# Monthly Report

**Zhang Qi**


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

**January 3, 2016**

# Outlines

Multiple Models for Risk Assessment

Simulation

Task Planning

# Multiple Models for Risk Assessment

# Seven Factors about the Risk

- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.

# Seven Factors about the Risk

- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.
- **System Function** refers to the function of control system.

# Seven Factors about the Risk

- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.
- **System Function** refers to the function of control system.
- **Security Strategy** is a kind of defense strategy which can prevent attack strategy.

# Seven Factors about the Risk

- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.
- **System Function** refers to the function of control system.
- **Security Strategy** is a kind of defense strategy which can prevent attack strategy.
- **Recover Strategy** is a kind of defense strategy which can recover the failed system function.

# Seven Factors about the Risk

- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.
- **System Function** refers to the function of control system.
- **Security Strategy** is a kind of defense strategy which can prevent attack strategy.
- **Recover Strategy** is a kind of defense strategy which can recover the failed system function.
- **Hazardous Incident** refers to the unexpected incident which will cause monetary loss of ICSs.

# Seven Factors about the Risk

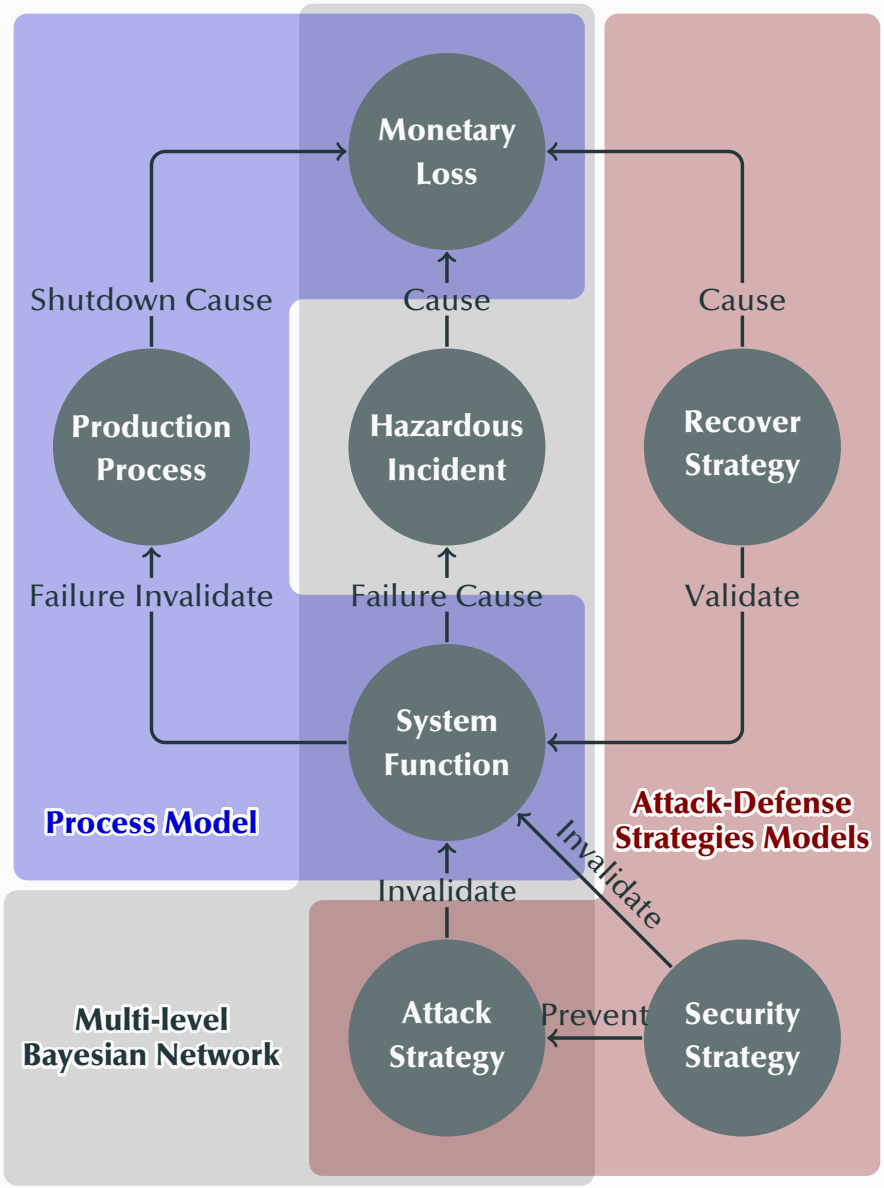
- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.
- **System Function** refers to the function of control system.
- **Security Strategy** is a kind of defense strategy which can prevent attack strategy.
- **Recover Strategy** is a kind of defense strategy which can recover the failed system function.
- **Hazardous Incident** refers to the unexpected incident which will cause monetary loss of ICSs.
- **Production Process** refers a manufacturing step which is a part of in a production chain.

# Seven Factors about the Risk

- **Attack Strategy** refers to the atom attack which is launched by an attacker to achieve his destructive purpose.
- **System Function** refers to the function of control system.
- **Security Strategy** is a kind of defense strategy which can prevent attack strategy.
- **Recover Strategy** is a kind of defense strategy which can recover the failed system function.
- **Hazardous Incident** refers to the unexpected incident which will cause monetary loss of ICSs.
- **Production Process** refers a manufacturing step which is a part of in a production chain.
- **Monetary Loss** is the sum of the loss caused by malicious attacks, the loss of production process shutdown, and the enforcement cost of defense strategy.

