

Argumentaires de sûreté : comment formaliser les évaluations des experts avec la méthode SERENE

Marc BOUISSOU

Marc.Bouissou@edfgdf.fr

EDF

Electricité de
France

DER/RNE/ESF/DESF

Plan de l'exposé

- Les difficultés d'évaluation des systèmes critiques
- La méthode SERENE
- Conclusion

Comment maîtriser la SdF d'un système programmé ?

- La situation est très différente suivant le niveau d'exigences sur le système :
 - faible -> avoir un bon processus de production, + analyse statistique, pour mesurer et extrapoler la croissance de fiabilité
 - élevé -> le seul moyen est d'agir sur le processus de production du système, et d'utiliser des techniques de tolérance aux fautes

Systemes critiques : des efforts de test irrealisables...

- Tous les modeles de croissance de fiabilite font l'hypothese que, au moins en moyenne, le taux de defaillance du logiciel decroit
OR
- Effet de discontinuite -> il n'est pas admissible de supposer que le systeme est meilleur apres une correction qu'avant : **l'extrapolation n'est plus permise dans le cas des systemes critiques**
- => il ne faut tenir compte que du temps de fonctionnement sans aucune defaillance depuis la derniere correction
or, si on observe un temps T sans defaillance, $\lambda = -\ln(\epsilon)/T$ est la valeur du taux de defaillance (suppose constant) telle que l'on ait une proba $(1-\epsilon)$ d'observer au moins une defaillance sur une duree T.
- avec $\epsilon = 0,01$, $\lambda = 4,6 / T \iff$
il faut $T = 4,6 \cdot 10^n$ pour «demontrer» un taux en 10^{-n}

Autres problèmes liés au test statistique

- Injection de données choisies aléatoirement dans le domaine des entrées du logiciel
- Le test doit être représentatif (distribution des entrées) des conditions réelles d'exploitation
- Cela peut être difficile à réaliser
- Problème de l'oracle :
 - comment valider les résultats d'un test ?
 - écriture d'un autre programme -> celui-ci peut contenir des erreurs
 - problème des erreurs de spécification

L'évaluation du système programmé accorde donc beaucoup d'importance aux points suivants

- qualité du processus de développement (techniques employées, expérience de l'équipe ...)
- méthodes formelles :
 - en tant que processus de développement,
 - en tant que preuve de propriétés
- évaluation par AMDEC (AEEL), arbres de défaillances, réseaux de Petri...
- tolérance aux fautes (redondance, codage des données, programmation en N versions, points de reprise, traitements d'exception...)
- élimination des fautes (V&V)
- **en pratique, c'est un expert qui décide, en fonction de toutes ces informations, si le système peut être mis en exploitation, via un raisonnement informel**

Comment modéliser toutes les influences des facteurs identifiés?

- influences non déterministes :
 - facteurs -> produit
- pas de retour d'expérience quantitatif, mais des experts
- => modélisation par réseau bayésien bien adaptée
- c'est la solution pronée par le projet Esprit **SERENE**
(SafEty and Risk Evaluation using bayesian Nets)

Utilisations possibles du modèle

- Un R.B. permettra de donner des estimations d'autant plus précises que l'on aura plus de données sur le système évalué
- Il pourra servir dès les premières phases (spécifications) pour donner des premières tendances
- On pourra simuler l'impact de différents processus de développements et en choisir un qui satisfaira les objectifs que l'on se fixe
- En fin de développement, aide à l'élaboration d'un argumentaire de sûreté, et outil de dialogue avec les autorités de sûreté

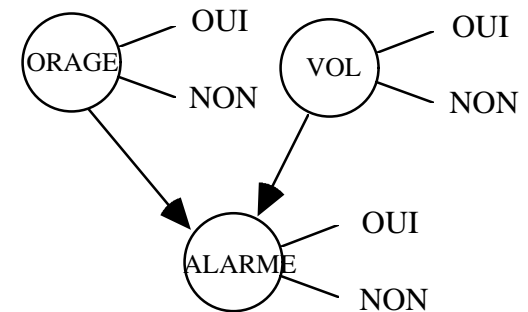
Présentation des réseaux bayésiens : exemple introductif

