Comment gérer les incertitudes dans les études de Sûreté de Fonctionnement

Mohamed Sallak
Maître de Conférences / HDR
Université de Technologie de Compiègne
Laboratoire Heudiasyc CNRS UMR 7253, France

3ème Conférence Internationale sur la Maintenance et la Sécurité Industrielle, CIMSI'2015 09 et 10 Novembre 2015, Algérie

De quelles incertitudes on parle ?

Incertitude aléatoire vs. Incertitude épistémique

Incertitude aléatoire

- Variabilité naturelle des phénomènes aléatoires (Exemple : choix de la loi exponentielle en fiabilité).
- Irréductible.

Incertitude épistémique

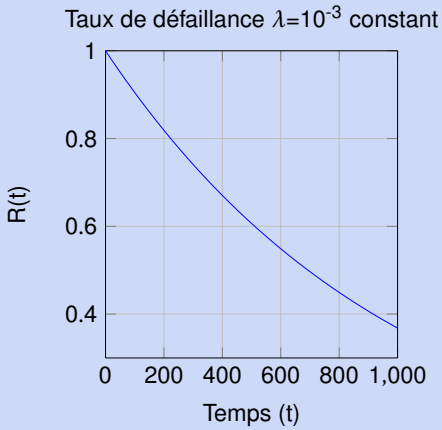
- Manque de données ou de connaissances (Exemple : taux de défaillance imprécis).
- Réductible.

Pourquoi cette distinction ?

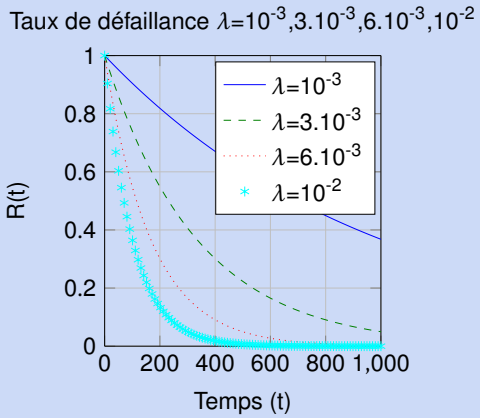
- Choix de la bonne théorie de représentation des incertitudes.
- Aide à la décision en se concentrant sur les incertitudes réductibles.

Incertitude aléatoire vs. Incertitude épistémique

- Fiabilité d'un composant R(t)=exp(-λ.t).
- Légitimité du choix de la loi : période de vie utile, calculs simples.



→ **Incertitude aléatoire**



→ **Incertitude épistémique**

Incertitudes des modèles vs. Incertitudes des paramètres

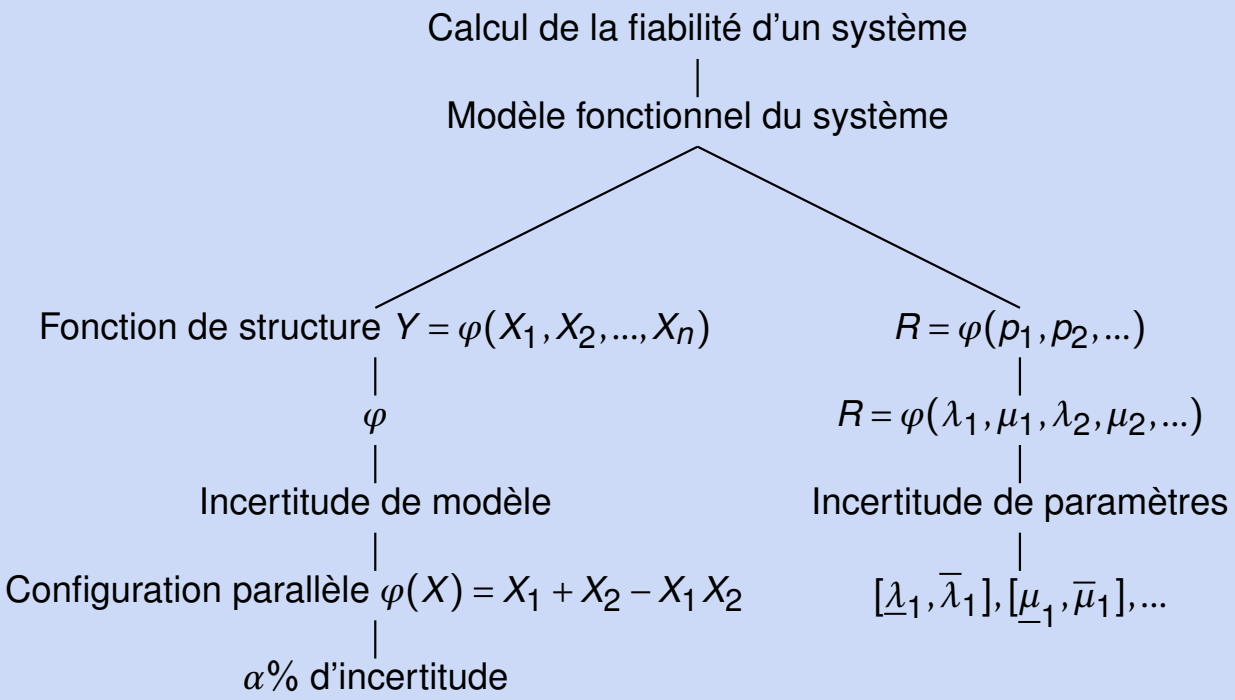
Incertitudes des modèles

- Tous les modèles (fonctionnels et dysfonctionnels) ne correspondent pas exactement au systèmes réels.
- On s'intéresse aux incertitudes liées aux relations (ET,OU,k/n,...) entre les composants d'un système.
- Incertitudes associées aux hypothèses simplificatrices du modèle (dépendances, états dégradés, ...).

