SÛRETÉ DE FONCTIONNEMENT

« COMMENT GARANTIR QU'UN SYSTÈME EST SÛR ? »

B. Monsuez
ENSTA PT

Qu'entendons nous par SdF ?

- **Le niveau de confiance** que nous pouvons avoir dans un **système**.

- Opposition entre deux grandeurs
  - Une subjective : est ce que je suis dans un véhicule « sûr » ?
  - Une objective et quantifiable : la probabilité que cet évènement se passe est de x% !

- Attention
  - Un système subjectivement sûr n'est pas un système objectivement sûr et vice versa.

Emergence de la SdF

- Apparition concomitante avec la révolution industrielle (250 ans)
  - Industrie chimique & métallurgique
  - Transports
- Puis avec le développement de la médecine
  - Apparition de la notion coût/bénéfice
  - Evaluation statistique du risque
- Et enfin avec l'automatisation
  - Automatisation & autonomie décisionnelle des systèmes

Le cadre de la SdF aujourd'hui

- Ensemble de règles métiers
  - Règles de conception
  - Règles d'exploitation
  - Règles de démantèlement
- Ensemble de normes
  - Définition des attendus en terme de conceptions, d'exploitation et de démantèlement
- Ensemble de loi
  - Définition des procédures de qualification/certification, autorisations et autres agréments

Le cadre de la SdF (suite)

- Vision « métier » des règles
  - ISO26262 dans l'automobile
  - EN50126, EN50128 EN50129 dans le ferroviaire
  - DO254, DO178 dans l'aviation
- Pratique « nationale » ou « internationale »
  - ISO, DO : normes à portée internationales
  - EN : normes européennes
- Attention
  - Une norme peut-être « internationale » mais son interprétation nationale

Le cadre de la SdF (suite)

- Multiplicité des normes applicables
  - Normes relatives à la conception
    - ISO 26262 mais EN pour les aspects électriques
  - Normes relatives à la fabrication
    - IEC pour les aspects automatisation de la fabrication, EN pour les aspects électriques, …
  - Normes relatives à l'exploitation
    - EN + Nationales

La « sûreté » en terme d'objectifs

- La question « fondamentale » est :

  How safe is safe enough ?

- Deux visions de la gestion de risque :
  - Une vision « individualiste » : le risque qu'un individu décède ou soit blessé.
  - Une vision « sociétale » : le risque pour la population suite à un dysfonctionnement

La « sûreté » en terme d'objectifs

- Plusieurs notions d'acceptation
  - Une notion « sociétale » : la perception du risque est acceptable pour les individus et la société.
  - Une notion « économique » : le risque est économiquement supportables.
  - Une notion « bénéfice » : le risque existe mais les avantages sont tels que le risque est ignoré.

La qualification/certification

- Soit déclarative
  - Le constructeur fournit l'ensemble des procédures et résultats de test pour la validation
- Soit suite à audit
  - Un audit par des experts indépendant est réalisé.
- Soit par une instruction administrative du dossier
  - Evaluation des risques sur dossier

La SdF et les Systèmes Complexes

Un système complexe critique est un système dont :

- Le niveau de sûreté et de sécurité ne peut pas être démontré uniquement par du test
- La logique de fonctionnement est délicate à appréhender
- Un dysfonctionnement peut mettre en péril la sécurité des biens et des personnes

Les Systèmes Automatisés sont des Système Complexe Critiques

- Recours à une électronique de gestion de l'énergie
- Recours à une électronique de pilotage

- Problématique de la sûreté
  - Sûreté des composants du systèmes
    batteries, chaîne électrotechnique, composants électroniques, capteurs
  - Sûreté des fonctions du système
  - Gestion des modes de sécurisation

Quelques exemples de sous-systèmes critiques

- Le « drive-by-wire »
- Le circuit de charge d'un téléphone/ordinateur
- Le déplacement d'un robot
- L'ATP (Automated Train Protection) d'un système ferroviaire
- La déclenchement de l'arrêt d'un réacteur.

