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

Zhang Qi

qiqi@hust.edu.cn

October 17, 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 2

Then, enerate $\boldsymbol{C'} = (\boldsymbol{c}'_1, \boldsymbol{c}'_2, \cdots, \boldsymbol{c}'_{m'})$ based on $\boldsymbol{C} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_m)$.
The following conditions must be met:

$$\text{Completeness: } \bigcup_{i=1}^{m} \boldsymbol{c}_i = \bigcup_{i=1}^{m'} \boldsymbol{c}'_{i'},$$

$$\text{Independence: } \forall \boldsymbol{c}'_i, \boldsymbol{c}'_j \in \boldsymbol{C'} : \boldsymbol{c}'_i \cap \boldsymbol{c}'_j = \varnothing,$$

$$\text{Traceability: } \forall \boldsymbol{c}' \in \boldsymbol{C'}, \exists \boldsymbol{c} \in \boldsymbol{C} : \boldsymbol{c}' \subseteq \boldsymbol{c}.$$

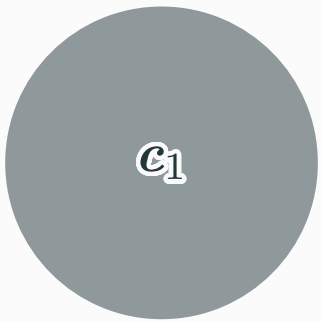
Decouple of Incident Consequences – Step 2

Then, enerate $C' = (c'_1, c'_2, \cdots, c'_{m'})$ based on $C = (c_1, c_2, \cdots, c_m)$.
The following conditions must be met:

$$\text{Completeness: } \bigcup_{i=1}^{m} c_i = \bigcup_{i=1}^{m'} c'_{i'},$$

$$\text{Independence: } \forall c'_i, c'_j \in C' : c'_i \cap c'_j = \varnothing,$$

$$\text{Traceability: } \forall c' \in C', \exists c \in C : c' \subseteq c.$$



$C = (c_1,$

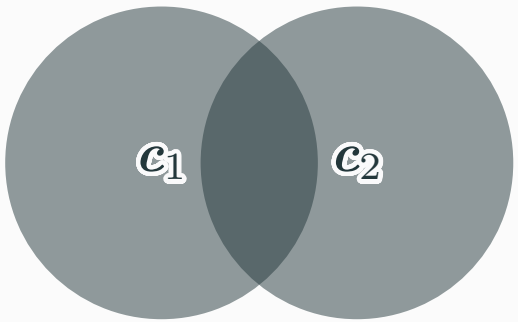
Decouple of Incident Consequences – Step 2

Then, enerate $C' = (c'_1, c'_2, \cdots, c'_{m'})$ based on $C = (c_1, c_2, \cdots, c_m)$.
The following conditions must be met:

$$\text{Completeness: } \bigcup_{i=1}^{m} c_i = \bigcup_{i=1}^{m'} c'_{i'},$$

$$\text{Independence: } \forall c'_i, c'_j \in C' : c'_i \cap c'_j = \varnothing,$$

$$\text{Traceability: } \forall c' \in C', \exists c \in C : c' \subseteq c.$$



$C = (c_1, c_2,$

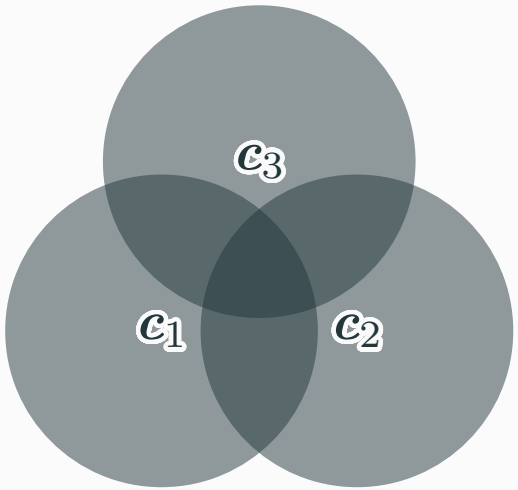
Decouple of Incident Consequences – Step 2

