Monthly Report

Zhang Qi

School of Automation,
Huazhong University of Science and Technology,
Wuhan, China.

May 3, 2016

Outlines

Introduction of Simulation Platform

Simulation of State Controller

Simulation of Optimal Defense Strategy Generator

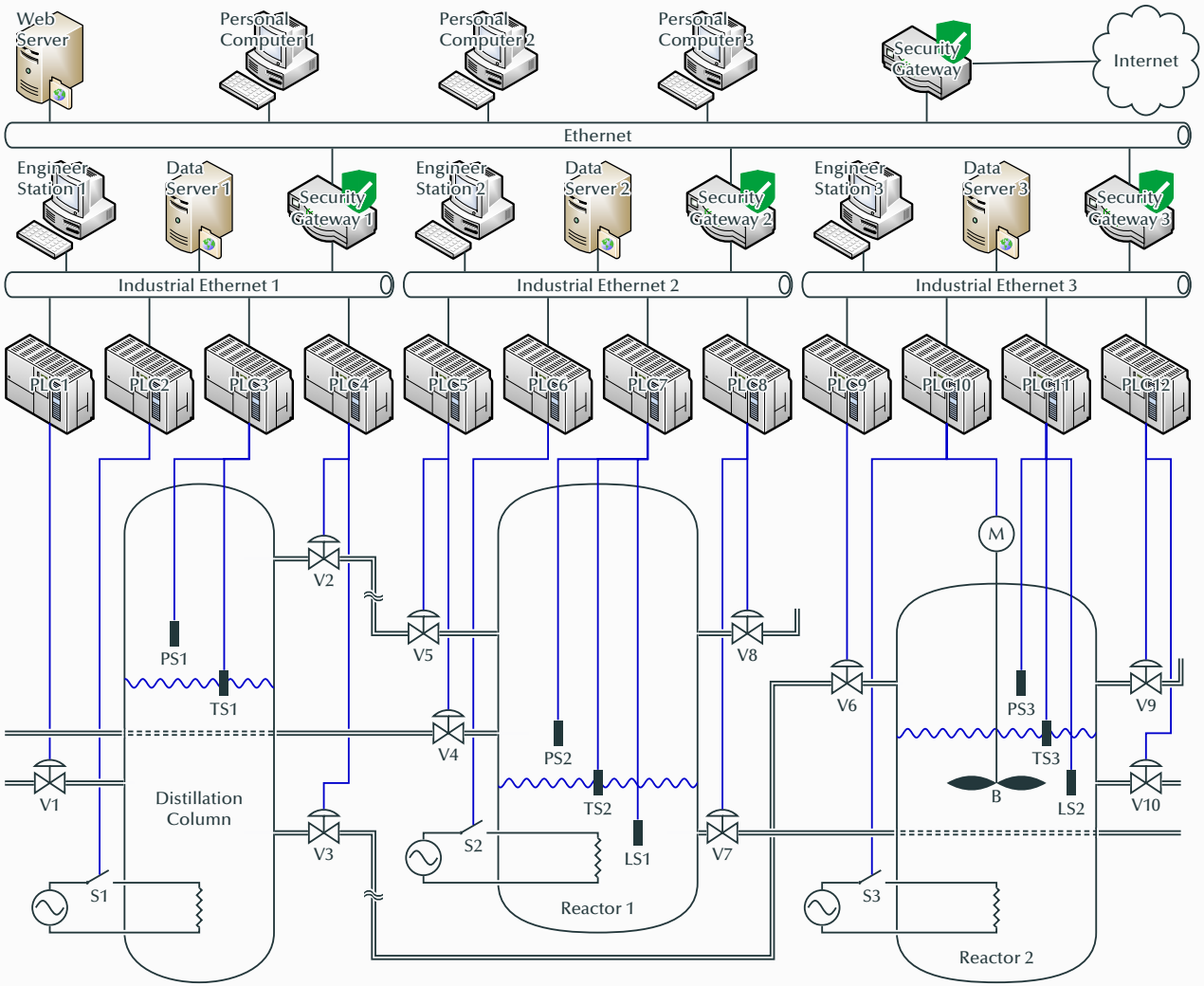
Simulation of Real-Time Capability

Task Planning

Introduction of Simulation Platform

The Structure of Chemical Reactor Control System

The simplified chemical reactor control system is shown in the following figure.



Attack Analysis

The potential attacks are shown as follows.

Symbol	Description	Launch Condition
a_1	network scanning of the Ethernet in the management layer	—
a_2	vulnerability scanning of the devices in the management layer	launch of a_1
a_3	buffer overflow attack on the web server	launch of a_2
a_4	brute force attack on the web server	launch of a_2
a_5	brute force attack on the personal computer 1	launch of a_2
a_6	brute force attack on the personal computer 2	launch of a_2
a_7	brute force attack on the personal computer 3	launch of a_2
a_8	network scanning of the industrial Ethernet 1 in the control layer	launch of a_3, a_4, a_5, a_6, a_7

Attack Analysis

The potential attacks are shown as follows.

Symbol	Description	Launch Condition
a_9	vulnerability scanning of the devices in the industrial Ethernet 1	launch of a_8
a_{10}	buffer overflow attack on the data server 1	launch of a_9
a_{11}	brute force attack on the data server 1	launch of a_9
a_{12}	brute force attack on the engineer station 1	launch of a_9
a_{13}	network scanning of the industrial Ethernet 2 in the control layer	launch of a_3, a_4, a_5, a_6, a_7
a_{14}	vulnerability scanning of the devices in the industrial Ethernet 2	launch of a_{13}
a_{15}	buffer overflow attack on the data server 2	launch of a_{14}
a_{16}	brute force attack on the data server 2	launch of a_{14}

Attack Analysis

The potential attacks are shown as follows.

Symbol	Description	Launch Condition
a_{17}	brute force attack on the engineer station 2	launch of a_{14}
a_{18}	network scanning of the industrial Ethernet 3 in the control layer	launch of a_3, a_4, a_5, a_6, a_7
a_{19}	vulnerability scanning of the devices in the industrial Ethernet 3	launch of a_{18}
a_{20}	buffer overflow attack on the data server 3	launch of a_{19}
a_{21}	brute force attack on the data server 3	launch of a_{19}
a_{22}	brute force attack on the engineer station 3	launch of a_{19}
a_{23}	DoS attack on PLC1	launch of a_{10}, a_{11}, a_{12}
a_{24}	DoS attack on PLC2	launch of a_{10}, a_{11}, a_{12}

Attack Analysis

The potential attacks are shown as follows.

Symbol	Description	Launch Condition
a_{25}	DoS attack on PLC3	launch of a_{10}, a_{11}, a_{12}
a_{26}	DoS attack on PLC4	launch of a_{10}, a_{11}, a_{12}
a_{27}	DoS attack on PLC5	launch of a_{15}, a_{16}, a_{17}
a_{28}	DoS attack on PLC6	launch of a_{15}, a_{16}, a_{17}
a_{29}	DoS attack on PLC7	launch of a_{15}, a_{16}, a_{17}
a_{30}	DoS attack on PLC8	launch of a_{15}, a_{16}, a_{17}
a_{31}	DoS attack on PLC9	launch of a_{20}, a_{21}, a_{22}
a_{32}	DoS attack on PLC10	launch of a_{20}, a_{21}, a_{22}

Attack Analysis

The potential attacks are shown as follows.