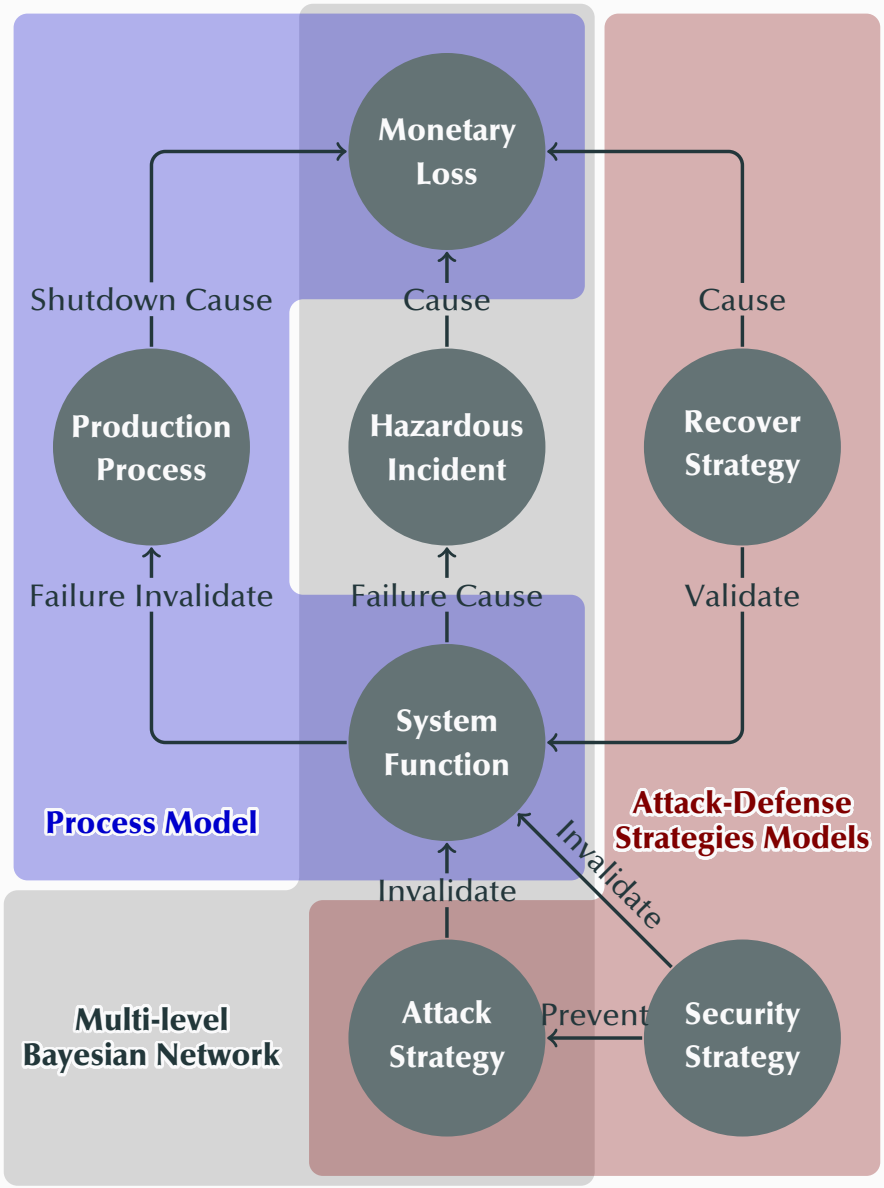
# The relationships amongst these seven factors

- The attack strategy can invalidate the system function.



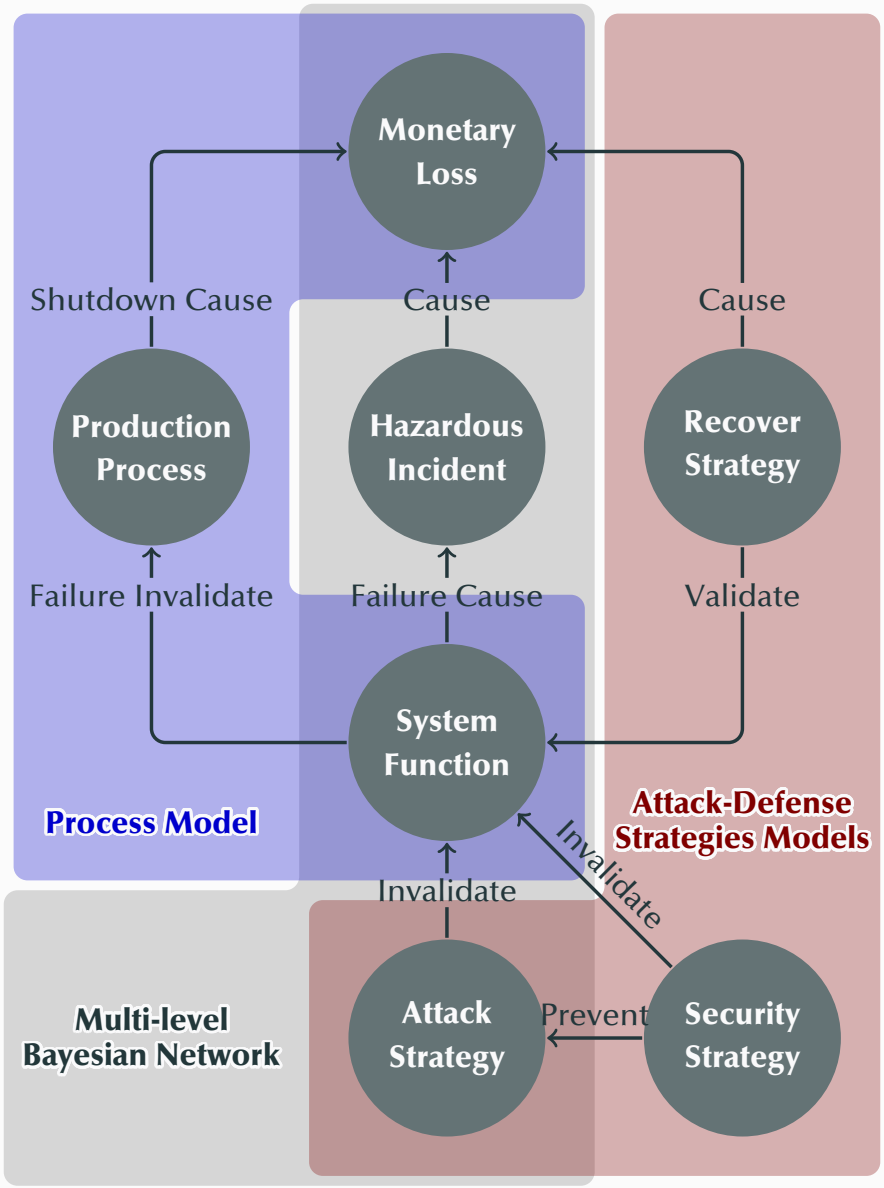
# The relationships amongst these seven factors

- The attack strategy can invalidate the system function.
- The failure of the system function can lead to hazardous incident and product process shutdown.



