Multi-Model Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems

Zhang Qi

qiqi@hust.edu.cn

October 11, 2015

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

Outlines

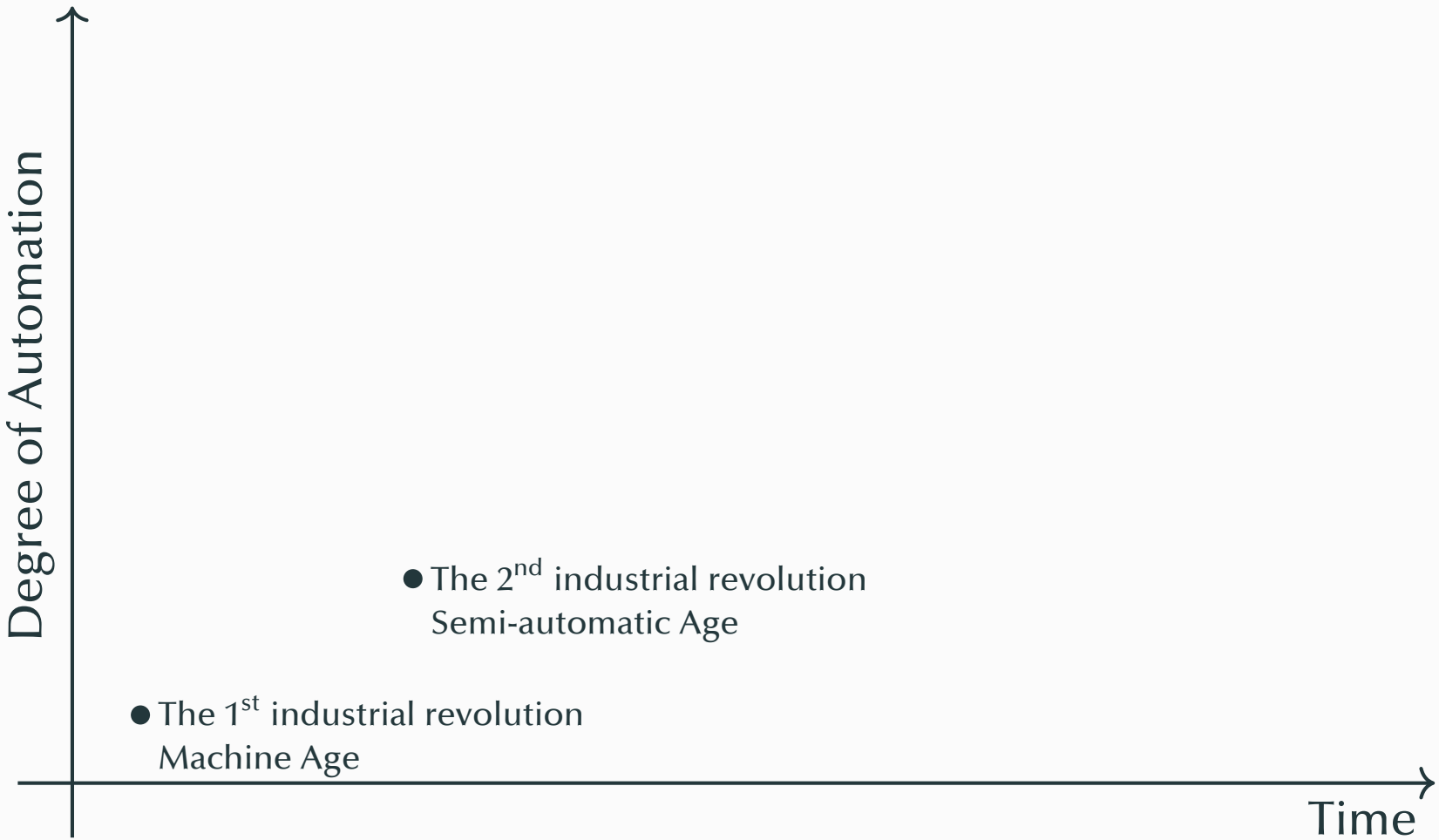
Introduction

Background

Driven by computer technology, communication technology and intellectual technology, Industrial Control Systems (ICSs) develop towards the direction of intellectualization and network.

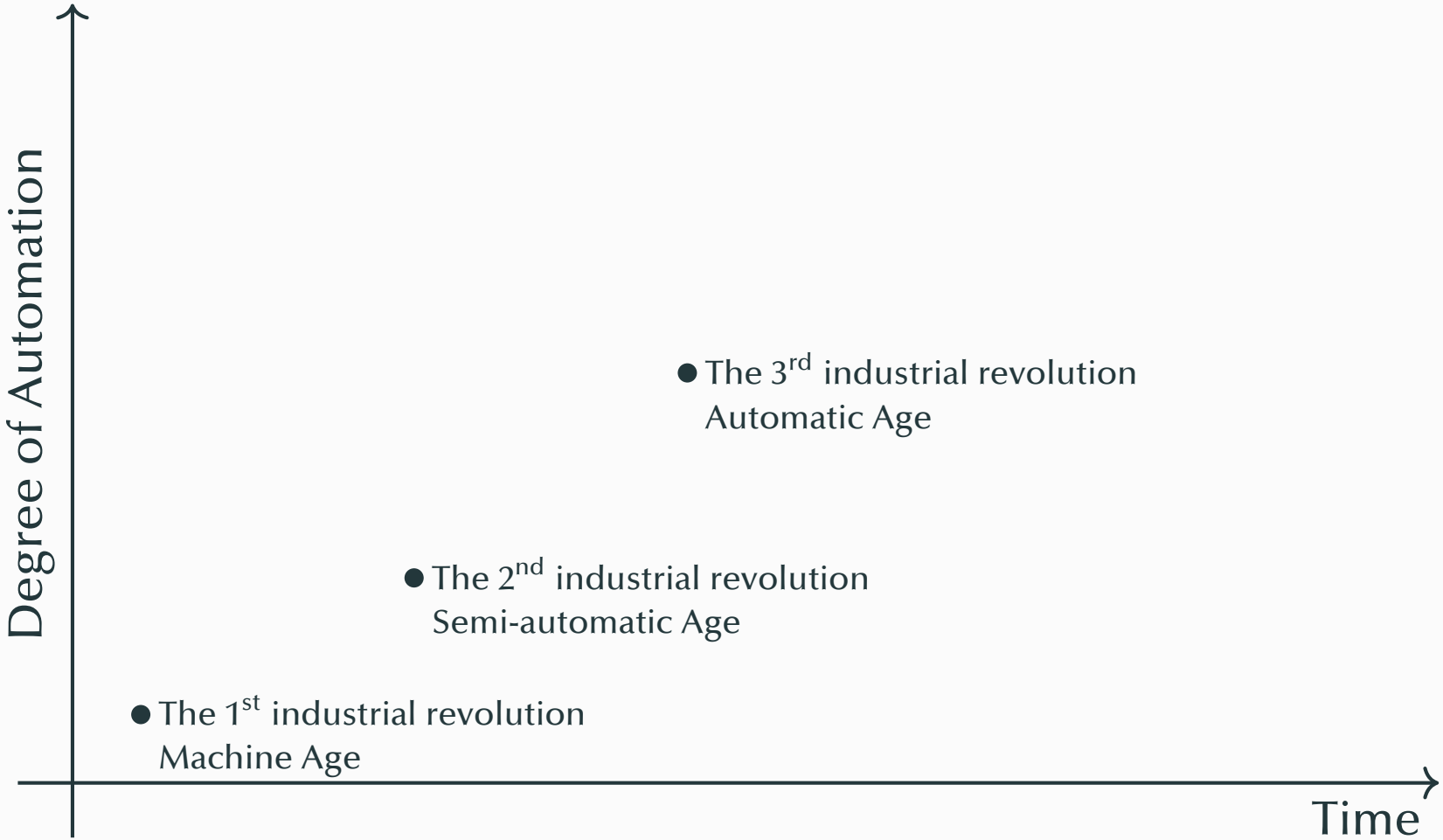
Background

Driven by computer technology, communication technology and intellectual technology, Industrial Control Systems (ICSs) develop towards the direction of intellectualization and network.



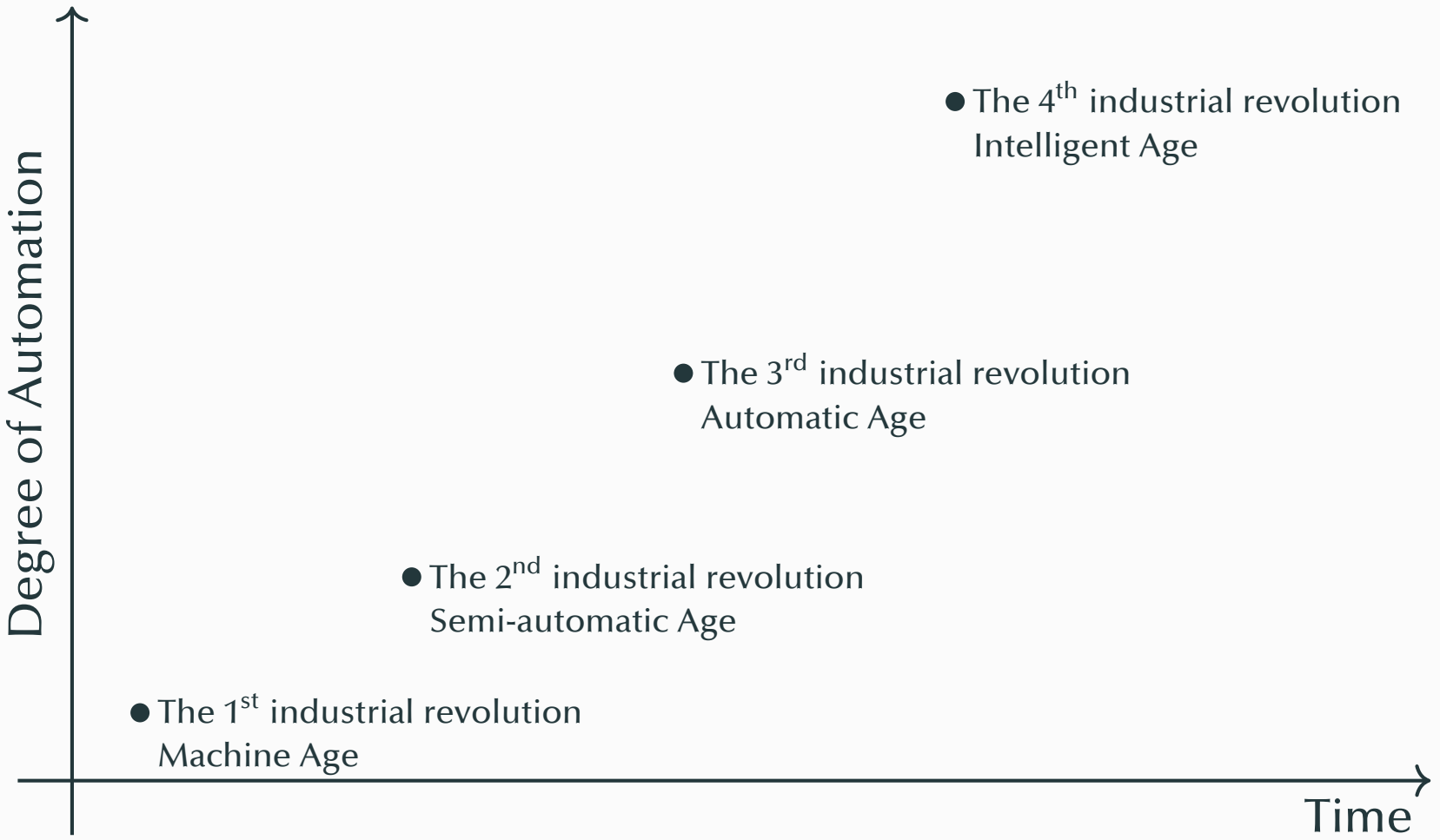
Background

Driven by computer technology, communication technology and intellectual technology, Industrial Control Systems (ICSs) develop towards the direction of intellectualization and network.



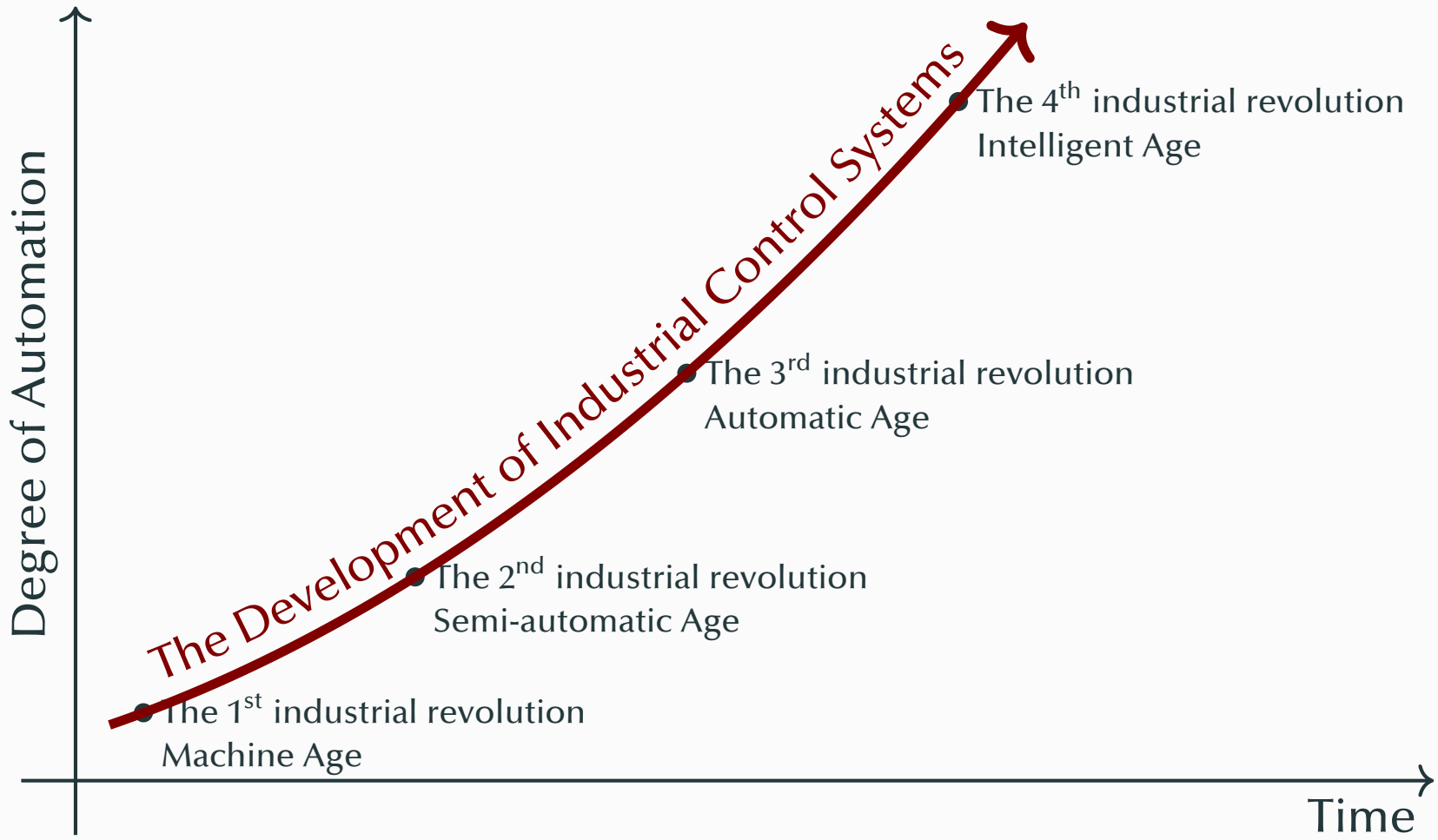
Background

Driven by computer technology, communication technology and intellectual technology, Industrial Control Systems (ICSs) develop towards the direction of intellectualization and network.



