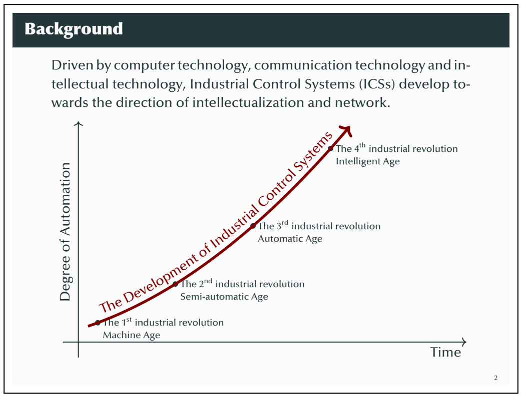
Hello everyone, my name is Zhang Qi, and I am the Ph.D student of Professor Zhou Chunjie. I am very glad to be invited by Professor Yang Shuanghuang to make a presentation about my recent research.

My research interests are related to risk assessment and decision-making for industrial control systems. The title of my presentation is "Multi-Model Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems".

My presentation is separated into six parts:

- Firstly, I will introduce the background and the problems of risk assessment for industrial control systems.
- Secondly, I will give the architecture of our risk assessment solution for industrial control systems.
- Thirdly, I will elaborate the detail of our method.
- Then, I will show you the effectiveness of our approach by using a numerical simulation.
- At last, I will discuss the problems of our approach and introduce the future works.

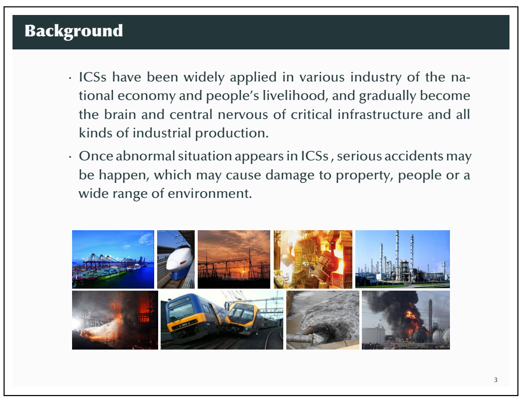
In this part, I will introduce the development history and the cybersecurity issues of industrial control systems. And, I will compare the cybersecurity issues of industrial control systems and traditional IT systems.



There are four great changes in the development of industrial control systems:

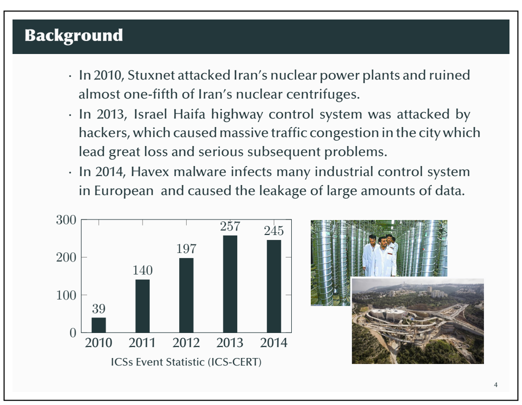
- Machine Age
- Semi-automatic Age
- Automatic Age
- Intelligent Age

From this figure, we can see that with the development of industrial control systems, the degree of automation is increasing. Intelligence and networking are the development trend of industrial control systems.



Nowadays, the industrial control systems have been widely applied in various industry, and they are becoming more and more important for the national economy and our life.

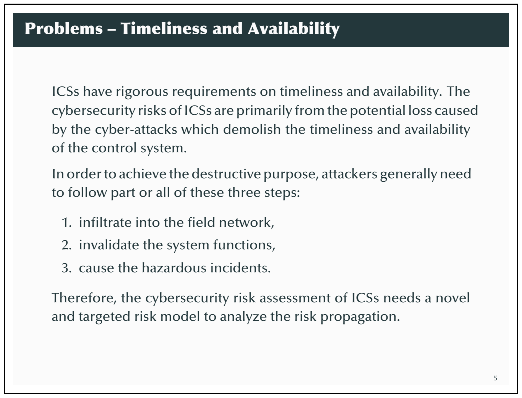
As mentioned before, the industrial control systems are evolving towards intelligence and networking. The rapid development of the industrial control systems reduce the difficulty of the development and the cost of construction, on the other hand, it has also introduced the cybersecurity issues into the industrial control systems.



For example, in 2010, the 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.