Symbol	Description	Launch Condition
a_{33}	DoS attack on PLC11	launch of a_{20}, a_{21}, a_{22}
a_{34}	DoS attack on PLC12	launch of a_{20}, a_{21}, a_{22}
a_{35}	man-in-the-middle attack on PLC1	launch of a_{12}
a_{36}	man-in-the-middle attack on PLC2	launch of a_{12}
a_{37}	man-in-the-middle attack on PLC3	launch of a_{12}
a_{38}	man-in-the-middle attack on PLC4	launch of a_{12}
a_{39}	man-in-the-middle attack on PLC5	launch of a_{17}
a_{40}	man-in-the-middle attack on PLC6	launch of a_{17}

Attack Analysis

The potential attacks are shown as follows.

Symbol	Description	Launch Condition
a_{41}	man-in-the-middle attack on PLC7	launch of a_{17}
a_{42}	man-in-the-middle attack on PLC8	launch of a_{17}
a_{43}	man-in-the-middle attack on PLC9	launch of a_{22}
a_{44}	man-in-the-middle attack on PLC10	launch of a_{22}
a_{45}	man-in-the-middle attack on PLC11	launch of a_{22}
a_{46}	man-in-the-middle attack on PLC12	launch of a_{22}

Function Analysis

The system functions are shown as follows.

Symbol	Description	Failure Condition
f_1	distillation	failure of f_2, f_3
f_2	the temperature control function of distillation column	failure of f_4, f_6, f_7, f_8
f_3	the pressure control function of distillation column	failure of f_5, f_7, f_9
f_4	the traffic control function of V1	launch of a_{23}, a_{35}
f_5	the traffic control function of V2	launch of a_{26}, a_{38}
f_6	the traffic control function of V3	launch of a_{26}, a_{38}
f_7	the switch control function of S1	launch of a_{24}, a_{36}
f_8	the temperature sensation function of distillation column	launch of a_{25}, a_{37}

Function Analysis

The system functions are shown as follows.

Symbol	Description	Failure Condition
f_9	the pressure sensation function of distillation column	launch of a_{25}, a_{37}
f_{10}	heating	failure of f_{11}, f_{12}, f_{13}
f_{11}	the temperature control function of reactor 1	failure of f_{14}, f_{15}, f_{16}, f_{18}, f_{19}
f_{12}	the pressure control function of reactor 1	failure of f_{17}, f_{18}, f_{20}
f_{13}	the level control function of reactor 1	failure of f_{14}, f_{15}, f_{16}, f_{21}
f_{14}	the traffic control function of V4	launch of a_{27}, a_{39}
f_{15}	the traffic control function of V5	launch of a_{27}, a_{39}
f_{16}	the traffic control function of V7	launch of a_{30}, a_{42}

Function Analysis

The system functions are shown as follows.

Symbol	Description	Failure Condition
f_{17}	the pressure reducing function of reactor 1	launch of a_{30}, a_{42}
f_{18}	the switch control function of S2	launch of a_{28}, a_{40}
f_{19}	the temperature sensation function of reactor 1	launch of a_{29}, a_{41}
f_{20}	the pressure sensation function of reactor 1	launch of a_{29}, a_{41}
f_{21}	the level sensation function of reactor 1	launch of a_{29}, a_{41}
f_{22}	mixing & heating	failure of f_{23}, f_{24}, f_{25}, f_{26}
f_{23}	the temperature control function of reactor 2	failure of f_{27}, f_{30}, f_{31}, f_{33}
f_{24}	the pressure control function of reactor 2	failure of f_{28}, f_{32}, f_{33}

Function Analysis

The system functions are shown as follows.

Symbol	Description	Failure Condition
f_{25}	the mixing function of reactor 2	launch of a_{32}, a_{44}
f_{26}	the level control function of reactor 2	failure of f_{29}, f_{30}, f_{31}
f_{27}	the temperature sensation function of reactor 2	launch of a_{33}, a_{45}
f_{28}	the pressure sensation function of reactor 2	launch of a_{34}, a_{46}
f_{29}	the level sensation function of reactor 2	launch of a_{33}, a_{45}
f_{30}	the traffic control function of V6	launch of a_{31}, a_{43}
f_{31}	the traffic control function of V10	launch of a_{34}, a_{46}
f_{32}	the pressure reducing function of reactor 2	launch of a_{34}, a_{46}

Function Analysis

The system functions are shown as follows.

Symbol	Description	Failure Condition
f_{33}	the switch control function of S3	launch of a_{32}, a_{44}
f_{34}	production scheduling	failure of f_{35}, f_{36}, f_{37}, f_{41}, f_{42}, f_{43}
f_{35}	the production scheduling function provided by personal computer 1	failure of f_{38}, f_{39}, f_{40}
f_{36}	the production scheduling function provided by personal computer 2	failure of f_{38}, f_{39}, f_{40}
f_{37}	the production scheduling function provided by personal computer 3	failure of f_{38}, f_{39}, f_{40}
f_{38}	the data service of industrial Ethernet 1	some security strategies
f_{39}	the data service of industrial Ethernet 2	some security strategies
f_{40}	the data service of industrial Ethernet 3	some security strategies

Function Analysis

The system functions are shown as follows.

Symbol	Description	Failure Condition
f_{41}	the configuration of PLCs of distillation column	some security strategies
f_{42}	the configuration of PLCs of reactor 1	some security strategies
f_{43}	the configuration of PLCs of reactor 2	some security strategies

Incident Analysis

The potential hazardous incidents are shown as follows.

Symbol	Description	Location	Inducement
e_1	pressure anomaly	distillation column	failure of f_3
e_2	temperature anomaly	distillation column	failure of f_2
e_3	traffic of anomaly	distillation column	failure of f_4, f_6
e_4	excessive pressure	reactor 1	failure of f_{12}
e_5	low pressure	reactor 1	failure of f_{12}
e_6	temperature anomaly	reactor 1	failure of f_{11}
e_7	excessive liquid level	reactor 1	failure of f_{13}
e_8	low liquid level	reactor 1	failure of f_{13}

Incident Analysis

The potential hazardous incidents are shown as follows.

Symbol	Description	Location	Inducement
e_9	explosion	reactor 1	occurrence of e_4
e_{10}	heater dry fired	reactor 1	occurrence of e_8
e_{11}	liquid overflow	reactor 1	occurrence of e_7
e_{12}	excessive pressure	reactor 2	failure of f_{24}
e_{13}	low pressure	reactor 2	failure of f_{24}
e_{14}	temperature anomaly	reactor 2	failure of f_{23}
e_{15}	excessive liquid level	reactor 2	failure of f_{26}
e_{16}	low liquid level	reactor 2	failure of f_{26}

Incident Analysis

The potential hazardous incidents are shown as follows.

Symbol	Description	Location	Inducement
e_{17}	explosion	reactor 2	occurrence of e_{12}
e_{18}	heater dry fired	reactor 2	occurrence of e_{16}
e_{19}	liquid overflow	reactor 2	occurrence of e_{15}
e_{20}	blender stop	reactor 2	failure of f_{25}
e_{21}	out of control	distillation column	failure of f_{41}
e_{22}	out of control	reactor 1	failure of f_{42}
e_{23}	out of control	reactor 2	failure of f_{43}
e_{24}	production scheduling error	control layer	failure of f_{34}

Asset Analysis

The system assets are shown as follows.