Background

Driven by computer technology, communication technology and intellectual technology, Industrial Control Systems (ICSs) develop towards the direction of intellectualization and network.

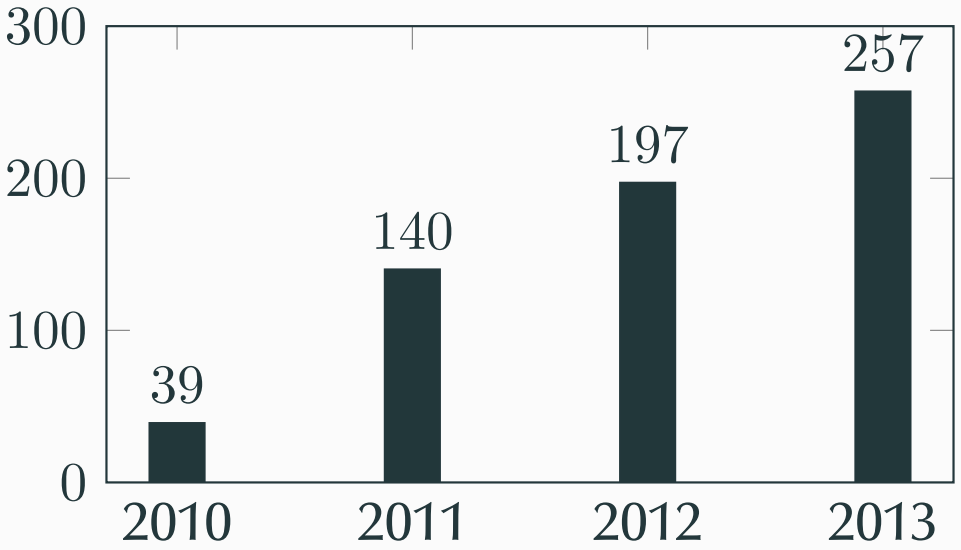


Background

- ICSs have been widely applied in various industry of the national economy and people's livelihood, and gradually become the brain and central nervous of critical infrastructure and all kinds of industrial production.
- Once abnormal situation appears in ICSs , serious accidents may be happen, which may cause damage to property, people or a wide range of environment.

Background

- In 2010, Stuxnet attacked Iran's nuclear power plants and ruined almost one-fifth of Iran's nuclear centrifuges.
- In 2013, Israel Haifa highway control system was attacked by hackers, which caused massive traffic congestion in the city which lead great loss and serious subsequent problems.
- In 2014, Havex malware infects many industrial control system in European and caused the leakage of large amounts of data.



ICSs Event Statistic (ICS-CERT)

Problems – Timeliness and Availability

ICSs have rigorous requirements on timeliness and availability. The cybersecurity risks of ICSs are primarily from the potential loss caused by the cyber-attacks which demolish the timeliness and availability of the control system.

In order to achieve the destructive purpose, attackers generally need to follow part or all of these three steps:

1. infiltrate into the field network,
2. invalidate the system functions,
3. cause the hazardous incidents.

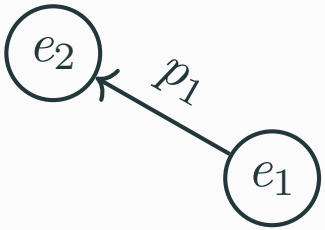
Therefore, the cybersecurity risk assessment of ICSs needs a novel and targeted risk model to analyze the risk propagation.

Problems – Overlapping amongst Consequences

The majority of existing quantitative risk assessment approaches used the following definition to calculate the risk $\mathscr{R}$.

$$\mathscr{R} = \sum_i S(e_i)P(e_i)$$

However, the overlapping amongst difference consequences may cause the error of risk value. For example,



incident e_1 is the temperature anomaly of reactor, incident e_2 is the explosion of reactor, when e_1 or e_2 happens, the product will be damaged.

Assume that $P(e_1) = 1$, so $P(e_2) = p_1$, then

$$\mathscr{R} = S(e_1) + p_1 S(e_2) = S(e_1) + p_1 S(e_1) = (1 + p_1)S(e_1) \geq S(e_1).$$

Problems – Unknown Attacks

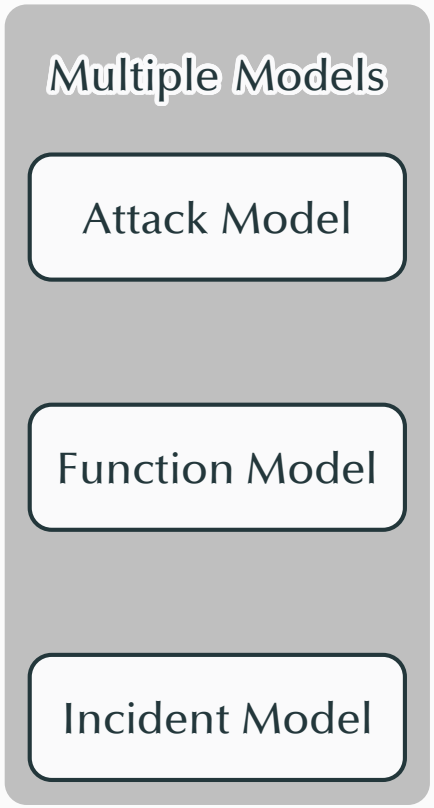
Many ICSs run 24/7/365, and therefore the updates must be planned and scheduled days or weeks in advance. After the updates, exhaustive testing is necessary to ensure the high availability of the ICS.

This leads to inability of the attack knowledge of ICSs to be updated in time. Several attack knowledge-based risk assessments cannot work well on ICSs.

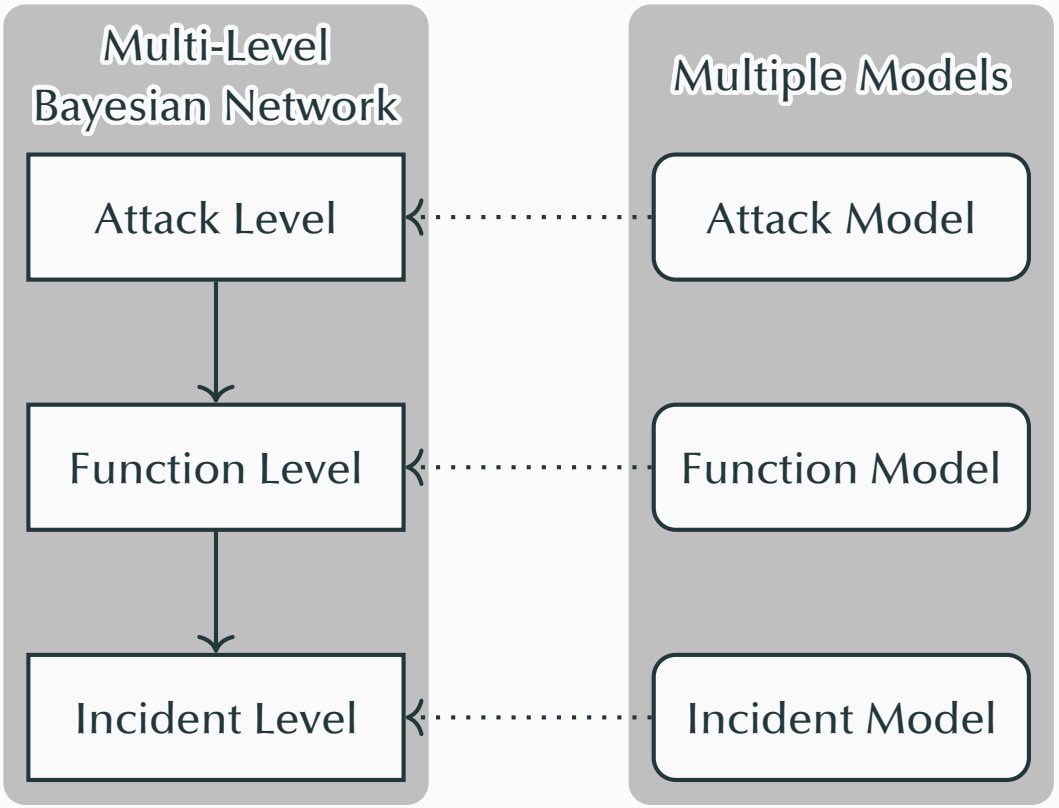
Therefore, the risk assessment should have the ability of assessing the risk caused by unknown attacks without the corresponding attack knowledge.

Architecture

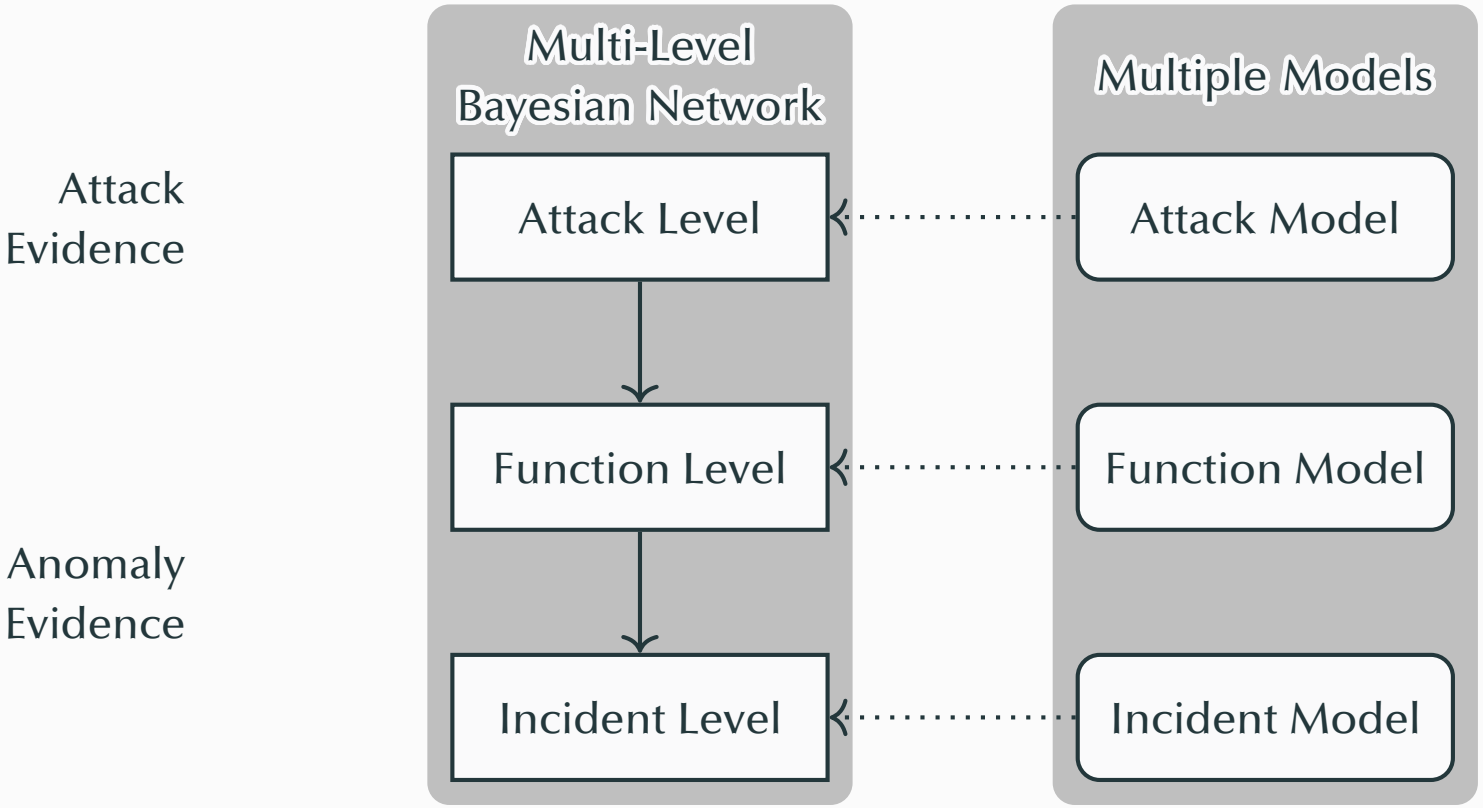
Architecture of Cybersecurity Risk Assessment for ICSs



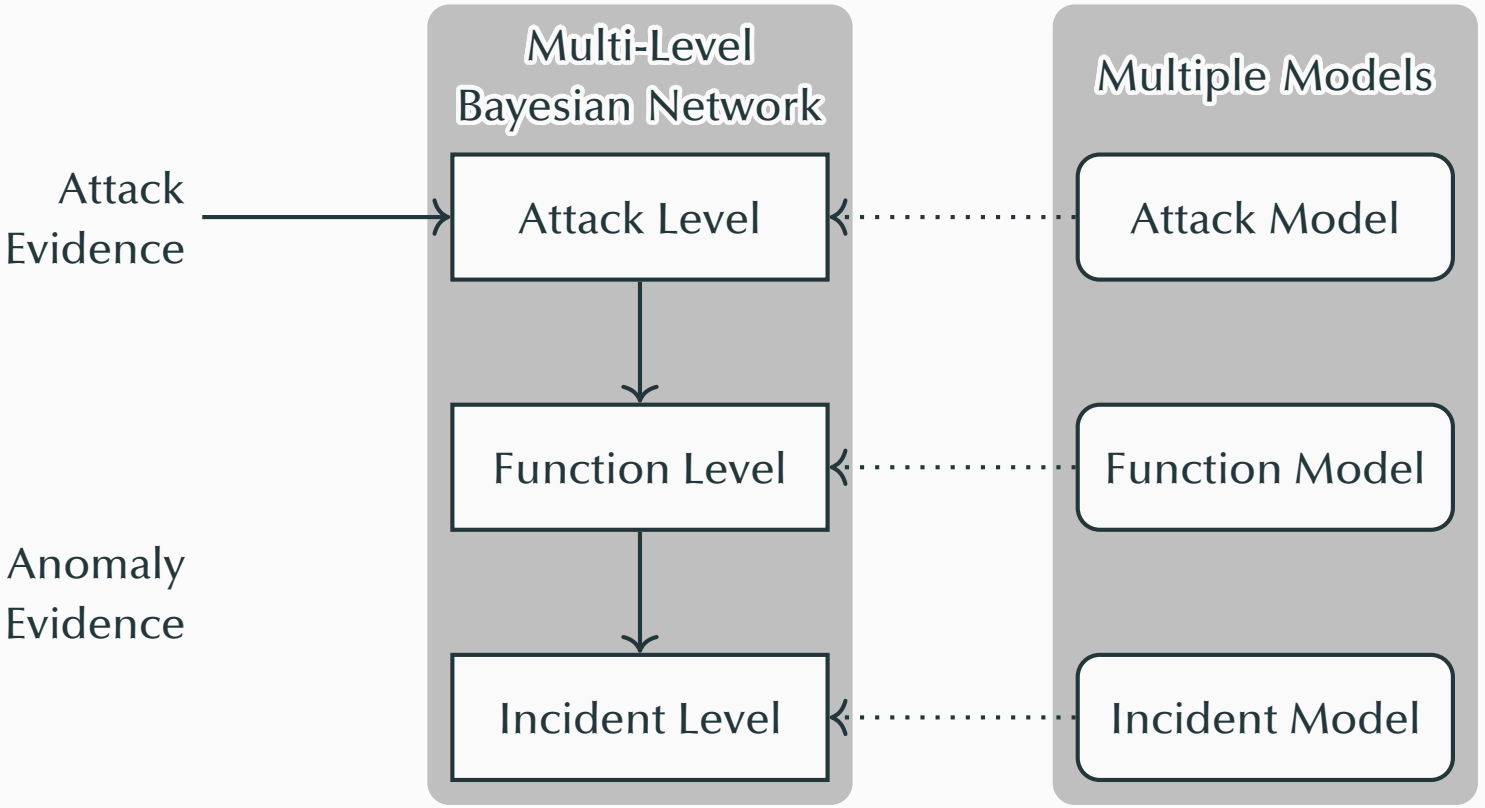
Architecture of Cybersecurity Risk Assessment for ICSs