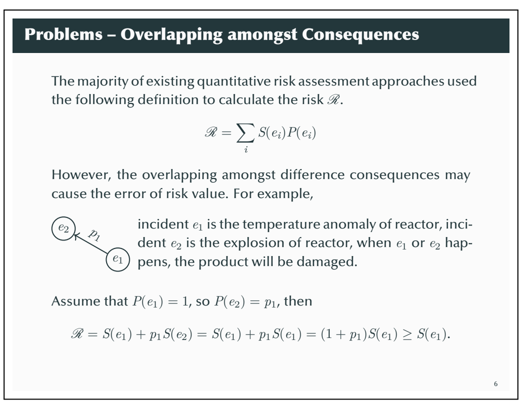
According to the statistical data from "Year in Review 2014" published by the ICS-CERT which is short for "Industrial Control Systems Cyber Emergency Response Team", the number of attacks for industrial control systems increases year by year. In 2010, there were only 39 security incidents of industrial control systems, but in 2014, this number has grown to 245.

Unlike traditional IT systems, the security incidents of industrial control systems can cause irreparable harm to the physical systems being controlled and to the people dependent on them. Basically, protecting industrial control systems against cyber-attacks is vital to both the economy and stability of a nation. Therefore, the cybersecurity issue of industrial control systems must be taken seriously and solved as soon as possible.



In recent years, considerable researches have been undertaken to study cybersecurity risk assessment methods. However, the cybersecurity risk assessment in the IT domain is not entirely applicable to industrial control systems because industrial control systems are relatively different from traditional IT systems in some aspects.

Firstly, the cybersecurity objectives are different. Traditional IT systems first require an ensuring of confidentiality, then integrity, and finally availability. For industrial control systems, in contrast, the priorities of these three security objectives are first availability, then integrity, and finally confidentiality, because the timeliness and availability are the primary concerns. The malicious attacks induce the cybersecurity risk to industrial control systems by demolishing the timeliness and availability. Therefore, the risk assessment of industrial control systems needs a novel risk propagation analysis approach.



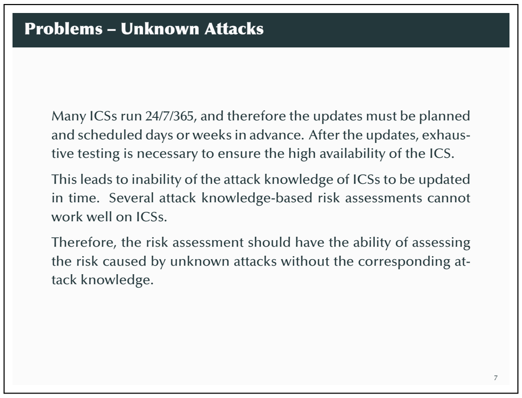
The majority of existing quantitative risk assessment approaches used this definition to calculate the risk, where $S(e_i)$ is the severity of the incident e_i and $P(e_i)$ is the probability of the incident e_i.

It is also worth noting that there is a problem when this definition is used in industrial control systems risk assessment. This is due to the fact that, for industrial control systems, different hazardous incidents may cause the same consequence; whereby, using this definition to assess risk will cause the severity of the same consequence to be accumulated multiple times. As a result, there is an error in the risk assessment, which cannot be ignored. Even worse, the decision-making may generate a wrong policy with this inaccurate 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

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

It is obviously wrong, because the risk of system can't be larger than the total value of all assets.

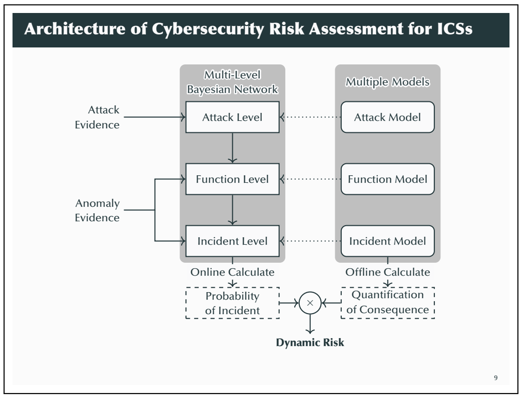


As continuous operation systems, the industrial control systems cannot tolerate frequent software patching or updates. This causes the database of attack signatures to lag far behind the rapid development of attacks. With this defect, several intrusion detection system based misuse detections would miss the unknown attacks.

On the other hand, without the information about unknown attacks, such as purposes, consequences, and further steps, these unknown attacks and their consequences cannot be predicted accurately. As a result, the risk assessment module will generate erroneous risk value, which may lead to a wrong decision.

