Evaluation probabiliste de la fiabilité & la disponibilité

B. Monsuez
Mastère IRVEA
Année 2020/2021
Séance du 25 juin 2021

Evaluation probabiliste des risques (PRA)

- Méthode pour appréhender de manière systématique et complète les risques d'un système complexe

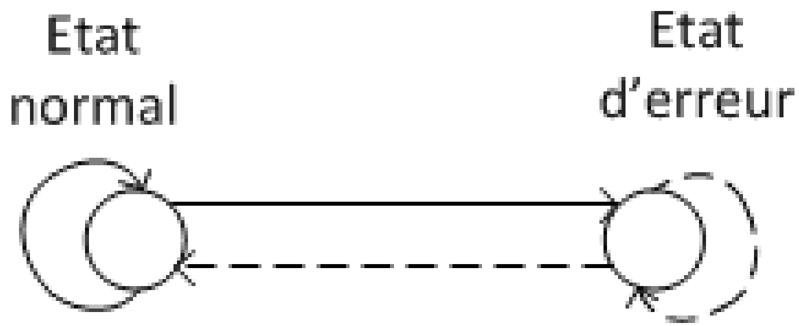
- Le risque est caractérisé par
  - La sévérité (magnitude) de chacune des conséquences.
  - La probabilité d'occurence.

EPR (suite)

- Le but de l'EPR est de répondre à ces 3 questions
  - Quels sont les évènements pouvant se produire ?
  - Quelles sont les conséquences d'un évènement ?
  - Quelle est la probabilité et la fréquence d'occurrence de ces évènements ?
- L'EPR historiquement prend ses origines
  - Dans le nucléaire (NRC)
  - Se généralise à toutes les activités industrielles

Caractérisation d'un évènement élémentaire

- Système de transitions élémentaires à deux états



- Fiabilité
  - $N_{[0,t]}$durée de fonctionnement dans l'état sans faute.
  - N_0 composant réparé au temps 0.
  - $R(t) \equiv \Pr\{N_{[0,t]} | N_0\}$ $\quad F(t) \equiv \Pr\{\overline{N}_{[0,t]} | N_0\}$

Estimation de la fiabilité

- $f(t) \equiv \frac{\mathrm{d}F(t)}{dt}$ Densité de défaillance
- $r(t)dt \equiv \Pr\{\overline{N}_{[t,t+dt]}|\mathrm{N}_0, \mathrm{N}_{[0,\mathrm{t}]}\}$ Taux de défaillance
- MTTF$\equiv \int_0^\infty t\, f(t)dt$ *(Mean Time To Failure)*

- $\overline{G}(t) \equiv \Pr\{F_{[0,t]}|F_0\}$ *Absence de réparabilité*
- $G(t) \equiv \Pr\left\{\overline{F}_{[0,t]}\middle|F_0\right\} = 1 - \overline{G}(t)$ *Réparabilité*

- $g(t) \equiv \frac{\mathrm{d}G(t)}{dt}$ Densité de réparation
- $m(t)dt \equiv \Pr\left\{\overline{F}_{[t,t+dt]}\middle|F_0, F_{[0,t]}\right\}$ *Taux de réparation*
- MTTR$\equiv \int_0^\infty t\, g(t)dt$ *(Mean Time To Repair)*

Estimation de la disponibilité

- Disponibilité
  - $x(t) \equiv \begin{cases} 0 & le\ composant\ est\ dans\ l'état\ normal \\ 1 & le\ composant\ est\ dans\ l'état\ d'erreur \end{cases}$
  - $A(t) \equiv \Pr\{x(t) = 0|N_0\}$
- Indisponibilité
  - $U(t) \equiv \Pr\{x(t) = 1|N_0\} = 1 - A(t)$

Notion d’architectures

- Un système est composé d’un ensemble de fonctions
  - Assurant le fonctionnement
  - Assurant la sécurité
  - Assurant les replis
- Une fonction est composée d’un ensemble de composants
  - Actionneurs
  - Capteurs
  - Décisions
- Estimation de la fiabilité & la disponibilité du système
  - Par composition des fonctions élémentaires