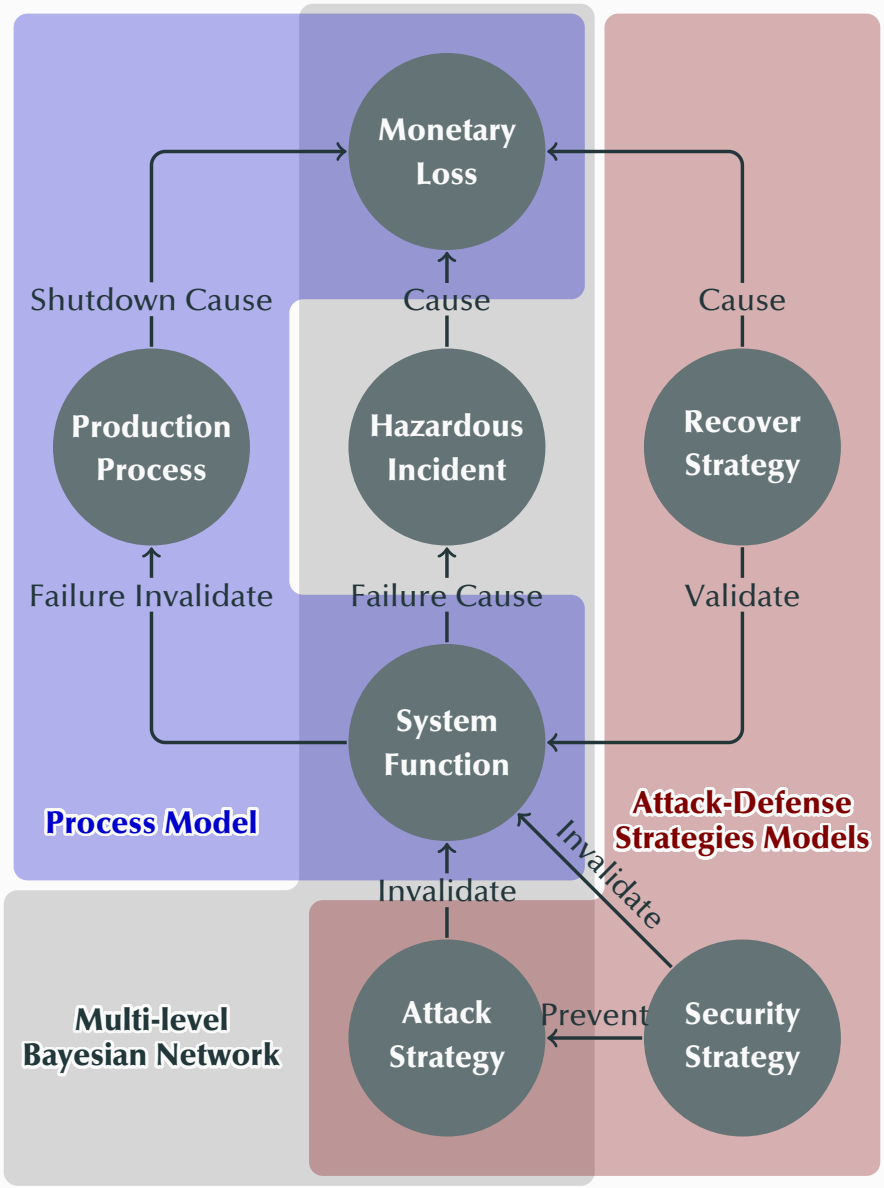
# The relationships amongst these seven factors

- The attack strategy can invalidate the system function.
- The failure of the system function can lead to hazardous incident and product process shutdown.
- The occurrence of these two unexpected events will both cause the monetary loss of ICSs.



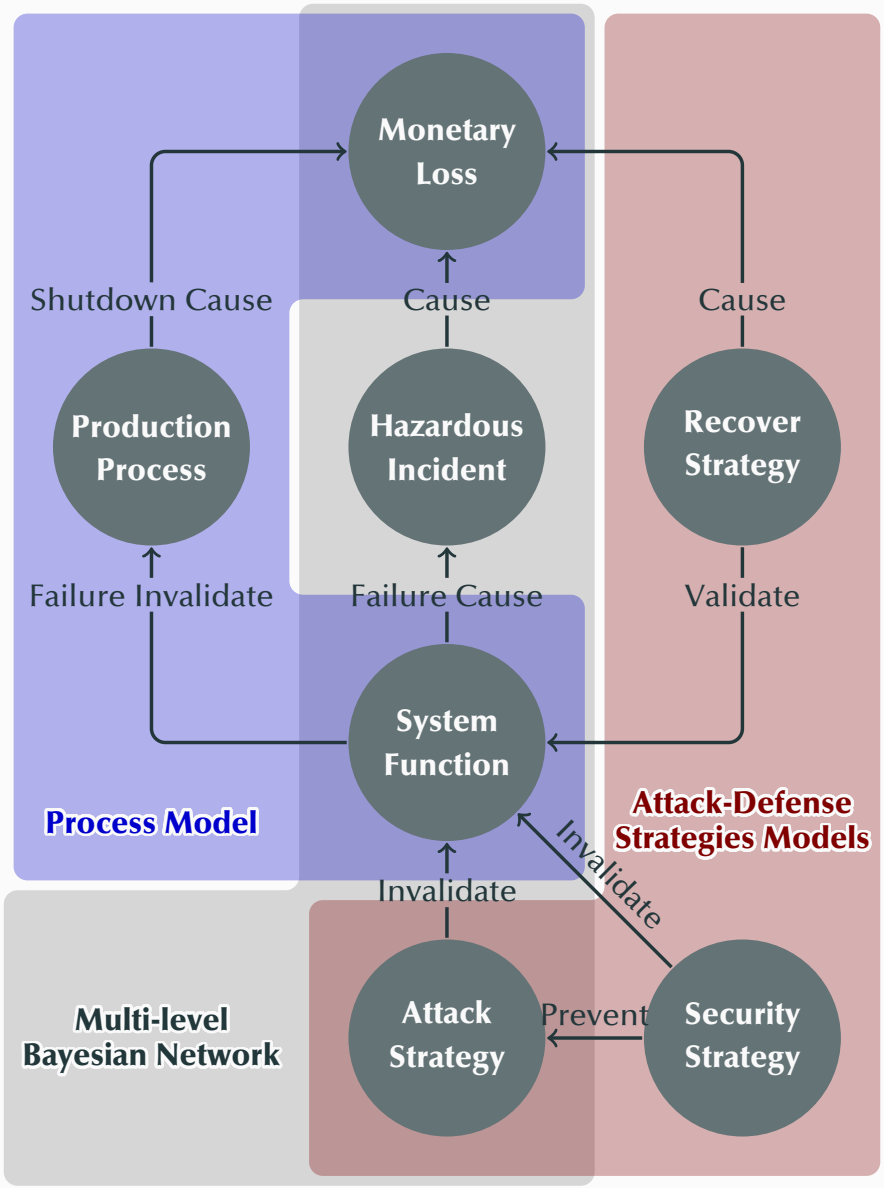
# The relationships amongst these seven factors

- The attack strategy can invalidate the system function.
- The failure of the system function can lead to hazardous incident and product process shutdown.
- The occurrence of these two unexpected events will both cause the monetary loss of ICSs.
- The security strategy will prevent the enforcement of attack strategy, but its side effect is that it may invalidate the system function.



# The relationships amongst these seven factors

- The attack strategy can invalidate the system function.
- The failure of the system function can lead to hazardous incident and product process shutdown.
- The occurrence of these two unexpected events will both cause the monetary loss of ICSs.
- The security strategy will prevent the enforcement of attack strategy, but its side effect is that it may invalidate the system function.
- The recover strategy has ability of recovering the failed system function, and it has the enforcement cost.



# Multiple Models of Risk Assessment for ICSs

The following three models are used to described the relationships amongst these seven factors.

- The **multi-level Bayesian network**, involves attack strategy, system function, hazardous incident, and monetary loss. This model uses Bayesian network to describe the causal relationship of these four factors and it can be used to assess the risk caused by the malicious attacks.

# Multiple Models of Risk Assessment for ICSs

The following three models are used to described the relationships amongst these seven factors.