Based on the above analysis, the requirements of cybersecurity risk assessment for industrial control systems can be summarized. The risk assessment of industrial control systems needs:

- a novel and targeted risk model to analyze the risk propagation,
- a unified quantification approach to calculate the risk quantitatively without the error caused by overlapping amongst consequences,
- the ability of assessing the risk caused by unknown attacks without the corresponding attack knowledge.

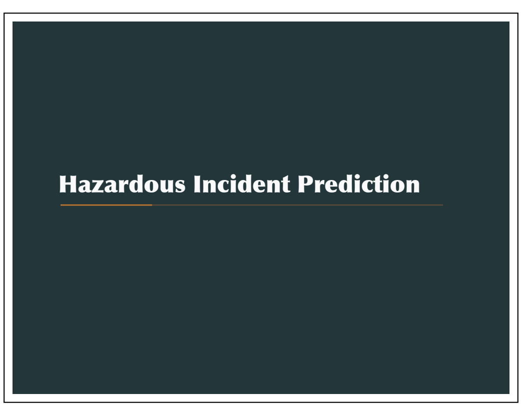


To meet the requirement of the risk assessment for industrial control systems, a dynamic cybersecurity risk assessment based on the multi-model is proposed.

To analyze the propagation of cybersecurity risk, the attack model, the function model, and the incident model are considered. Then, these three models are converted into a multi-level Bayesian network. This Bayesian network has three levels: the attack level, the function level, and the incident level.

There are two kinds of inputs for the dynamic cybersecurity risk assessment: attack evidence and anomaly evidence. Attack evidence, which contains information about the type, target, and timestamp of the detected attack, is derived from intrusion detection system. Anomaly evidence, containing the information of the anomaly, such as the invalidation of a function, the occurrence of a hazardous incident, etc., can be obtained from the supervisor system of industrial control systems.

The dynamic cybersecurity risk assessment is divided into two phases: the hazardous incident prediction and the risk assessment. During the hazardous incident prediction phase, attack evidence and anomaly evidence are collected and marked in the multi-level Bayesian network. Then, probabilities of all the potential hazardous incidents can be calculated by analyzing the collected evidences and the multi-level Bayesian network. During the risk assessment phase, the consequences of the hazardous incidents are first classified, and then each type of consequence is quantified in the same unit. Secondly, the overlapping amongst hazardous incidents must be addressed, so the error caused by multiple accumulation of consequences can be eliminated. Finally, the probabilities and consequences of the hazardous incidents are combined into the cybersecurity risk.

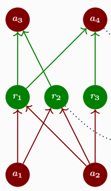


Next, I will elaborate the proposed approach of risk assessment for industrial control systems from two parts:

- hazardous incident prediction
- dynamic risk assessment

Attack Level

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



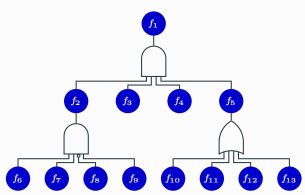
$O(r_1)$	T	T	F	F
$O(r_3)$	T	F	T	F
$L(a_4)$	$\ell_{a_4,1}$	$\ell_{a_4,2}$	$\ell_{a_4,3}$	$\ell_{a_4,4}$
$\overline{L}(a_4)$	$1-\ell_{a_4,1}$	$1-\ell_{a_4,2}$	$1-\ell_{a_4,3}$	$1-\ell_{a_4,4}$

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

11

Function Level

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

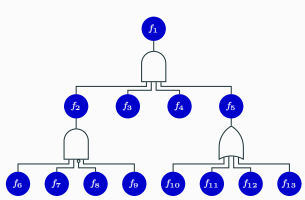


$$F_1 = F_2F_3F_4F_5$$

12

Function Level

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

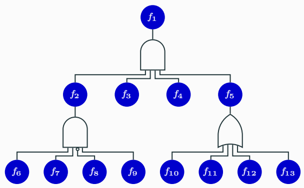


$$F_2 = F_6F_7\overline{F_8}F_9$$

12

Function Level

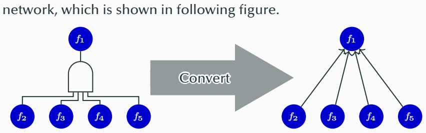
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

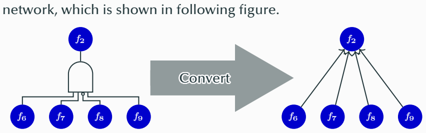
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_2)$	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

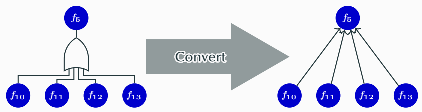
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_6)$	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

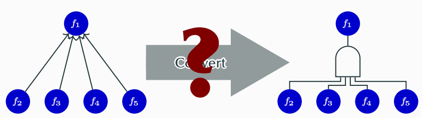
Function Level

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



$F(f_{10})$	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

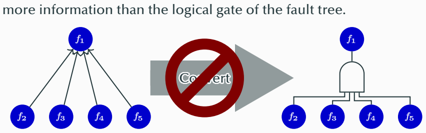
Function Level



$F(f_2)$	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.

