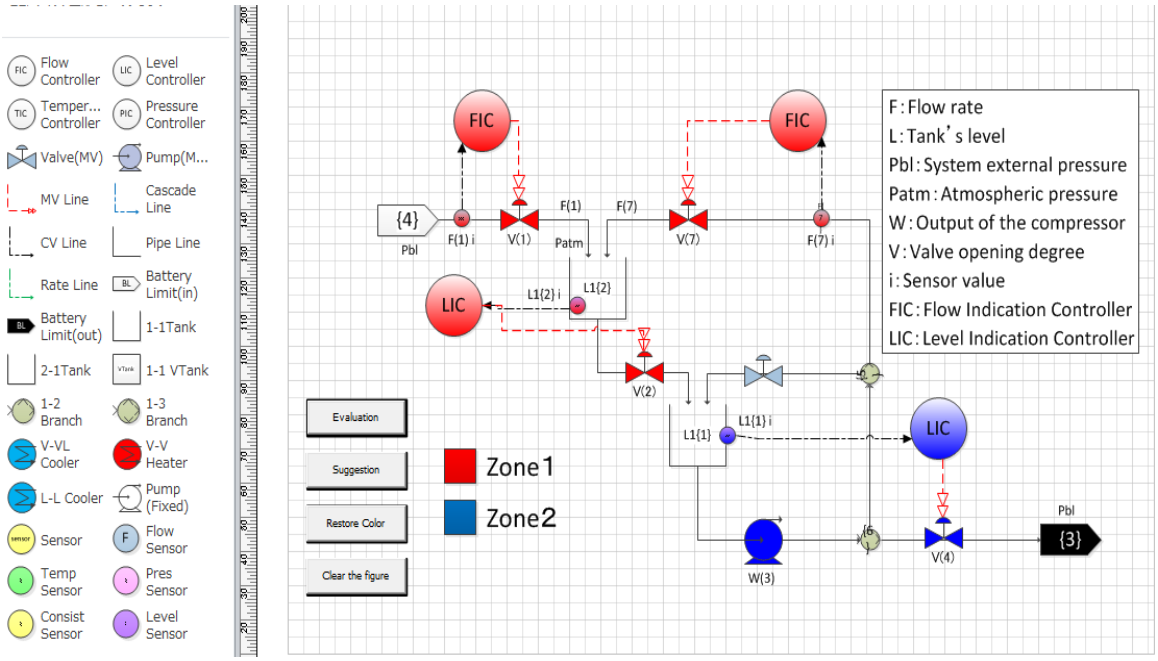

Fig. 4 water circulation system with zone division

$$D(m) = \sum_{k=1}^{m} S \cdot (O \cdot P \cdot C)^{k-1} \cdot O \cdot P \cdot M$$

Matrix D is the matrix to assess the ability to detect the cyber-attacks with sensor values in the surviving zone. The calculation procedure and its meaning is illustrated.

From the right term in the right side of the definition of Detectability matrix (D), the illustration is begun.

is fixed, the calculation of Detectability matrix (D) must be executed as many times as the variation of the assumption which zones fell or survived.

The following calculation is the assessment of the detectability of cyber-attacks in Zone 1 by using the sensors in Zone 2, which is assumed to survive.

Table 7 Matrix P of the plant of Fig. 4

P		2	1	1	1	1	1	2	2	1	0	0	2	1	1	1	1	1	2	2	1
		L1[1]	L1[2]	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1[1]ｉ	L1[2]ｉ	F(1)ｉ	F(7)ｉ	V(1)ｉ	V(2)ｉ	W(3)ｉ	V(4)ｉ	V(7)ｉ
2	L1[1]	1	1	0	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0
1	L1[2]	0	1	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
1	F(1)	0	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
1	F(7)	1	0	0	1	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	V(1)	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	V(2)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	W(3)	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	V(4)	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	V(7)	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0	Patm	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	Pbl	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
2	L1[1]ｉ	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
1	L1[2]ｉ	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	F(1)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	F(7)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	V(1)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
1	V(2)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
2	W(3)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	V(4)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	V(7)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Table 8 Matrix C of the plant of Fig. 4

Cb		2	1	1	1	1	1	2	2	1	0	0	2	1	1	1	1	1	2	2	1
		L1[1]	L1[2]	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1[1]ｉ	L1[2]ｉ	F(1)ｉ	F(7)ｉ	V(1)ｉ	V(2)ｉ	W(3)ｉ	V(4)ｉ	V(7)ｉ
2	L1[1]	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	L1[2]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	F(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	F(7)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	V(1)	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	V(2)	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
2	W(3)	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	V(4)	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	V(7)	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
0	Patm	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	Pbl	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
2	L1[1]ｉ	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
1	L1[2]ｉ	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	F(1)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	F(7)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	V(1)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
1	V(2)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0
2	W(3)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	V(4)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	V(7)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1

