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

Zhang Qi

qiqi@hust.edu.cn

October 8, 2015

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

Outlines

Hazardous Incident Prediction

- The Bayesian Network Based Knowledge Modeling
- Incident Prediction

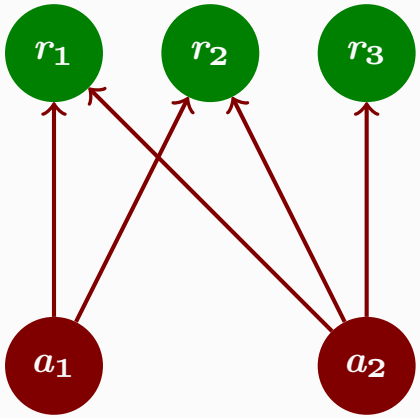
Hazardous Incident Prediction

Attack Level

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

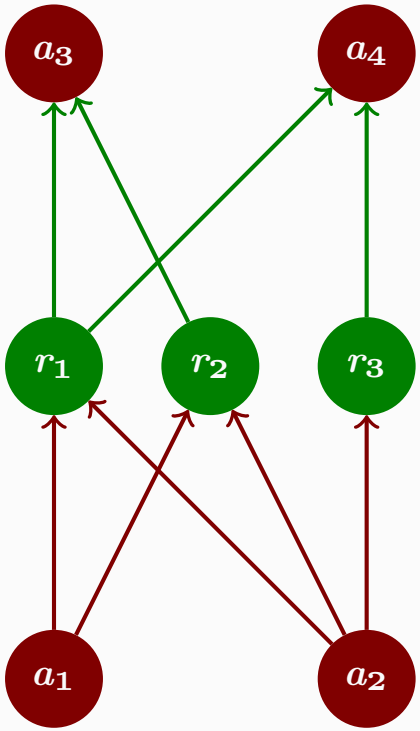
Attack Level

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



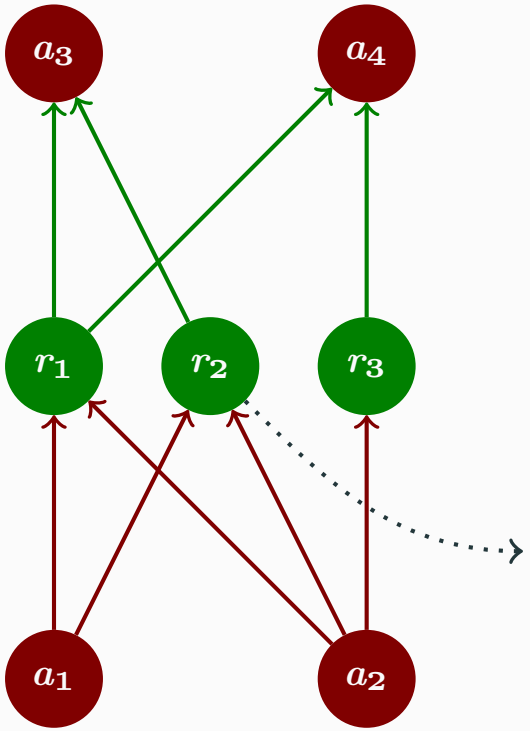
Attack Level

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



Attack Level

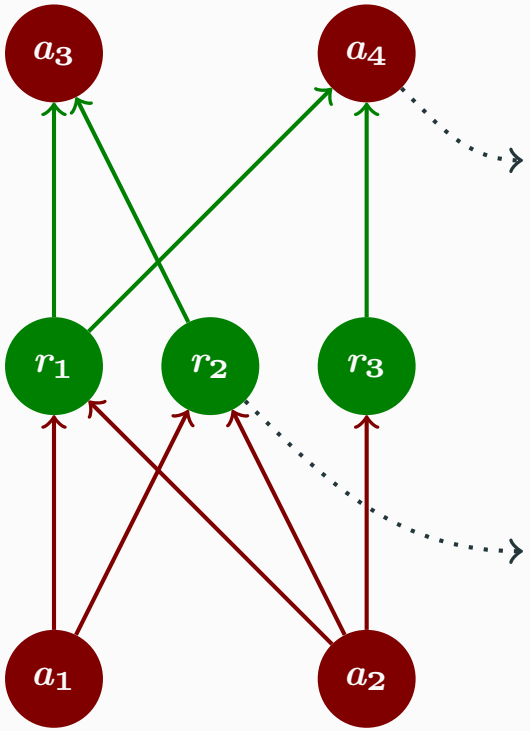
In this paper, the Bayesian network is used to model the relationship between attacks and resources.



$L(a_1)$	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.

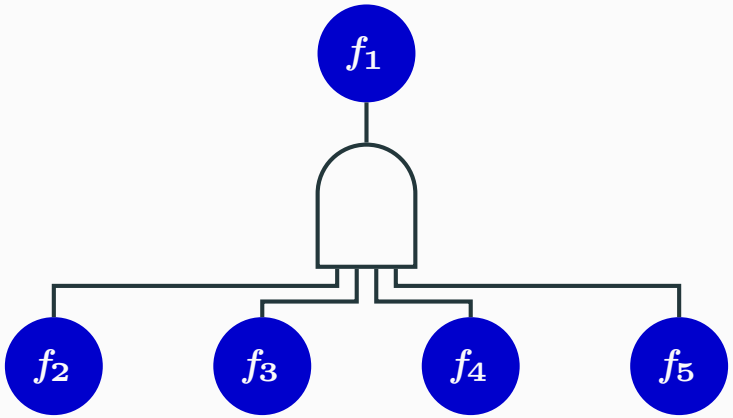
Function Level

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

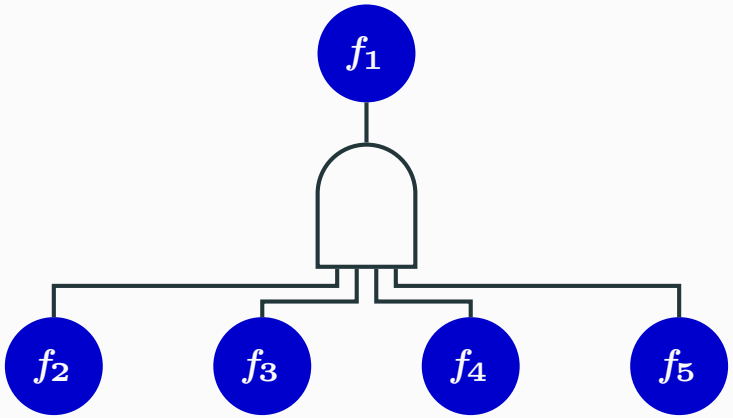
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

