

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

Zhang Qi

qiqi@hust.edu.cn

October 9, 2015



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

Dynamic Risk Assessment

- Decouple of Incident Consequences

- Classification of Incident Consequences

- Quantification of Incident Consequences

- Calculation of Dynamic Risk

Dynamic Risk Assessment

Decouple of Incident Consequences – Step 1

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

$$c_i = (c_1, c_2, \dots, c_n).$$

The meaning of c_i is that the occurring of the incident e_i will threaten the elements in consequence set 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

$$c_i = (\text{workers, air, facilities, products}).$$

Decouple of Incident Consequences – Step 3

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

$$\forall c' \in C', \exists c \in C, c' \subseteq c,$$

there must be a consequence set $c_i \in C$, where $c'_j \subseteq c_i$.

Decouple of Incident Consequences – Step 3

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

$$\forall c' \in C', \exists c \in C, c' \subseteq c,$$

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

$$e_j = (e_{i_1}, e_{i_2}, \dots, e_{i_n}).$$

Decouple of Incident Consequences – Step 3

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

$$\forall c' \in C', \exists c \in C, c' \subseteq c,$$

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

$$e_j = (e_{i_1}, e_{i_2}, \dots, e_{i_n}).$$

For each incident e_k of the incident set e_j , the corresponding consequence set c_k satisfies the following condition:

$$c'_j \subseteq c_k.$$

Decouple of Incident Consequences – Step 3

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

$$\forall c' \in C', \exists c \in C, c' \subseteq c,$$

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

$$e_j = (e_{i_1}, e_{i_2}, \dots, e_{i_n}).$$

For each incident e_k of the incident set e_j , the corresponding consequence set c_k satisfies the following condition:

$$c'_j \subseteq c_k.$$

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

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

Harm to Humans

Environmental Pollution

Property Loss

Quantification of Harm to Humans

Quantification of Environmental Pollution

Quantification of Property Loss

Calculation of Dynamic Risk

Questions?