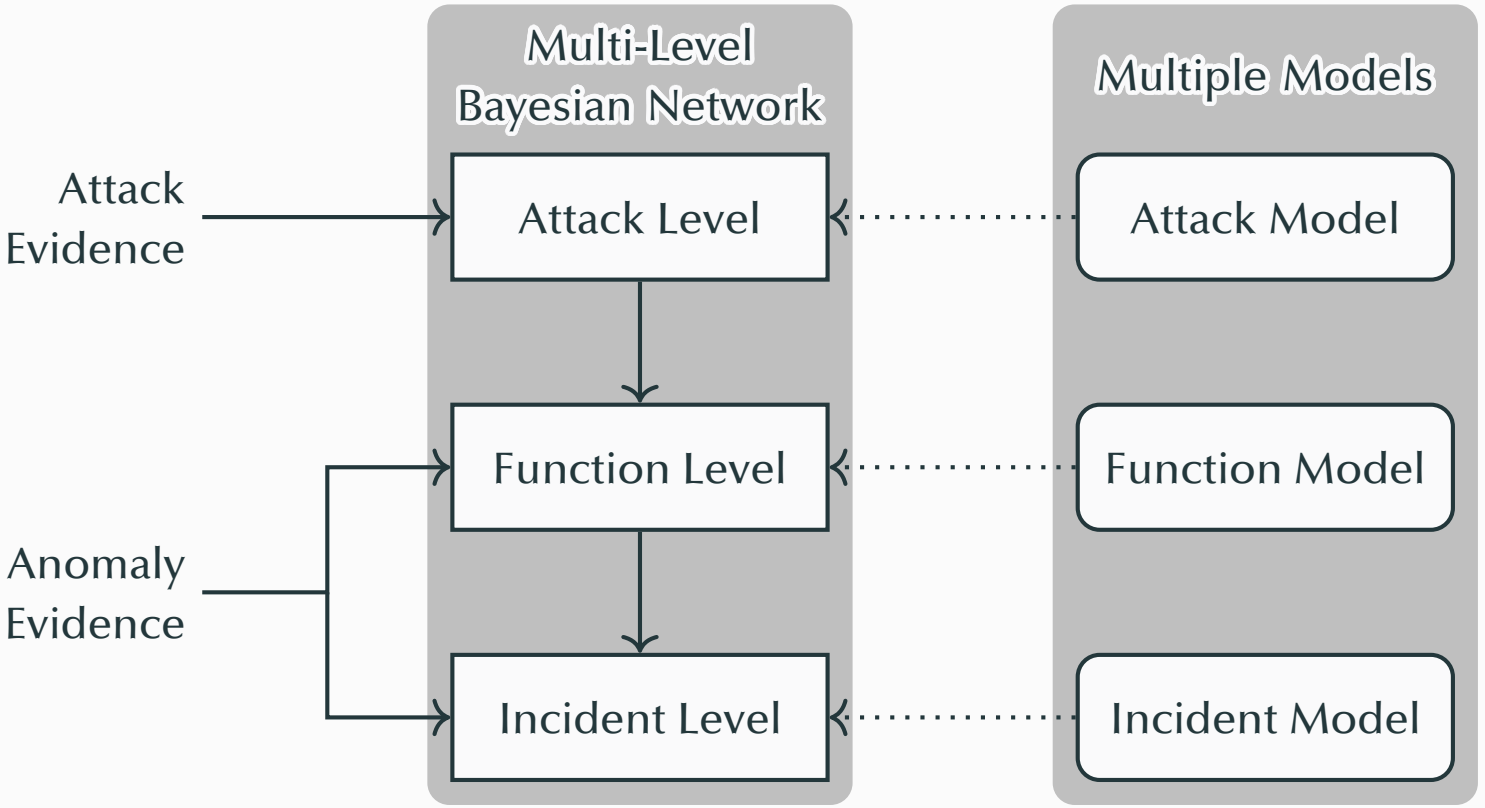
Architecture of Cybersecurity Risk Assessment for ICSs



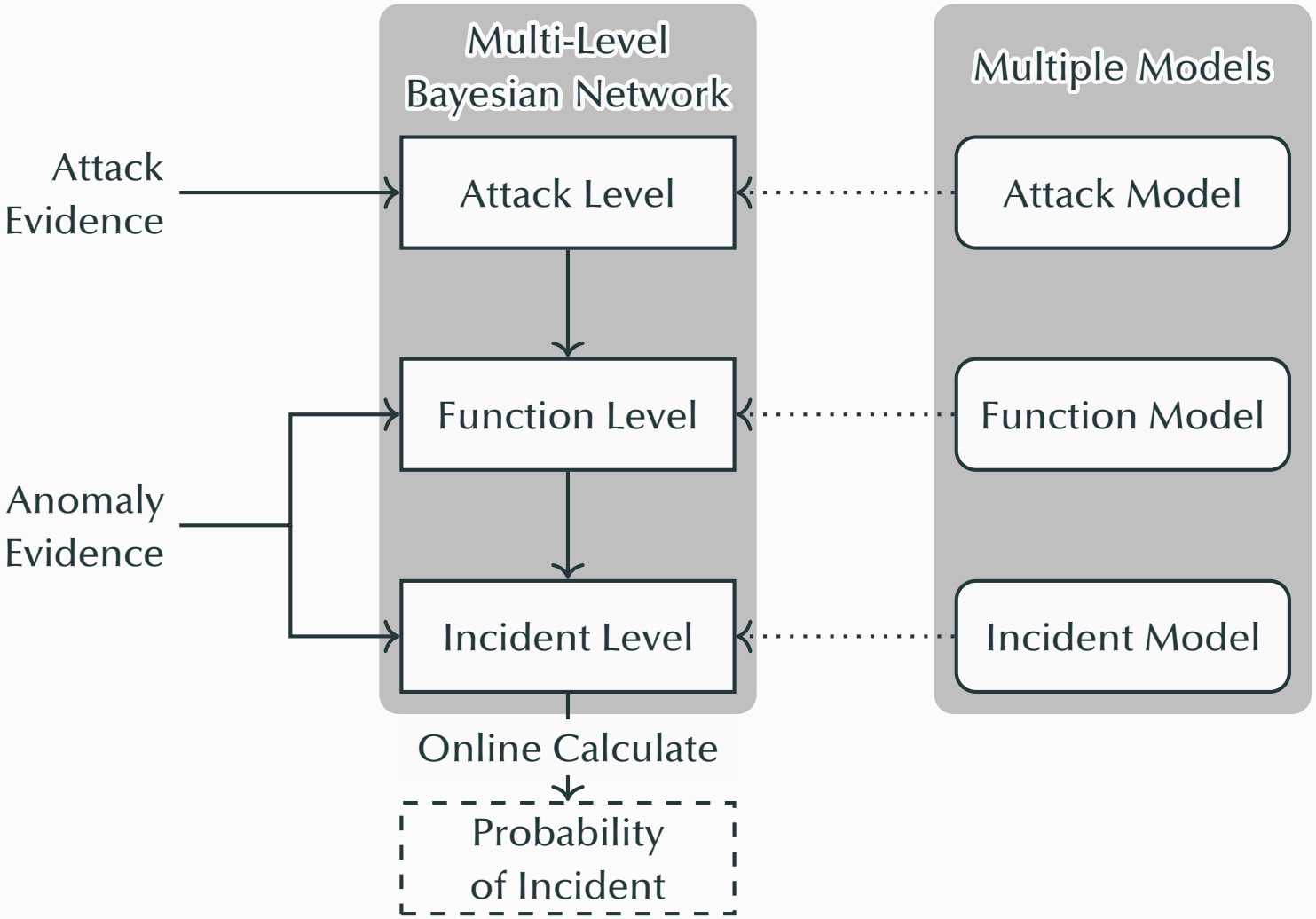
Architecture of Cybersecurity Risk Assessment for ICSs



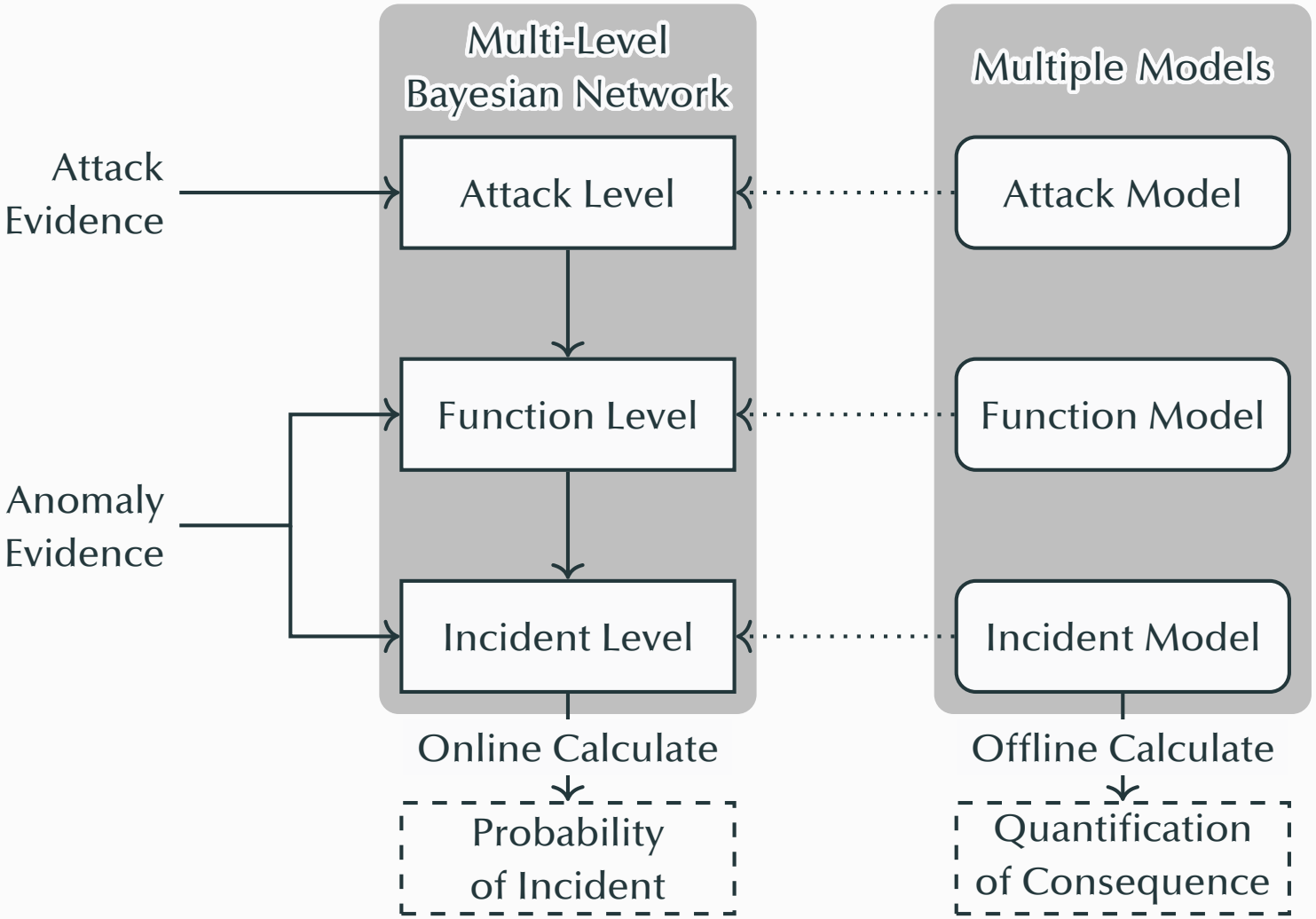
Architecture of Cybersecurity Risk Assessment for ICSs