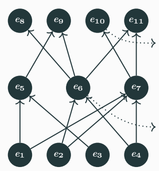


$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

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.



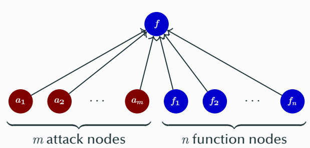
$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

$H(e_2)$	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.

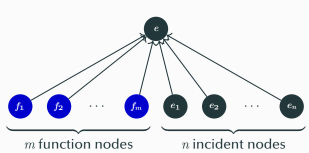
The following figures show two kind of information transfer.



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.



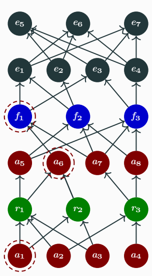
Collection of Evidence

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.

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.

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

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

20

Decouple of Incident Consequences – Step 2

21

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 $e_{i_1}, e_{i_2}, \cdots, e_{i_n}$.

22

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

23

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.

24

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.

25

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

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

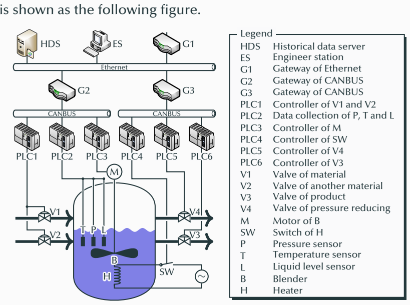
where

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

Simulation

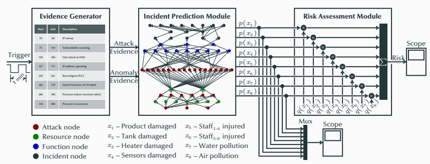
Simulation Platform

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



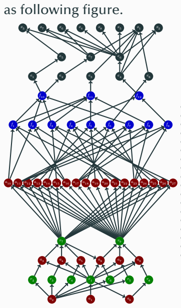
Simulation Platform

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 Platform

The multi-level Bayesian network of the chemical reactor is shown as following figure.



a_1 – Network Scanning
a_2 – Vulnerability scanning
a_3 – Buffer overflow attack on HDS
a_4 – FTP attack on HDS
a_5 – Brute force attack on HDS
a_6 – DoS attack on HDS
a_7 – Buffer overflow attack on ES
a_8 – Privilege escalation attack on ES
a_9 – Spoofing attack on ES
a_{10} – DoS attack on PLC1
a_{11} – DoS attack on PLC2
a_{12} – DoS attack on PLC3
a_{13} – DoS attack on PLC4
a_{14} – DoS attack on PLC5
a_{15} – DoS attack on PLC6
a_{16} – Reconfigure PLC1
a_{17} – Reconfigure PLC2
a_{18} – Reconfigure PLC3
a_{19} – Reconfigure PLC4
a_{20} – Reconfigure PLC5
a_{21} – Reconfigure PLC6
a_{22} – Man-in-the-middle attack on PLC1
a_{23} – Man-in-the-middle attack on PLC2
a_{24} – Man-in-the-middle attack on PLC3
a_{25} – Man-in-the-middle attack on PLC4
a_{26} – Man-in-the-middle attack on PLC5
a_{27} – Man-in-the-middle attack on PLC6
r_1 – IP addresses of HDS and ES
r_2 – Buffer overflow vulnerability
r_3 – FTP server vulnerability
r_4 – Login vulnerability
r_5 – Buffer overflow vulnerability
r_6 – Authentication vulnerability
r_7 – Administrator authority of HDS
r_8 – Crash of HDS
r_9 – Administrator authority of ES
f_1 – Traffic control of V1
f_2 – Traffic control of V2
f_3 – Traffic control of V3
f_4 – Pressure reducing
f_5 – Heating function
f_6 – Mixing function
f_7 – Liquid level sensation
f_8 – Temperature sensation
f_9 – Pressure sensation
f_{10} – Liquid level control
f_{11} – Temperature control
f_{12} – Pressure control
e_1 – Excessive liquid level
e_2 – Low liquid level
e_3 – Temperature anomaly
e_4 – Excessive pressure
e_5 – Heater dry fired
e_6 – Reactor explosion
e_7 – Liquid overflow
e_8 – Blender stop
x_1 – Production damaged
x_2 – Tank damaged
x_3 – Heater damaged
x_4 – Sensors damaged
x_5 – Staff$_{1\text{-}4}$ injured
x_6 – Staff$_{5\text{-}9}$ injured
x_7 – Water pollution
x_8 – Air pollution

Simulation Platform

The list of evidences is shown as following table.