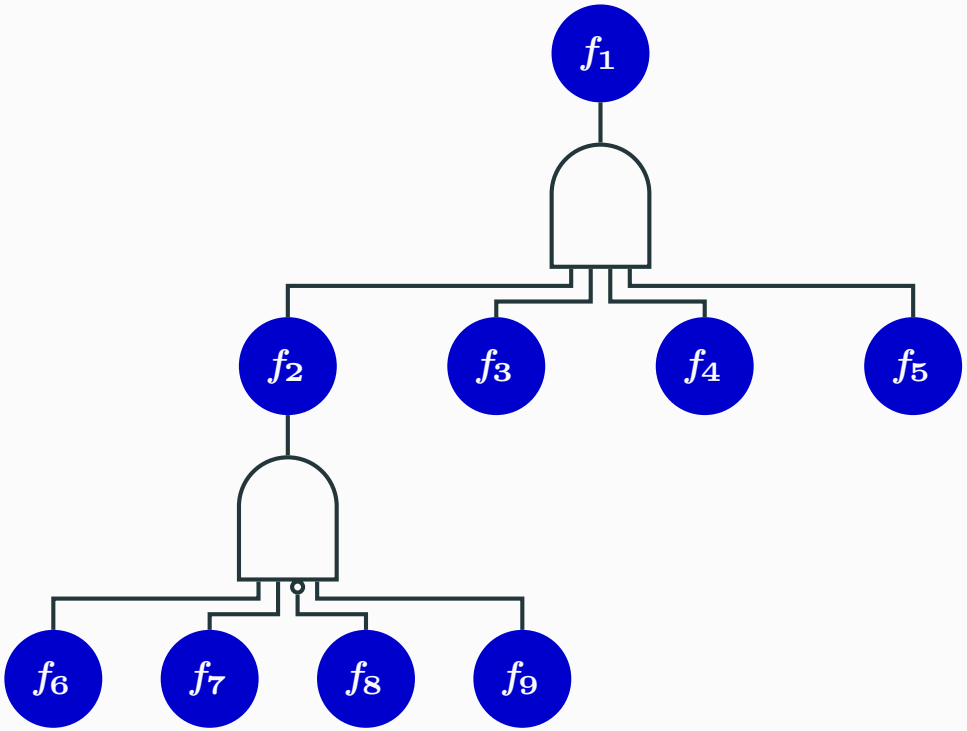
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

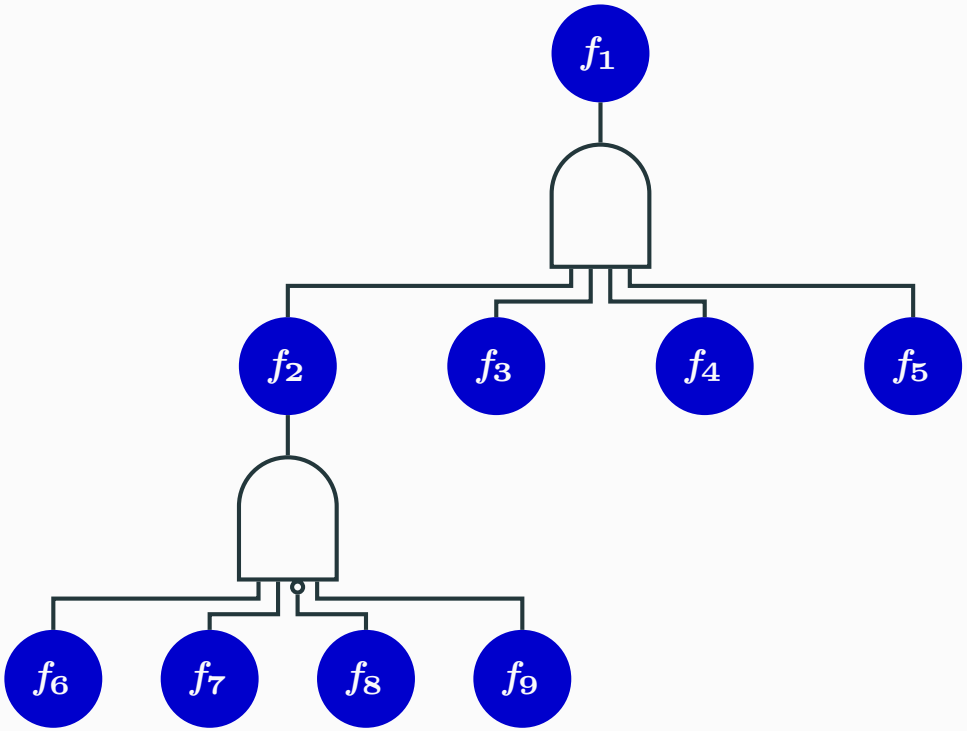
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