Symbol	Description	Value($)	Hazardous Incident
z_1	semi-product s01 and s02	30,000	e_1, e_2, e_3, e_{21}, e_{24}
z_2	product s03	60,000	e_5, e_6, e_9, e_{11}, e_{22}, e_{24}
z_3	product s04	70,000	e_{13}, e_{14}, e_{17}, e_{20}, e_{23}, e_{24}
z_4	tank and sensors of reactor 1	200,000	e_9
z_5	heater of reactor 1	40,000	e_9, e_{10}
z_6	tank, sensors and blender of reactor 2	300,000	e_{17}
z_7	heater of reactor 2	50,000	e_{17}, e_{18}
z_8	staff 1-4	800,000	e_9, e_{11}

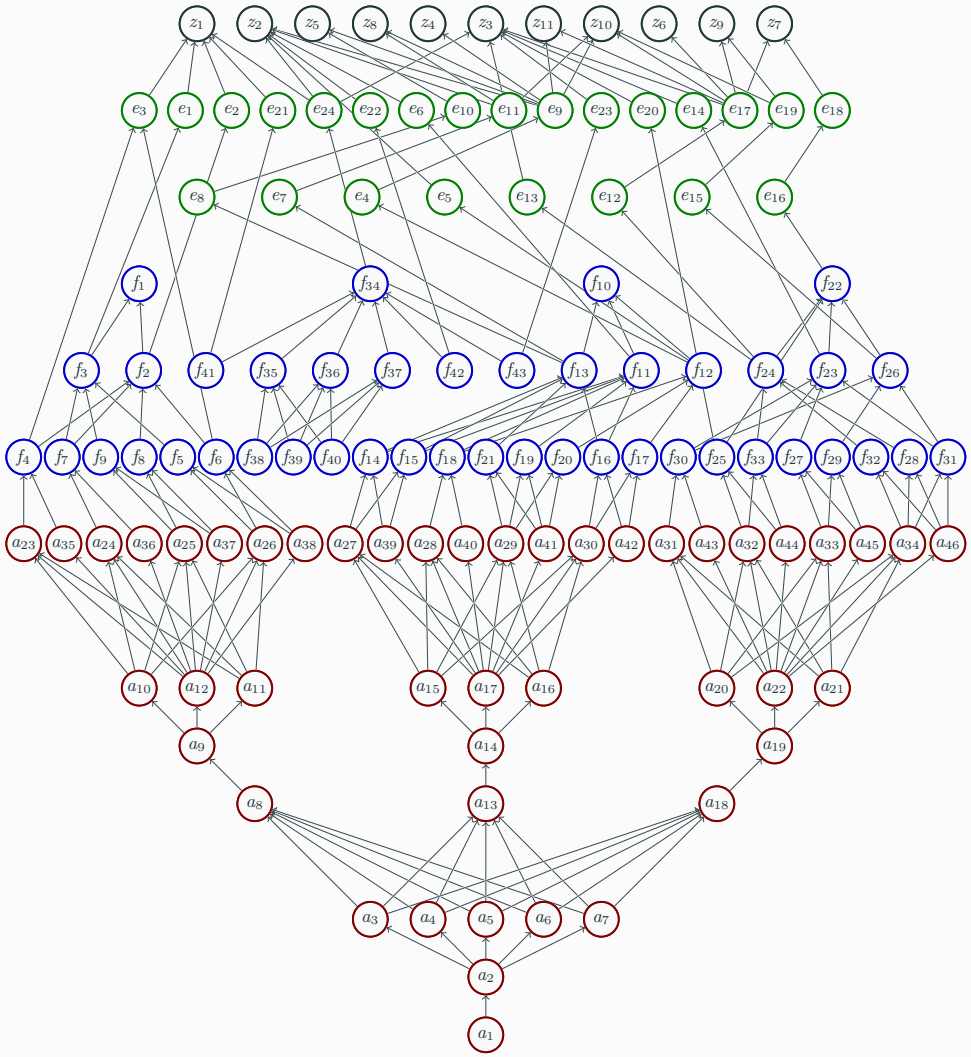
Asset Analysis

The system assets are shown as follows.

Symbol	Description	Value($)	Hazardous Incident
z_9	staff 5-9	100,000	e_{17}, e_{19}
z_{10}	river and solid	900,000	e_9, e_{11}, e_{17}, e_{19}
z_{11}	air	400,000	e_9, e_{17}

Multi-Level Bayesian Network

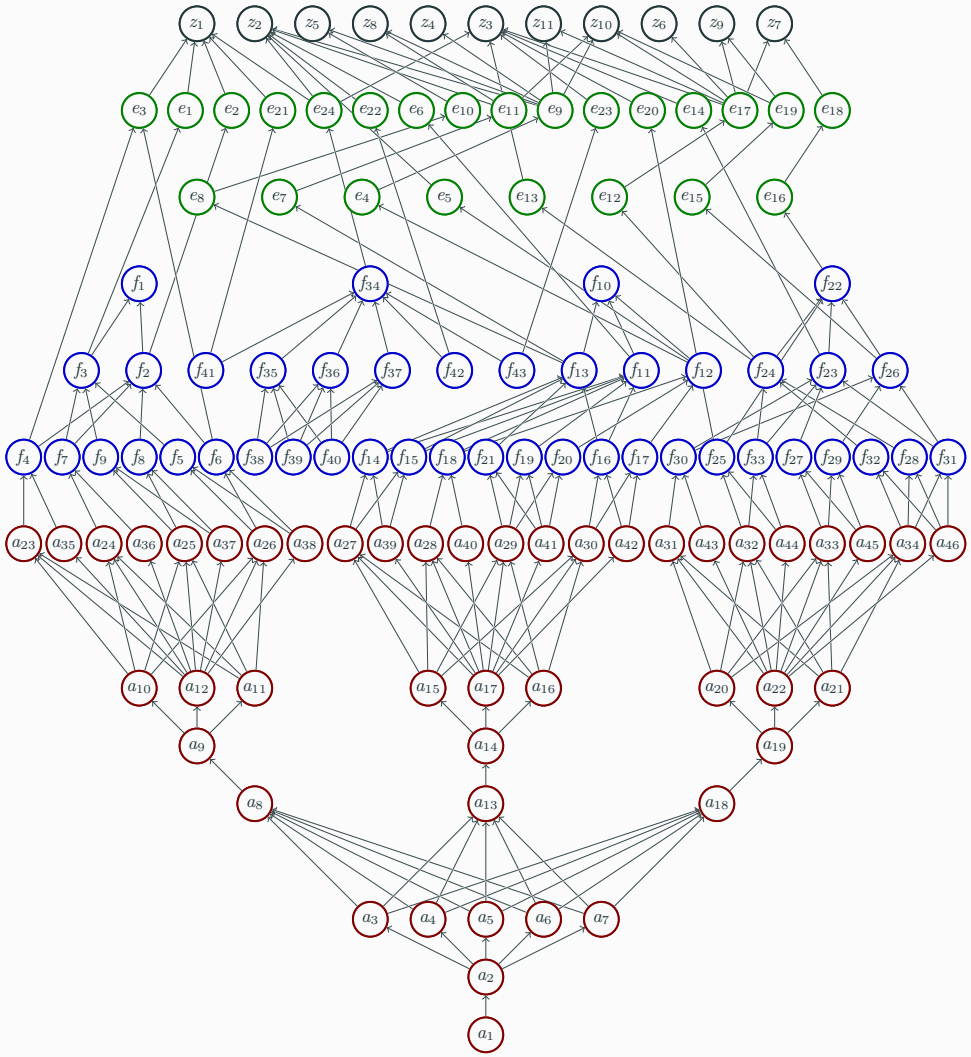
The multi-level Bayesian network is shown in the following figure.