Incertitudes des paramètres de fiabilité

- Associées à la vraie valeur de chaque paramètre (taux de défaillance, taux de réparation, MTBF, etc.).
- Chaque incertitude sur un paramètre peut être représentée par un intervalle, une distribution, une masse, ...

Incertitudes des modèles vs. Incertitudes des paramètres



Quelques théories de l'incertain

Théories de l'incertain

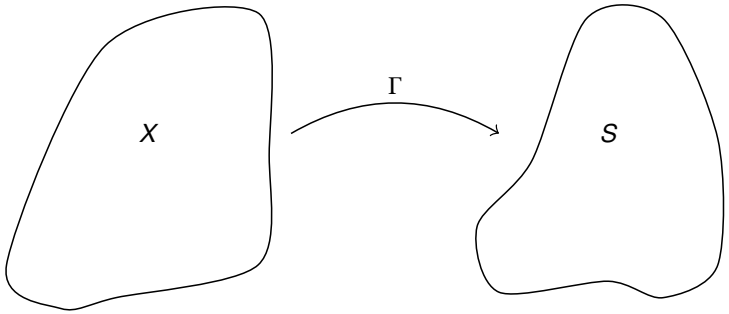
- Théorie des probabilités : probabilités objectives et subjectives.
- Théorie des ensembles flous.
- Théorie des possibilités.
- Théorie des fonctions de croyance.
  - La théorie des fonctions de croyance a été introduite par Dempster en 1969 et développée par la suite par Shafer.
  - Elle constitue un cadre unique pour la prise en compte des incertitudes aléatoires et épistémiques.
- Théorie des probabilités imprécises (au sens de Walley).
- Théorie des ensembles aléatoires.
- ...

Théorie des fonctions de croyance

- La théorie des fonctions de croyance a été introduite par Dempster en 1969 par l'utilisation des probabilités inférieures et supérieures.
- Elle a été développée par la suite par Shafer.
- Elle a été largement utilisée dans certains domaines comme la classification, la fusion d'information, les systèmes experts, ...
- Elle est bien adaptée à la modélisation de l'ignorance totale.
- Elle constitue un cadre unique pour la prise en compte des incertitudes aléatoires et épistémiques.

Théorie des fonctions de croyance

- $X = \{c_1, c_2, ..., c_n\}$: ensemble d'un lot d'un composant C.
- $S = \{s_1, s_2, ..., s_k\}$: Ensemble d'états possibles.
- Γ : application multi-valuée de X dans 2^S.



$R = \{s_i, s_j, s_k\}$
$T^* = \{c_i \in X | \Gamma(c_i) \cap R \neq \emptyset\}$, $T_* = \{c_i \in X | \Gamma(c_i) \subset R\}$, $T = \{c_i \in X | \Gamma(c_i) = R\}$

- $bel : 2^S \rightarrow [0,1]$, $bel(T) = P(T_*)$
- $pl : 2^S \rightarrow [0,1]$, $pl(T) = P(T^*)$
- $m : 2^S \rightarrow [0,1]$, $m(T) = P(T)$

Si Γ est une application mono-valuée de X dans S ($T^* = T_* = T$) : mesure de probabilité classique.

Construction des données de fiabilité des composants

A partir des données statistiques

- La construction des données de fiabilité des composants est une étape indispensable dans toute étude de SdF.
- Proposition de méthodes pour cette construction (taux de défaillance) dans le cadre des fonctions de croyance.
- On réalise *n* tests d'un composant binaire (loi de Bernoulli) afin d'évaluer son taux de défaillance $\lambda \in [0,1]$.
- Objectif : Obtenir les masses, les fonctions de crédibilités, et les fonctions de plausibilités de $\lambda \in [\alpha, \beta]$.

Construction des données de fiabilité des composants : Loi de Bernoulli

Formules établies (à partir des travaux d'Almond)

X : Nombre total de défaillances observées lors de n tests.

$$bel(\lambda \in [\alpha,\beta]) = X\binom{n}{X}\int_{u=\alpha}^{u=\beta} u^{X-1}(1-u)^{n-X}du - \binom{n}{X}(\beta^X - \alpha^X)(1-\beta)^{n-X}; \quad 0 < X < n$$

$$pl(\lambda \in [\alpha,\beta]) = X\binom{n}{X}\int_{u=\alpha}^{u=\beta} u^{X-1}(1-u)^{n-X}du + \binom{n}{X}\alpha^X(1-\alpha)^{n-X}; \quad 0 < X < n$$

Exemple

On a testé 60 échantillon d'un produit c : 11 ont été trouvés défectueux. On souhaite obtenir les masses, les fonctions de crédibilités, et les fonctions de plausibilités de λ tel que : $\lambda = 0.1$ et $\lambda \in [0, 0.2]$.