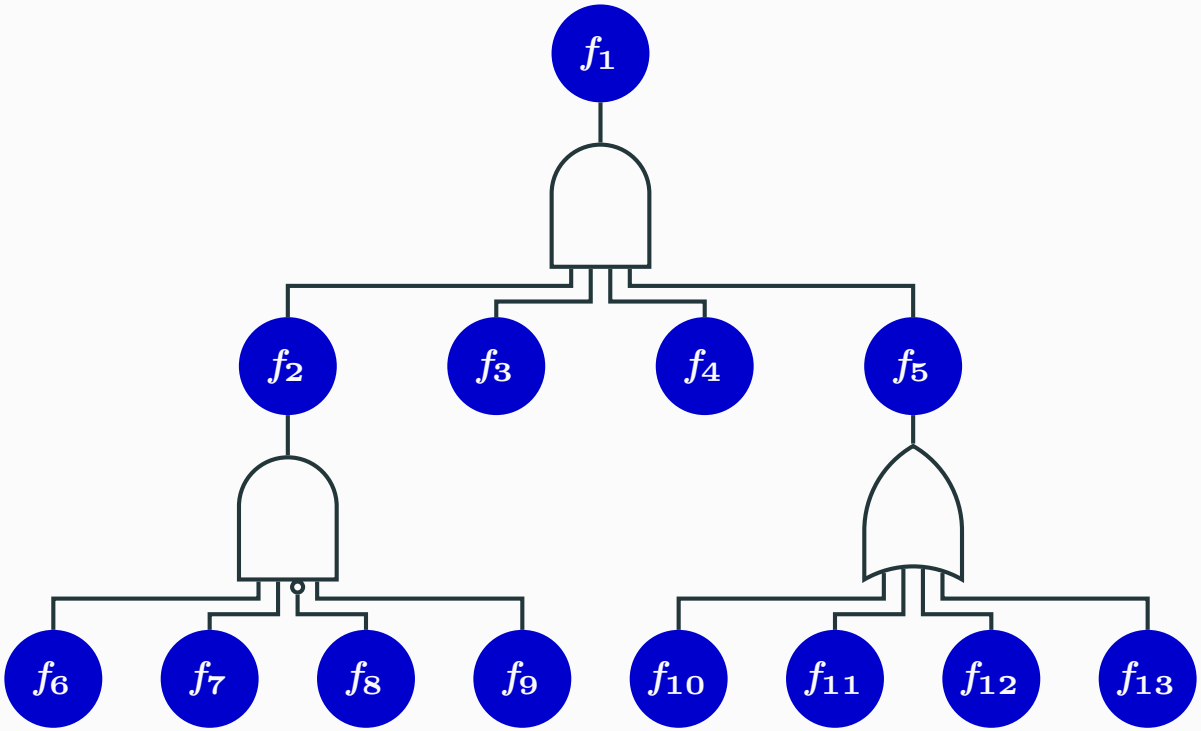
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

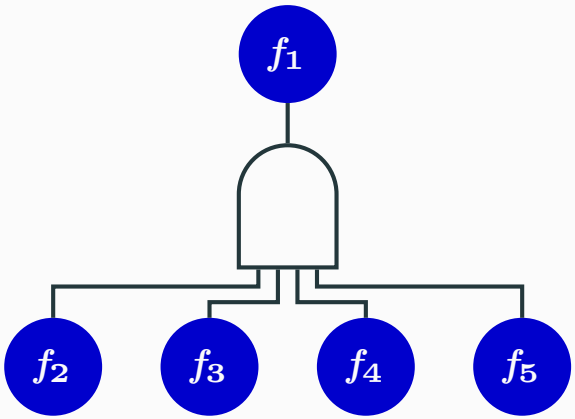
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