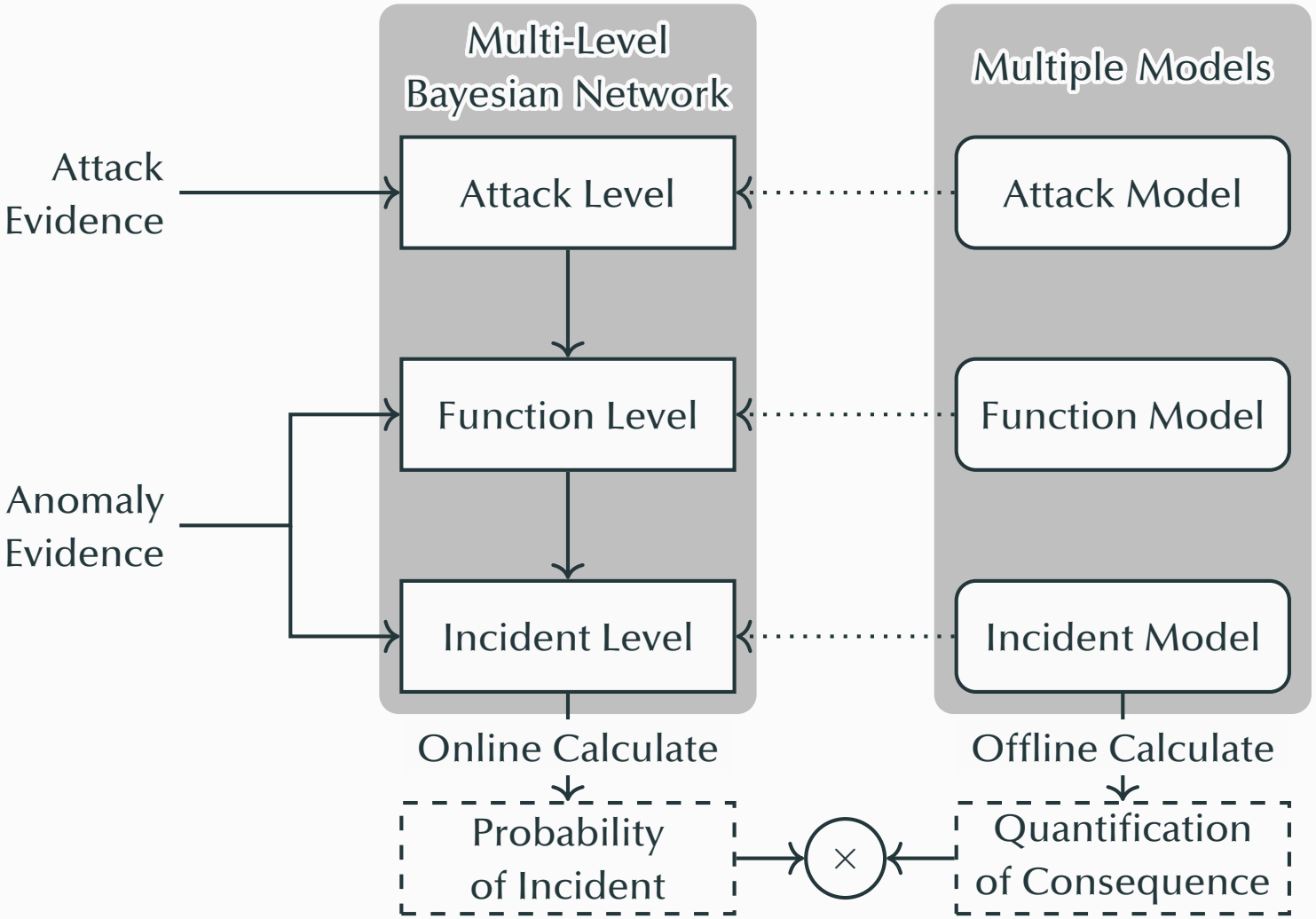
Architecture of Cybersecurity Risk Assessment for ICSs



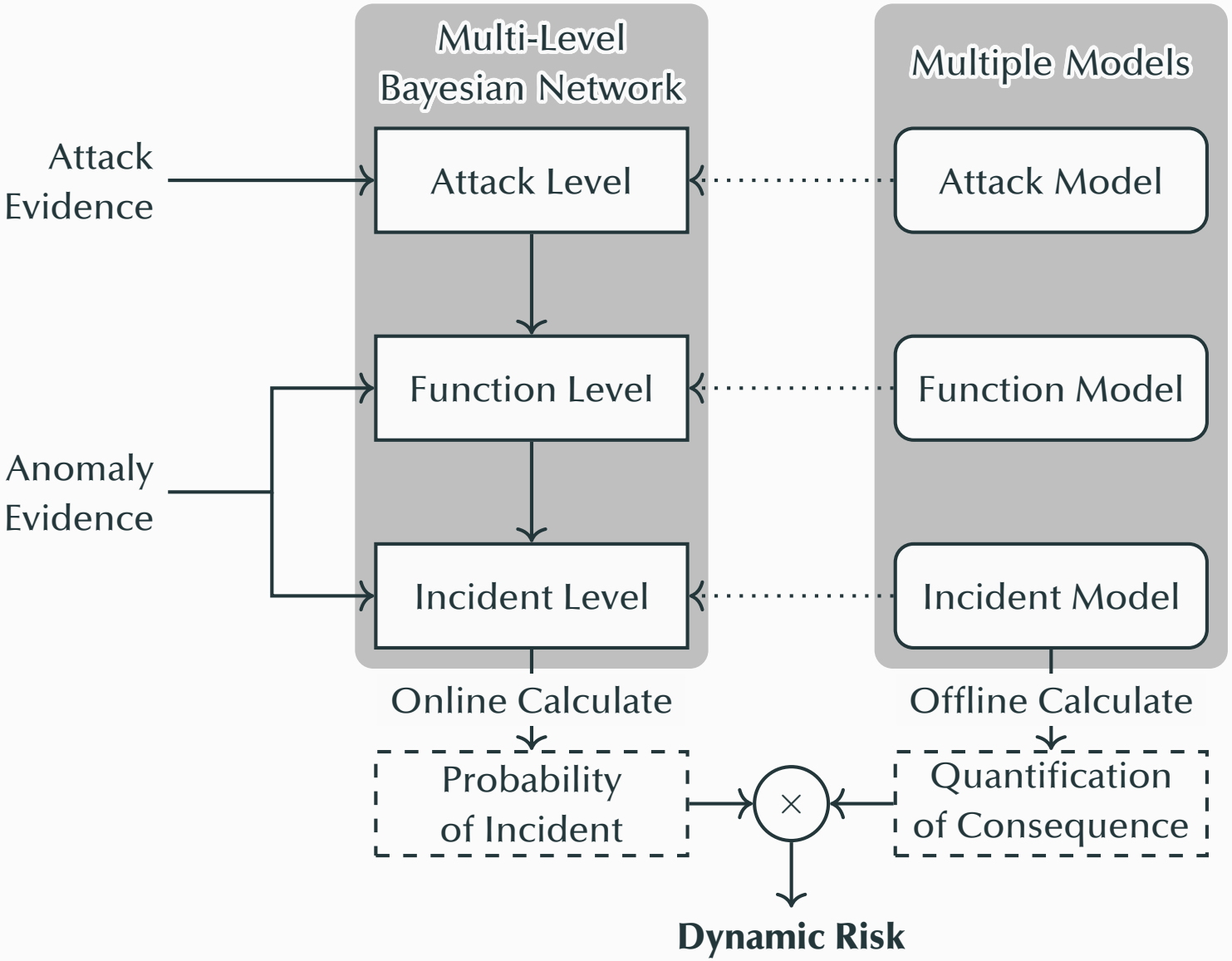
Architecture of Cybersecurity Risk Assessment for ICSs



Architecture of Cybersecurity Risk Assessment for ICSs



Architecture of Cybersecurity Risk Assessment for ICSs



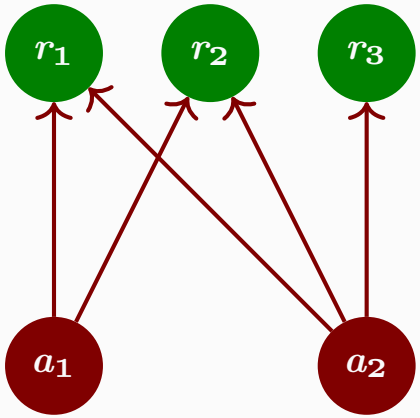
Hazardous Incident Prediction

Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.

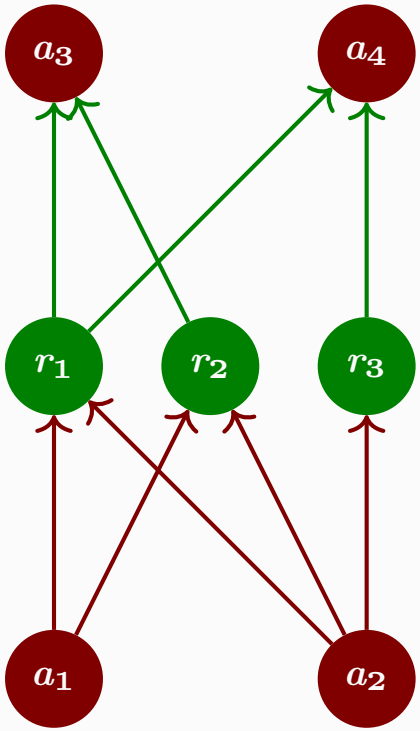
Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.



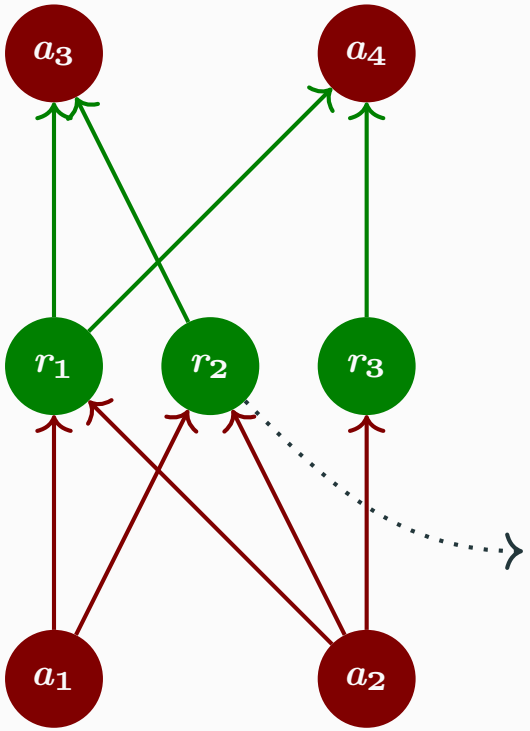
Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.



Attack Level

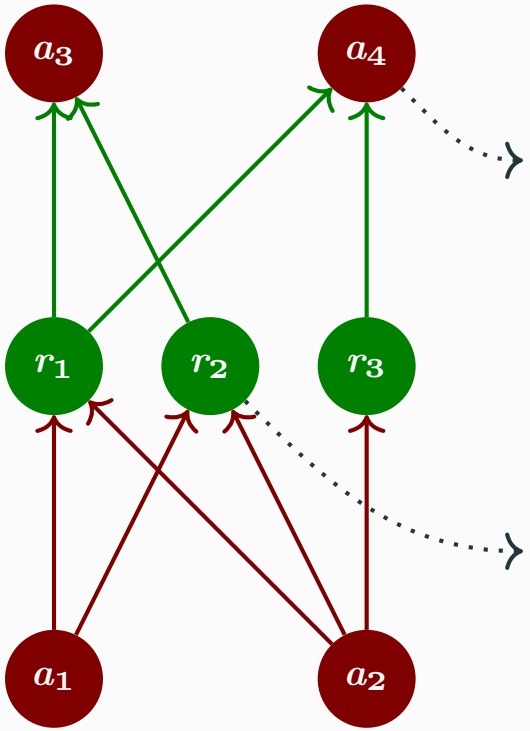
In this paper, the Bayesian network is used to model the relationship between attacks and resources.



$L(a_1)$	T	T	F	F
$L(a_2)$	T	F	T	F
$O(r_2)$	$o_{r_2,1}$	$o_{r_2,2}$	$o_{r_2,3}$	$o_{r_2,4}$
$\overline{O}(r_2)$	$1-o_{r_2,1}$	$1-o_{r_2,2}$	$1-o_{r_2,3}$	$1-o_{r_2,4}$

Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.



$O(r_1)$	T	T	F	F
$O(r_3)$	T	F	T	F
$L(a_4)$	$\ell_{a_4,1}$	$\ell_{a_4,2}$	$\ell_{a_4,3}$	$\ell_{a_4,4}$
$\overline{L}(a_4)$	$1-\ell_{a_4,1}$	$1-\ell_{a_4,2}$	$1-\ell_{a_4,3}$	$1-\ell_{a_4,4}$

$L(a_1)$	T	T	F	F
$L(a_2)$	T	F	T	F
$O(r_2)$	$o_{r_2,1}$	$o_{r_2,2}$	$o_{r_2,3}$	$o_{r_2,4}$
$\overline{O}(r_2)$	$1-o_{r_2,1}$	$1-o_{r_2,2}$	$1-o_{r_2,3}$	$1-o_{r_2,4}$

Function Level

Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.

Function Level

Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.

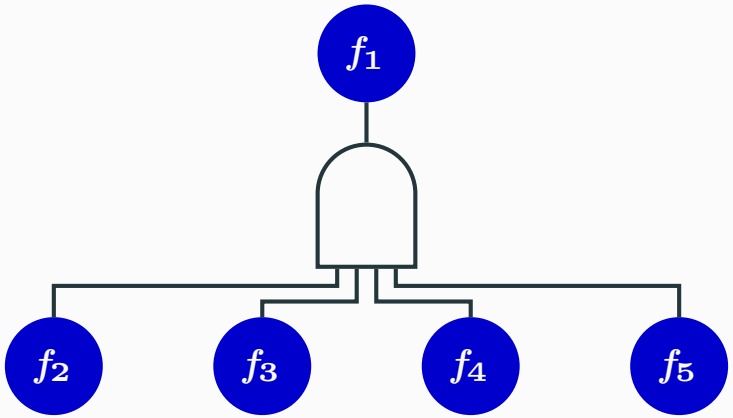
Function Level

Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.