a_1 – network scanning of the Ethernet in the management layer
a_2 – vulnerability scanning of the devices in the management layer
a_3 – buffer overflow attack on the web server
a_4 – brute force attack on the web server
a_5 – brute force attack on the personal computer 1
a_6 – brute force attack on the personal computer 2
a_7 – brute force attack on the personal computer 3
a_8 – network scanning of the industrial Ethernet 1 in the control layer
a_9 – vulnerability scanning of the devices in the industrial Ethernet 1
a_{10} – buffer overflow attack on the data server 1
a_{11} – brute force attack on the data server 1
a_{12} – brute force attack on the engineer station 1
a_{13} – network scanning of the industrial Ethernet 2 in the control layer
a_{14} – vulnerability scanning of the devices in the industrial Ethernet 2
a_{15} – buffer overflow attack on the data server 2
a_{16} – brute force attack on the data server 2
a_{17} – brute force attack on the engineer station 2
a_{18} – network scanning of the industrial Ethernet 3 in the control layer
a_{19} – vulnerability scanning of the devices in the industrial Ethernet 3
a_{20} – buffer overflow attack on the data server 3
a_{21} – brute force attack on the data server 3
a_{22} – brute force attack on the engineer station 3
a_{23} – DoS attack on PLC1
a_{24} – DoS attack on PLC2
a_{25} – DoS attack on PLC3
a_{26} – DoS attack on PLC4
a_{27} – DoS attack on PLC5
a_{28} – DoS attack on PLC6
a_{29} – DoS attack on PLC7
a_{30} – DoS attack on PLC8
a_{31} – DoS attack on PLC9

Multi-Level Bayesian Network

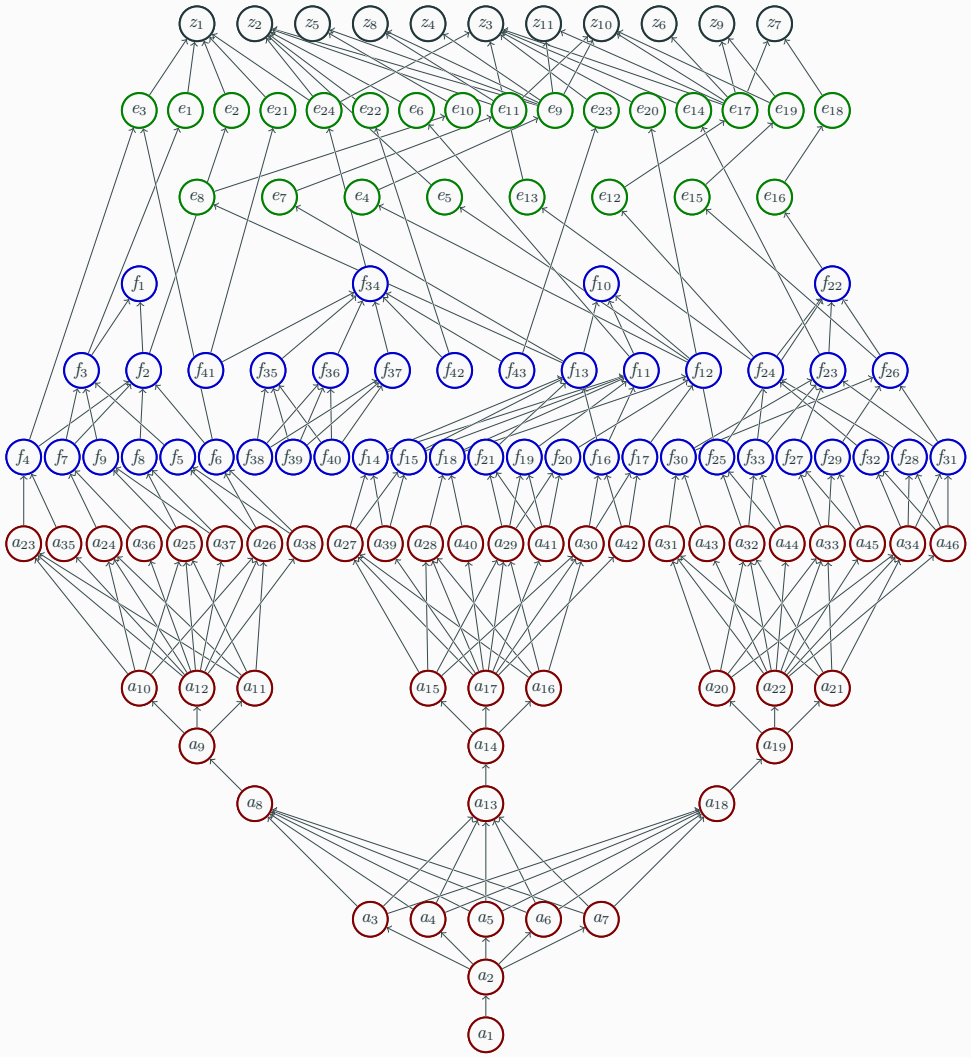
The multi-level Bayesian network is shown in the following figure.



a_{32} – DoS attack on PLC10
a_{33} – DoS attack on PLC11
a_{34} – DoS attack on PLC12
a_{35} – man-in-the-middle attack on PLC1
a_{36} – man-in-the-middle attack on PLC2
a_{37} – man-in-the-middle attack on PLC3
a_{38} – man-in-the-middle attack on PLC4
a_{39} – man-in-the-middle attack on PLC5
a_{40} – man-in-the-middle attack on PLC6
a_{41} – man-in-the-middle attack on PLC7
a_{42} – man-in-the-middle attack on PLC8
a_{43} – man-in-the-middle attack on PLC9
a_{44} – man-in-the-middle attack on PLC10
a_{45} – man-in-the-middle attack on PLC11
a_{46} – man-in-the-middle attack on PLC12
f_1 – distillation
f_2 – the temperature control function of distillation column
f_3 – the pressure control function of distillation column
f_4 – the traffic control function of V1
f_5 – the traffic control function of V2
f_6 – the traffic control function of V3
f_7 – the switch control function of S1
f_8 – the temperature sensation function of distillation column
f_9 – the pressure sensation function of distillation column
f_{10} – heating
f_{11} – the temperature control function of reactor 1
f_{12} – the pressure control function of reactor 1
f_{13} – the level control function of reactor 1
f_{14} – the traffic control function of V4
f_{15} – the traffic control function of V5
f_{16} – the traffic control function of V7

Multi-Level Bayesian Network

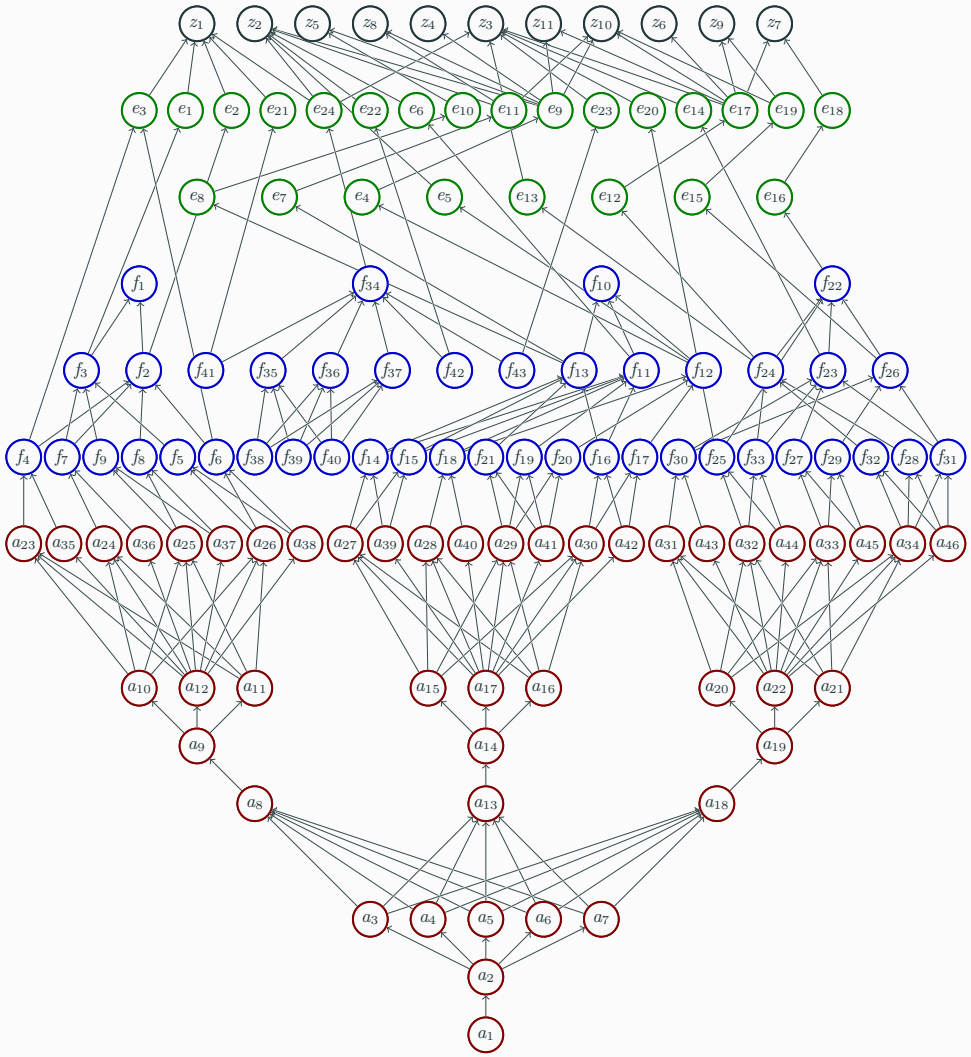
The multi-level Bayesian network is shown in the following figure.