λ	$[bel, pl]$
0.1	$[0, 0.0196]$
$[0, 0.2]$	$[0.5173, 0.6623]$

Construction des données de fiabilité des composants

A partir des avis des experts

- Cadre de discernement d'un composant binaire c : $\Omega_c = \{1_c, 0_c\}$.
- Un expert peut donner w_c et f_c :

$$\begin{cases} m_c^{\Omega_c}(1_c) & = & w_c \\ m_c^{\Omega_c}(0_c) & = & f_c \\ m_c^{\Omega_c}(\Omega_c) & = & 1 - f_c - w_c \end{cases}$$

- Un expert peut donner $\lambda \in \left[\underline{\lambda}, \overline{\lambda}\right]$:

$$\begin{cases} bel^c(1_c) & = & e^{-\overline{\lambda}t} \\ pl^c(1_c) & = & e^{-\underline{\lambda}t} \\ m_c^{\Omega_c}(\Omega_c) & = & e^{-\underline{\lambda}t} - e^{-\overline{\lambda}t} \end{cases}$$

Construction des données de fiabilité des composants

Conclusions

- Des formules de construction ont été établies pour les lois usuelles utilisées en SdF : loi exponentielle et loi de Bernoulli.
- Des cas d'études avec des différents types de données ont été présentés pour illustrer la méthodologie de construction.
- Des comparaisons avec les paramètres de fiabilités obtenus en utilisant des a priori bayésiens (a priori de Jeffrey, a priori uniforme) ont été proposés.
- Les cas des taux de défaillances non constants et des taux de réparation doivent être traités.

Facteurs d'importance étendus

- Il est essentiel de pouvoir identifier les composants qui jouent un rôle plus important que d'autres en termes de fiabilité.
- En pratique, cette identification se fait au moyen des facteurs d'importance : mesurer l'effet du fonctionnement (la défaillance) d'un composant sur la défaillance du système complet.
- Extension des facteurs d'importance classiques : Birnbaum, RAW, RRW, et CR pour la prise en compte des fiabilités imprécises.
- Utilisation de l'arithmétique affine d'intervalles pour calculer les bornes inférieurs et supérieures des facteurs d'importance.

Facteurs d'importance étendus

- L'arithmétique affine est une nouvelle approche présentée en 1994 pour la prise en compte les problèmes de dépendances dans l'arithmétique d'intervalles (surestimation des résultats).
- Le principe est le même que celui de l'arithmétique d'intervalles, à part que l'on va conserver une information affine tout au long des calculs.
- Intervalle → Forme affine : $x = [\underline{x}, \overline{x}] \rightarrow x^* = \frac{\underline{x}+\overline{x}}{2} + \frac{\overline{x}-\underline{x}}{2}\epsilon$.

	Intervalle (IA)	Intervalle (AA)
Birnbaum	$[\underline{R}_{S\|1_i}, \overline{R}_{S\|1_i}] - [\underline{R}_{S\|0_i}, \overline{R}_{S\|0_i}]$	$[I_0^B(i) - h_i^B, I_0^B(i) + h_i^B]$ $h_i^B = \|I_1^B(i)\| + \|I_2^B(i)\|$ $I_0^B(i) = R_{S\|1_i,0} - R_{S\|0_i,0}$ $I_1^B(i) = R_{S\|1_i,1}$ $I_2^B(i) = R_{S\|0_i,2}$

Facteurs d'importance étendus
Conclusions

- Nous avons proposé des facteurs d'importance permettant de traiter à la fois les incertitudes épistémiques et aléatoires.
- Ces facteurs sont basés sur l'arithmétique affine.
- Des facteurs d'importance d'incertitudes et de dépendances sont aussi en cours de développement.

Quelques applications

Sécurité Fonctionnelle : Evaluation du PFD

Application

- La sécurité fonctionnelle a depuis longtemps retenu l'attention des industriels.
- Pour mener à bien leur démarche sécurité, ils peuvent s'appuyer sur des normes.
- Ces normes de sécurité fonctionnelle introduisent une approche probabiliste qui vient compléter l'approche déterministe classique.
- Elles préconisent l'utilisation de certaines méthodes (équations simplifiées, arbres de défaillance, approches markoviennes) sans pour autant les rendre obligatoire.
- La norme IEC 61508 porte plus particulièrement sur les systèmes E/E/PE (électriques/électroniques/électroniques programmables) de sécurité.