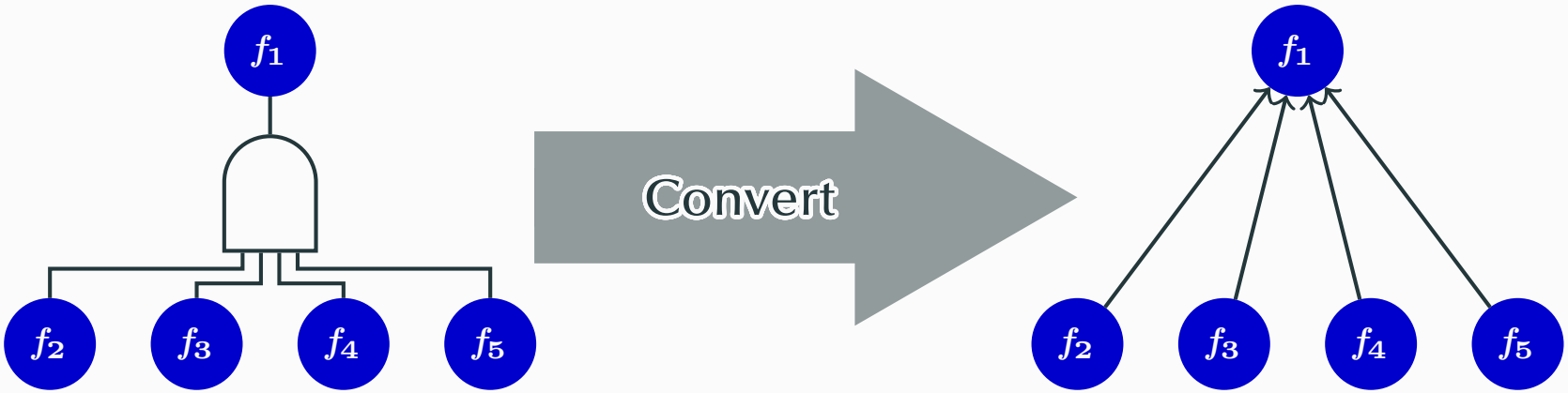
Function Level

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



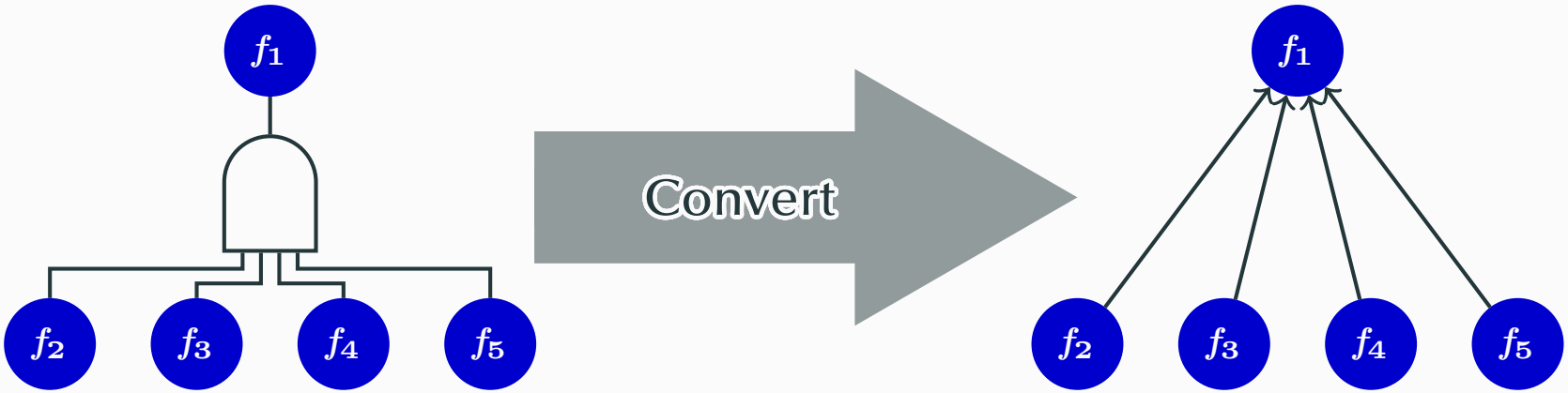
Function Level

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



Function Level

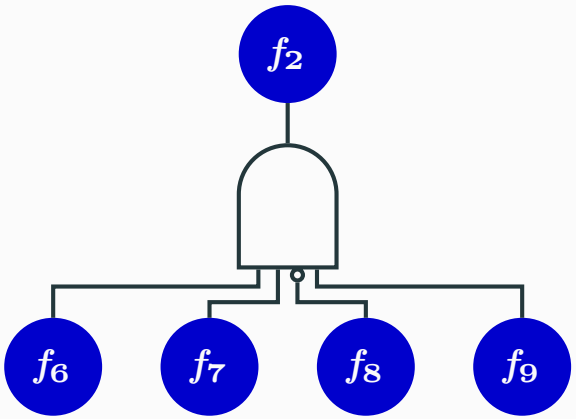
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_2)$	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