f_{17} – the pressure reducing function of reactor 1
f_{18} – the switch control function of S2
f_{19} – the temperature sensation function of reactor 1
f_{20} – the pressure sensation function of reactor 1
f_{21} – the level sensation function of reactor 1
f_{22} – mixing and heating
f_{23} – the temperature control function of reactor 2
f_{24} – the pressure control function of reactor 2
f_{25} – the mixing function of reactor 2
f_{26} – the level control function of reactor 2
f_{27} – the temperature sensation function of reactor 2
f_{28} – the pressure sensation function of reactor 2
f_{29} – the level sensation function of reactor 2
f_{30} – the traffic control function of V6
f_{31} – the traffic control function of V10
f_{32} – the pressure reducing function of reactor 2
f_{33} – the switch control function of S3
f_{34} – production scheduling
f_{35} – the production scheduling function provided by personal computer 1
f_{36} – the production scheduling function provided by personal computer 2
f_{37} – the production scheduling function provided by personal computer 3
f_{38} – the data service of industrial Ethernet 1
f_{39} – the data service of industrial Ethernet 2
f_{40} – the data service of industrial Ethernet 3
f_{41} – the configuration of PLCs of distillation column
f_{42} – the configuration of PLCs of reactor 1
f_{43} – the configuration of PLCs of reactor 2
e_1 – pressure anomaly @ distillation column
e_2 – temperature anomaly @ distillation column
e_3 – traffic of anomaly @ distillation column
e_4 – excessive pressure @ reactor 1

Multi-Level Bayesian Network

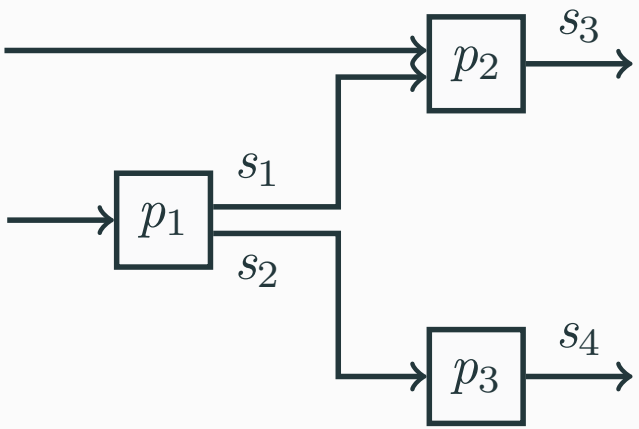
The multi-level Bayesian network is shown in the following figure.



e_5 – low pressure @ reactor 1
e_6 – temperature anomaly @ reactor 1
e_7 – excessive liquid level @ reactor 1
e_8 – low liquid level @ reactor 1
e_9 – explosion @ reactor 1
e_{10} – heater dry fired @ reactor 1
e_{11} – liquid overflow @ reactor 1
e_{12} – excessive pressure @ reactor 2
e_{13} – low pressure @ reactor 2
e_{14} – temperature anomaly @ reactor 2
e_{15} – excessive liquid level @ reactor 2
e_{16} – low liquid level @ reactor 2
e_{17} – explosion @ reactor 2
e_{18} – heater dry fired @ reactor 2
e_{19} – liquid overflow @ reactor 2
e_{20} – blender stop @ reactor 2
e_{21} – out of control @ distillation column
e_{22} – out of control @ reactor 1
e_{23} – out of control @ reactor 2
e_{24} – production scheduling error @ control layer
z_1 – semi-product s01 and s02
z_2 – product s03
z_3 – product s04
z_4 – tank and sensors of reactor 1
z_5 – heater of reactor 1
z_6 – tank, sensors and blender of reactor 2
z_7 – heater of reactor 2
z_8 – staff 1-4
z_9 – staff 5-9
z_{10} – river and solid
z_{11} – air

Process Model

The process model is shown in the following figure.



Symbol	Description	Symbol	Description	Value($)
p_1	distillation	s_1	semi-product 1	$10,000$
p_2	heating	s_2	semi-product 2	$20,000$
p_3	mixing & heating	s_3	product 1	$50,000$
		s_4	product 2	$70,000$

Security Strategies

The security strategies are shown as follows.

Symbol	Description	Prevented Attacks	Invalidated Functions
m_1	shut down the web server	a_3, a_4	—
m_2	shut down the personal computer 1	a_5	f_{35}
m_3	shut down the personal computer 2	a_6	f_{36}
m_4	shut down the personal computer 3	a_7	f_{37}
m_5	disconnect the security gateway 1	a_8	f_{38}
m_6	shut down the data server 1	a_{10}, a_{11}	f_{38}
m_7	shut down the engineer station 1	a_{12}	f_{41}
m_8	encrypt the data amongst the PLC 1-4	a_{35}, a_{36}, a_{37}, a_{38}	—

Security Strategies

The security strategies are shown as follows.

Symbol	Description	Prevented Attacks	Invalidated Functions
m_9	disconnect the security gateway 2	a_{13}	f_{39}
m_{10}	shut down the data server 2	a_{15}, a_{16}	f_{39}
m_{11}	shut down the engineer station 2	a_{17}	f_{42}
m_{12}	encrypt the data amongst the PLC 5-8	a_{39}, a_{40}, a_{41}, a_{42}	—
m_{13}	disconnect the security gateway 3	a_{18}	f_{40}
m_{14}	shut down the data server 3	a_{20}, a_{21}	f_{40}
m_{15}	shut down the engineer station 3	a_{22}	f_{43}
m_{16}	encrypt the data amongst the PLC 9-12	a_{43}, a_{44}, a_{45}, a_{46}	—

Recovery Strategies

The recovery strategies are shown as follows.

Symbol	Description	Recovered Functions	Cost($)
n_1	reboot PLC1	f_4	$9,000$
n_2	reboot PLC2	f_7	$9,000$
n_3	reboot PLC3	f_8, f_9	$10,000$
n_4	reboot PLC4	f_5, f_6	$15,000$
n_5	reboot PLC5	f_{14}, f_{15}	$8,000$
n_6	reboot PLC6	f_{18}	$10,000$
n_7	reboot PLC7	f_{19}, f_{20}, f_{21}	$2,000$
n_8	reboot PLC8	f_{16}, f_{17}	$13,000$

Recovery Strategies

The recovery strategies are shown as follows.