Table 9 Matrix O of the plant of Fig. 4

Ob		2	1	1	1	1	1	2	2	1	0	0	2	1	1	1	1	1	2	2	1
		L1[1]	L1[2]	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1[1]ｉ	L1[2]ｉ	F(1)ｉ	F(7)ｉ	V(1)ｉ	V(2)ｉ	W(3)ｉ	V(4)ｉ	V(7)ｉ
2	L1[1]	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	L1[2]	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	F(1)	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	F(7)	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	V(1)	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	V(2)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	W(3)	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	V(4)	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	V(7)	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0	Patm	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	Pbl	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
2	L1[1]ｉ	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
1	L1[2]ｉ	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	F(1)ｉ	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	F(7)ｉ	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	V(1)ｉ	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
1	V(2)ｉ	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0
2	W(3)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	V(4)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	V(7)ｉ	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1

Table 10 Matrix S of the plant of Fig. 4

Sb		2	1	1	1	1	1	2	2	1	0	0	2	1	1	1	1	1	2	2	1
		L1[1]	L1[2]	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1[1]ｉ	L1[2]ｉ	F(1)ｉ	F(7)ｉ	V(1)ｉ	V(2)ｉ	W(3)ｉ	V(4)ｉ	V(7)ｉ
1	L1[2]ｉ	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	F(1)ｉ	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	F(7)ｉ	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	V(1)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
1	V(2)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
2	W(3)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	V(4)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	V(7)ｉ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Table 11 Matrix M of the plant of Fig. 4

Mb		2	2
		W(3)	V(4)
2	L1[1]	0	0
1	L1[2]	0	0
1	F(1)	0	0
1	F(7)	0	0
1	V(1)	0	0
1	V(2)	0	0
2	W(3)	1	0
2	V(4)	0	1
1	V(7)	0	0
0	Patm	0	0
0	Pbl	0	0
2	L1[1] i	0	0
1	L1[2] i	0	0
1	F(1) i	0	0
1	F(7) i	0	0
1	V(1) i	0	0
1	V(2) i	0	0
2	W(3) i	0	0
2	V(4) i	0	0
1	V(7) i	0	0

Table 12 Matrix D of the plant of Fig. 4

Db		2	2
		W(3)	V(4)
1	L1[2] i	0	0
1	F(1) i	0	0
1	F(7) i	1	1
1	V(1) i	0	0
1	V(2) i	0	0
1	V(7) i	0	0

N ote
man hat
the are
incl ed.
T by

multiplying (P), which is the CE matrix of the plant.

Next, (O) is multiplied in the definition of (D). (O) is observation matrix, which express the concealment of the changes in the zones fell in the cyber-attacks. The values of L1(1)i, W(3)i and V(4)i in Zone 1 are made zero by multiplying (O) in Table 9, even when their real values are changed.

Then, the controllers operate the actuator based on the observed values affected by concealment. The behavior of the controllers is expressed by multiplying Controller matrix (C).

Next, the effects of the controller actions are calculated by multiplying (P). And the change in Zone 1 is concealed again by crackers. It is expressed by multiplying (O).

The procedure, (C) -> (P) -> (O), is repeated.

In this repeat the effects of the cyber-attacks in Zone 1 might be able to be detected in Zone 2. Survival matrix (S) in Table 10 means the abstraction of observation in the zones which survive.

By calculating of the series in the definition, Detectability matrix (D) can be obtained as shown in Table 12. (D) in Table 12 indicates that any remote manipulation in Zone 1 can be detected by monitoring F7(i) in Zone 2 even when the attacks were concealed.

In addition to it, the observation of any other variables in Zone 2 is not effective to detect the cyber-attacks in Zone 1, when the concealment was executed.

As mentioned before, this procedure should be applied to other scenarios. In this case, (D) must be re-calculated by changing (M), (O) and (S) to express the cyber-attacks in Zone 2 and observation of Zone 1.

If the zone division is assumed, the modification of these matrices can be executed automatically.

5. DEVELOPMENT OF CAD TOOL FOR ZONE DESIGN

We developed a zone design tool based on the explained method. It is developed by using Microsoft Visio, Excel, Visual Basic for Application, and MATLAB. Fig. 4 shows the zone design tool screen. Equipment modules are prepared in the library in the left part of the window. Each module has its DAE information which is contained in an Excel worksheet. Stream icons are also prepared. By using them, connection of equipment is determined. Each stream has the equations of the relationships between flow rate and pressure loss.

By putting equipment modules on the display and connecting them as shown in Fig. 4, the DAE for the whole plant are automatically generated.

Icons for sensors, actuators, controllers and information link between them are also prepared. By connecting sensors and actuators to the plant model, MVs and PVs are determined. Present version of our CAD can assess any zone division and propose the zone design that can detect an abnormality.

6. CONCLUSION

In this study a method to generate CE matrices of the whole system using DAE registered in the plant modules was proposed. Based on it, CAD tool using Visio and so on were developed. It can assess the detectability of cyber-attacks and propose the preferable zone division.

REFERENCES

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

[2] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, J. Sun, I. Koshijima, “Safety securing approach against cyber-attacks for process control system,” *Computers & Chemical Engineering*, Vol. 57, pp. 181-186, 2013.

[3] Y. Hashimoto, “Consideration of security measures to improve in testbed and expectation for OPC-UA,” *Keisou [Instrumentation]*, October 2013.