$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

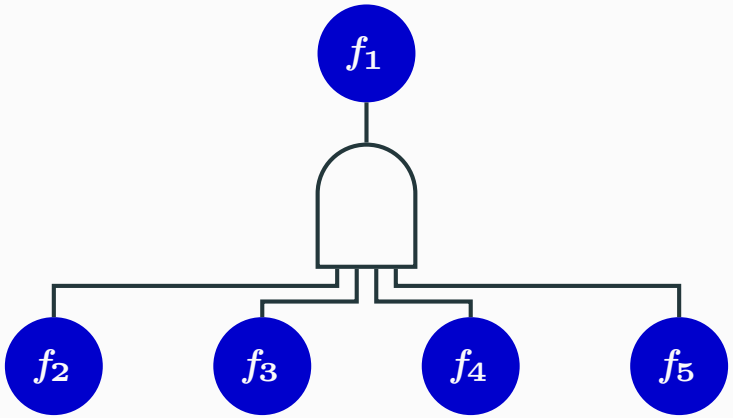
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

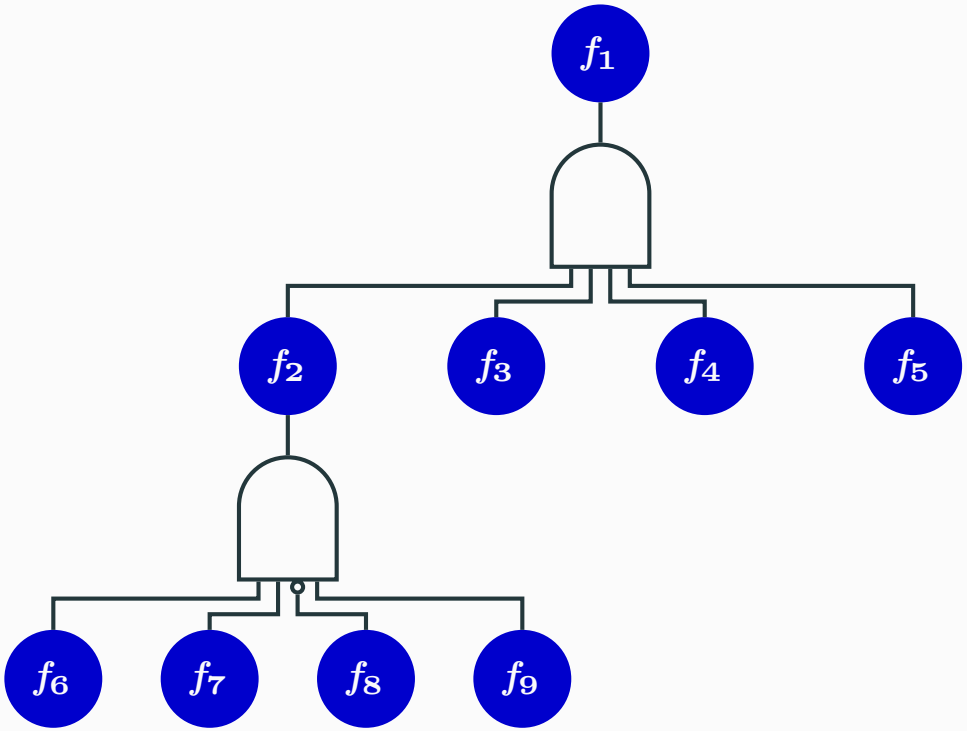
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_2 = F_6 F_7 \overline{F_8} F_9$$

Function Level

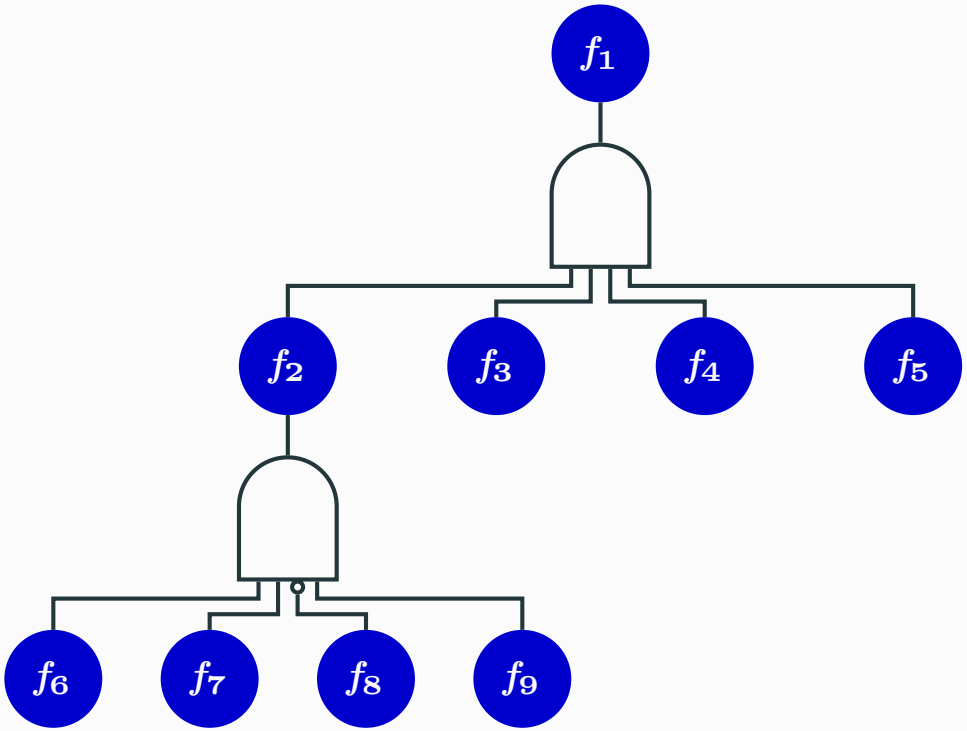
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_2 = F_6 F_7 \overline{F_8} F_9$$

Function Level

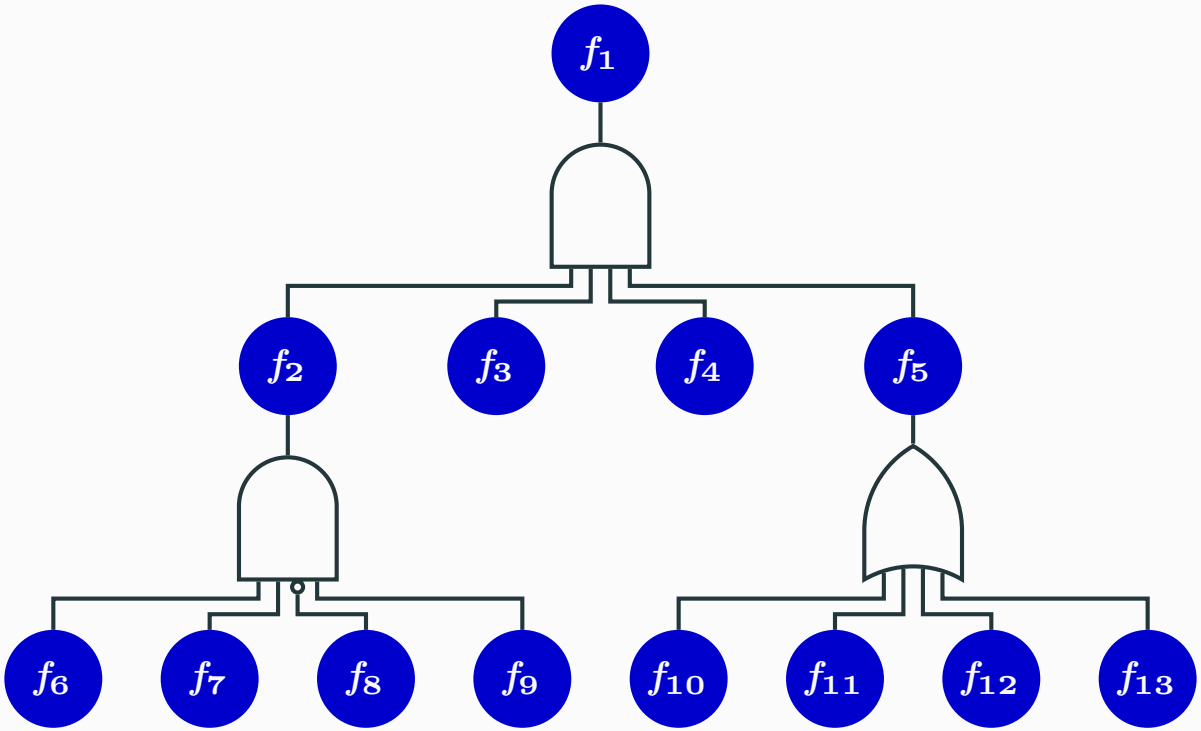
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_5 = F_{10} + F_{11} + F_{12} + F_{13}$$

Function Level

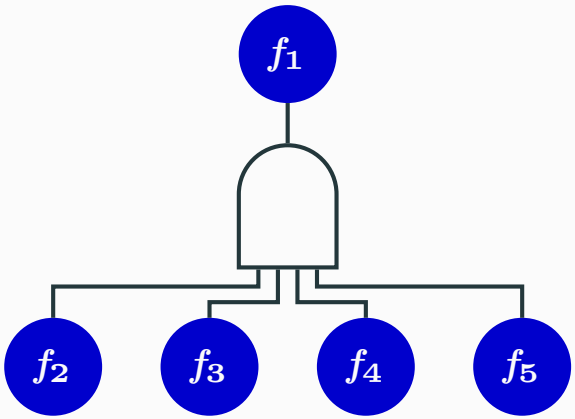
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_5 = F_{10} + F_{11} + F_{12} + F_{13}$$

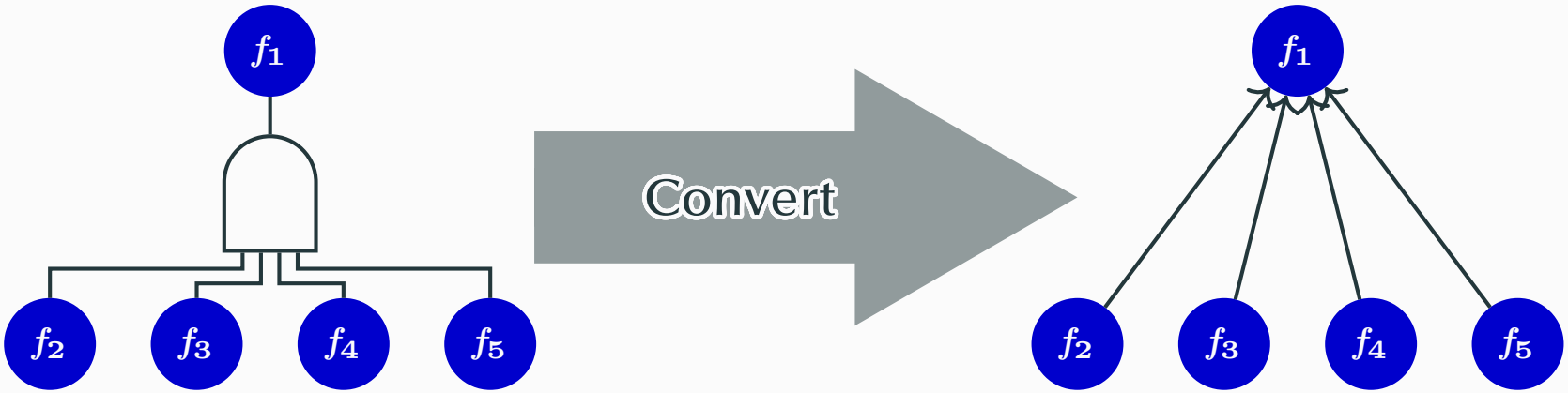
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



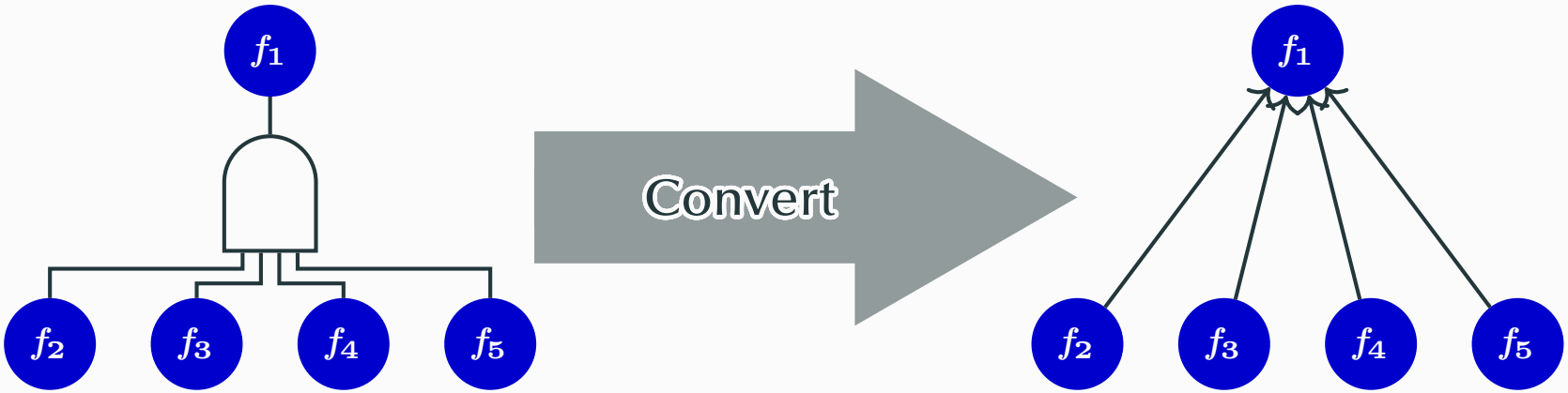
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



Function Level

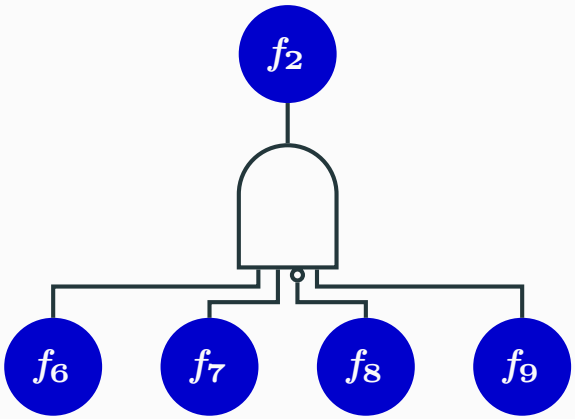
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

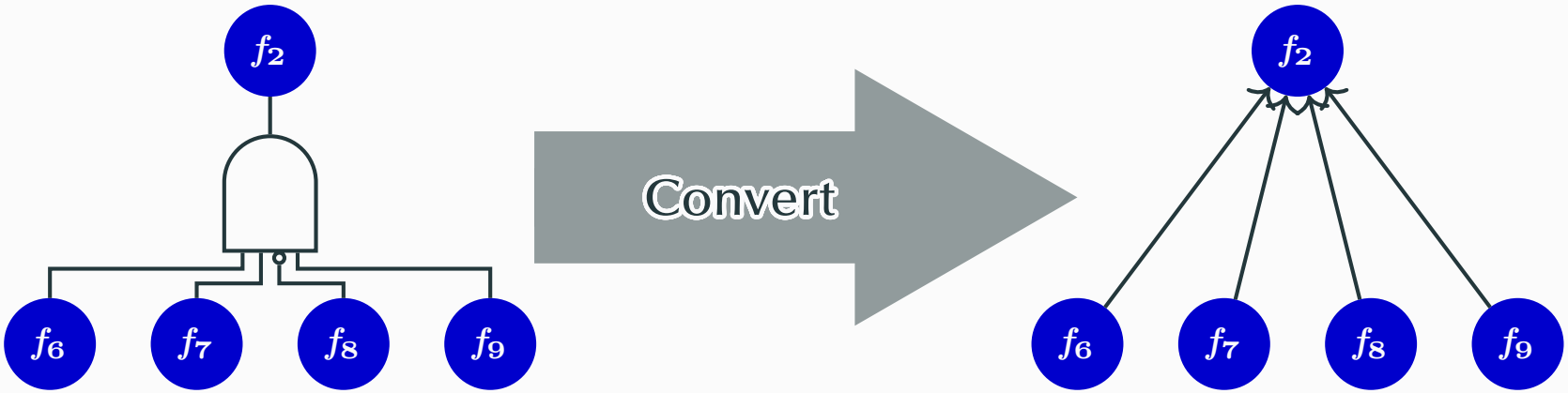
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