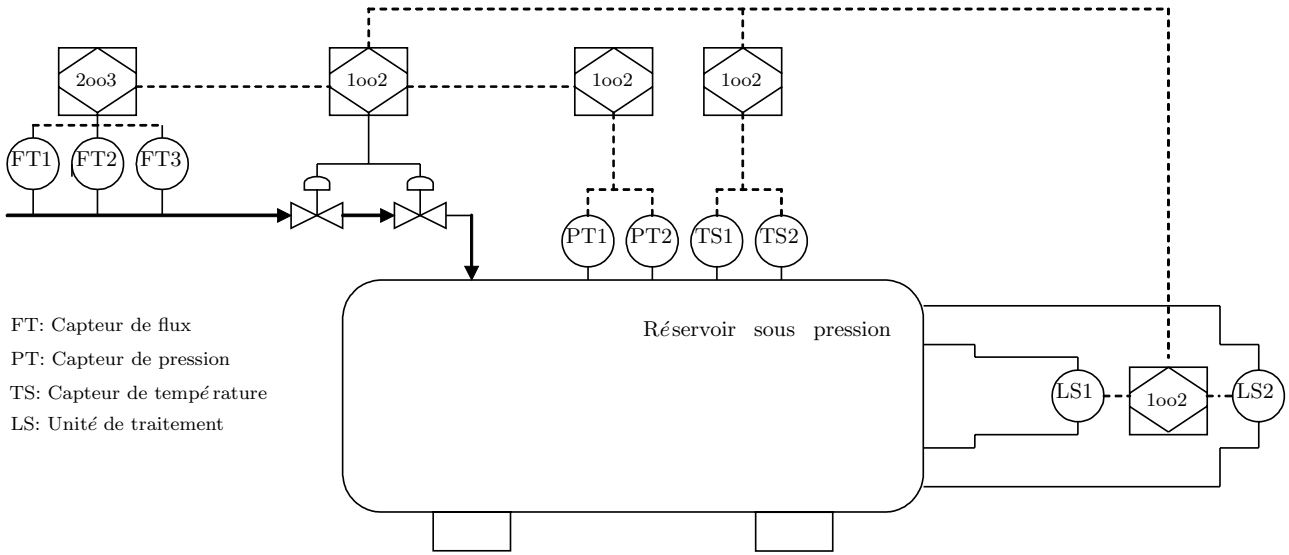
Application

- La norme IEC 61508 fixe le niveau d'intégrité de sécurité (SIL) qui doit être atteint par un SIS qui réalise la Fonction Instrumentée de Sécurité (SIF).

SIL	Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})
1	$[10^{-2}, 10^{-1}[$
2	$[10^{-3}, 10^{-2}[$
3	$[10^{-4}, 10^{-3}[$
4	$[10^{-5}, 10^{-4}[$

SIL	Fréquence des défaillances dangereuses par heure (N)
1	$[10^{-6}, 10^{-5}[$
2	$[10^{-7}, 10^{-6}[$
3	$[10^{-8}, 10^{-7}[$
4	$[10^{-9}, 10^{-8}[$

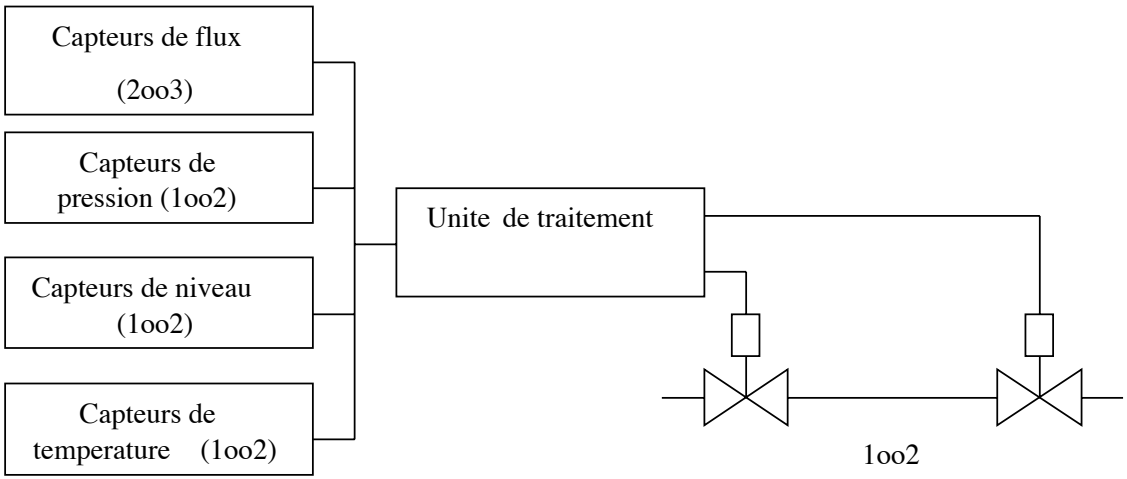
Application



- Système constitué d'un réservoir sous pression contenant un liquide inflammable volatil
- Ce réservoir peut rejeter des gazs dans l'atmosphère : risque acceptable est défini sous forme d'un taux moyen de rejet de gaz de fréquence inférieure à 10^{-4} par an.