- Mr X possède une superbe PEURONO, qu'il a munie d'une alarme. Hélas, cette alarme est sensible aux orages, et se déclenche souvent intempestivement lors de coups de foudre. Comment modéliser mathématiquement les raisonnements intuitifs suivants ?
- si Mr X voit quelqu'un en train de forcer la porte de sa PEURONO, il s'attend à un déclenchement de l'alarme,
- s'il y a de l'orage, et si l'alarme se déclenche, Mr X attribuera le déclenchement à une fausse alerte,
- si Mr X est réveillé en pleine nuit par l'alarme, son premier réflexe va être de penser qu'il y a de l'orage, car les vols sont rares dans son quartier. Si il n'y en a pas, il va sortir dans la rue et aller voir si sa voiture n'est pas victime d'un vol.

Définition d'un Réseau Bayésien

Un R.B. est un graphe acyclique, tel que :

- 1 noeud \leftrightarrow 1 variable aléatoire discrète (ici, 2 valeurs possibles)
- + (pour noeuds sans parent) une loi de probabilité
- ensemble des arcs pointant sur 1 noeud \leftrightarrow 1 table de probabilités conditionnelles
- Le R.B. est formellement correct dès lors que l'état d'un noeud, conditionnellement à l'état de ses noeuds parents, est indépendant des autres noeuds du réseau.
- ex : soit un noeud parent du noeud "VOL", tel que le taux de délinquance dans le quartier. Mais la probabilité que l'alarme se déclenche, conditionnellement à la présence (ou absence) de vol et/ou d'orage, est indépendante de l'état du noeud "taux de délinquance"



Données quantitatives pour le réseau de l'exemple

- $p(\text{ORAGE}=\text{OUI}) = 0.1$ $p(\text{VOL}=\text{OUI}) = 0.001$,
- $p(\text{ALARME}=\text{OUI} / \text{ORAGE}=\text{OUI}, \text{VOL}=\text{OUI}) = 0.97$,
- $p(\text{ALARME}=\text{OUI} / \text{ORAGE}=\text{OUI}, \text{VOL}=\text{NON}) = 0.1$,
- $p(\text{ALARME}=\text{OUI} / \text{ORAGE}=\text{NON}, \text{VOL}=\text{OUI}) = 0.96$
- $p(\text{ALARME}=\text{OUI} / \text{ORAGE}=\text{NON}, \text{VOL}=\text{NON}) = 0.01$

- Les probabilités pour ALARME = NON sont les complémentaires des précédentes.

Interprétation d'un Réseau Bayésien

- Un RB = *une* représentation *concise* de la **loi conjointe** sur l'ensemble des variables aléatoires du réseau. Cette loi est l'information la plus complète que l'on puisse avoir sur l'ensemble des variables aléatoires considérées, et leurs inter-relations.
- **loi conjointe** = $\{ p (X_1 = V_1 , X_2 = V_2 , \dots , X_n = V_n) \}$
où V_1, V_2, \dots, V_n prennent toutes les combinaisons de valeurs possibles pour les X_i ($X_i =$ V.A. associée au noeud i du RB).
- *une* : la relation entre les faits "pair" et "égal à 6" pour le résultat d'un jet de dé peut se représenter par :
pair -> **égal à 6**, $p(\text{pair})=1/2$, $p(\text{égal à 6} \mid \text{pair}) = 1/3$, $p(\text{égal à 6} \mid \text{impair}) = 0$
ou bien par :
égal à 6 -> **pair** , $p(\text{égal à 6}) = 1/6$, $p(\text{pair} \mid \text{égal à 6}) = 1$, $p(\text{pair} \mid \text{non égal à 6}) = 2/5$
- *concise* :
 - Ex d'un RB dans lequel tout noeud est binaire, et a 2 parents, sauf P noeuds initiaux : on représente la loi conjointe par $4(N - P) + P$ nombres, au lieu de 2^N

Application des réseaux bayésiens dans le cadre du projet SERENE

- méthode + outil SERENE = moyen de construire rapidement un réseau bayésien modélisant un "argumentaire de sûreté" relatif à un système programmé critique
- NB : argumentaire de sûreté (safety argument) est la partie "synthèse" et raisonnement s'appuyant sur l'ensemble des informations (safety evidence) relatives au produit