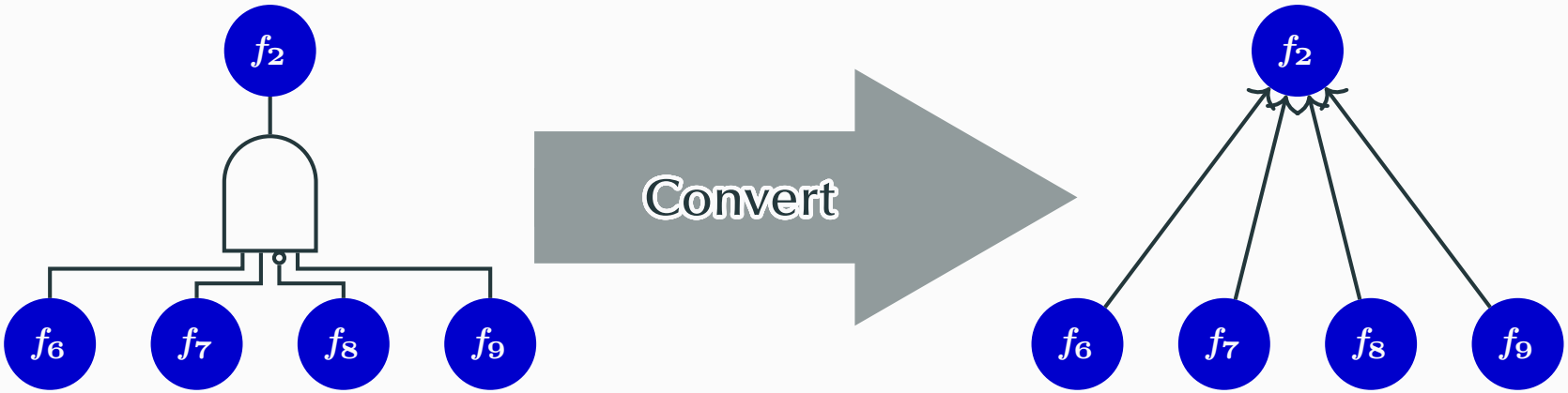
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



Function Level

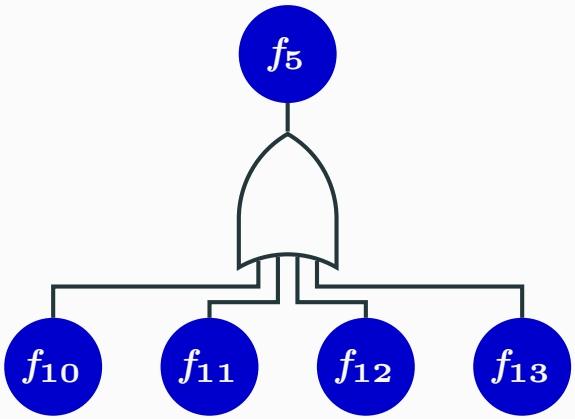
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_6)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_7)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_8)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_9)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_1)$	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
$\overline{F}(f_1)$	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0

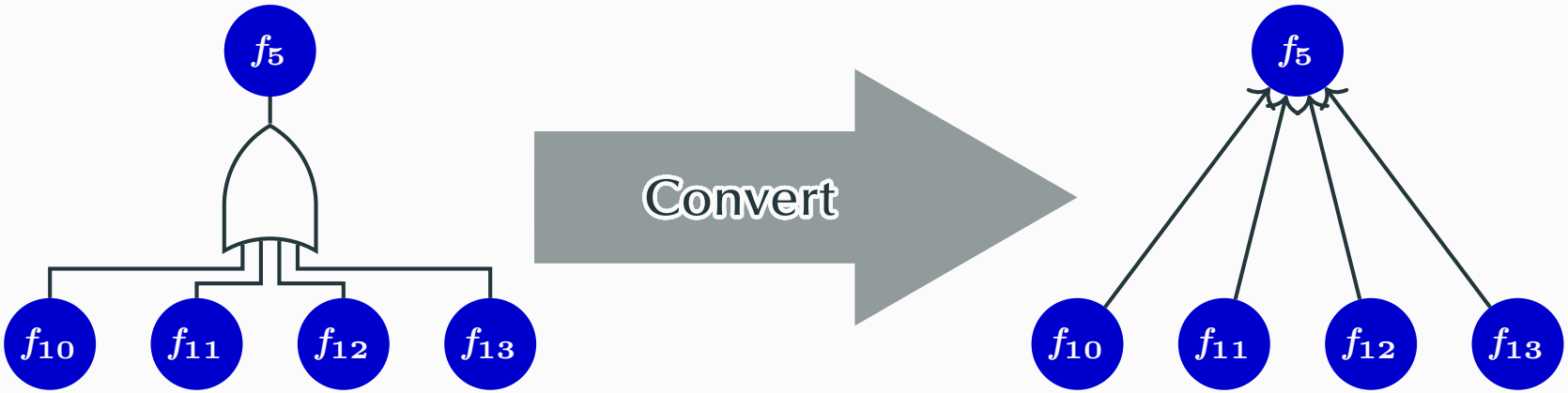
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



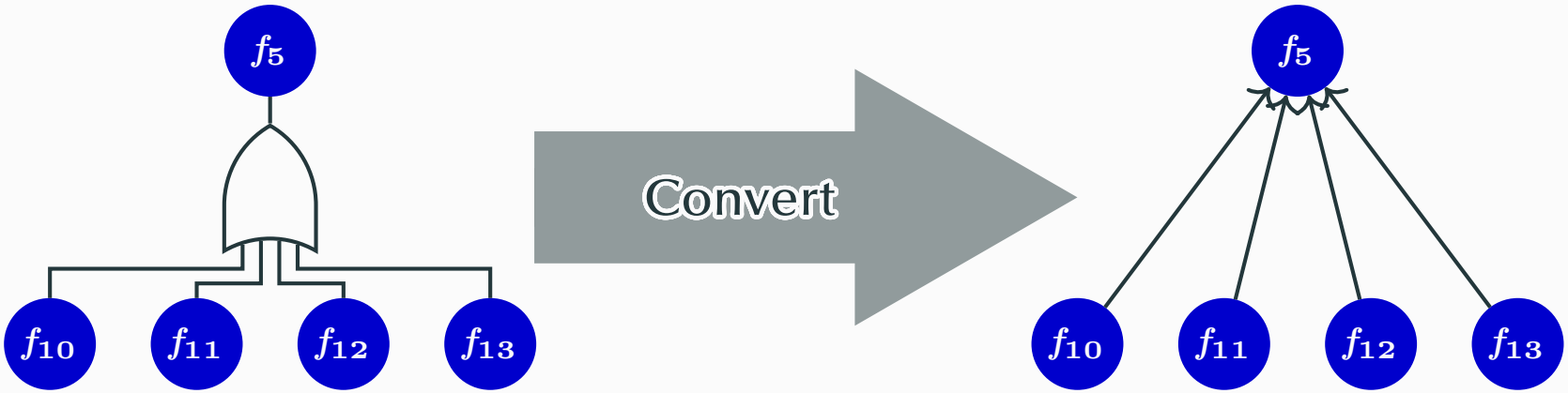
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



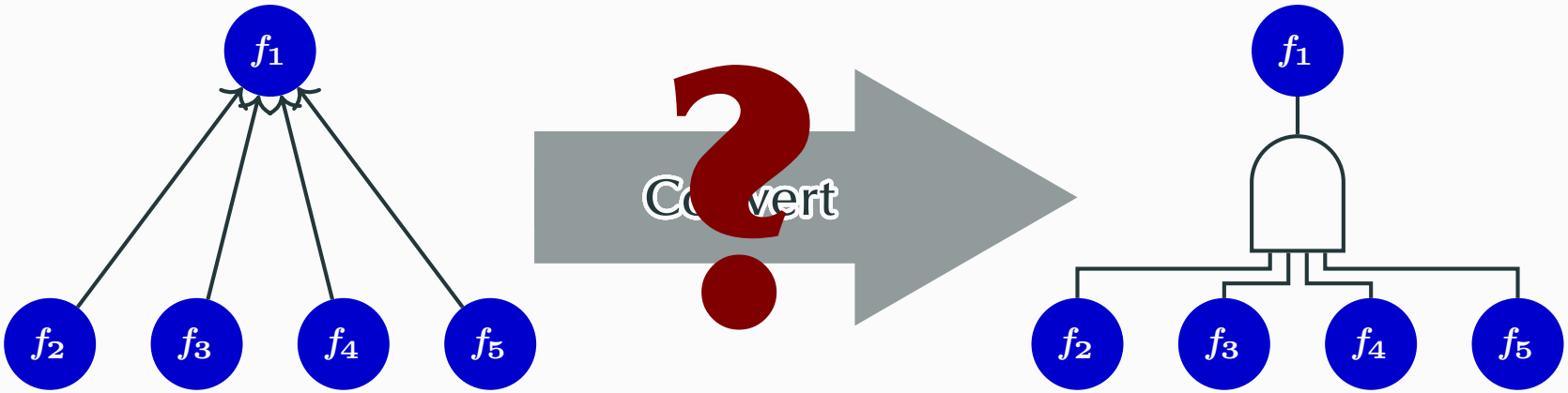
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.

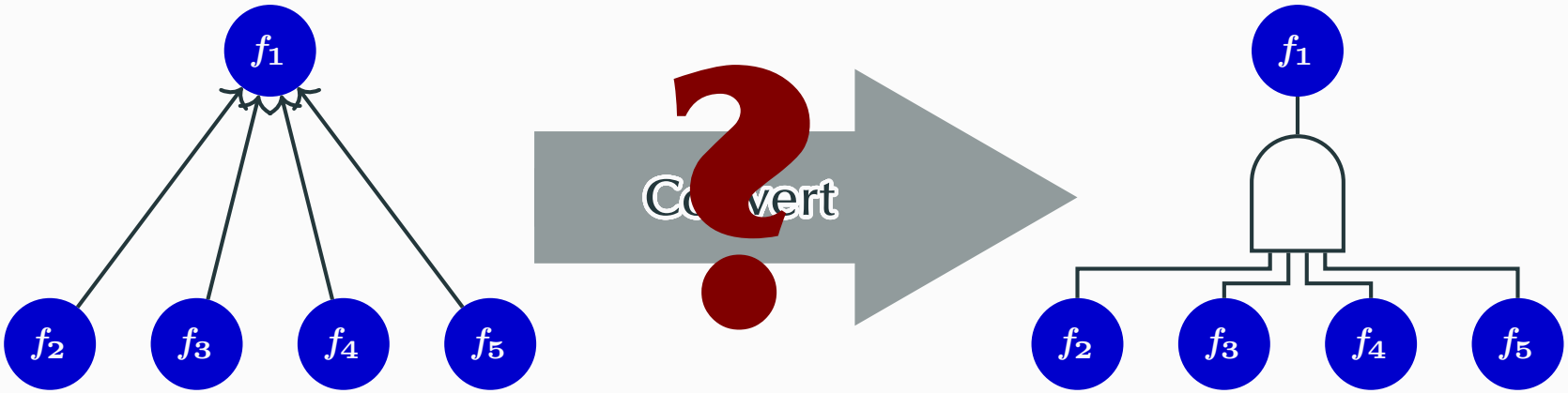


$F(f_{10})$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_{11})$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_{12})$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_{13})$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_5)$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\overline{F}(f_5)$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Function Level

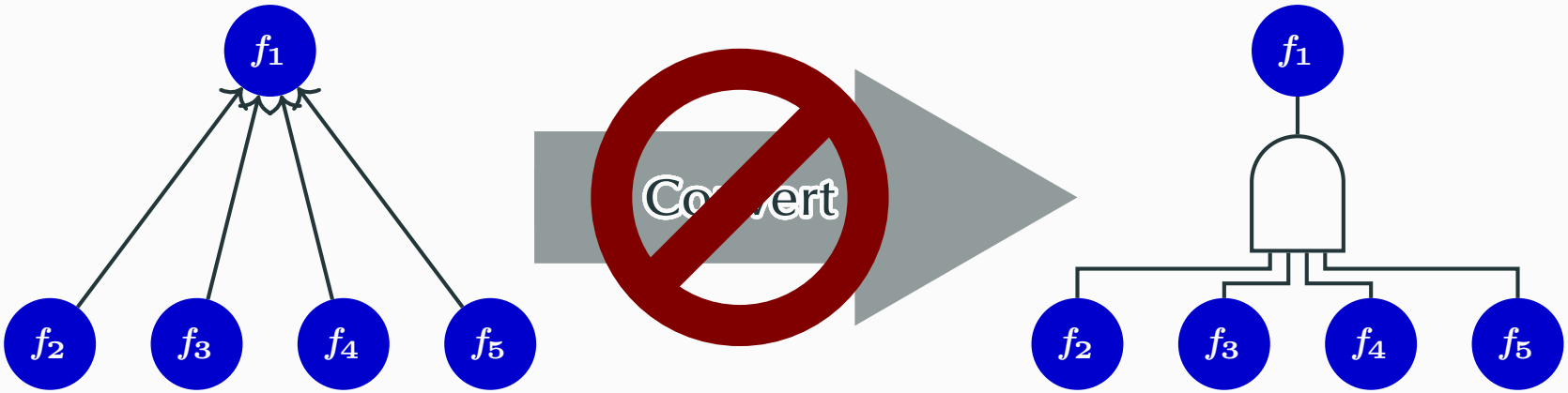


Function Level



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

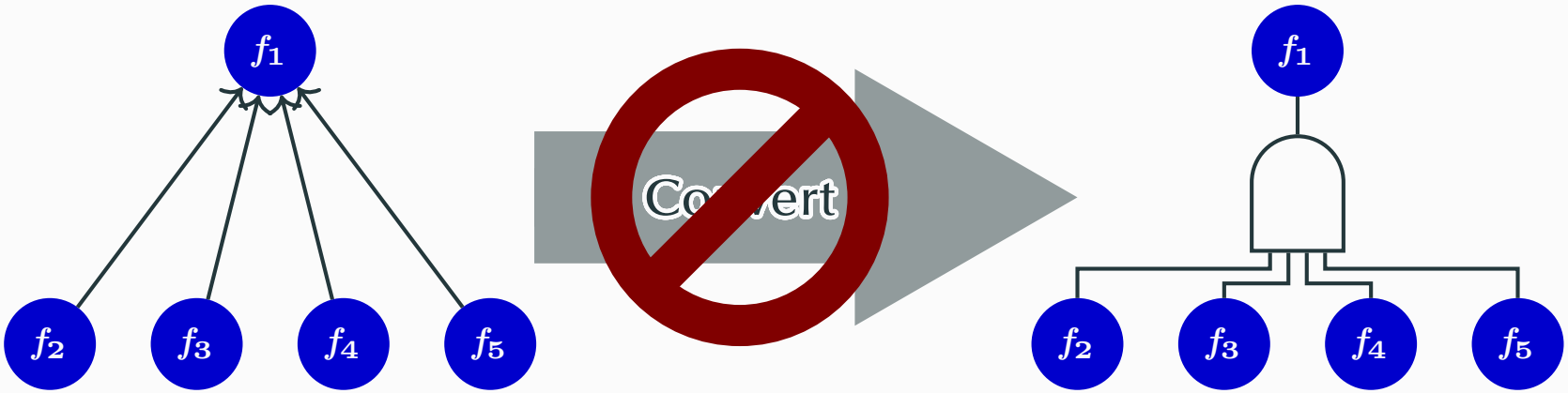
Function Level



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

Function Level

The conditional probability table of the Bayesian network contains more information than the logical gate of the fault tree.