Les structures pour décrire un système

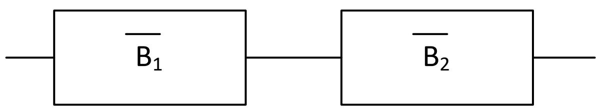
- Les arbres d’évènements
- Les arbres de défaillance
- Les expressions de logiques booléennes
- Les diagramme de fiabilité
- Les diagrammes de transitions markoviennes

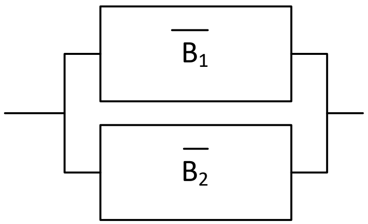
Arbres d’évènement

- Part d’un évènement initial (initiating event)
- Analyse pour chaque état les évènements ultérieurs
  - Jusqu’à atteindre un état stable
  - Jusqu’à atteindre l’état nominal
  - Jusqu’à atteindre un état d’erreur

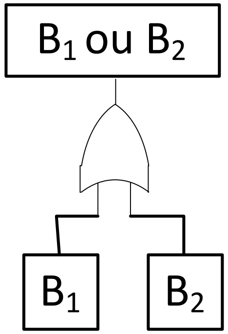
Arbres de défaillance & les diagrammes de défaillance

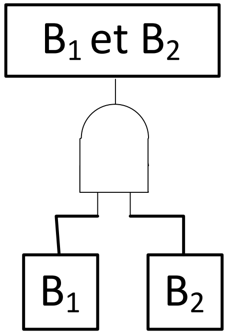
- Diagramme de défaillance





- Arbre de défaillance





Systèmes en série ou en parallèle

	B1	B2	Actif	Probabilité
1	oui	oui	oui	$\Pr\{B_1\}\Pr\{B_2\}$
2	oui	non	oui	$\Pr\{B_1\}\Pr\{\overline{B}_2\}$
3	non	oui	oui	$\Pr\left\{\overline{B}_1\right\}\Pr\{B_2\}$
4	non	non	non	$\Pr\left\{\overline{B}_1\right\}\Pr\{\overline{B}_2\}$

	B1	B2	Actif	Probabilité
1	oui	oui	Oui	$\Pr\{B_1\}\Pr\{B_2\}$
2	oui	Non	Non	$\Pr\{B_1\}\Pr\{\overline{B}_2\}$
3	non	Oui	Non	$\Pr\left\{\overline{B}_1\right\}\Pr\{B_2\}$
4	non	Non	Non	$\Pr\left\{\overline{B}_1\right\}\Pr\{\overline{B}_2\}$

$$Q_S(t) = \Pr\{B_1\} + \Pr\{B_2\} - \Pr\{B_1\}\Pr\{B_2\}$$

$$Q_S(t) = \Pr\{B_1\}\Pr\{B_2\}$$

Systèmes de vote

- Principe :
  - *m* sous-évènements sur *n* doivent être actifs pour que l'évènement se produise

$$\Pr(k; n, Q) \equiv \binom{n}{k} Q^k (1-Q)^{n-k}$$

$$Q_s(t) \equiv \sum_{k=m}^{n} \binom{n}{k} Q^k (1-Q)^{n-k}$$

- Pour un système 2/3, nous avons donc

$$Q_{2/3} = \binom{3}{2} Q^2 (1-Q)^1 + \binom{3}{3} Q^3 (1-Q)^0$$

$$= 3Q^2 - 2\,Q^3$$

$\sim 3Q^2$ pour Q petit

Quantification des évènements d’un système – Les approches Markoviennes

- Chaîne de Markov
  - toute l'information utile pour la prédiction du futur est contenue dans l'état présent du processus

$$\forall n \geq 0, \forall (i_0, \dots, i_{n-1}, i, j) \in E^{n+2},$$
$$\Pr(X_{n+1} = j \mid X_0 = i_0, X_1 = i_1, \dots, X_{n-1} = i_{n-1}, X_n = i) = \Pr(X_{n+1} = \mathrm{j} \mid \mathrm{X_n} = \mathrm{i})$$