Argumentaire de sûreté utilisant un RB

Sources d'information

Hazard
Analysis

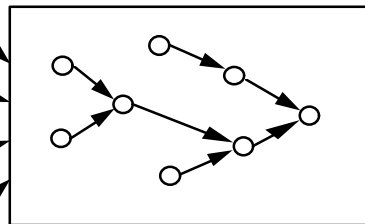
Software
Testing

Hardware
Reliability

Design
Review

⋮

Argumentaire de sûreté



Prediction
de sécurité

Facteurs hors système

Decision de mise en service

EDF

Electricité de
France

DER/RNE/ESF/DESF

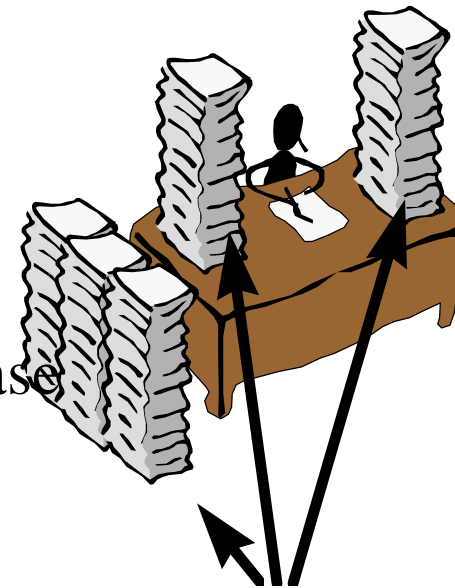
Information disponible (vers la fin du cycle de vie)

audits sur processus :

- specification
- design
- developpement
- activité de validation pour chaque phase

documentation technique

resultats de tests ...