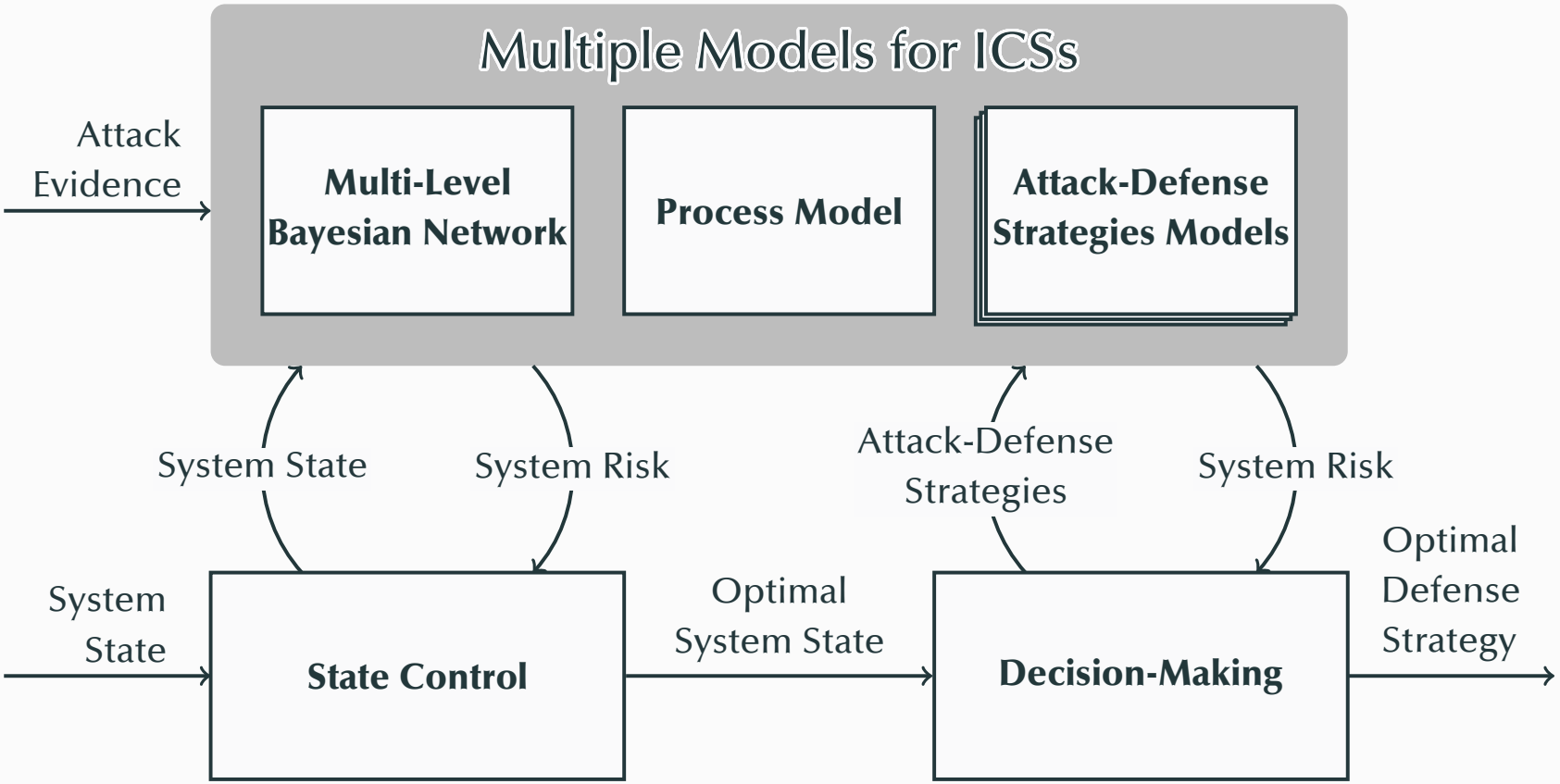
- The **multi-level Bayesian network**, involves attack strategy, system function, hazardous incident, and monetary loss. This model uses Bayesian network to describe the causal relationship of these four factors and it can be used to assess the risk caused by the malicious attacks.
- The **process model** involves system functions, production process, and monetary loss. It can be used to calculate the risk cause by the degradation of control system.

# Multiple Models of Risk Assessment for ICSs

The following three models are used to described the relationships amongst these seven factors.

- The **multi-level Bayesian network**, involves attack strategy, system function, hazardous incident, and monetary loss. This model uses Bayesian network to describe the causal relationship of these four factors and it can be used to assess the risk caused by the malicious attacks.
- The **process model** involves system functions, production process, and monetary loss. It can be used to calculate the risk cause by the degradation of control system.
- The **attack-defense strategies models**, include attack strategy model, security strategy model, and recover strategy model. These three models contain the relationships amongst these three kinds of strategies and system functions, and they can be used to quantify the cost and benefit of attack-defense strategies.

# Chemical Reactor Control System



# Simulation

# A Failed Attempt — C++ Version

I had implemented the class `Node` and the class `BayesianNetwork` with C++ language.

The inference of Bayesian network is provided by `dlib`, which is a C++ library. But the computation time of the Bayesian network inference is 30 times slower than that of the implementation by Matlab.

| Runtime Environment | Computation Time(ms) |
|---|---|
| C++ in Debug Mode | 40,000 |
| C++ in Release Mode | 3,600 |
| Matlab | 90 |

The Matlab has optimized the algorithm for a large amount of computation.

# Common Classes

For the simulation, the following common classes are designed:

class `Node` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node` , class `Evidence` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node`, class `Evidence`, class `BayesianNetwork`,

# Common Classes

For the simulation, the following common classes are designed:

class `Node`, class `Evidence`, class `BayesianNetwork`, class `Product`,

# Common Classes

For the simulation, the following common classes are designed:

class `Node` , class `Evidence` , class `BayesianNetwork` , class `Product` , class `Process` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node` , class `Evidence` , class `BayesianNetwork` , class `Product` , class `Process` , class `ProductionModel` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node` , class `Evidence` , class `BayesianNetwork` , class `Product` , class `Process` , class `ProductionModel` , class `SystemState` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node` , class `Evidence` , class `BayesianNetwork` , class `Product` , class `Process` , class `ProductionModel` , class `SystemState` , class `RiskModel` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node` , class `Evidence` , class `BayesianNetwork` , class `Product` , class `Process` , class `ProductionModel` , class `SystemState` , class `RiskModel` , class `Strategies.Security` ,

# Common Classes

For the simulation, the following common classes are designed:

class `Node`, class `Evidence`, class `BayesianNetwork`, class `Product`, class `Process`, class `ProductionModel`, class `SystemState`, class `RiskModel`, class `Strategies.Security`, class `Strategies.Recover`, and

# Common Classes

For the simulation, the following common classes are designed:

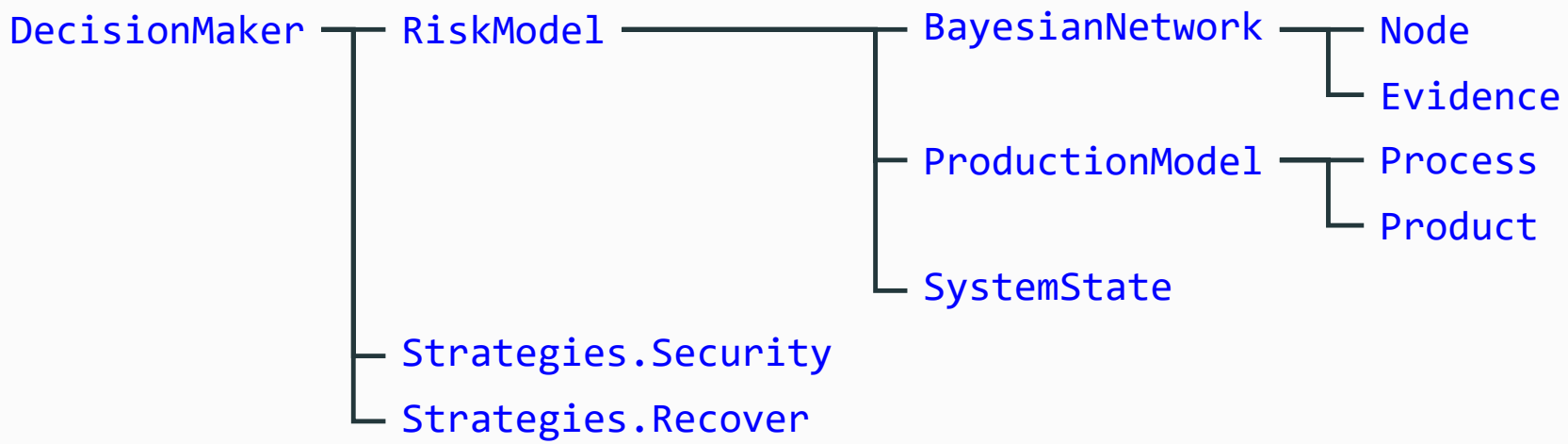
class `Node`, class `Evidence`, class `BayesianNetwork`, class `Product`, class `Process`, class `ProductionModel`, class `SystemState`, class `RiskModel`, class `Strategies.Security`, class `Strategies.Recover`, and class `DecisionMaker`.

# Common Classes

For the simulation, the following common classes are designed:

class `Node`, class `Evidence`, class `BayesianNetwork`, class `Product`, class `Process`, class `ProductionModel`, class `SystemState`, class `RiskModel`, class `Strategies.Security`, class `Strategies.Recover`, and class `DecisionMaker`.

The relationship amongst these classes are shown as follows.



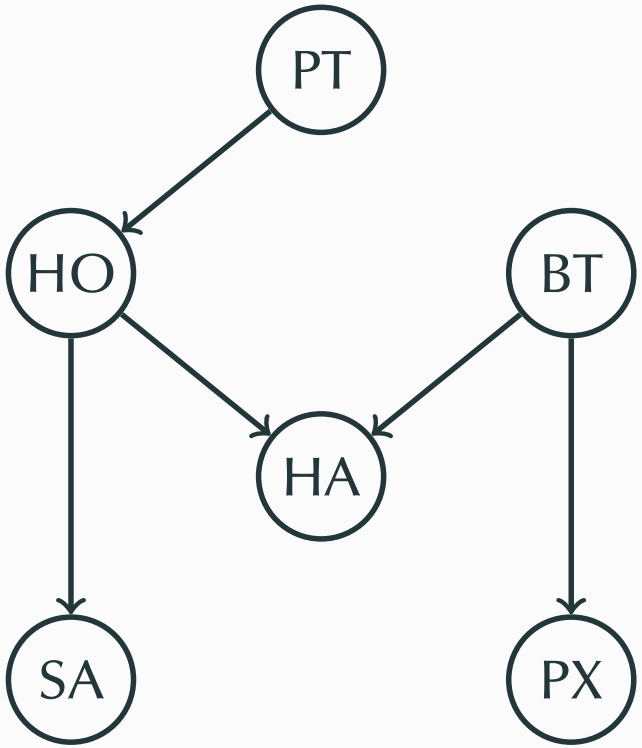
# How to Use?

The following example is used to introduce how to use the class `Node` and class `BayesianNetwork` to model and inference the Bayesian network.

# How to Use?

The following example is used to introduce how to use the class `Node` and class `BayesianNetwork` to model and inference the Bayesian network.

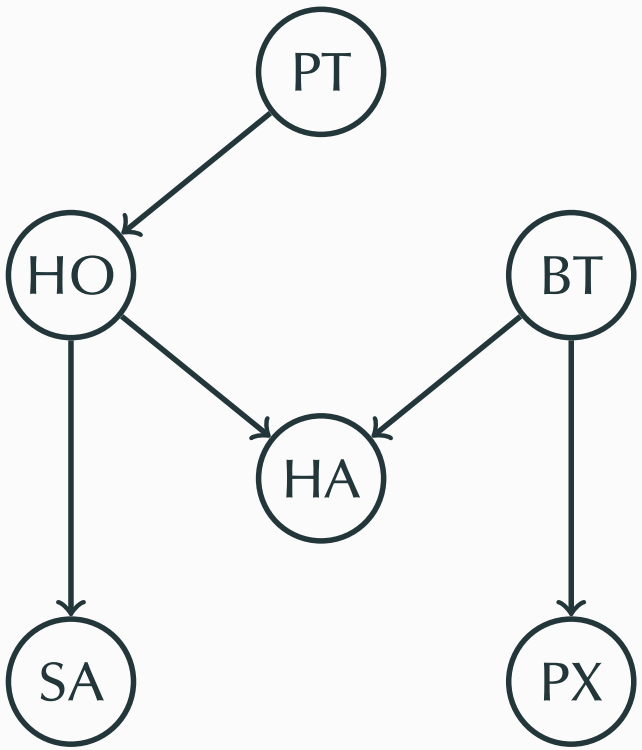
The Bayesian network is shown as follows.



# How to Use?

The following example is used to introduce how to use the class `Node` and class `BayesianNetwork` to model and inference the Bayesian network.

The Bayesian network is shown as follows.