Start	End	Description	Symbol
50	60	IP sweep	$L(a_1)$
75	110	Vulnerability scanning	$L(a_2)$
120	180	DoS attack to HDS	$L(a_6)$
157	171	IP address spoofing	$L(a_9)$
259	261	Reconfigure PLC5	$L(a_{20})$
266	378	Switch function of V4 failed	$F(f_4)$
286	390	Pressure reduce function failed	$F(f_{12})$
310	400	Pressure is excessive	$H(e_4)$

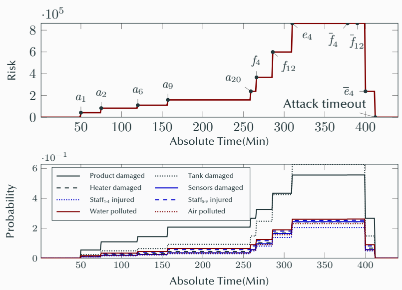
Simulation Platform

The quantification of consequences is shown as following table.

Incident Symbol	Description of Incident	Quantification of Consequence($)
x_1	Product damaged	50,000
x_2	Tank damaged	500,000
x_3	Heater damaged	10,000
x_4	Sensors damaged	10,000
x_5	$\text{Staff}_{1\text{-}4}$ injured	800,000
x_6	$\text{Staff}_{5\text{-}9}$ injured	1,000,000
x_7	Water pollution	200,000
x_8	Air pollution	200,000

32

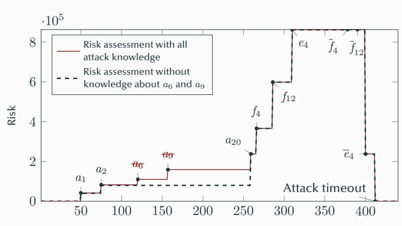
Simulation and Result Analysis



33

Simulation and Result Analysis

Then an identical multi-step attack on the system is launched to the system. The new cybersecurity risk curve is shown the dashed line in the following figure.



34

Simulation and Result Analysis

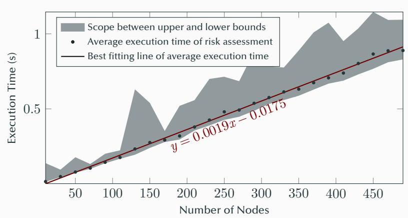
Some parameters of the following figure:

- The average execution time of a risk assessment is 94.1ms.
- The minimum execution time of a risk assessment is 89.9ms.
- The maximum execution time of a risk assessment is 131.6ms.

35

Simulation and Result Analysis

This means that the execution time of the risk assessment scales linearly with the increase of the node size of the multi-level Bayesian network.



36

Conclusion and Prospect

Conclusion

- By considering the characteristics of ICSs, a novel multi-level Bayesian network was proposed, which integrated a knowledge of attack, system function, and hazardous incident.
- The attack knowledge and system knowledge were combined to analyze the potential impact of attacks, so the proposed approach had the ability of assessing the risk caused by unknown attacks.
- A unified quantification approach for a variety of consequences of industrial accidents was introduced. Furthermore, the proposed approach could eliminate the error of risk caused by the overlapping amongst hazardous incidents.
- By using a simplified chemical reactor control system in Matlab environment, the designed dynamic risk assessment approach was verified.

Prospect

There are some shortcomings of the proposed risk assessment approach need to be improved.

- **Current research work has no ability for self-learning.**
- **The sub-second computation time cannot meet some hard real-time systems requirements.**

In the future, a dynamic cybersecurity risk assessment, which can automatically adjust the conditional probability and structure of the multi-level Bayesian network by analyzing the real-time data, will be researched, and several approximate inference methods will be attempted in the risk assessment.

Thank You!

Thank You!

You can obtain this slide from my Github:
`zqmillet@github.com:Presentation.for.Loughborough.University`

And I have pushed the code of the simulation to my Github, too.
`zqmillet@github.com:Multi-level.Bayesian.Network`

41

Any Questions?