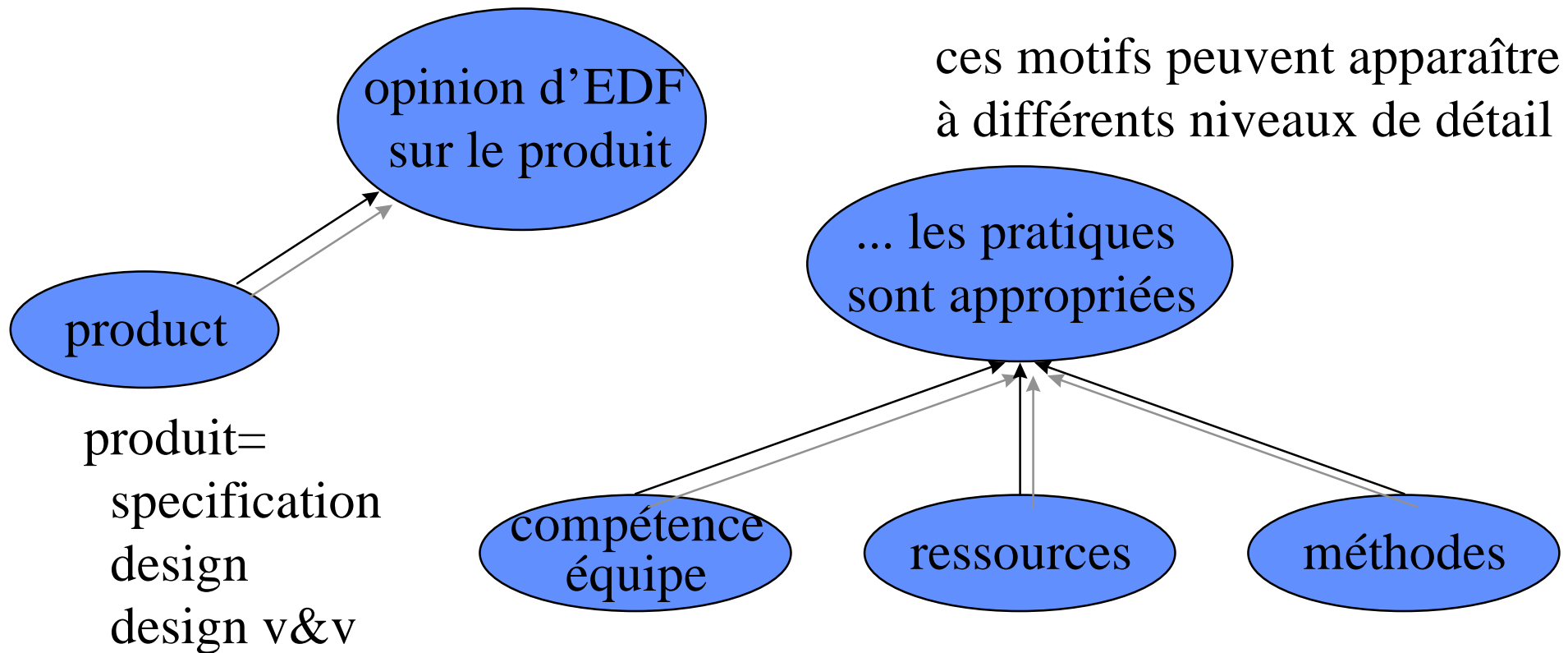
Sources d'information

EDF

Electricité de
France

DER/RNE/ESF/DESF

Identification de «motifs» répétitifs



EDF

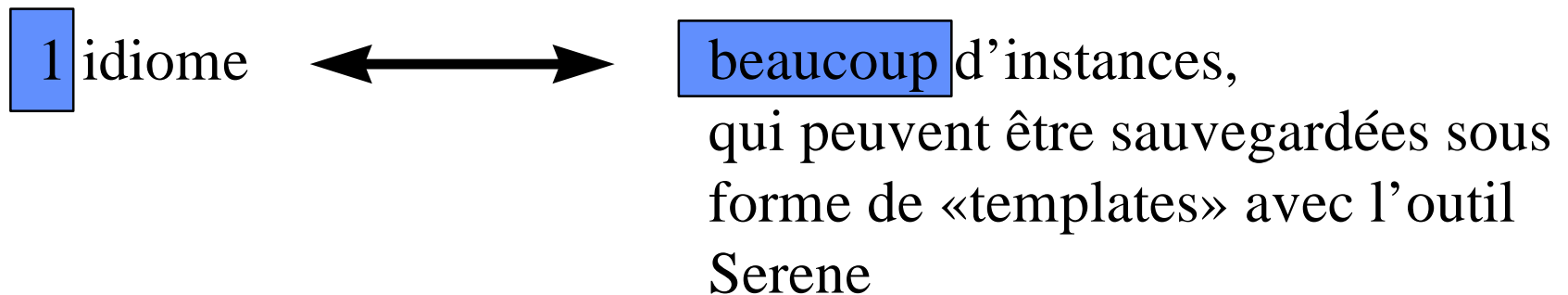
Electricité de
France

La méthode Serene introduit le concept d' «idiome»

DER/RNE/ESF/DESF

Qu'est ce qu'un idiome ?

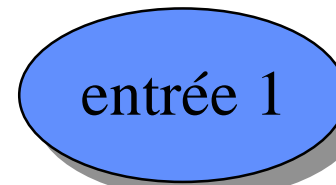
- résume une classe de raisonnements typiques dans un argumentaire de sûreté
- concept abstrait:
pas de réalisation informatique directe



L'idiome processus-produit

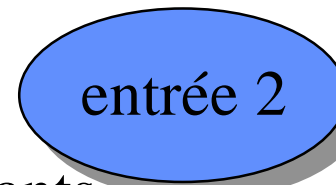


ex :
design

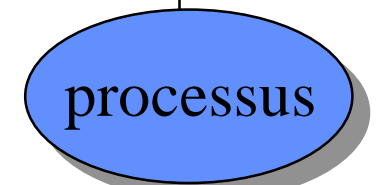


ex :
développement

ex :
composants
réutilisés



ex :
pratiques de
développement

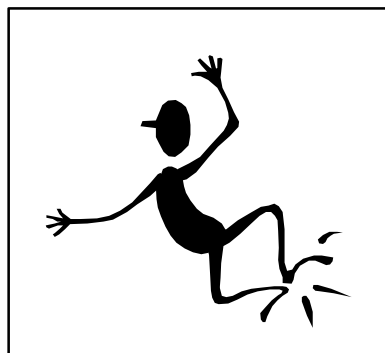


EDF

Electricité de
France

DER/RNE/ESF/DESF

L'idiome «mesure»