Then, enerate $C' = (c'_1, c'_2, \cdots, c'_{m'})$ based on $C = (c_1, c_2, \cdots, c_m)$.
The following conditions must be met:

$$\text{Completeness: } \bigcup_{i=1}^{m} c_i = \bigcup_{i=1}^{m'} c'_{i'},$$

$$\text{Independence: } \forall c'_i, c'_j \in C' : c'_i \cap c'_j = \varnothing,$$

$$\text{Traceability: } \forall c' \in C', \exists c \in C : c' \subseteq c.$$



$C = (c_1, c_2, c_3)$

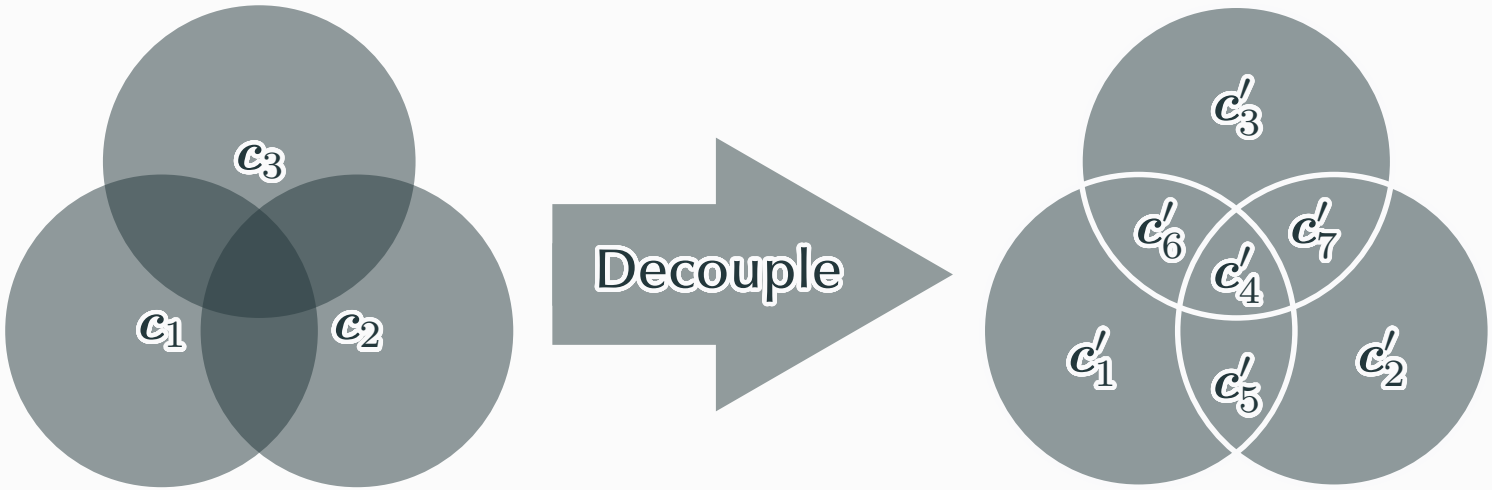
Decouple of Incident Consequences – Step 2

Then, enerate $C' = (c'_1, c'_2, \cdots, c'_{m'})$ based on $C = (c_1, c_2, \cdots, c_m)$.
The following conditions must be met:

$$\text{Completeness: } \bigcup_{i=1}^{m} c_i = \bigcup_{i=1}^{m'} c'_{i'},$$

$$\text{Independence: } \forall c'_i, c'_j \in C' : c'_i \cap c'_j = \varnothing,$$

$$\text{Traceability: } \forall c' \in C', \exists c \in C : c' \subseteq c.$$



$C = (c_1, c_2, c_3)$ $\qquad$ $C' = (c'_1, c'_2, \cdots, c'_7)$

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.

Thank You!

Thank You!

You can obtain this slide from my Github:

`zqmillet@github.com:Presentation.for.Loughborough.University`

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`

Any Questions?