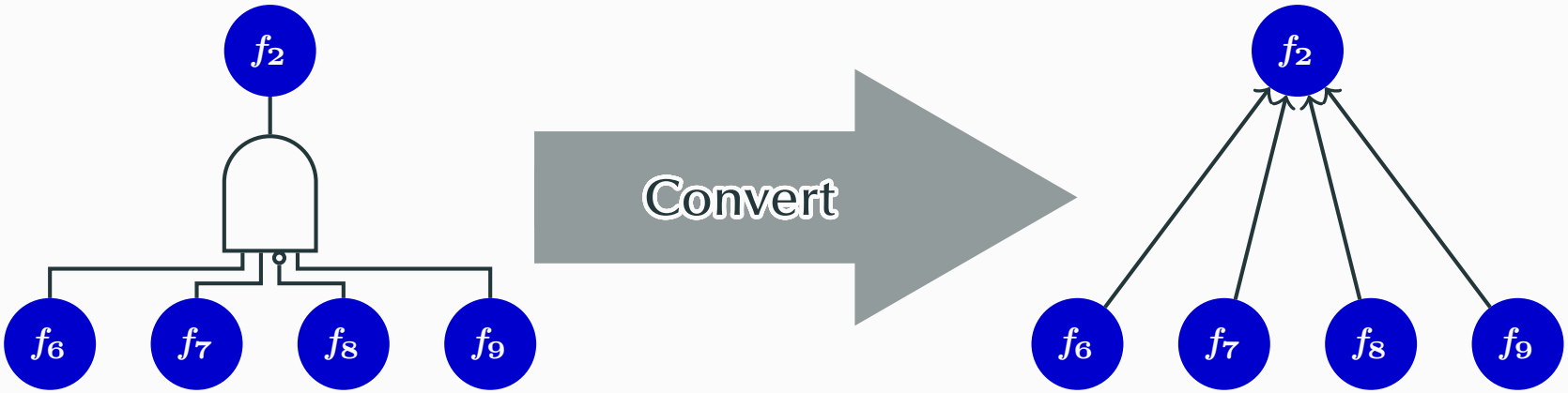
Function Level

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



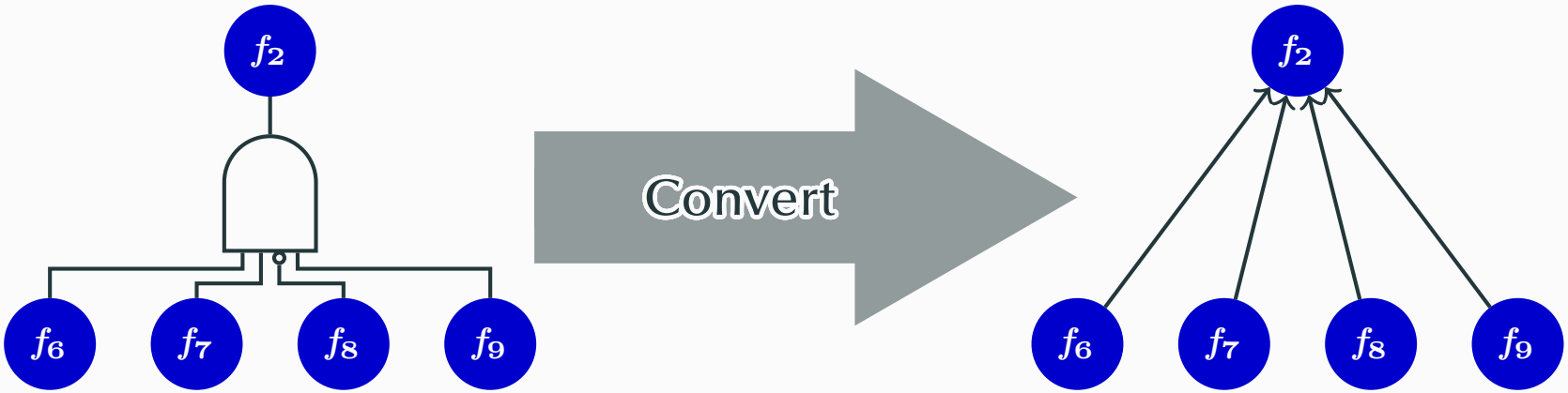
Function Level

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



Function Level

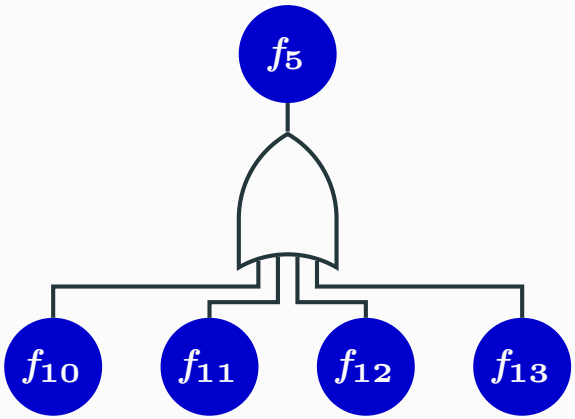
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_6)$	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