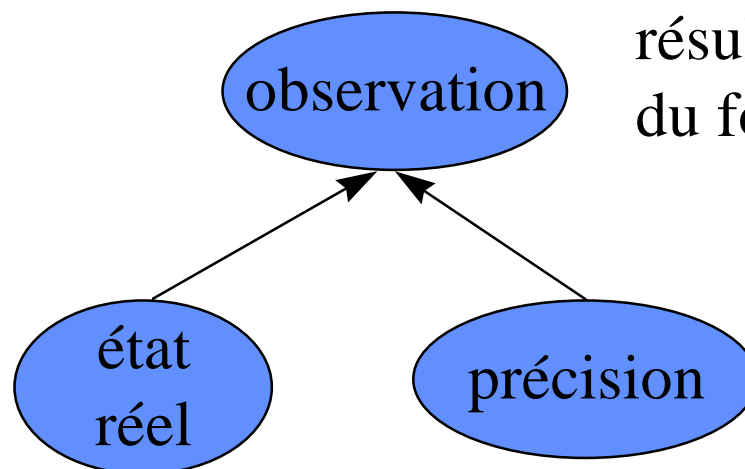
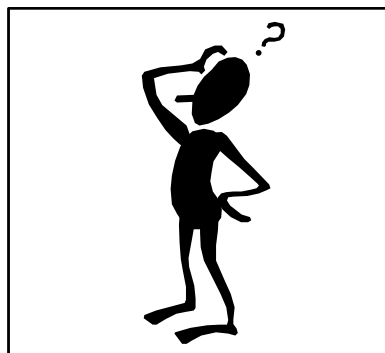
résultats des tests
du fournisseur

EDF

Electricité de
France

DER/RNE/ESF/DESF

L'idiome « mesure »