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

Incident Level

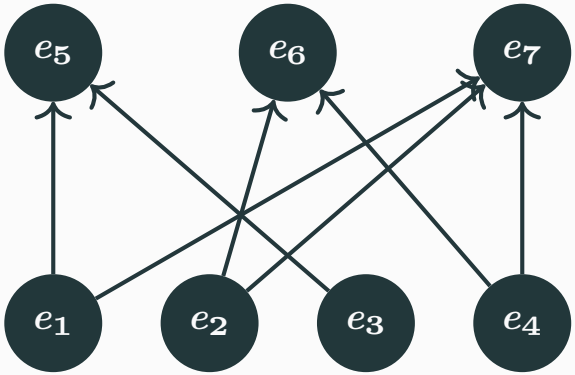
The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

A typical Bayesian network of incident is shown in following figure.

Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

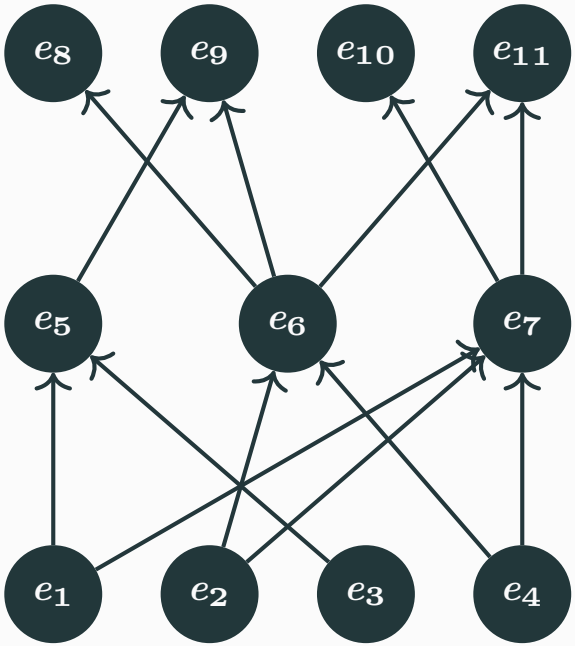
A typical Bayesian network of incident is shown in following figure.



Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

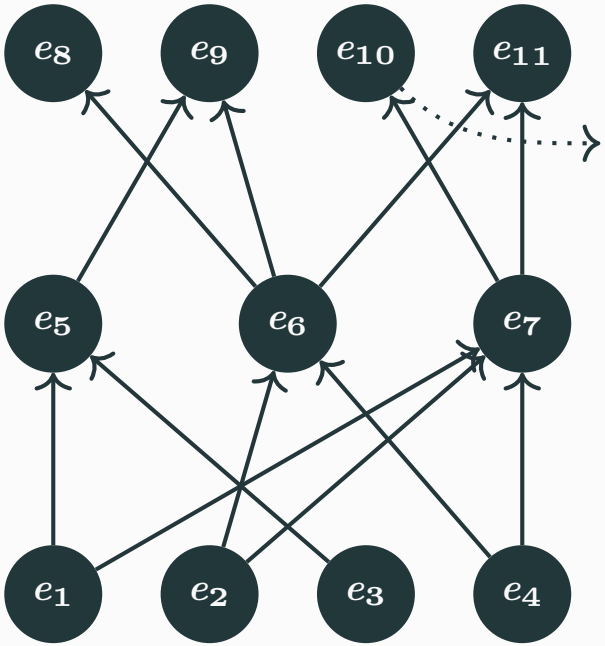
A typical Bayesian network of incident is shown in following figure.



Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

A typical Bayesian network of incident is shown in following figure.

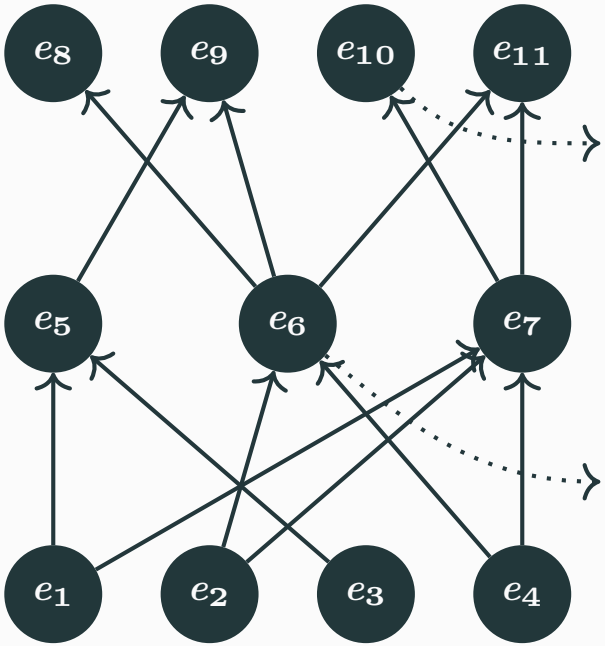


$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

A typical Bayesian network of incident is shown in following figure.



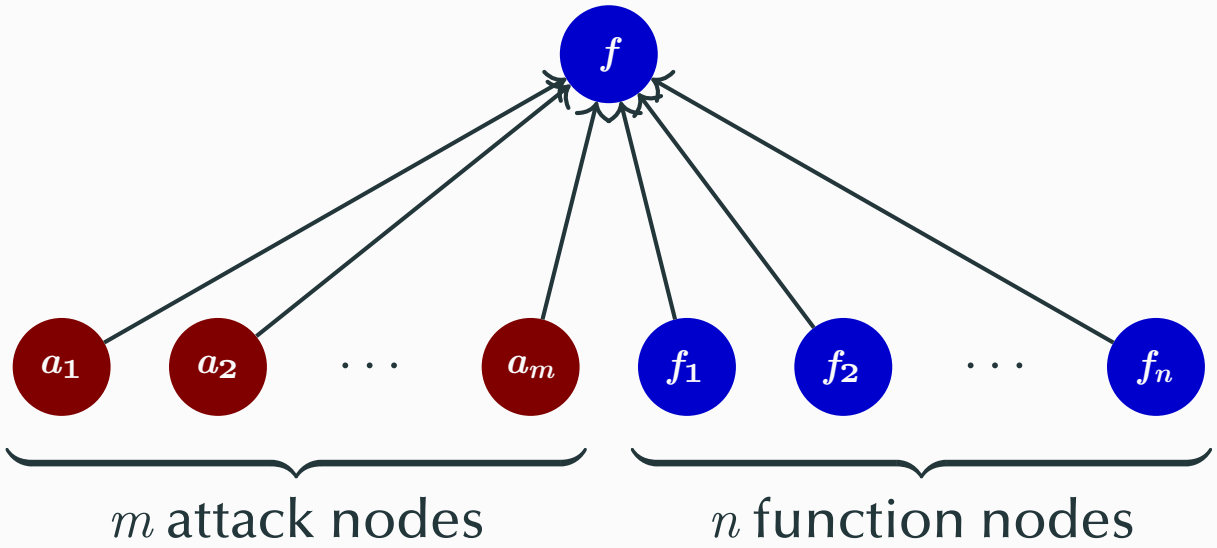
$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

$H(e_2)$	T	T	F	F
$H(e_4)$	T	F	T	F
$H(e_6)$	$h_{e_6,1}$	$h_{e_6,2}$	$h_{e_6,3}$	$h_{e_6,4}$
$\overline{H}(e_6)$	$1-h_{e_6,1}$	$1-h_{e_6,2}$	$1-h_{e_6,3}$	$1-h_{e_6,4}$

Information Transfer between Levels

The cyber attacks can lead to system function failures, and the function failures may cause the industrial incidents. To analyze the risk propagation, an information transfer is necessary between the three aforementioned layers.

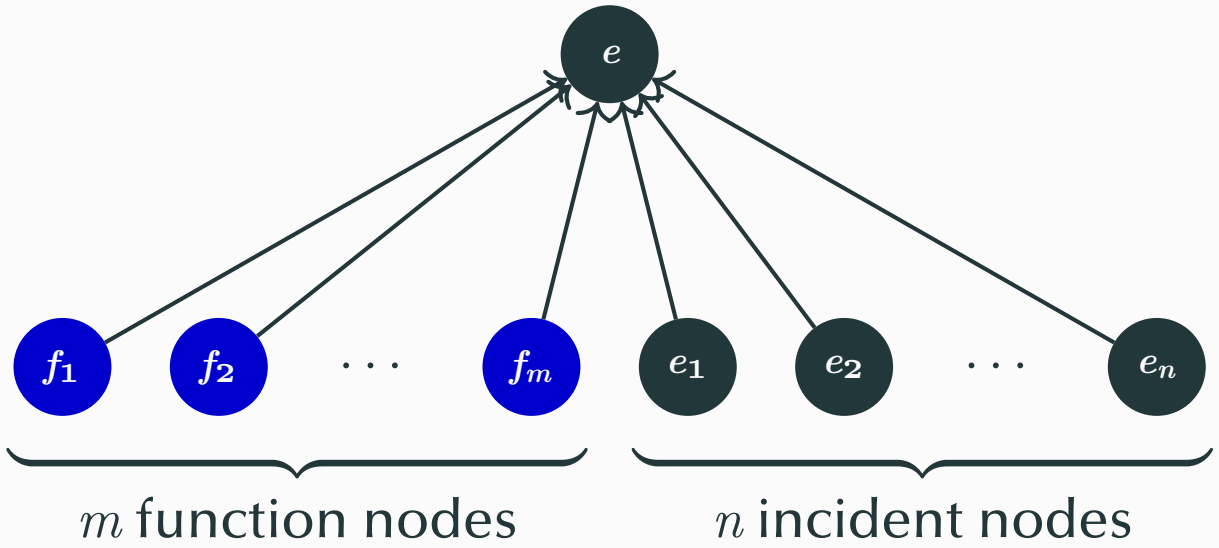
The following figures show two kind of information transfer.



Information Transfer between Levels

The cyber attacks can lead to system function failures, and the function failures may cause the industrial incidents. To analyze the risk propagation, an information transfer is necessary between the three aforementioned layers.

The following figures show two kind of information transfer.



Collection of Evidence

There are two kind of evidence need to be collected:

- **Attack Evidence**, contains the attack information, such as attack time, attack type, attack object, etc.
- **Anomaly Evidence**, contains the information about the anomaly, such as function failure, function restoration, incident occurrence, etc.

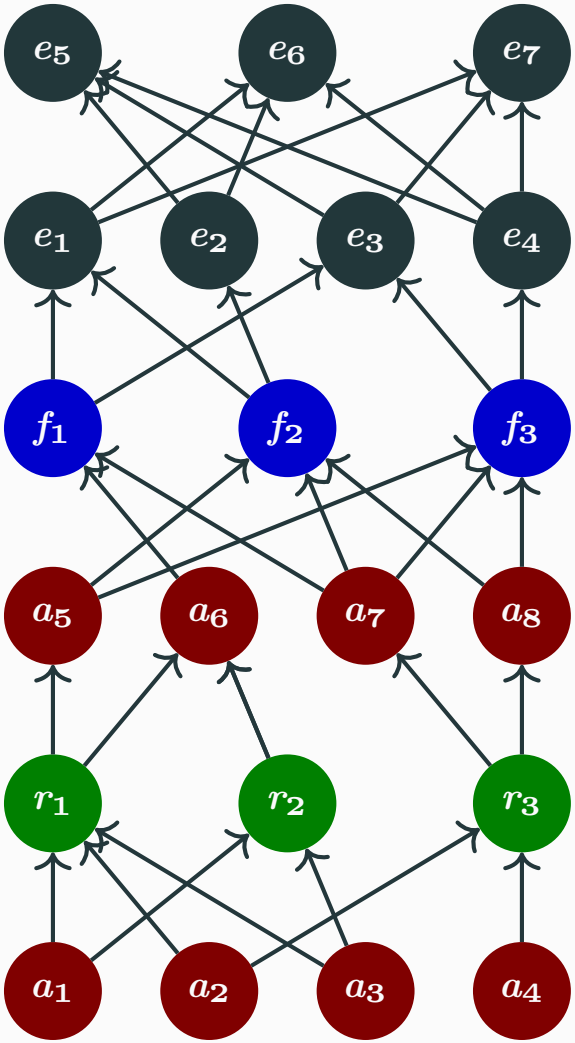
Collection of Evidence

There are two kind of evidence need to be collected:

- **Attack Evidence**, contains the attack information, such as attack time, attack type, attack object, etc.
- **Anomaly Evidence**, contains the information about the anomaly, such as function failure, function restoration, incident occurrence, etc.

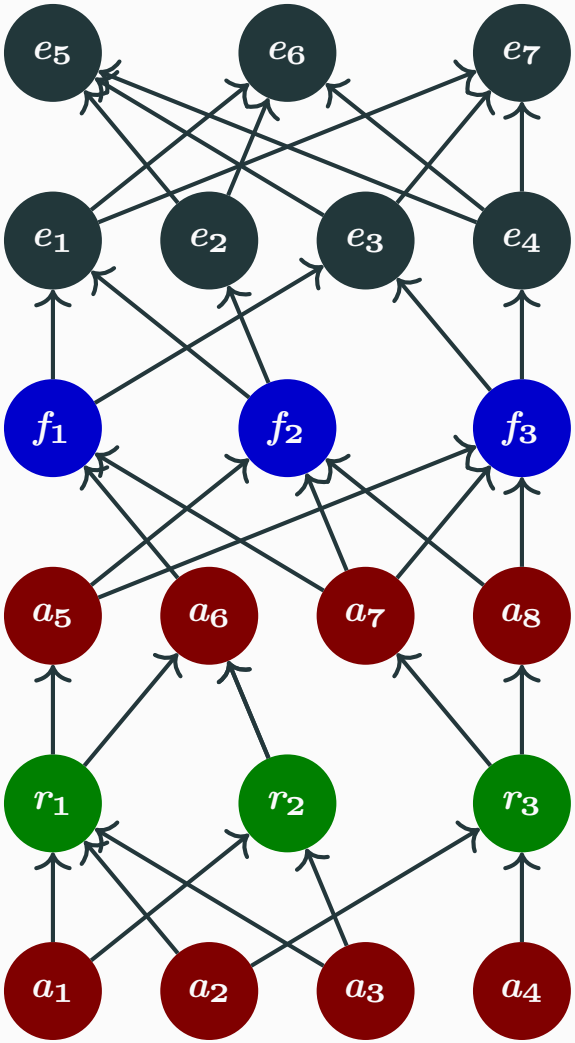
For each evidence, there exists a corresponding node in the multi-level Bayesian network. When the intrusion detection system or the monitoring system finds an evidence, the corresponding node will be marked in the multi-level Bayesian network.

Calculation of Incident Probability



The left figure shows a typical multi-level Bayesian network.