Symbol	Description	Recovered Functions	Cost($)
n_9	reboot PLC9	f_{30}	$14,000$
n_{10}	reboot PLC10	f_{25}, f_{33}	$7,500$
n_{11}	reboot PLC11	f_{27}, f_{28}, f_{29}	$14,000$
n_{12}	reboot PLC12	f_{31}, f_{32}	$11,000$

Simulation of State Controller

Definition of System State

The state space of this chemical reactor control system is defined as

$$\boldsymbol{F} = (F_1, F_{10}, F_{22}, F_{34}),$$

where

$$F_i = \begin{cases} 0, & \text{the system function } f_i \text{ runs normally,} \\ 1, & \text{otherwise.} \end{cases}$$

Symbol	Description	System States															
f_1	distillation	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
f_{10}	heating	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
f_{22}	mixing & heating	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
f_{34}	production scheduling	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Is the System State Feasible?		√	×	×	×	×	×	×	×	×	√	×	√	×	√	×	√

Notes:

"√" means system state is feasible;

"×" means system state is unfeasible.

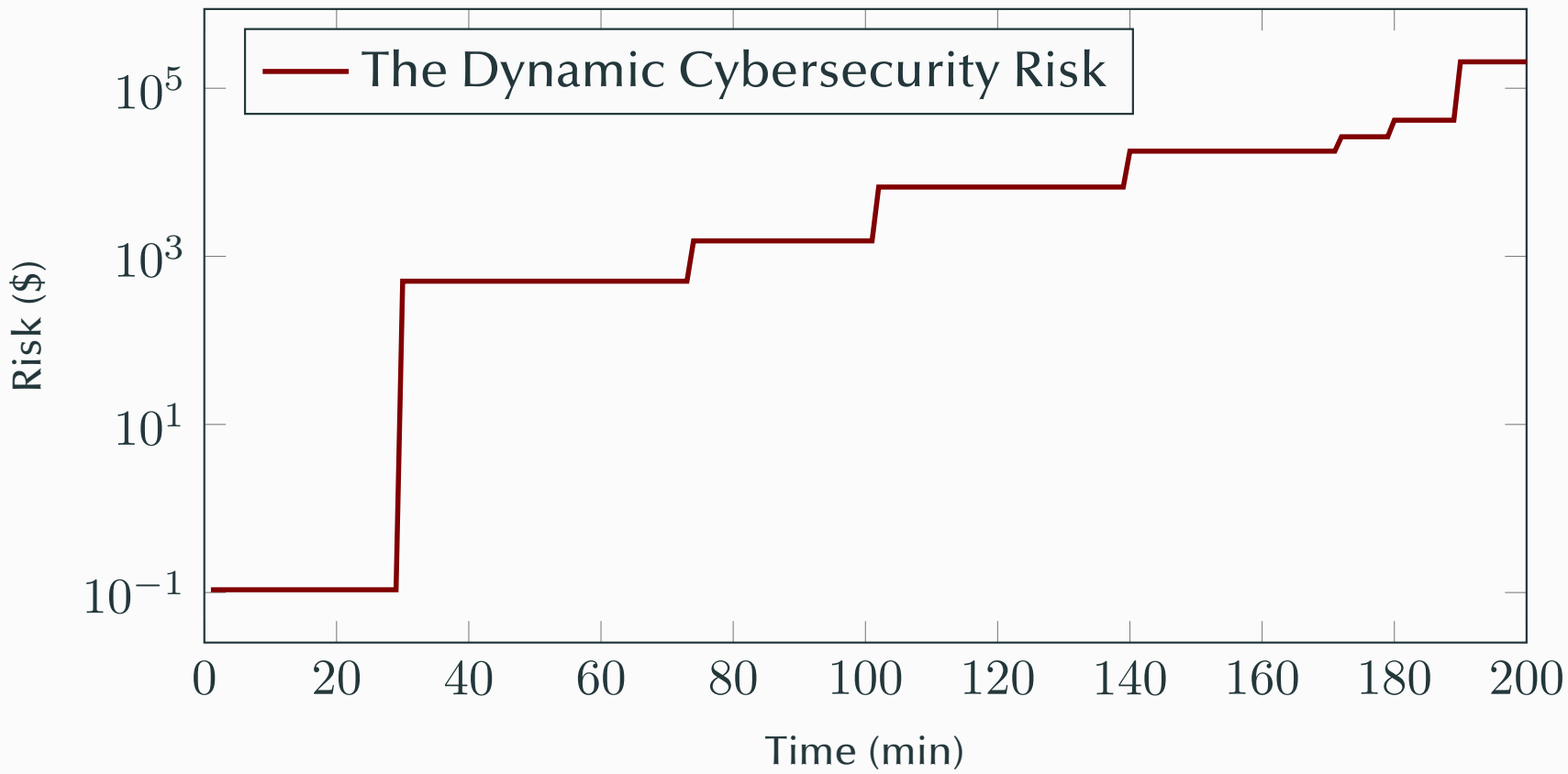
Attack Scenario and Evidence List

The attack scenario and the evidence list is shown as follows.

Step	Description	Time	Evidence
1	network scanning of the Ethernet in the management layer is launched	30	$a_1 = T$
2	vulnerability scanning of the devices in the management layer is launched	40	$a_2 = T$
3	buffer overflow attack on the web server is launched	74	$a_3 = T$
4	network scanning of the industrial Ethernet 2 in the control layer is launched	102	$a_{13} = T$
5	vulnerability scanning of the devices in the industrial Ethernet 2 is launched	111	$a_{14} = T$
6	brute force attack on the data server 2 is launched	140	$a_{16} = T$
7	DoS attack on PLC5 is launched	172	$a_{27} = T$
8	the traffic control function of V4 is failed	180	$f_{14} = T$
9	the level control function of reactor 1 is failed	190	$f_{13} = T$

Simulation Result and Analysis

The curve of the cybersecurity risk is shown in following figure.



Simulation Result and Analysis

The results of system control are shown as follows.

Evidence List	Optimal System State			
	f_1	f_{10}	f_{22}	f_{34}
–	1	1	1	1
a_1	1	1	1	1
a_1, a_2	1	1	1	1
a_1, a_2, a_3	1	1	1	1
a_1, a_2, a_3, a_{13}	1	1	1	1
a_1, a_2, a_3, a_{13}, a_{14}	1	1	1	1
a_1, a_2, a_3, a_{13}, a_{14}, a_{16}	1	1	1	1
a_1, a_2, a_3, a_{13}, a_{14}, a_{16}, a_{27}	1	1	1	1
a_1, a_2, a_3, a_{13}, a_{14}, a_{16}, a_{27}, f_{14}	1	0	0	1
a_1, a_2, a_3, a_{13}, a_{14}, a_{16}, a_{27}, f_{14}, f_{13}	0	0	0	0

Simulation of Optimal Defense Strategy Generator

Decision-Making Detail 1

If the evidence list is (a_1, a_2), the detail of the decision-making is shown as follows.

Payoff Matrix of Defense System: Attack Strategy / Defense Strategy		a_3 buffer overflow attack on the web server	a_4 brute force attack on the web server	a_5 brute force attack on the personal computer 1	a_6 brute force attack on the personal computer 2	a_7 brute force attack on the personal computer 3	Distribution of defense System's Mixed Strategy Probability
m_1	shut down the web server	$2.12 \cdot 10^2$	$2.12 \cdot 10^2$	$-6.69 \cdot 10^2$	$-6.69 \cdot 10^2$	$-6.69 \cdot 10^2$	100%
–	do nothing	$-1.02 \cdot 10^3$	$-9.59 \cdot 10^2$	$-8.87 \cdot 10^2$	$-9.43 \cdot 10^2$	$-8.78 \cdot 10^2$	0%
Distribution of Attacker's Mixed Strategy Probability		0%	0%	33%	35%	32%	

Decision-Making Detail 2

If the evidence list is $(a_1, a_2, a_3, a_8, a_9, a_{10}, a_{25}, f_8)$, the detail of the decision-making is shown as follows.