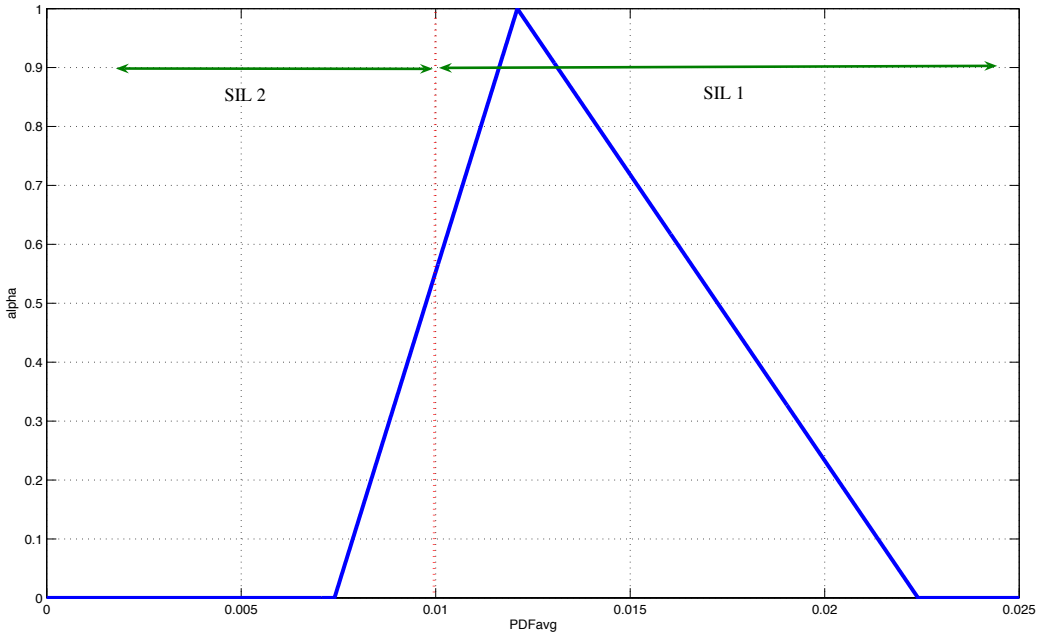
Application

- Une analyse des phénomènes dangereux a indiqué qu'une nouvelle fonction instrumentée de sécurité (SIF) de niveau SIL2 doit être implémentée dans un SIS pour réduire le taux de rejet du réservoir sous pression.
- Objectif : vérifier si le SIS proposé au concepteur est capable de satisfaire à l'exigence SIL 2.



Application

- Obtention de la distribution de la probabilité floue d'occurrence de l'événement sommet : SIL 1 ($PFD_{avg} \in [10^{-2}, 10^{-1}]$) ou un SIL2 ($PFD_{avg} \in [10^{-3}, 10^{-2}]$).
- Facteurs d'importance probabilistes flous pour tenter de réduire cette incertitude.



Sécurité Fonctionnelle : Conception optimale des SIS

- Dans le cadre de la conception des SIS, les fiabilistes assignent aux SIS la réalisation des objectifs de sûreté de fonctionnement (PFD_{avg} ou disponibilité moyenne $A_{avg} = 1 - PFD_{avg}$) dès la phase d'expression du besoin en réduction de risque.
- Cet assignement a pour but, d'une part, d'aider le concepteur à rationaliser ses choix de composants et, d'autre part, de garantir à l'exploitant les objectifs de sûreté de fonctionnement exigés.

- Pouvoir exprimer les exigences de sûreté de fonctionnement au niveau des composants.
- Vérifier que les principes retenus (architecture, concepts technologiques, etc.) sont compatibles avec les exigences de sûreté de fonctionnement émises par les fiabilistes.
- Procéder à la comparaison des concepts envisageables dans l'optique d'une optimisation du coût. Il est certain qu'une stratégie de conception, dont le souci est purement technique, permet d'atteindre les objectifs de sûreté de fonctionnement, mais elle le fait au détriment du coût de conception.
- Par contre, si la stratégie de conception cherche uniquement à réduire le coût de conception, le résultat est un nombre important de défaillances dangereuses et le non respect des objectifs.

1. Définition de l'objectif SIL.
2. Proposition de différents types de composants pour la conception du SIS. Pour concevoir le SIS, les fiabilistes disposent de différents types de composants disponibles sur le marché. Pour chaque composant, nous disposons de son taux de défaillance et de son coût. Un SIS est généralement constitué de trois parties :
   - Partie Capteurs ;
   - Partie Unités de traitement ;
   - Partie Actionneurs.

   Chaque partie pouvant contenir plusieurs composants de différents types placés souvent en parallèle, notre objectif est de choisir les composants de chaque partie et leur connexion qui permettent d'atteindre le SIL exigé avec un coût global minimal.
3. Modélisation de la structure générale du SIS par un réseau de fiabilité.

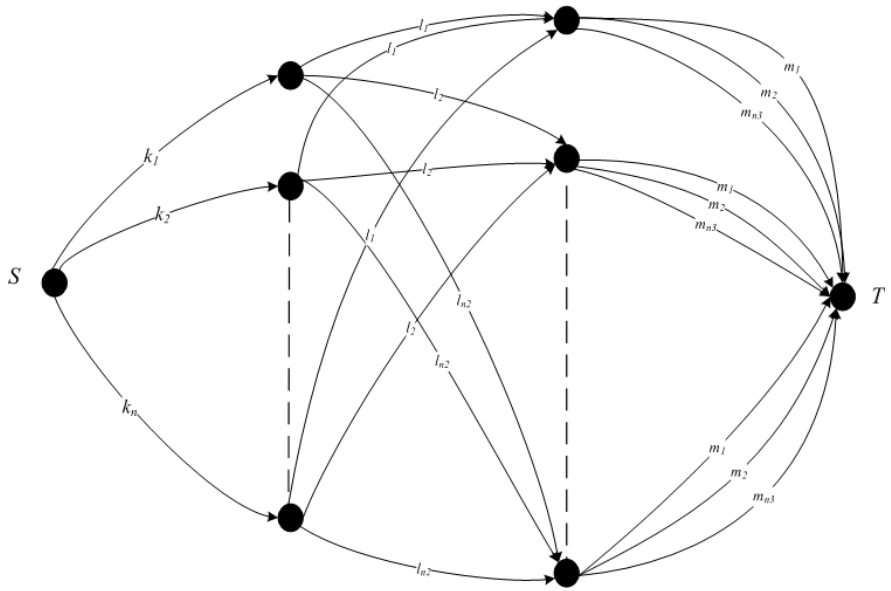


FIGURE – Réseau de fiabilité général d'un SIS

La fonction objectif est donc la somme du coût total des composants et une erreur quadratique moyenne de la disponibilité moyenne du SIS. La fonction objectif est donnée par :