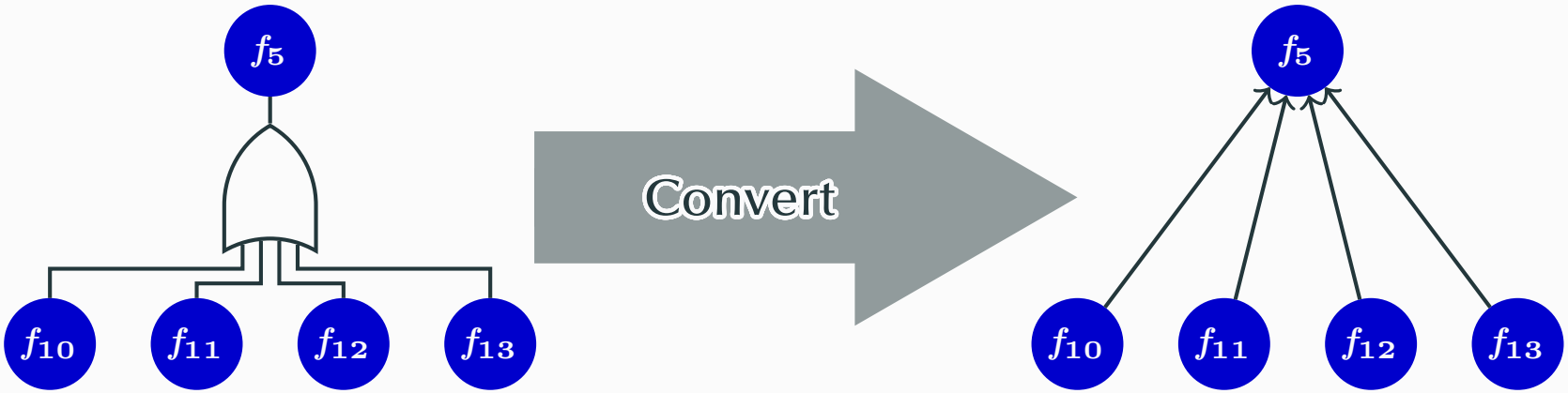
Function Level

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



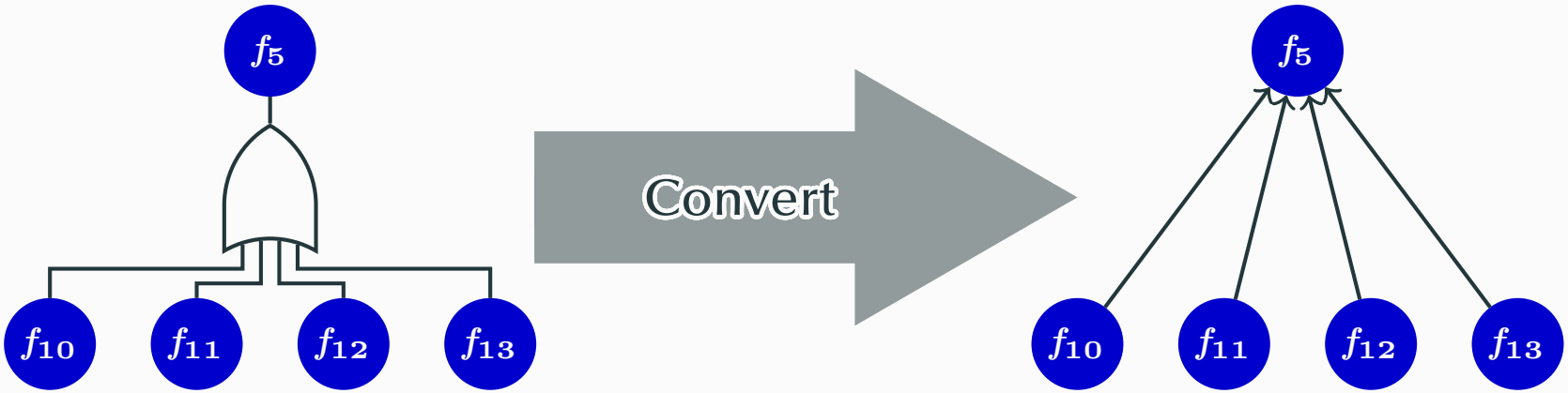
Function Level

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



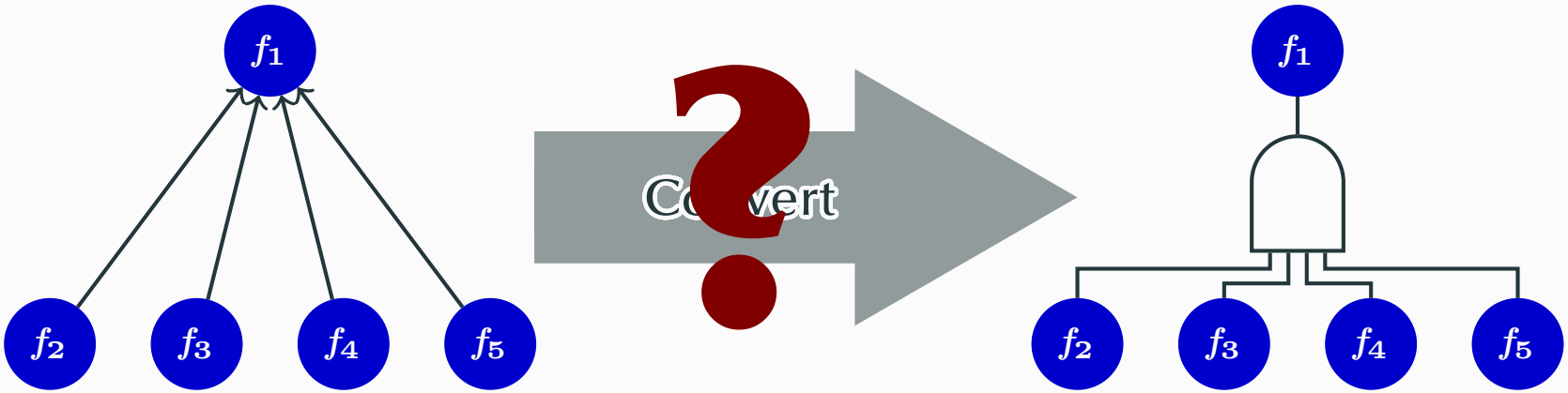
Function Level

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

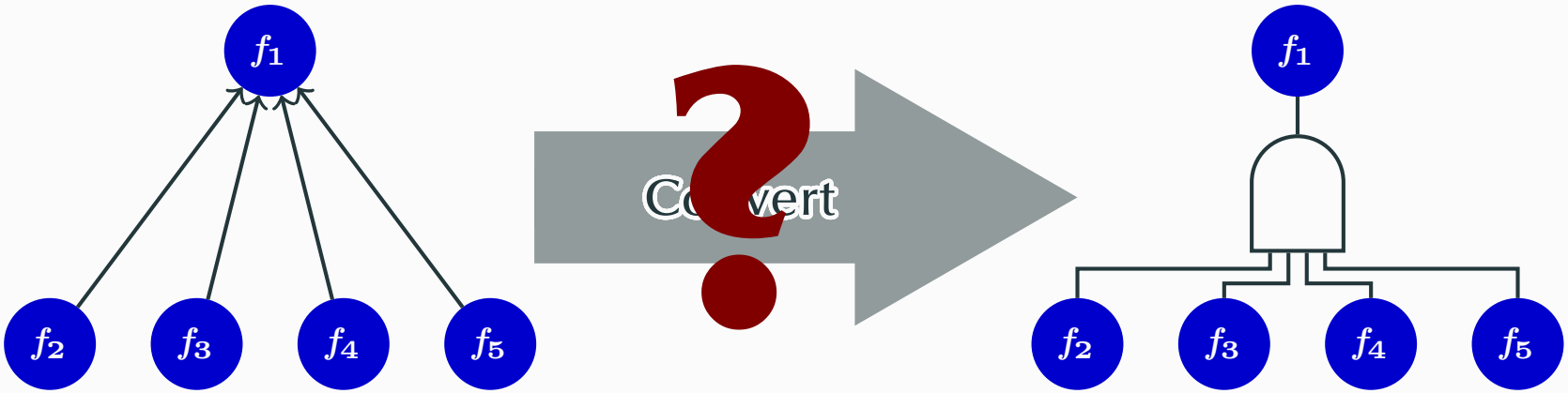


$F(f_{10})$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_{11})$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_{12})$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_{13})$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_5)$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\overline{F}(f_5)$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Function Level