Payoff Matrix of Defense System: Attack Strategy / Defense Strategy		a_4 brute force attack on the web server	a_5 brute force attack on the personal computer 1	a_6 brute force attack on the personal computer 2	a_7 brute force attack on the personal computer 3	a_{11} brute force attack on the data server 1	a_{12} brute force attack on the engineer station 1	a_{13} network scanning of the industrial Ethernet 2 in the control layer	a_{18} network scanning of the industrial Ethernet 3 in the control layer	a_{23} DoS attack on PLC1	a_{24} DoS attack on PLC2	a_{26} DoS attack on PLC4	Distribution of defense System's Mixed Strategy Probability
m_1	shut down the web server	$-9.10 \cdot 10^3$	$-9.24 \cdot 10^3$	$-9.24 \cdot 10^3$	$-9.24 \cdot 10^3$	$-9.10 \cdot 10^3$	$-9.32 \cdot 10^3$	$-1.43 \cdot 10^4$	$-1.25 \cdot 10^4$	$-9.31 \cdot 10^3$	$-9.16 \cdot 10^3$	$-9.34 \cdot 10^3$	0%
n_3	reboot PLC3												
m_1	shut down the web server	$8.09 \cdot 10^2$	$6.64 \cdot 10^2$	$6.64 \cdot 10^2$	$6.64 \cdot 10^2$	$8.09 \cdot 10^2$	$5.83 \cdot 10^2$	$-4.42 \cdot 10^3$	$-2.64 \cdot 10^3$	$5.95 \cdot 10^2$	$7.37 \cdot 10^2$	$5.55 \cdot 10^2$	100%
n_3	reboot PLC3	$-1.11 \cdot 10^4$	$-1.06 \cdot 10^4$	$-1.10 \cdot 10^4$	$-1.04 \cdot 10^4$	$-9.90 \cdot 10^3$	$-1.01 \cdot 10^4$	$-1.48 \cdot 10^4$	$-1.33 \cdot 10^4$	$-1.01 \cdot 10^4$	$-9.97 \cdot 10^3$	$-1.02 \cdot 10^4$	0%
–	do nothingi	$-1.11 \cdot 10^3$	$-5.82 \cdot 10^2$	$-1.02 \cdot 10^3$	$-4.01 \cdot 10^2$	$9.53 \cdot 10^1$	$-1.34 \cdot 10^2$	$-4.80 \cdot 10^3$	$-3.26 \cdot 10^3$	$-1.15 \cdot 10^2$	$2.82 \cdot 10^1$	$-1.54 \cdot 10^2$	0%
Distribution of Attacker's Mixed Strategy Probability		0%	0%	0%	0%	0%	0%	100%	0%	0%	0%	0%	

Decision-Making Detail 3

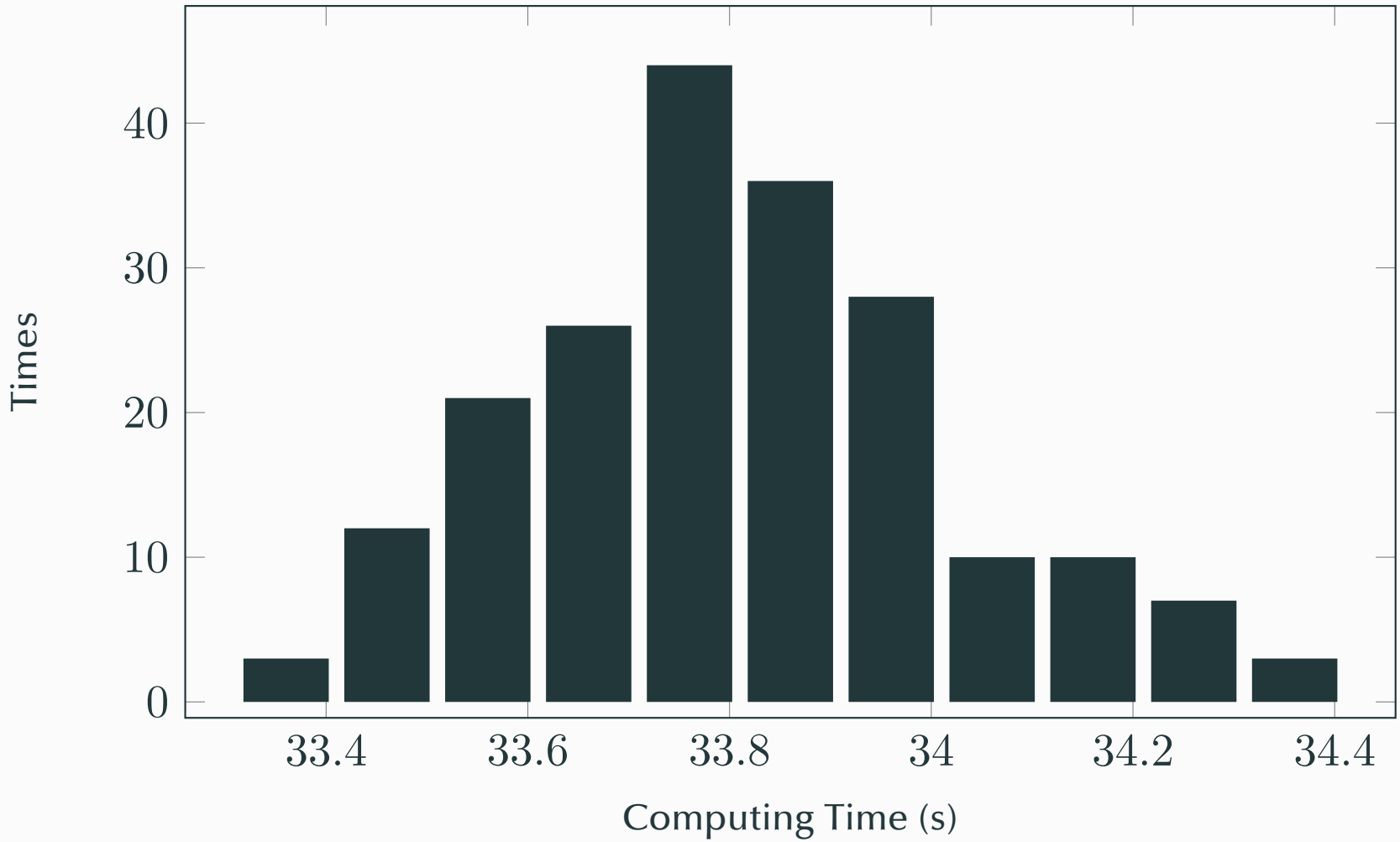
New, the cost of recovery strategy n_3 is reduced to 0, the detail of the decision-making is shown as follows.

