Monthly Report

Zhang Qi

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

May 3, 2016

Outlines

Simulation Platform

Simulation of State Controller

Simulation of Optimal Defense Strategy Generator

Simulation of Real-Time Capability

Task Planning

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

Process Model

Security Strategies

Recovery Strategies

Simulation of State Controller

Definition of System State

Attack Scenario

Evidence List

Simulation Result and Analysis

Simulation of Optimal Defense Strategy Generator

Attack Scenario 1

Decision-Making Detail 1

Attack Scenario 2

Decision-Making Detail 2

Attack Scenario 3

Decision-Making Detail 3

Simulation of Real-Time Capability

Result of Real-Time Simulation

Result of Scalability Simulation

Task Planning

Task Planning

- Finish the simulation of 2nd paper.
- Finish the outline of 4th paper.