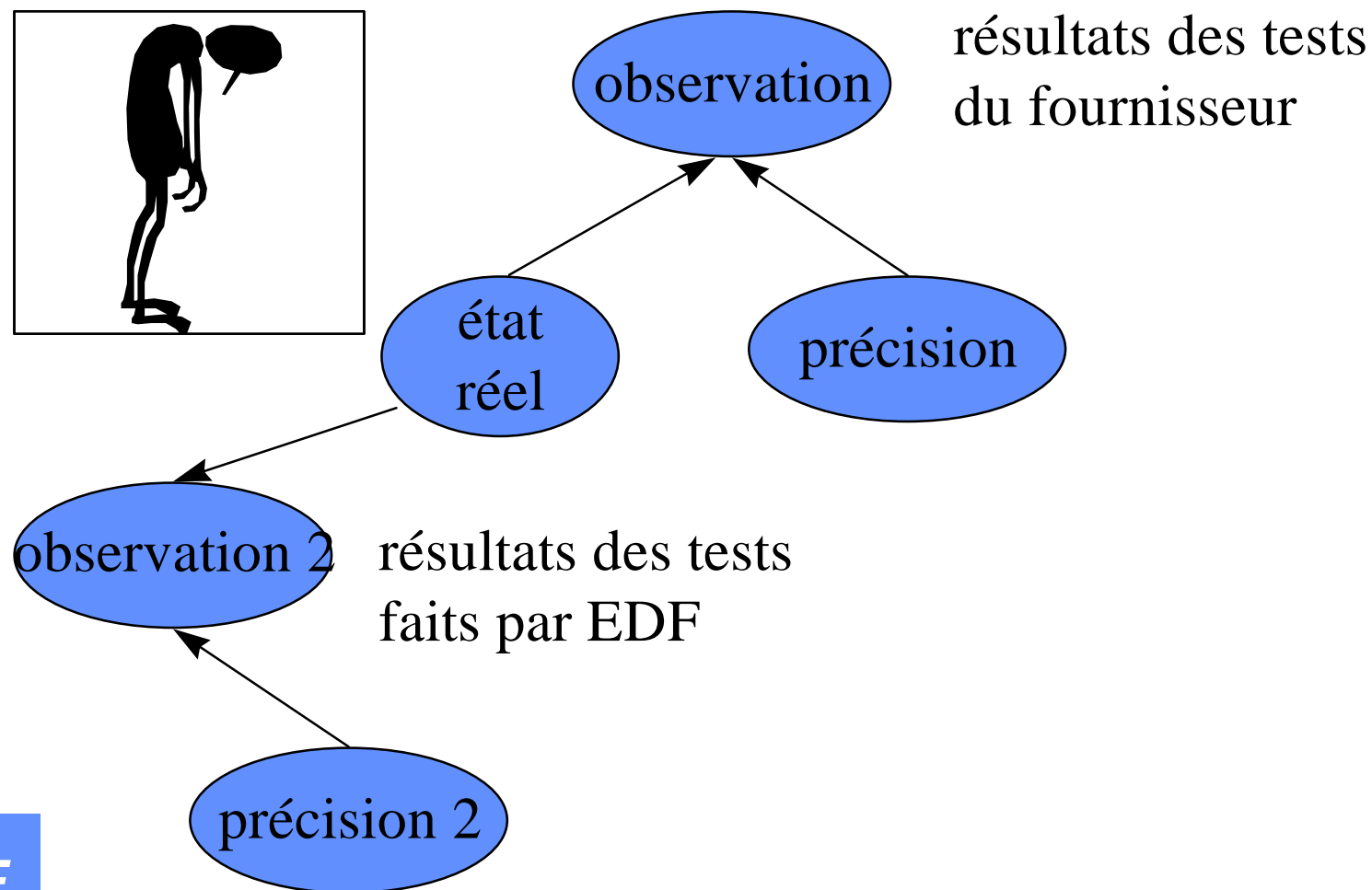
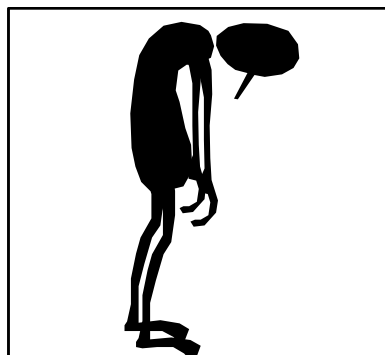
résultats des tests
du fournisseur

EDF

Electricité de
France

DER/RNE/ESF/DESF

L'idiome « mesure »