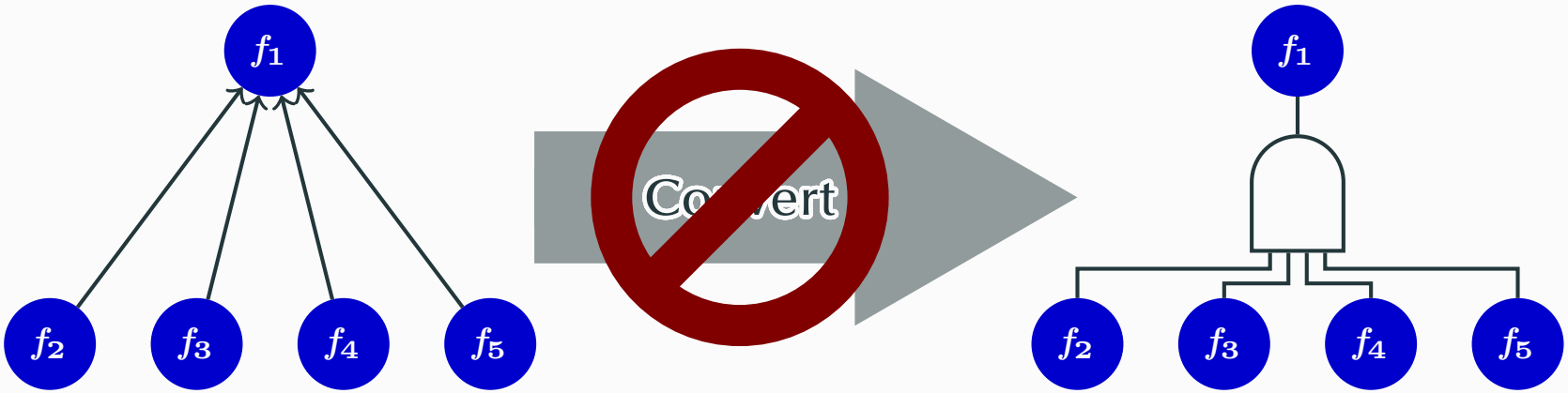


Function Level



$F(f_2)$	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**

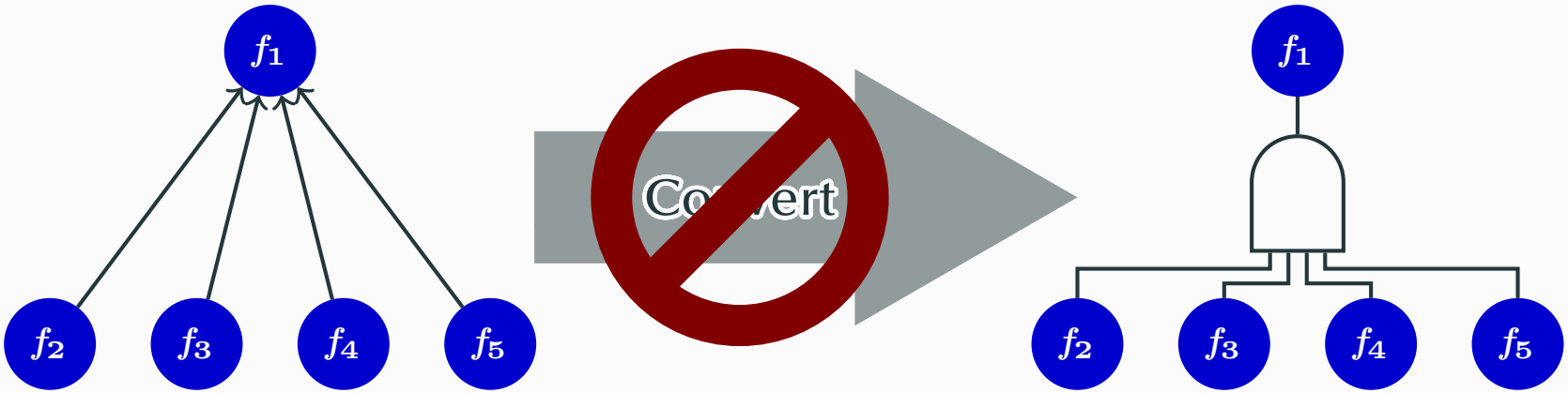
Function Level



$F(f_2)$	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

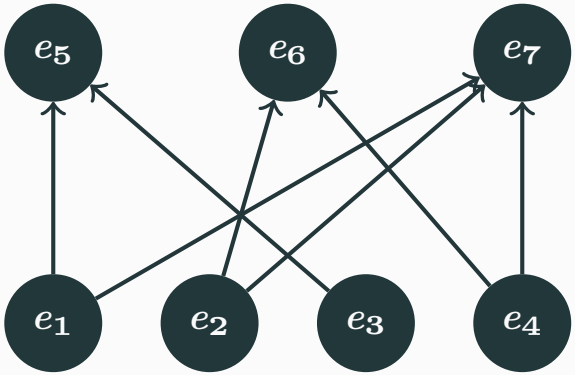
The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

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.

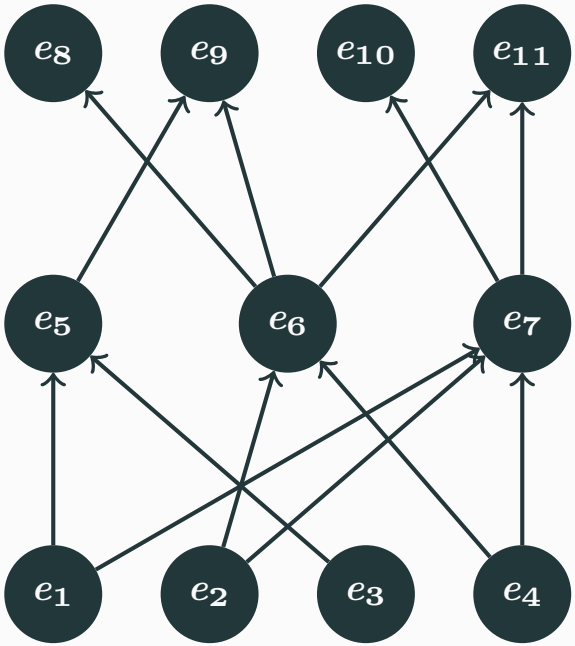
A typical Bayesian network of incident is shown in following figure.



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.

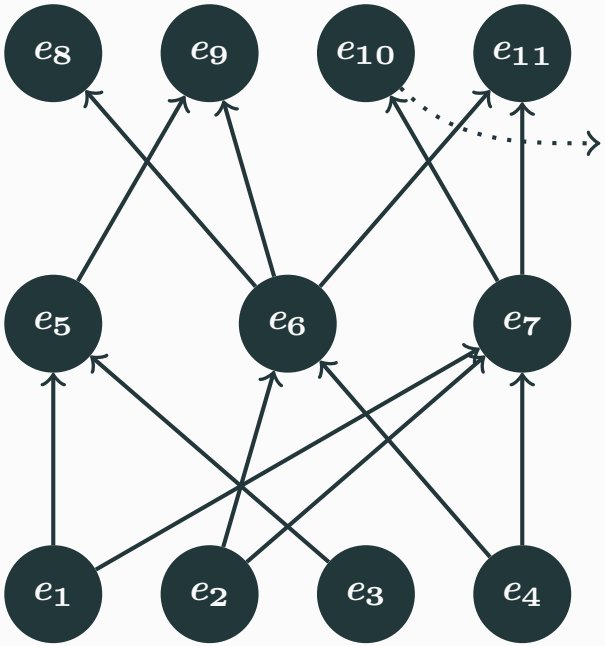
A typical Bayesian network of incident is shown in following figure.



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.