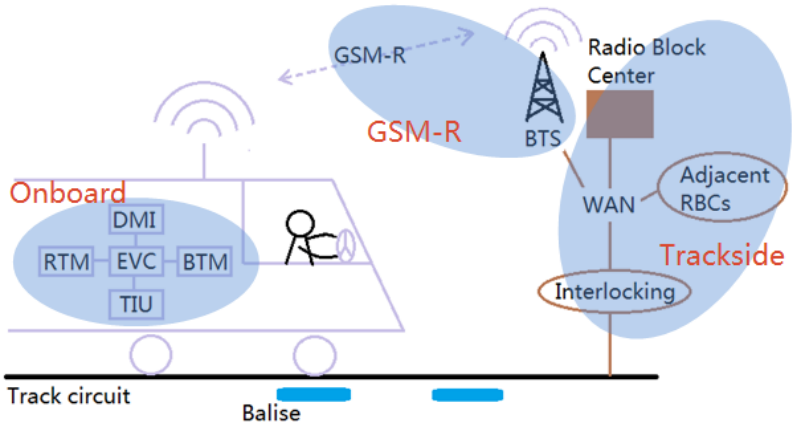
$$f(x) = C(x) + \delta(cmax(\frac{(A_{max}(x) - A_{avg}(x))}{2} + \frac{(A_{avg}(x) - A_{min})}{2})^2)) \quad (1)$$

$$\delta = 1 \quad si \quad A_{avg} \leq A_{min}, \quad et \quad 0 \quad sinon. \quad (2)$$

Évaluation de la SdF des systèmes ferroviaires

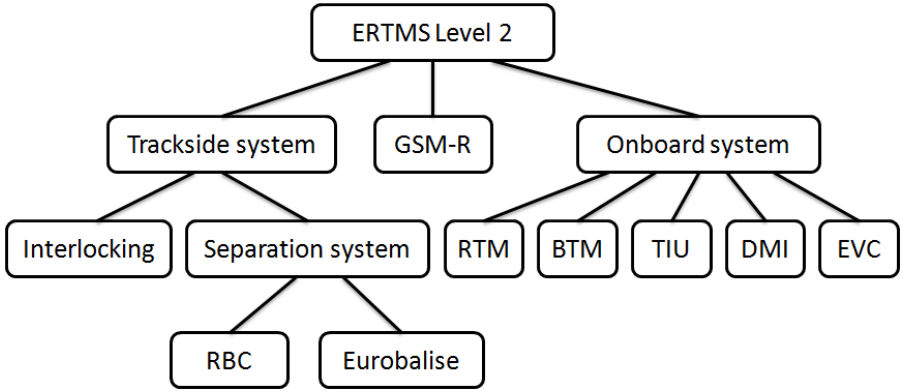
Évaluation de la SdF des ERTMS

- Système Européen de gestion ferroviaire (ERTMS)
  - Système Européen de contrôle des trains (ETCS).
  - GSM-R : sert à communiquer entre les trains et les équipements au sol de gestion du trafic.



- Objectifs
  - Proposition d'un modèle fonctionnel de l'ERTMS niveau 2 ;
  - Modélisation et propagation des incertitudes.
  - Évaluation de la disponibilité de l'ERTMS niveau 2 et du respect des exigences RAM des normes ;

1ère Application : Évaluation de la SdF des ERTMS



- « ERTMS/ETCS RAMS Requirements Specification », 1998.
- « Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 », 2009.

		Indisponibilité
Onboard	Kernel	<1E-6
	Odometer	<1E-7
Lineside	Balise	<1E-7
	LEU	<1E-7
Trackside	RBC	<1E-6