La problématique particulière des systèmes complexes critiques

Nombre de fonctions

- Chaîne de contrôle entre un ensemble de capteurs et d'actionneurs
- Problème de la ségrégation des fonctions ?
- Problème de la distribution des fonctions ?
- Problème de la gestion des modes communs
- Problème des défaillance des fonctions

La problématique particulière des systèmes complexes critiques

Nombre d'états

- Problème de l'explosion combinatoire.
  - 2 capteurs, 2 valeurs : 4 états
  - 6 capteurs, 10 valeurs : $6^{10} = 60466176$
- Problème du test exhaustif
  - Impossibilité d'énumérer l'ensemble des états
- Problème des cas de défaillance
  - Augmenter encore le nombre d'état

La problématique particulière des systèmes complexes critiques

Le comportement discret

- Passage d'un état à un autre topologiquement différent
  - ABS : régulation de l'état « freine » à l'état « ne freine pas »
- Difficulté de mise en place de marge de sécurité
  - En mécanique : **surdimensionnement** de x% de la structure
  - En commande : prise d'une marge pour ne pas être aux frontières de stabilité
- Une ligne d'un programme code permet de passer d'un état à l'autre ?
  - Comment assurer la stabilité dans une telle situation ?

La problématique particulière des systèmes complexes critiques

Le couplage « systèmes continus » et « systèmes discret »

- Les fonctions sont « continues »
- La commande est « discrète »

Comment modéliser un système à la fois « continu » et « discret » ?

- Problématique des démonstrations mathématiques
- Cf. la tartine beurrée

La problématique particulière des systèmes complexes critiques

Le temps-réel

- Existence d'un délai de traitement
- Garantir la décision dans le temps imparti

- Temps-réel dur : action obligatoire dans le temps imparti
- Temps-réel mou : si l'action n'est pas effectuée dans le temps imparti, on passe à la suivante

La problématique particulière des systèmes complexes critiques

La gestion des défaillances

- Détecter une défaillance
- Prendre les actions nécessaires
  - Mettre le système en sécurité
  - Mettre le système dans un état où il est possible de continuer la mission

La protection contre les intrusions

- S'assurer que le code n'est pas modifié
- S'assurer qu'une attaque par saturation n'est pas possible

La problématique particulière des systèmes complexes critiques

La gestion des configurations

- Véhicule électrique pouvant recevoir les options suivantes
  - Batterie
  - Générateur
  - Super-Capacité
- Souhait : une seule plateforme pouvant être configurée pour les différentes options.

Que recouvre la notion de système sûr ?

Confiance justifiée que l'on peut placer dans un système, se caractérise par les 6 attributs suivants :

- **Availability ("readiness for correct service"),**
- **Reliability ("continuity of correct service"),**
- **Integrity ("maintaining the consistency of data"),**
- **Maintainability ("ability for a process to undergo modifications and repairs"),**
- **Safety ("absence of catastrophic consequences on the users and the environment")**
- **Security ("prevention of unauthorized disclosure of information").**

EVALUATION PROBABILISTE DE LA FIABILITÉ & LA DISPONIBILITÉ

B. Monsuez -- ENSTA PT

Evaluation probabiliste des risques (PRA)

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

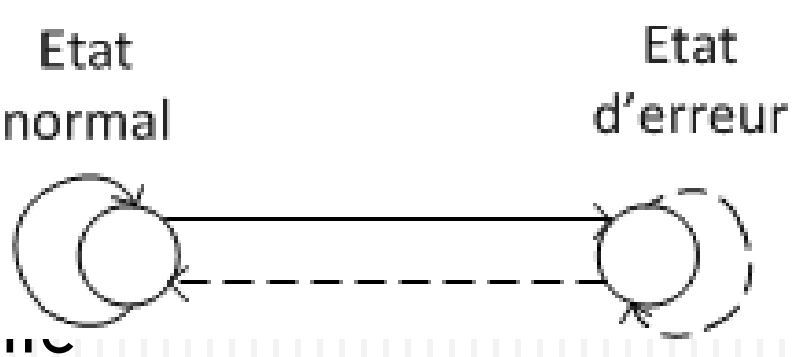
- Le risque est caractérisé par
  - La sévérité (magnitude) de chacune des conséquences.
  - La probabilité d'occurence.