EDF

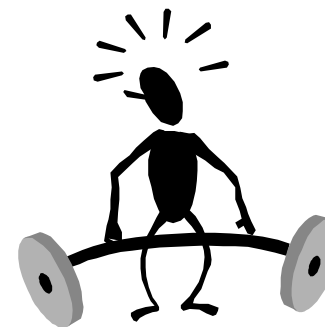
Electricité de
France

DER/RNE/ESF/DESF

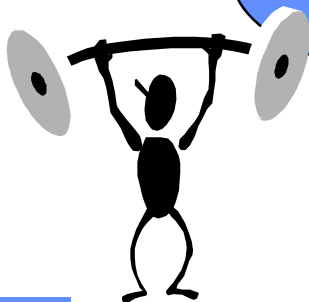
L'idiome expérience historique

ex : compétence
de l'équipe sur
la tâche 2

attribut de l'entité 2
à la date $S' > S$

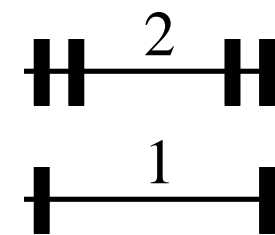


attribut de l'entité 1
à la date S



ex : compétence
de l'équipe sur
la tâche 1

degré de similitude
entre 1 and 2



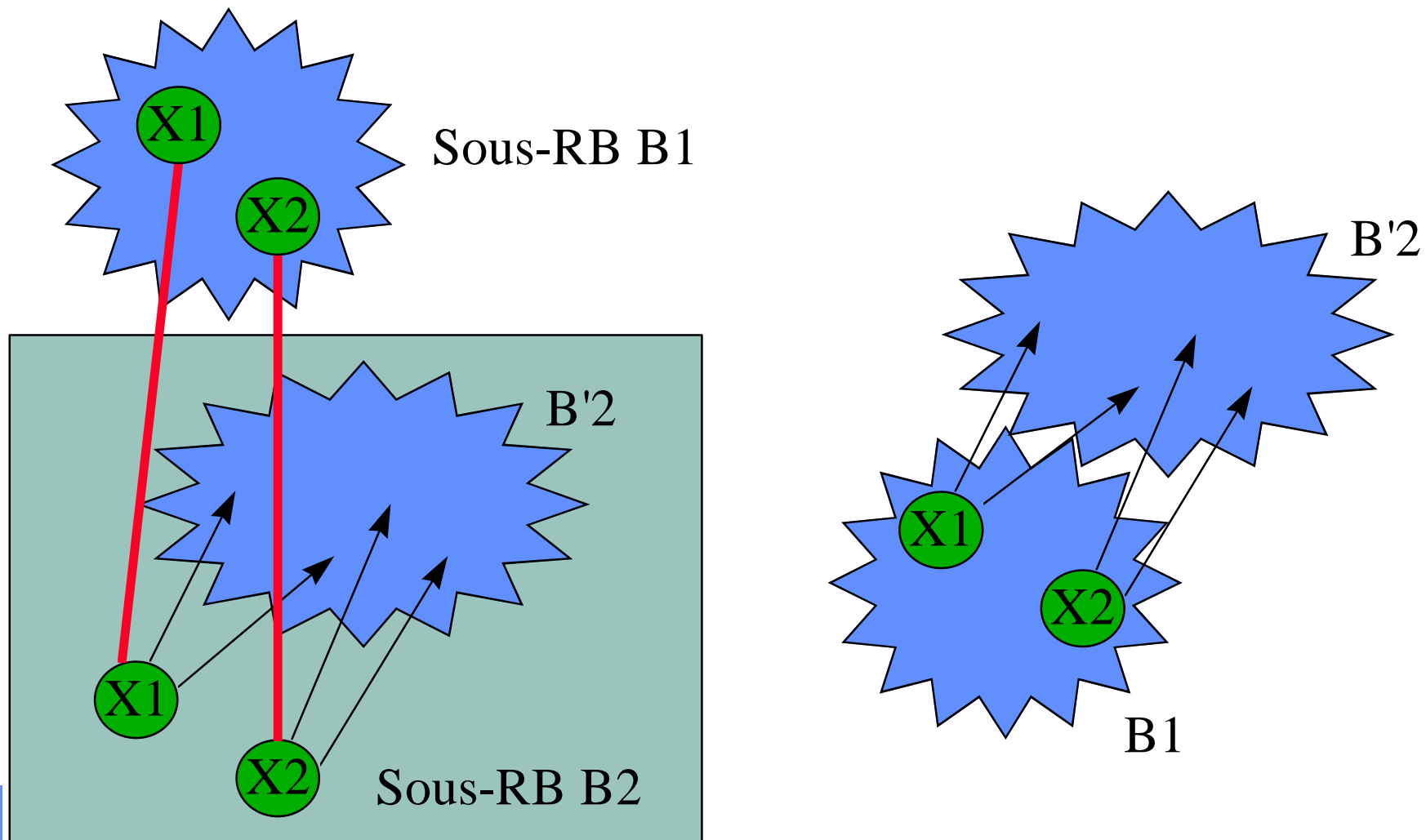
ex : similitude des tâches 1 et 2

EDF

Electricité de
France

DER/RNE/ESF/DESF

L'opération de jonction automatisée



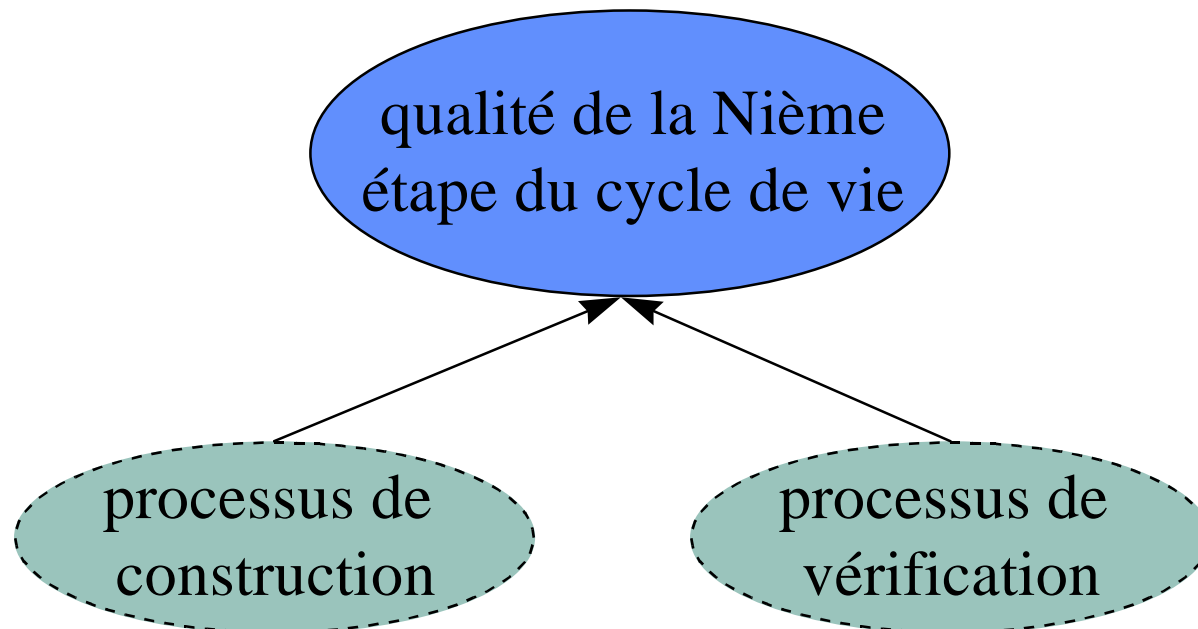
EDF

Electricité de
France

DER/RNE/ESF/DESF

Structure hiérarchique d'un argumentaire de sûreté en RB

concept de noeuds abstraits, possible grâce à la jonction automatisée
ex :



Récapitulation

- la méthode Serene est fondée sur deux mécanismes
 - une décomposition top-down : des noeuds abstraits (qui représentent des sous-arguments) aux noeuds concrets
 - un mécanisme d'assemblage entre idiomes
- ces deux mécanismes seront supportés par l'outil Serene

Elicitation des tables de probabilités des noeuds (NPT)

- quelques choix pragmatiques pour réduire le temps d'élicitation des NPTs
 - 2 états pour chaque noeud : oui et non
 - Probabilités: 0 - 0.25 - 0.5 - 0.75 - 1
- valeurs 0 et 1 modélisent des relations déterministes => signifient en fait "proche de 0/1"