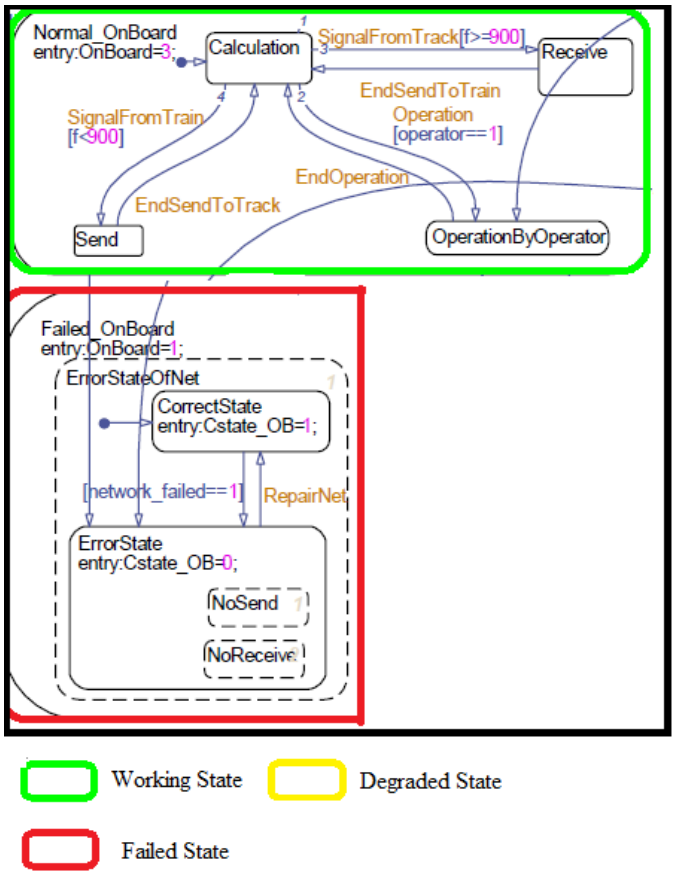
Objectif de disponibilité

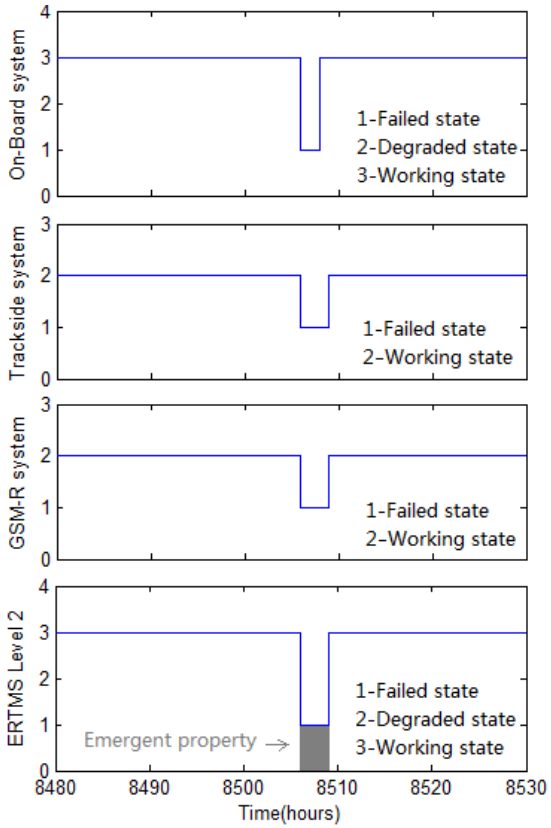
Exigence RAM : La disponibilité opérationnelle due à toutes les causes de défaillances ne doit pas être inférieure à 0.99973

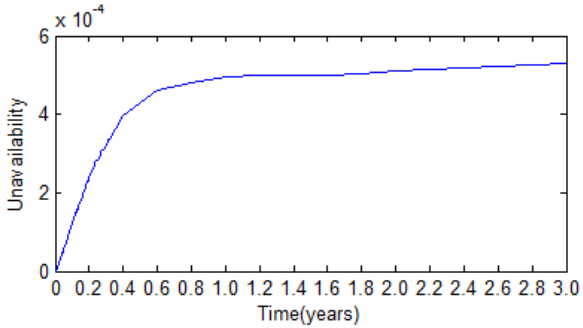
Évaluation de la SdF des ERTMS

Modèle Statechart de l'ERTMS

- Description des états de chaque sous-système de l'ERTMS et les communications entre ces systèmes.