Chaîne de Markov homogène

- Chaîne de Markov homogène : système de transition qui ne change pas dans le temps

$$\forall n \geq 0, \forall (i_0, \dots, i_{n-1}, i, j) \in E^{n+2},$$
$$\Pr(X_{n+1} = j \mid X_0 = i_0, X_1 = i_1, \dots, X_{n-1} = i_{n-1}, X_n = i)$$
$$= \Pr(X_1 = \mathrm{j} \mid \mathrm{X}_0 = \mathrm{i})$$

- Propriété forte que :

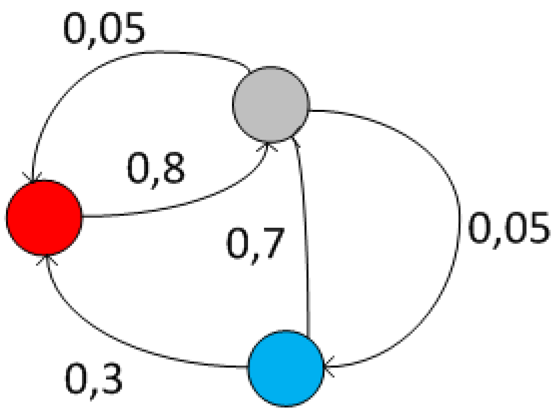
$$\forall n \geq 0, \forall (i_0, \dots, i_{n-1}, i, j) \in E^{n+2},$$
$$\Pr(X_{n+1} = j \mid X_n = i) = \Pr(X_1 = \mathrm{j} \mid X_0 = \mathrm{i})$$

Calcule de fiabilité en utilisant les chaînes de Markov

- Supposons un système de régulation de température simplifié fonctionnant à 3 niveaux comme suit:
  - 9/10, pas besoin de produire du chaud ou du froid.
  - 1/20 ventilation
  - 1/20, production de froid pendant 1 min.
  - 3/10 production de chaud après avoir produit trop de froid.
  - 7/10 retour à l’état neutre après avoir produit du froid.
  - 8/10 retour à l’état neutre après avoir produit du chaud.
  - 2/10 de continuer de produire du chaud.

Schéma & matrice de transitions

- Schéma de transition



- Matrice de transition

$$P = \begin{bmatrix} 0{,}9 & 0{,}05 & 0{,}05 \\ 0{,}7 & 0 & 0{,}3 \\ 0{,}8 & 0 & 0{,}2 \end{bmatrix}$$

- Utilisation de la matrice

$$x^{(1)} = x^0\, P$$
$$x^{(2)} = P\, x^{(1)} = P^2 x^0$$
$$q = \lim_{n\to\infty} x^{(n)}$$

- Si la chaîne est apériodique et irréductible alors nous avons la convergence

$$qP = q \; (Point\ fixe)$$
$$q(I - P) = 0$$
$$= [q_1, q_2, q_3] \begin{bmatrix} 0{,}1 & -0{,}05 & -0{,}05 \\ -0{,}7 & 1 & -0{,}3 \\ -0{,}8 & 0 & 0{,}8 \end{bmatrix} = 0$$
$$[q_1, q_2, q_3] = [0{,}884, 0{,}0442, 0{,}0718]$$

Conclusion

- Ensemble de méthode permettant d'estimer & de quantifier la survenance d'un évènement.
- Méthodes actuellement « poussées » par les réglementations (ISO 26262, EN 50128, directive SEVESO)
- Différentes des méthodes « déterministes » (Soit il y a une erreur soit pas d'erreurs)
- Peuvent servir à estimer aussi des propriétés autres que la fiabilité ou disponibilité (exemple : la consommation)