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



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

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

- $g(t) \equiv \frac{\mathrm{d}G(t)}{dt}$ Densité de réparation
- $m(t)dt \equiv \Pr\{F_{[t,t+dt]} | F_0, F_{[0,t]}\}$ *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

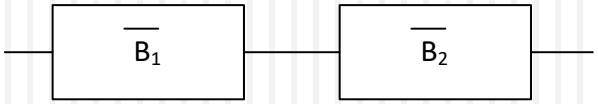
- Les arbres d'évènements
- Les arbres de défaillance
- Les expressions de logiques booléennes
- Les diagramme de fiabilité
- Les diagrammes de transitions markoviennes

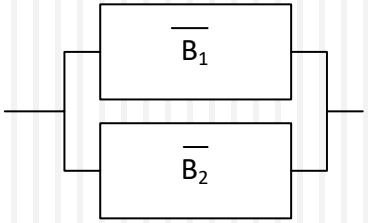
Arbres d'évènement

- 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

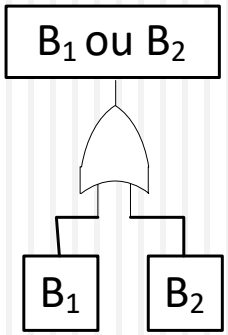
Arbres de défaillance & les diagrammes de défaillance

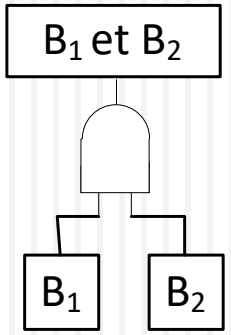
- Diagramme de défaillance





- 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	$\Pr\ \overline{B}_1\ \Pr\{B_2\}$
4	non	non	non	$\Pr\ \overline{B}_1\ \Pr\{\overline{B}_2\}$

	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	$\Pr\ \overline{B}_1\ \Pr\{B_2\}$
4	non	Non	Non	$\Pr\ \overline{B}_1\ \Pr\{\overline{B}_2\}$

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

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

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

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

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 :

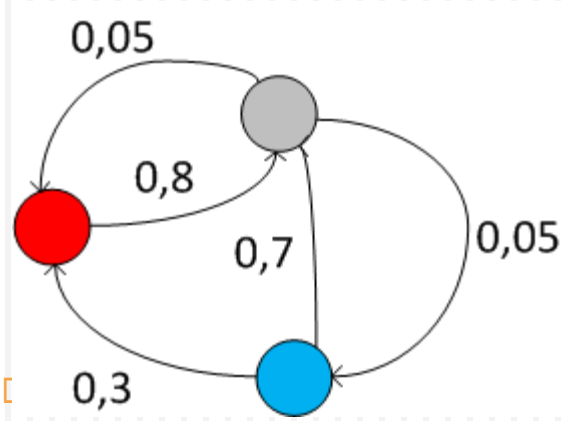
$$\forall n \geq 0, \forall (i_0, \dots, i_{n-1}, i, j) \in E^{n+2},$$
$$\Pr(X_{n+1} = j \mid X_n = i) = \Pr(X_1 = \mathrm{j} \mid X_0 = \mathrm{i})$$

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



- 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

$$qP = q \; (Point \; fixe)$$

$$q(I - P) = 0$$

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

$$= [q_1, q_2, q_3] \begin{bmatrix} 0{,}1 & -0{,}05 & -0{,}05 \\ -0{,}7 & 1 & -0{,}3 \\ -0{,}8 & 0 & 0{,}8 \end{bmatrix}$$

$$= 0$$

$$[q_1, q_2, q_3] = [0{,}884, 0{,}0442, 0{,}0718]$$

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)