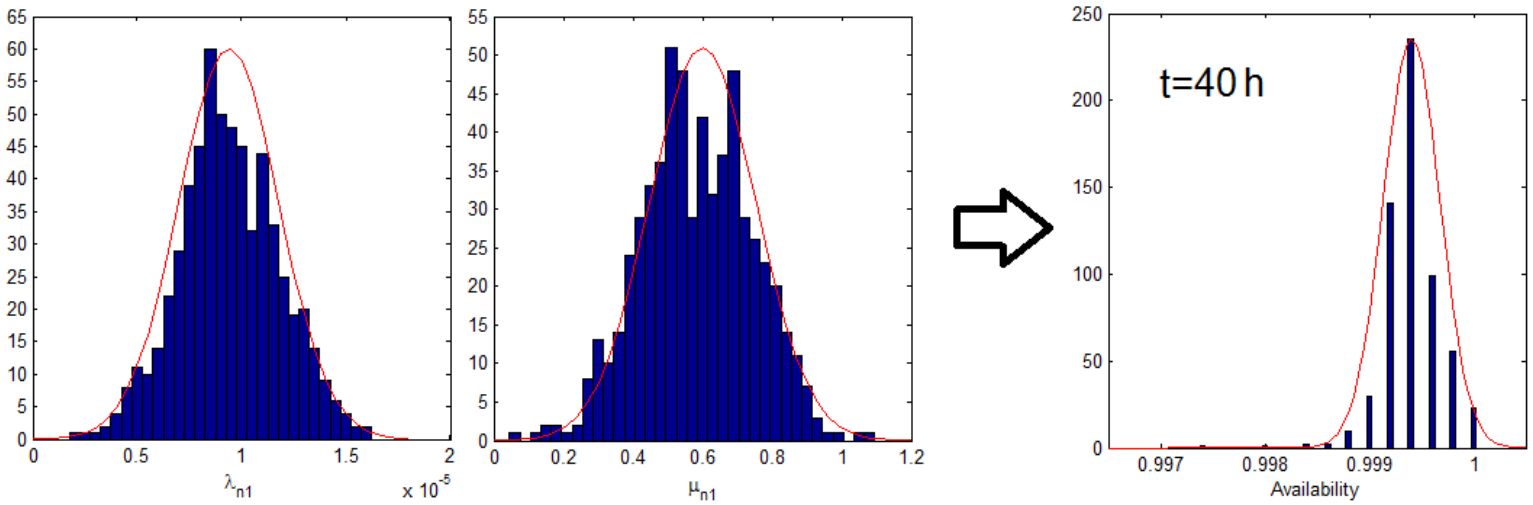




Évaluation de la SdF des ERTMS

Prise en compte des incertitudes paramétriques dans le modèle Statechart

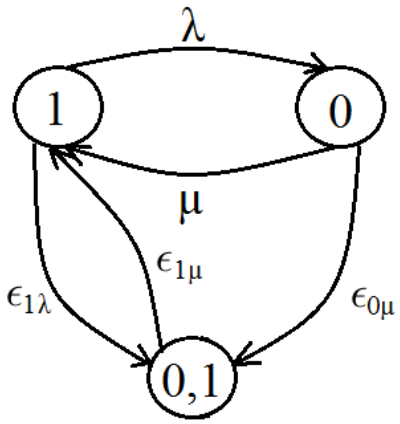
- Modélisation de l'imprécision des taux de transition $\lambda \in [\underline{\lambda}, \overline{\lambda}]$ et $\mu \in [\underline{\mu}, \overline{\mu}]$.
- Simulation Monte-Carlo à deux niveaux
  - Boucle extérieure : Tirage des taux de transition (λ, μ) modélisés par des distributions de probabilité : Uniforme et normale.
  - Boucle intérieure : Exécution du modèle.

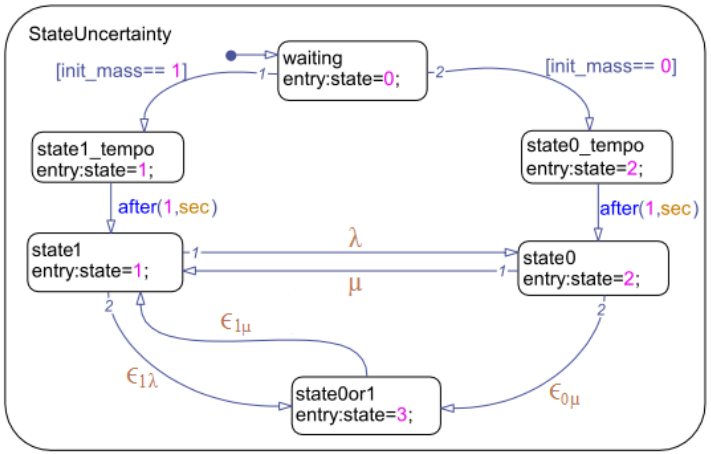


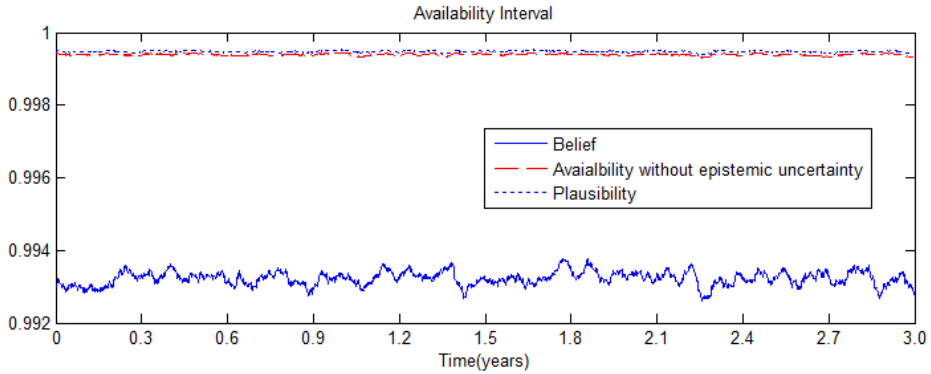
Évaluation de la SdF des ERTMS

Introduction d'états incertains dans le modèle Statechart

- État incertain fictif pour représenter l'incertitude sur l'état du système (fonctions de croyance + Statecharts).







Évaluation de la SdF des ERTMS par le modèle Statechart

Conclusions

- les Statecharts constituent un modèle intéressant pour la modélisation fonctionnelle des systèmes de signalisation ferroviaires : facilité de construction, régions orthogonales, modèles plus réduits.
- Un ensemble de modèles fonctionnels des sous-systèmes de l'ERTMS a été développé avec l'outil Stateflow de Matlab.
- Une méthodologie de modélisation des incertitudes a été développée pour l'évaluation de la SdF de l'ERTMS niveau 2.

Conclusion

- Ne pas hésiter à demander aux experts des intervalles (ou les valeurs les plus probables) de données de fiabilité (taux de défaillance, ...).
- Appliquer les théories de l'incertain dans les études de SdF.
- Proposer des méthodes innovantes pour la gestion et la propagation des incertitudes.
- Fournir l'aide à la décision dans l'interpretation des résultats quantitatives de la SdF.
- Beaucoup de travail reste à faire dans ce domaine.

Merci pour votre attention !

https ://www.hds.utc.fr/~sallakmo/

Contact : mohamed.sallak@utc.fr