The meanings of nodes are shown as follows.

| Symbol | Meaning |
|---|---|
| PT | Qiqi goes to the Party. |
| HO | Qiqi has a Hangover. |
| BT | Qiqi has a Brain Tumor. |
| HA | Qiqi has a Headache. |
| SA | Qiqi has an Alcohol Smell. |
| PX | Qiqi has a Pos Xray. |

# How to Use?

Step 1, create the nodes of Bayesian network.

```
PT = Classes.Node('Party');
HO = Classes.Node('Hangover');
BT = Classes.Node('Brain Tumor');
HA = Classes.Node('Headache');
SA = Classes.Node('Smell Alcohol');
PX = Classes.Node('Pos Xray');
```

Step 2, set the conditional probabilities of nodes.

```
PT.AddAllParents(... Has no parent node
    0.200);

BT.AddAllParents(... Has no parent node
    0.001);
```

# How to Use?

```
12  HO.AddAllParents(PT, ...
13      0.000, ...    F
14      0.700);  %    T
15
16  SA.AddAllParents(HO, ...
17      0.100, ...    F
18      0.800);  %    T
19
20  PX.AddAllParents(BT, ...
21      0.010, ...    F
22      0.980);  %    T
23
24  HA.AddAllParents(HO, BT, ...
25      0.020, ...    F   F
26      0.900, ...    F   T
27      0.700, ...    T   F
28      0.990);  %    T   T
```

# How to Use?

Step 3, create the Bayesian network.

```
29 BayesianNetwork = Classes.BayesianNetwork();
```

Step 4, add the nodes into the Bayesian network.

```
30 BayesianNetwork.AddNodes(PT, BT, HO, SA, PX, HA);
```

Step 5, initialize the Bayesian network.

```
31 BayesianNetwork.Initialize();
```

Step 6, infer the Bayesian network.

```
32 BayesianNetwork.Inference();
33 BayesianNetwork.Display(HA);
```

# How to Use?

**Question:** if Qiqi has a Pos Xray (PX), what's the probability that Qiqi has a Brain Tumor (BT)?

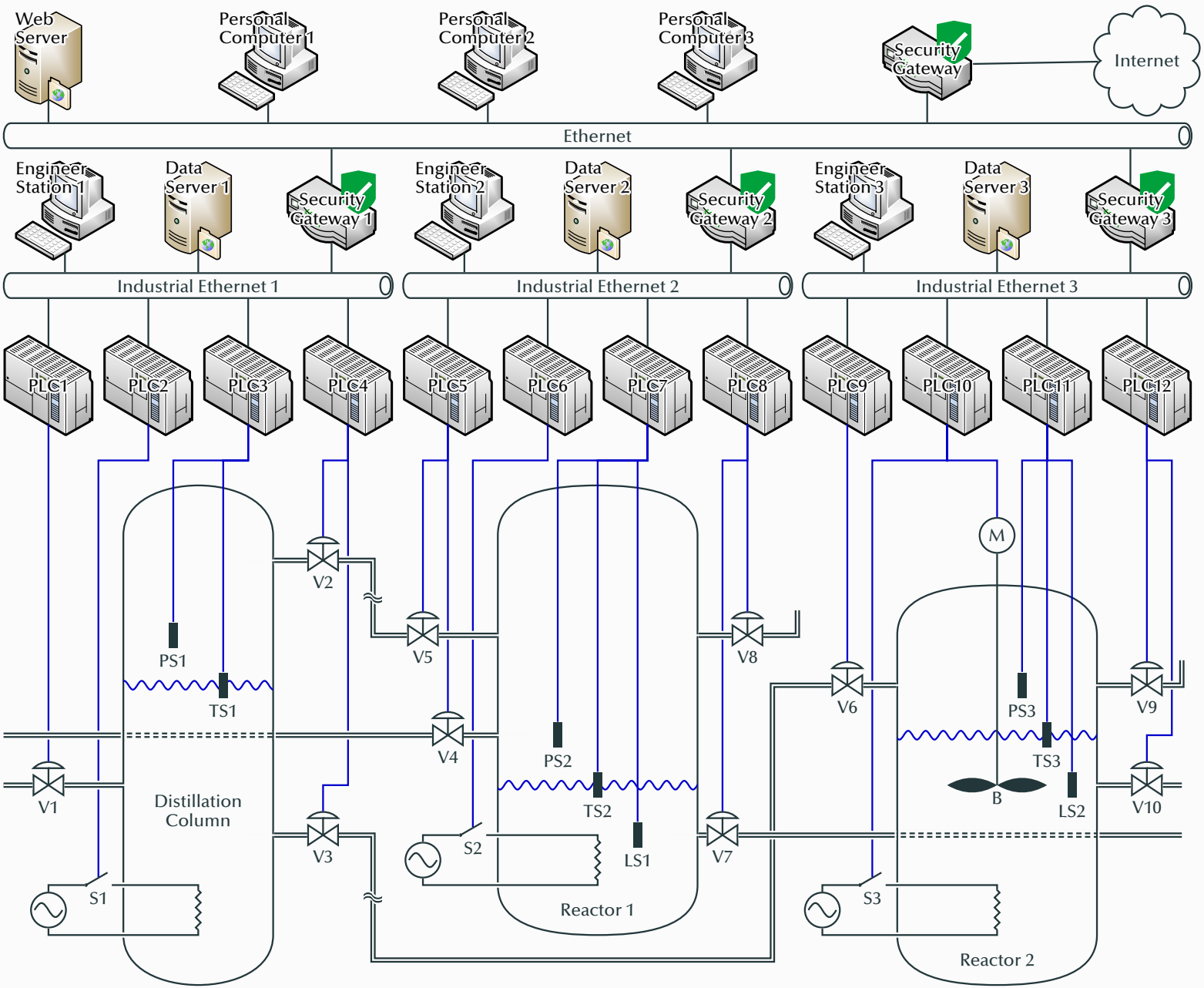
The Matlab codes are shown as follows.

```
34 % Remove all the evidences in the Bayesian network.
35 BayesianNetwork.RemoveEvidences();
36
37 % Add the evidence PX into the evidence list.
38 BayesianNetwork.AddEvidences(PX);
39
40 % Infer the Bayesian network with the evidences.
41 BayesianNetwork.Inference();
42
43 % Show the probability of the node BT.
44 BayesianNetwork.Display(BT);
```

The output of the program is shown as follows.

```
1 P(+Brain Tumor|+Pos Xray) = 0.089335
```

# Chemical Reactor Control System



# The Analysis of the Chemical Reactor Control System

In this chemical reactor control system, there are 2 semi-product and 2 product which is shown as follows.

| Symbol | Type | Description |
|---|---|---|
| `s01` | semi-product | the semi-product which is the output from the top of the distillation column |
| `s02` | semi-product | the semi-product which is the other outputs from the bottom of the distillation column |
| `s03` | product | the product which is the output from the reactor 1 |
| `s04` | product | the product which is the output from the reactor 2 |

# The Analysis of the Chemical Reactor Control System

The potential attacks are shown as follows.

| Symbol | Description | Launch Condition |
|---|---|---|
| a01 | network scanning of the Ethernet in the management layer | — |
| a02 | vulnerability scanning of the devices in the management layer | launch of a01 |
| a03 | buffer overflow attack on the web server | launch of a02 |
| a04 | brute force attack on the web server | launch of a02 |
| a05 | brute force attack on the personal computer 1 | launch of a02 |
| a06 | brute force attack on the personal computer 2 | launch of a02 |
| a07 | brute force attack on the personal computer 3 | launch of a02 |
| a08 | network scanning of the industrial Ethernet 1 in the control layer | launch of a03, a04, a05, a06, a07 |

# The Analysis of the Chemical Reactor Control System

The potential attacks are shown as follows.

