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

Zhang Qi

`qiqi@hust.edu.cn`

October 10, 2015

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

Outlines

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

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

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

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?