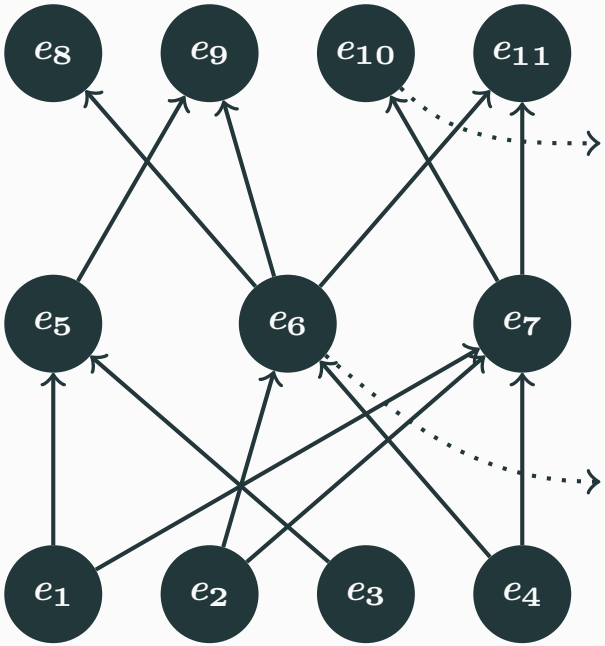


$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

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.



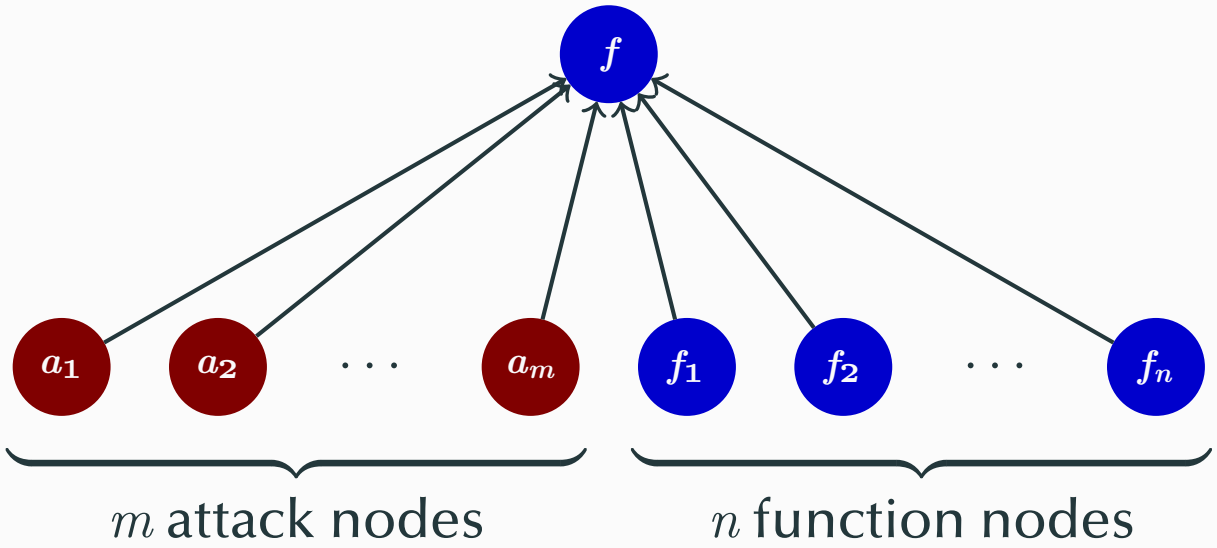
$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

$H(e_2)$	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.

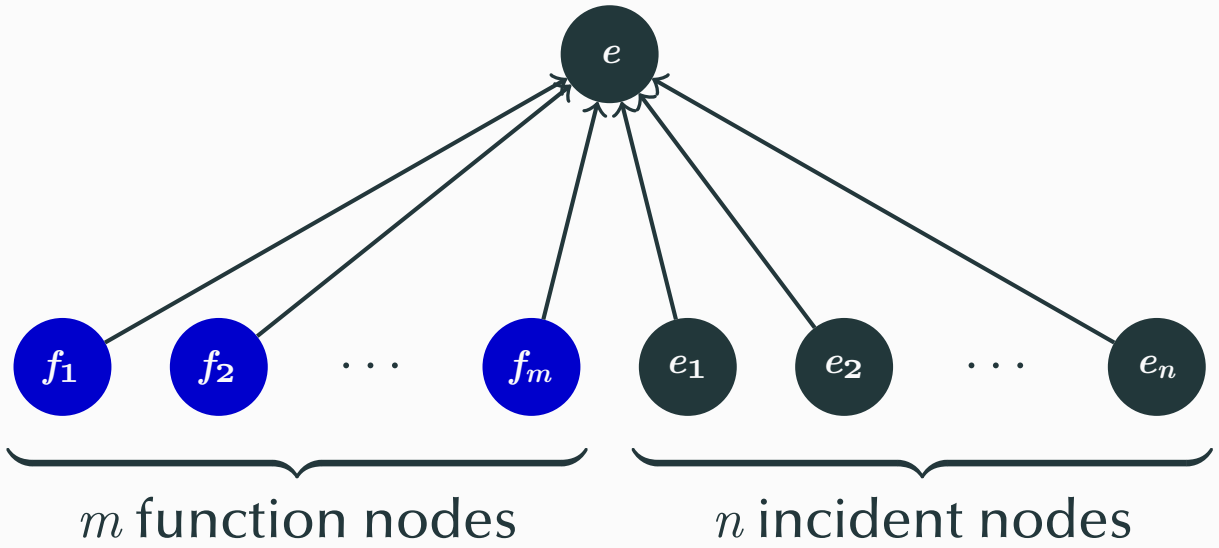
The following figures show two kind of information transfer.



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 find an evidence, the corresponding node will be marked in the multi-level Bayesian network.

Calculation of Incident Probability

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

Questions?