| Symbol | Description | Launch Condition |
|---|---|---|
| a09 | vulnerability scanning of the devices in the industrial Ethernet 1 | launch of a08 |
| a10 | buffer overflow attack on the data server 1 | launch of a09 |
| a11 | brute force attack on the data server 1 | launch of a09 |
| a12 | brute force attack on the engineer station 1 | launch of a09 |
| a13 | network scanning of the industrial Ethernet 2 in the control layer | launch of a03, a04, a05, a06, a07 |
| a14 | vulnerability scanning of the devices in the industrial Ethernet 2 | launch of a13 |
| a15 | buffer overflow attack on the data server 2 | launch of a14 |
| a16 | brute force attack on the data server 2 | launch of a14 |

# The Analysis of the Chemical Reactor Control System

The potential attacks are shown as follows.

| Symbol | Description | Launch Condition |
|---|---|---|
| a17 | brute force attack on the engineer station 2 | launch of a14 |
| a18 | network scanning of the industrial Ethernet 3 in the control layer | launch of a03, a04, a05, a06, a07 |
| a19 | vulnerability scanning of the devices in the industrial Ethernet 3 | launch of a18 |
| a20 | buffer overflow attack on the data server 3 | launch of a19 |
| a21 | brute force attack on the data server 3 | launch of a19 |
| a22 | brute force attack on the engineer station 3 | launch of a19 |
| a23 | DoS attack on PLC1 | launch of a10, a11, a12 |
| a24 | DoS attack on PLC2 | launch of a10, a11, a12 |

# The Analysis of the Chemical Reactor Control System

The potential attacks are shown as follows.

| Symbol | Description | Launch Condition |
|---|---|---|
| a25 | DoS attack on PLC3 | launch of a10, a11, a12 |
| a26 | DoS attack on PLC4 | launch of a10, a11, a12 |
| a27 | DoS attack on PLC5 | launch of a15, a16, a17 |
| a28 | DoS attack on PLC6 | launch of a15, a16, a17 |
| a29 | DoS attack on PLC7 | launch of a15, a16, a17 |
| a30 | DoS attack on PLC8 | launch of a15, a16, a17 |
| a31 | DoS attack on PLC9 | launch of a20, a21, a22 |
| a32 | DoS attack on PLC10 | launch of a20, a21, a22 |

# The Analysis of the Chemical Reactor Control System

The potential attacks are shown as follows.

| Symbol | Description | Launch Condition |
|---|---|---|
| a33 | DoS attack on PLC11 | launch of a20, a21, a22 |
| a34 | DoS attack on PLC12 | launch of a20, a21, a22 |
| a35 | man-in-the-middle attack on PLC1 | launch of a12 |
| a36 | man-in-the-middle attack on PLC2 | launch of a12 |
| a37 | man-in-the-middle attack on PLC3 | launch of a12 |
| a38 | man-in-the-middle attack on PLC4 | launch of a12 |
| a39 | man-in-the-middle attack on PLC5 | launch of a17 |
| a40 | man-in-the-middle attack on PLC6 | launch of a17 |

# The Analysis of the Chemical Reactor Control System

The potential attacks are shown as follows.

| Symbol | Description | Launch Condition |
|---|---|---|
| a41 | man-in-the-middle attack on PLC7 | launch of a17 |
| a42 | man-in-the-middle attack on PLC8 | launch of a17 |
| a43 | man-in-the-middle attack on PLC9 | launch of a22 |
| a44 | man-in-the-middle attack on PLC10 | launch of a22 |
| a45 | man-in-the-middle attack on PLC11 | launch of a22 |
| a46 | man-in-the-middle attack on PLC12 | launch of a22 |

# The Analysis of the Chemical Reactor Control System

The functions of the system are shown as follows.

| Symbol | Description | Failure Condition |
|---|---|---|
| f01 | the temperature control function of distillation column | failure of f03, f05, f06, f07 |
| f02 | the pressure control function of distillation column | failure of f04, f06, f08 |
| f03 | the traffic control function of V1 | launch of a23, a35 |
| f04 | the traffic control function of V2 | launch of a26, a38 |
| f05 | the traffic control function of V3 | launch of a26, a38 |
| f06 | the switch control function of S1 | launch of a24, a36 |
| f07 | the temperature sensation function of distillation column | launch of a25, a37 |
| f08 | the pressure sensation function of distillation column | launch of a25, a37 |

# The Analysis of the Chemical Reactor Control System

The functions of the system are shown as follows.

| Symbol | Description | Failure Condition |
|---|---|---|
| f09 | the temperature control function of reactor 1 | failure of f12, f13, f14, f16, f17 |
| f10 | the pressure control function of reactor 1 | failure of f15, f16, f18 |
| f11 | the level control function of reactor 1 | failure of f12, f13, f14, f19 |
| f12 | the traffic control function of V4 | launch of a27, a39 |
| f13 | the traffic control function of V5 | launch of a27, a39 |
| f14 | the traffic control function of V7 | launch of a30, a42 |
| f15 | the pressure reducing function of reactor 1 | launch of a30, a42 |
| f16 | the switch control function of S2 | launch of a28, a40 |

# The Analysis of the Chemical Reactor Control System

The functions of the system are shown as follows.

| Symbol | Description | Failure Condition |
|---|---|---|
| f17 | the temperature sensation function of reactor 1 | launch of a29, a41 |
| f18 | the pressure sensation function of reactor 1 | launch of a29, a41 |
| f19 | the level sensation function of reactor 1 | launch of a29, a41 |
| f20 | the temperature control function of reactor 2 | failure of f23, f24, f26, f27 |
| f21 | the pressure control function of reactor 2 | failure of f25, f26, f28 |
| f22 | the level control function of reactor 2 | failure of f23, f24, f29 |
| f23 | the traffic control function of V6 | launch of a31, a43 |
| f24 | the traffic control function of V10 | launch of a34, a46 |

# The Analysis of the Chemical Reactor Control System

The functions of the system are shown as follows.

| Symbol | Description | Failure Condition |
|---|---|---|
| f25 | the pressure reducing function of reactor 2 | launch of a34 , a46 |
| f26 | the switch control function of S3 | launch of a32 , a44 |
| f27 | the temperature sensation function of reactor 2 | launch of a33 , a45 |
| f28 | the pressure sensation function of reactor 2 | launch of a33 , a45 |
| f29 | the level sensation function of reactor 2 | launch of a33 , a45 |
| f30 | the mixing function of reactor 2 | launch of a32 , a44 |
| f31 | the data service of industrial Ethernet 1 | some security strategies |
| f32 | the data service of industrial Ethernet 2 | some security strategies |

# The Analysis of the Chemical Reactor Control System

The functions of the system are shown as follows.

| Symbol | Description | Failure Condition |
|---|---|---|
| f33 | the data service of industrial Ethernet 3 | some security strategies |
| f34 | the configuration of PLCs of distillation column | some security strategies |
| f35 | the configuration of PLCs of reactor 1 | some security strategies |
| f36 | the configuration of PLCs of reactor 2 | some security strategies |
| f37 | the data service of the Ethernet | some security strategies |
| f38 | the production scheduling function provided by personal computer 1 | some security strategies |
| f39 | the production scheduling function provided by personal computer 2 | some security strategies |
| f40 | the production scheduling function provided by personal computer 3 | some security strategies |