Payoff Matrix of Defense System: Attack Strategy / Defense Strategy		a_4 brute force attack on the web server	a_5 brute force attack on the personal computer 1	a_6 brute force attack on the personal computer 2	a_7 brute force attack on the personal computer 3	a_{11} brute force attack on the data server 1	a_{12} brute force attack on the engineer station 1	a_{13} network scanning of the industrial Ethernet 2 in the control layer	a_{18} network scanning of the industrial Ethernet 3 in the control layer	a_{23} DoS attack on PLC1	a_{24} DoS attack on PLC2	a_{26} DoS attack on PLC4	Distribution of defense System's Mixed Strategy Probability
m_1	shut down the web server	$9.05 \cdot 10^2$	$7.59 \cdot 10^2$	$7.59 \cdot 10^2$	$7.59 \cdot 10^2$	$9.05 \cdot 10^2$	$6.76 \cdot 10^2$	$-4.33 \cdot 10^3$	$-2.54 \cdot 10^3$	$6.94 \cdot 10^2$	$8.38 \cdot 10^2$	$6.56 \cdot 10^2$	100%
n_3	reboot PLC3												
m_1	shut down the web server	$8.09 \cdot 10^2$	$6.64 \cdot 10^2$	$6.64 \cdot 10^2$	$6.64 \cdot 10^2$	$8.09 \cdot 10^2$	$5.83 \cdot 10^2$	$-4.42 \cdot 10^3$	$-2.64 \cdot 10^3$	$5.95 \cdot 10^2$	$7.37 \cdot 10^2$	$5.55 \cdot 10^2$	0%
n_3	reboot PLC3	$-1.11 \cdot 10^3$	$-5.82 \cdot 10^2$	$-1.02 \cdot 10^3$	$-4.01 \cdot 10^2$	$9.53 \cdot 10^1$	$-1.34 \cdot 10^2$	$-4.80 \cdot 10^3$	$-3.26 \cdot 10^3$	$-1.15 \cdot 10^2$	$2.82 \cdot 10^1$	$-1.54 \cdot 10^2$	0%
–	do nothing	$-1.11 \cdot 10^3$	$-5.82 \cdot 10^2$	$-1.02 \cdot 10^3$	$-4.01 \cdot 10^2$	$9.53 \cdot 10^1$	$-1.34 \cdot 10^2$	$-4.80 \cdot 10^3$	$-3.26 \cdot 10^3$	$-1.15 \cdot 10^2$	$2.82 \cdot 10^1$	$-1.54 \cdot 10^2$	0%
Distribution of Attacker's Mixed Strategy Probability		0%	0%	0%	0%	0%	0%	100%	0%	0%	0%	0%	

Simulation of Real-Time Capability

Result of Real-Time Simulation

The evidence list is $(a_1, a_2, a_3, a_8, a_9, a_{10}, a_{25}, f_8)$, the distribution of computing time is shown in the following figure.



Result of Scalability Simulation

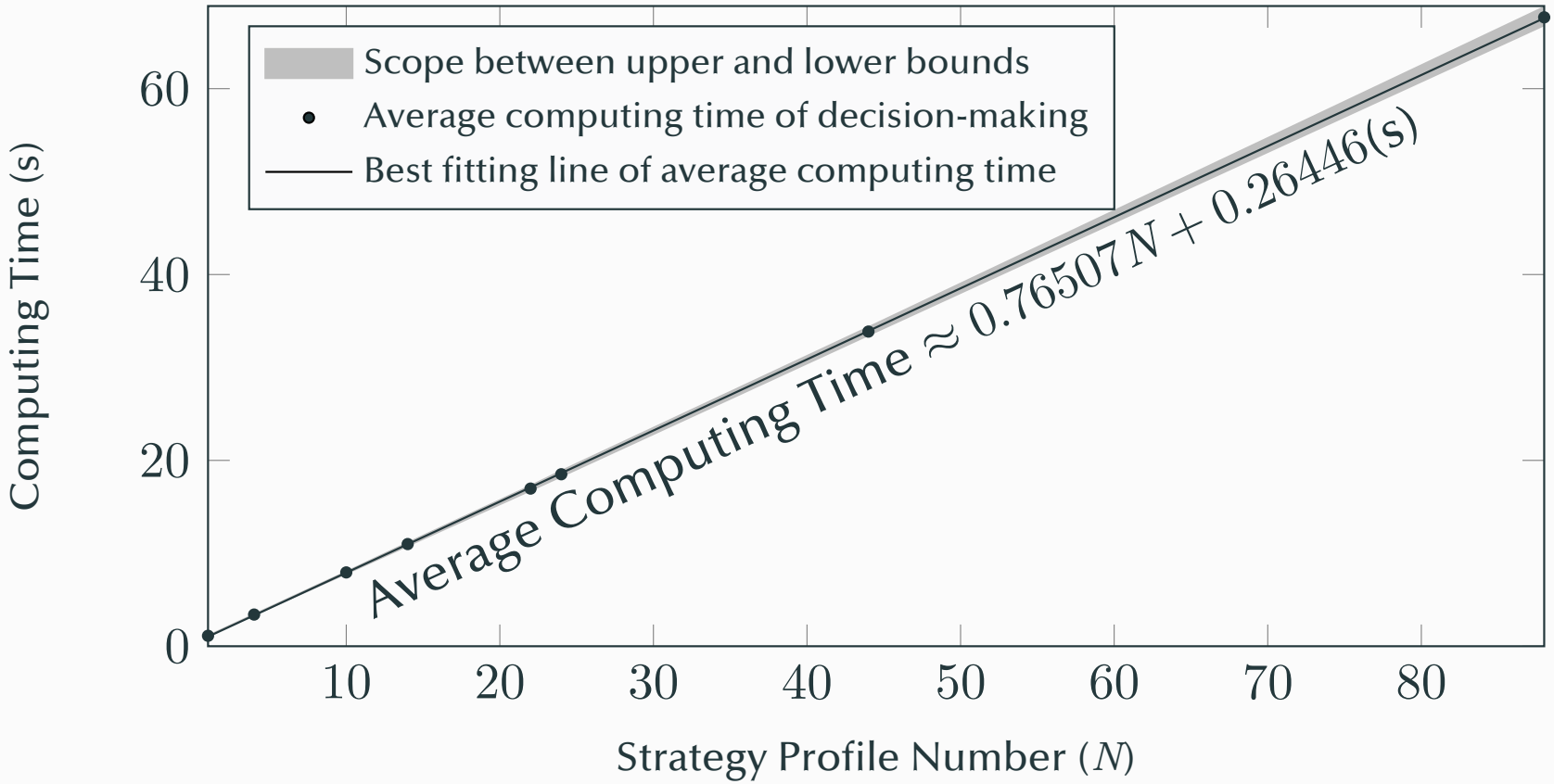
A variety of evidence lists are input into the decision-making system. For each evidence list, the decision-making process is repeated 200 times.
The computing time of all decision-making processes is recorded, and the key parameters are shown as follows.

Evidence List	Strategy Profile Number	Computing Time (s)		
		Minimum	Average	Maximum
a_1	$1 \times 1 = 1$	0.990514	1.124408	1.236192
f_8, f_7	$1 \times 4 = 4$	3.264095	3.409352	3.533821
a_1, a_2	$5 \times 2 = 10$	7.706280	7.943903	8.120606
a_1, a_2, a_3	$7 \times 2 = 14$	10.692101	10.994853	11.240887
a_1, a_2, a_3, a_8, a_9, a_{10}, a_{25}	$11 \times 2 = 22$	16.649827	16.965763	17.374881
a_1, a_2, a_3, a_8, a_9, a_{10}	$12 \times 2 = 24$	18.156836	18.508226	18.982261
a_1, a_2, a_3, a_8, a_9, a_{10}, a_{25}, f_8	$11 \times 4 = 44$	33.360343	33.861009	34.441684
a_1, a_2, a_3, a_8, a_9, a_{10}, a_{25}, f_8, f_7	$11 \times 8 = 88$	66.715091	67.676804	68.892430

Result of Scalability Simulation

A variety of evidence lists are input into the decision-making system. For each evidence list, the decision-making process is repeated 200 times.

The relationship between strategy profile number and computing time is shown in the following figure.



Task Planning

Task Planning

- Finish the outline of the 4th paper.
- Finish the first two sections of the 4th paper.