Exemple de table de probabilités pour un noeud

| | | | | | | | | |
|---|---|-----|-----|---|-----|----|---|---|
| Les méthodes de vérification de la spéc. sont appropriées. | O | | | | N | | | |
| Les experts du fournisseur sont compétents pour cette tâche | O | | N | | O | | N | |
| Cette tâche bénéficie de ressources suffisantes | O | N | O | N | O | N | O | N |
| La vérification de la spéc. par le fournisseur est correcte | 1 | .75 | .25 | 0 | .75 | .5 | 0 | 0 |

Est ce que la vérification de la spécification par le fournisseur est correcte ?

EDF

Electricité de
France

DER/RNE/ESF/DESF

Conclusion

- Techniques de quantification de la fiabilité des systèmes programmés les plus mûres :
 - fondées sur l'approche statistique (analyse du REX),
 - utilisables seulement pour des exigences modestes
- L'évaluation de la sécurité des systèmes programmés critiques est un exercice :
DIFFICILE, mais NECESSAIRE
- Projet Européen SERENE : réseaux bayésiens
 - combinaison de jugements de différentes natures
 - pondérations explicites -> outil de dialogue entre experts

Pour en savoir plus...

- Journée du 26 janvier 1999 à la Défense
- Organisateurs :
ISDF, EDF, Objectif Technologie
- Programme détaillé disponible auprès de
l'ISDF : tél 01 55 17 47 91

EDF

Electricité de
France

DER/RNE/ESF/DESF