# The Analysis of the Chemical Reactor Control System

The functions of the system are shown as follows.

| Symbol | Description | Failure Condition |
| --- | --- | --- |
| f41 | the production scheduling function | failure of f31, f32, f33, f38, f39, f40 |

# The Analysis of the Chemical Reactor Control System

The potential hazardous incident are shown as follows.

| Symbol | Description | Location | Inducement |
|---|---|---|---|
| e01 | pressure anomaly | distillation column | failure of f02 |
| e02 | temperature anomaly | distillation column | failure of f01 |
| e03 | traffic of anomaly | distillation column | failure of f03, f04, f05 |
| e04 | excessive pressure | reactor 1 | failure of f10 |
| e05 | low pressure | reactor 1 | failure of f10 |
| e06 | temperature anomaly | reactor 1 | failure of f09 |
| e07 | excessive liquid level | reactor 1 | failure of f11 |
| e08 | low liquid level | reactor 1 | failure of f11 |

# The Analysis of the Chemical Reactor Control System

The potential hazardous incident are shown as follows.

| Symbol | Description | Location | Inducement |
|---|---|---|---|
| e09 | explosion | reactor 1 | occurrence of e04 |
| e10 | heater dry fired | reactor 1 | occurrence of e08 |
| e11 | liquid overflow | reactor 1 | occurrence of e07 |
| e12 | excessive pressure | reactor 2 | failure of f21 |
| e13 | low pressure | reactor 2 | failure of f21 |
| e14 | temperature anomaly | reactor 2 | failure of f20 |
| e15 | excessive liquid level | reactor 2 | failure of f22 |
| e16 | low liquid level | reactor 2 | failure of f22 |

# The Analysis of the Chemical Reactor Control System

The potential hazardous incident are shown as follows.

| Symbol | Description | Location | Inducement |
|---|---|---|---|
| e17 | explosion | reactor 2 | occurrence of e12 |
| e18 | heater dry fired | reactor 2 | occurrence of e16 |
| e19 | liquid overflow | reactor 2 | occurrence of e15 |
| e20 | blender stop | reactor 2 | failure of f30 |
| e21 | out of control | distillation column | failure of f34 |
| e22 | out of control | reactor 1 | failure of f35 |
| e23 | out of control | reactor 2 | failure of f36 |
| e24 | production scheduling error | control layer | failure of f31 , f32 , f33 |

# The Analysis of the Chemical Reactor Control System

The potential hazardous incident are shown as follows.

| Symbol | Description | Location | Inducement |
|---|---|---|---|
| e25 | production scheduling error | plant | failure of f37 |

# The Analysis of the Chemical Reactor Control System

The potential hazardous incident are shown as follows.

| Symbol | Description | Value($) | Hazardous Incident |
|---|---|---|---|
| x01 | semi-product s01 and s02 | 30,000 | e01, e02, e03, e21 |
| x02 | product s03 | 60,000 | e06, e09, e11, e22 |
| x03 | product s04 | 70,000 | e14, e17, e20, e23 |
| x04 | tank and sensors of reactor 1 | 200,000 | e09 |
| x05 | heater of reactor 1 | 40,000 | e09, e10 |
| x06 | tank, sensors and blender of reactor 2 | 300,000 | e17 |
| x07 | heater of reactor 2 | 50,000 | e17, e18 |
| x08 | staff 1-4 | 800,000 | e09, e11 |

# The Analysis of the Chemical Reactor Control System

The potential hazardous incident are shown as follows.

| Symbol | Description | Value($) | Hazardous Incident |
|---|---|---|---|
| x09 | staff 5-9 | 100,000 | e17 , e19 |
| x10 | river and solid | 900,000 | e09 , e11 , e17 , e19 |
| x11 | air | 400,000 | e09 , e17 |

# The Analysis of the Chemical Reactor Control System

The security strategies of the system are shown as follows.

| Symbol | Description | Prevented Attacks | Invalidated Functions |
|---|---|---|---|
| m01 | disconnect the security gateway | a01 | f37 |
| m02 | shut down the web server | a03 , a04 | f37 |
| m03 | shut down the personal computer 1 | a05 | f38 |
| m04 | shut down the personal computer 2 | a06 | f39 |
| m05 | shut down the personal computer 3 | a07 | f40 |
| m06 | disconnect the security gateway 1 | a08 | f31 |
| m07 | shut down the data server 1 | a10 , a11 | f31 |
| m08 | shut down the engineer station 1 | a12 | f34 |

# The Analysis of the Chemical Reactor Control System

The security strategies of the system are shown as follows.

| Symbol | Description | Prevented Attacks | Invalidated Functions |
|---|---|---|---|
| m09 | encrypt the data amongst the PLC 1-4 | a35, a36, a37, a38 | — |
| m10 | disconnect the security gateway 2 | a13 | f32 |
| m11 | shut down the data server 2 | a15, a16 | f32 |
| m12 | shut down the engineer station 2 | a17 | f35 |
| m13 | encrypt the data amongst the PLC 5-8 | a39, a40, a41, a42 | — |
| m14 | disconnect the security gateway 3 | a18 | f33 |
| m15 | shut down the data server 3 | a20, a21 | f33 |
| m16 | shut down the engineer station 3 | a22 | f36 |

# The Analysis of the Chemical Reactor Control System

The security strategies of the system are shown as follows.

| Symbol | Description | Prevented Attacks | Invalidated Functions |
|---|---|---|---|
| m17 | encrypt the data amongst the PLC 9-12 | a43 , a44 , a45 , a46 | — |

# The Analysis of the Chemical Reactor Control System

The recover strategies of the system are shown as follows.

| Symbol | Description | Rocovered Functions | Cost($) |
|---|---|---|---|
| n01 | reboot PLC1 | f03 | 9,000 |
| n02 | reboot PLC2 | f06 | 9,000 |
| n03 | reboot PLC3 | f07 , f08 | 10,000 |
| n04 | reboot PLC4 | f04 , f05 | 15,000 |
| n05 | reboot PLC5 | f12 , f13 | 8,000 |
| n06 | reboot PLC6 | f16 | 10,000 |
| n07 | reboot PLC7 | f17 , f18 , f19 | 2,000 |
| n08 | reboot PLC8 | f14 , f15 | 13,000 |

# The Analysis of the Chemical Reactor Control System

The recover strategies of the system are shown as follows.

| Symbol | Description | Rocovered Functions | Cost($) |
|---|---|---|---|
| n09 | reboot PLC9 | f23 | 14,000 |
| n10 | reboot PLC10 | f26 , f30 | 7,500 |
| n11 | reboot PLC11 | f27 , f28 , f29 | 14,000 |
| n12 | reboot PLC12 | f24 , f25 | 11,000 |

# Task Planning

# Task Planning

- Finish the simulation of 2nd paper.
- Finish the 3rd paper for the special issue on Fuzzy Systems.