Calculation of Incident Probability

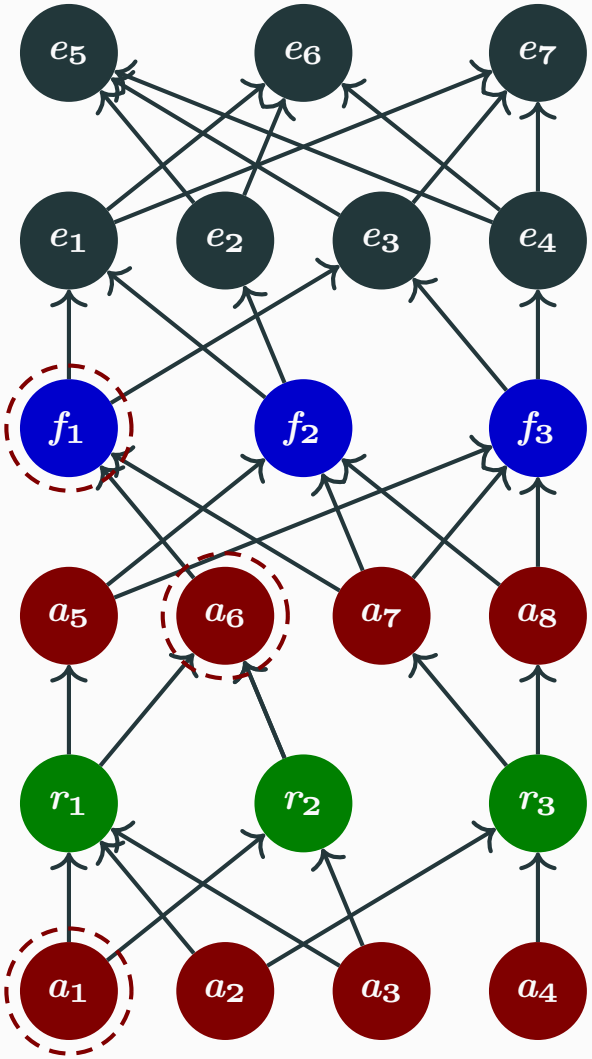


The left figure shows a typical multi-level Bayesian network.

Assuming that the evidence list is

$$a_1, a_6, f_1$$

Calculation of Incident Probability



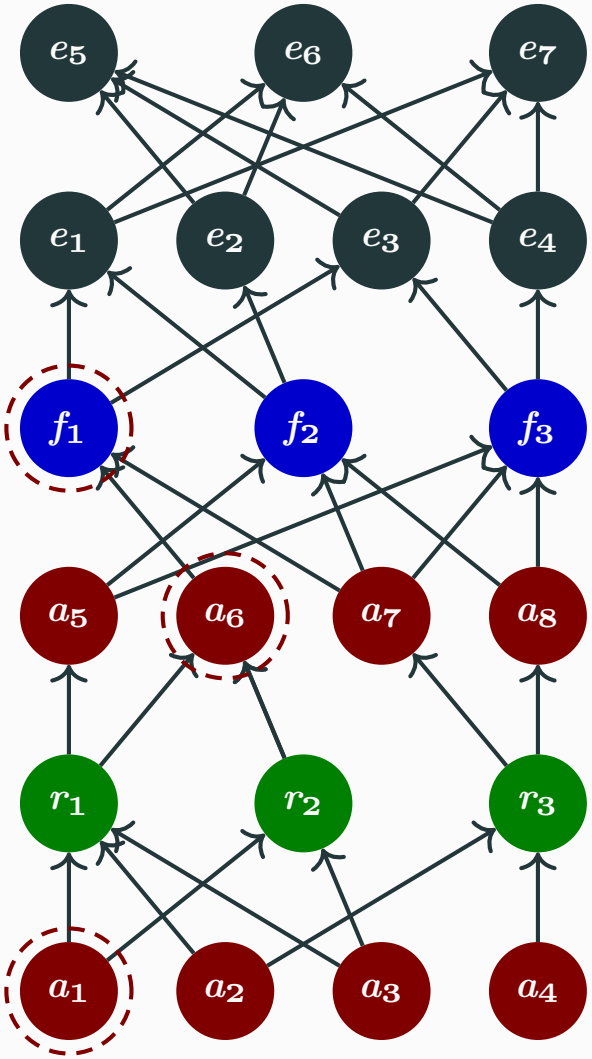
The left figure shows a typical multi-level Bayesian network.

Assuming that the evidence list is

$$a_1, a_6, f_1$$

Then the nodes a_1, a_6, and f_1 are marked with **red** dashed circles.

Calculation of Incident Probability



The left figure shows a typical multi-level Bayesian network.

Assuming that the evidence list is

$$a_1, a_6, f_1$$

Then the nodes a_1, a_6, and f_1 are marked with **red** dashed circles.

Finally, the algorithm named Probability Propagation in Trees of Clusters (PPTC) can calculate the probabilities of all the hazardous incidents.

Dynamic Risk Assessment

Decouple of Incident Consequences – Step 1

for each incident e_i, analyze its consequence and generate a consequence set

$$\boldsymbol{c}_i = (c_1, c_2, \cdots, c_n).$$

The meaning of $\boldsymbol{c}_i$ is that the occurring of the incident e_i will threaten the elements in consequence set $\boldsymbol{c}_i$.

For example, the incident e_i is an explosion of a reactor, which may cause worker casualties, air pollution, facilities damages, and products loss. The consequence set of e_i is

$$\boldsymbol{c}_i = (\text{workers}, \text{air}, \text{facilities}, \text{products}).$$

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$.

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$. So, for each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, we can find the incident set

$$\boldsymbol{e}_j = (e_{i_1}, e_{i_2}, \cdots, e_{i_n}).$$

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$. So, for each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, we can find the incident set

$$\boldsymbol{e}_j = (e_{i_1}, e_{i_2}, \cdots, e_{i_n}).$$

For each incident e_k of the incident set $\boldsymbol{e}_j$, the corresponding consequence set $\boldsymbol{c}_k$ satisfies the following condition:

$$\boldsymbol{c}'_j \subseteq \boldsymbol{c}_k.$$

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$. So, for each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, we can find the incident set

$$\boldsymbol{e}_j = (e_{i_1}, e_{i_2}, \cdots, e_{i_n}).$$

For each incident e_k of the incident set $\boldsymbol{e}_j$, the corresponding consequence set $\boldsymbol{c}_k$ satisfies the following condition:

$$\boldsymbol{c}'_j \subseteq \boldsymbol{c}_k.$$

Therefore, the parent nodes of the auxiliary node x_j are incident nodes $e_{i_1}, e_{i_2}, \cdots, e_{i_n}$.

Decouple of Incident Consequences – Step 4

For each auxiliary node x_j, generate a conditional probability table. A typical conditional probability table of auxiliary node x_j is shown as following table.

$H(e_{i_1})$	T	T	T	$\cdots$	F	F	F
$H(e_{i_2})$	T	T	T	$\cdots$	F	F	F
$H(e_{i_3})$	T	T	T	$\cdots$	F	F	F
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
$H(e_{i_{n-2}})$	T	T	T	$\cdots$	F	F	F
$H(e_{i_{n-1}})$	T	T	F	$\cdots$	T	F	F
$H(e_{i_n})$	T	F	F	$\cdots$	F	T	F
$H(x_j)$	1	1	1	$\cdots$	1	1	0
$\overline{H}(x_j)$	0	0	0	$\cdots$	0	0	1

Classification of Incident Consequences

In this paper, there are three main kinds of incident consequences to be considered:

- **Harm to Humans:**
  - temporary harm,
  - permanent disability,
  - fatality.
- **Environmental Pollution:**
  - air pollution,
  - soil contamination,
  - water pollution.
- **Property Loss:**
  - damage of materials,
  - damage of products,
  - damage of equipment.

Quantification of Incident Consequences

- **Harm to Humans Q_H:**
  If the decision-maker would like to increase the cost of an investment by Δc to reduce the probability of a fatality by Δp,

$$Q_H = \Delta c / \Delta p.$$

- **Environmental Pollution Q_E:**
  The monetary loss of environmental pollution is defined as

$$Q_E = Penalty + Compensation + HarnessCost.$$

- **Property Loss Q_P:**
  The cost of replacement is used to quantify the loss of property Q_P, such as the loss of materials, products, and equipment.

Calculation of Dynamic Risk

Due to the following two reasons:

- there is no overlapping between the consequences of any two auxiliary nodes x_i and x_j, $i \neq j$,
- the auxiliary nodes contain all the consequences of incidents,

the dynamic cybersecurity risk can be defined as

$$\mathscr{R} = \sum_{i=1}^{m'} p(x_i)\, q(x_i),$$

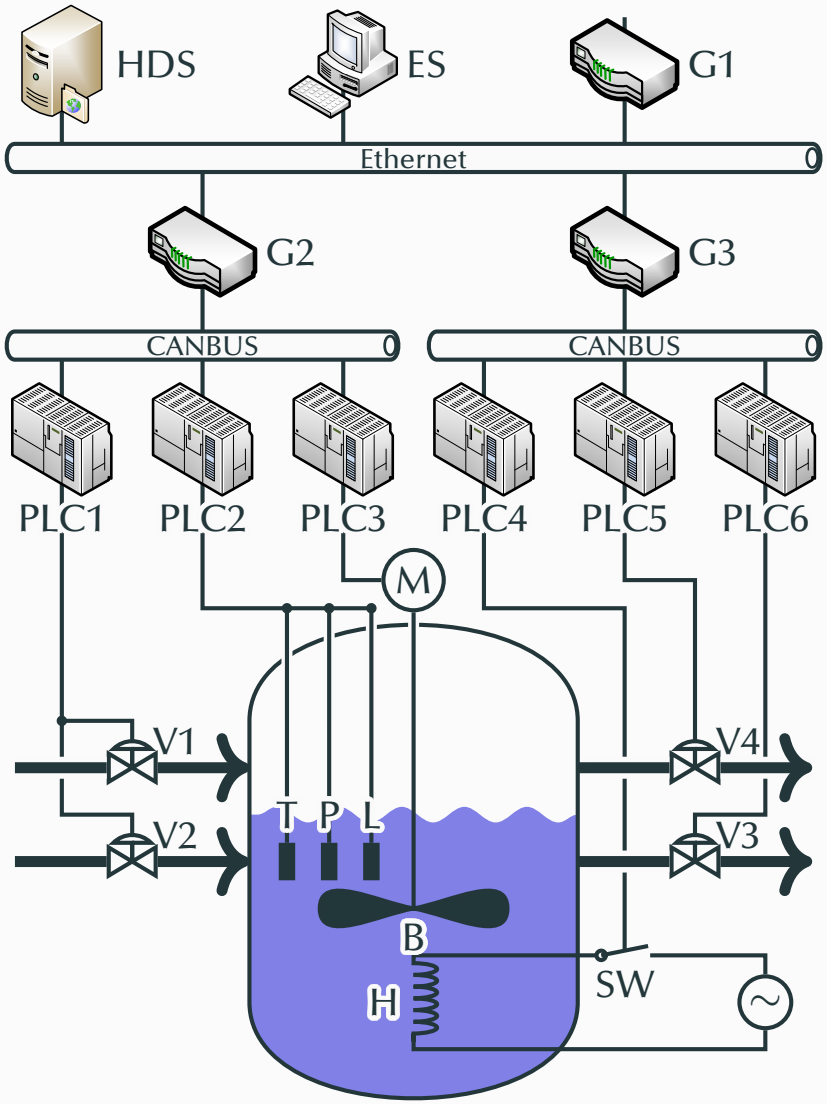
where

- $p(x_i)$ is the occurrence probability of the auxiliary node x_i,
- $q(x_i)$ is the monetary loss of the auxiliary node x_i.

Simulation

Simulation Platform

The simulation object is a chemical reactor whose control structure is shown as the following figure.

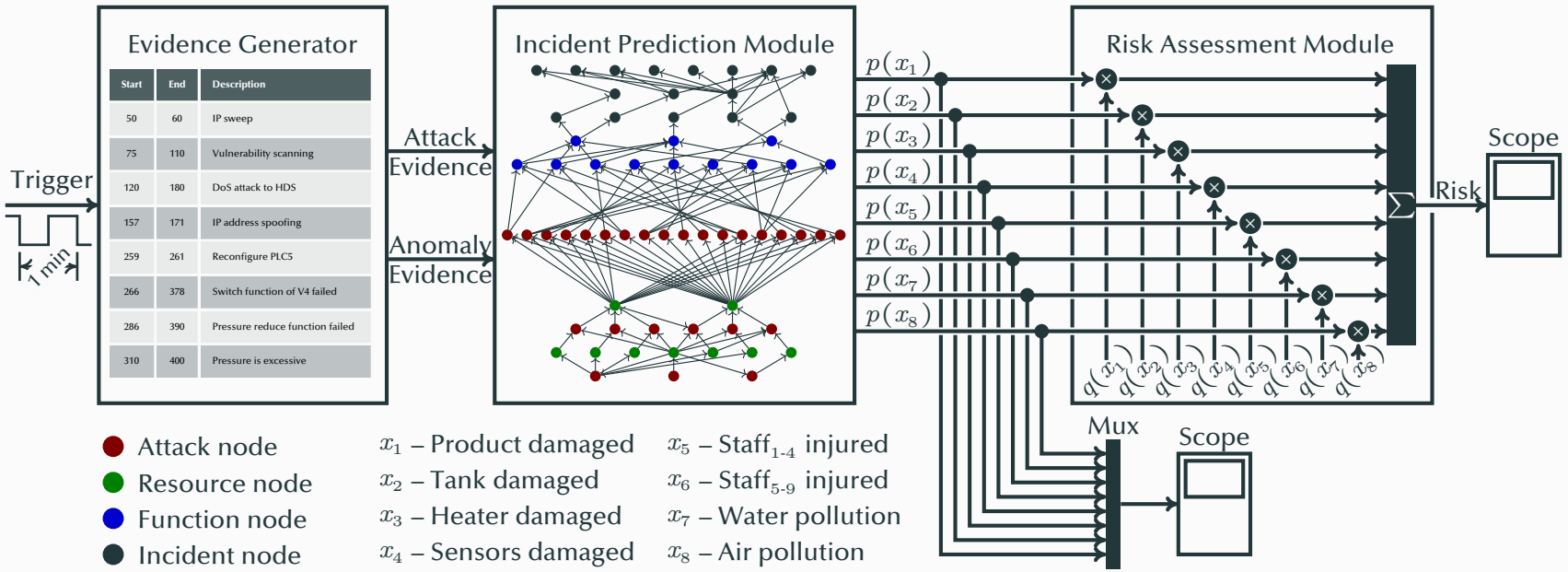


Legend

HDS	Historical data server
ES	Engineer station
G1	Gateway of Ethernet
G2	Gateway of CANBUS
G3	Gateway of CANBUS
PLC1	Controller of V1 and V2
PLC2	Data collection of P, T and L
PLC3	Controller of M
PLC4	Controller of SW
PLC5	Controller of V4
PLC6	Controller of V3
V1	Valve of material
V2	Valve of another material
V3	Valve of product
V4	Valve of pressure reducing
M	Motor of B
SW	Switch of H
P	Pressure sensor
T	Temperature sensor
L	Liquid level sensor
B	Blender
H	Heater

Simulation Platform

The simulation platform is implemented in Matlab, which consists of three modules: an evidence generator, an incident prediction module, and a risk assessment module.



Simulation and Result Analysis

Questions?