ECOLE DOCTORALE IAEM LORRAINE

Évaluation dynamique d'indicateurs de sûreté de fonctionnement d'une architecture de contrôle-commande tout au long de son cycle de vie.

BOYER Grâce

Directeur de thèse : PETIN Jean-François

Co-directeur de thèse : BRÎNZEI Nicolae

Contexte

- Thèse CIFRE en collaboration avec Schneider Electric
- **Objectif** : évaluation des indicateurs/performances de sûreté de fonctionnement (SdF) d'une architecture d'automatisation dans un contexte incertain d'avant-vente.

Problématique industrielle

- **Données d'entrées**
  - Description en phase d'appel d'offre des besoins du client (fonctions d'automatisation et performances en termes de disponibilité-fiabilité que l'architecture doit atteindre),
  - Expertise Schneider sur les éléments solutions d'architectures.
- **Pratiques actuelles**
  - Analyse statique des indicateurs SdF (diagrammes de fiabilité),
  - Pas de prise en compte des phénomènes liés aux contexte d'utilisation, vieillissement, à la charge des équipements.
- **Besoin industriel**
  - Pratiques actuelles : écarts par rapport à la réalité ou surdimensionnement (redondance) et test de ces performances pour chaque proposition d'architecture (coût élevé en termes de moyens matériels, humains et en temps),
  - Fournir des méthodes/outils en phase d'avant-vente pour évaluer les performances des architectures d'automatisation en :
    - réduisant les risques de sur ou sous dimensionnement et les écarts,
    - intégrant l'aspect dynamique (contexte, vieillissement…)

Problème scientifique

- **Incertitude sur la définition de l'architecture**
  - Caractéristiques des architectures non spécifiées en détail,
  - Sollicitations inconnues et souvent de nature aléatoire.
- **Processus de dégradation et données fiabilistes des composants**
  - Nécessité de modéliser le processus de dégradation à partir du taux de défaillance, du type de dégradation et des connaissances sur le composant (hypothèses définies avant la modélisation),
  - Nécessité de modéliser les interactions entre les composants pour déterminer les conséquences des défaillances sur l'architecture.
- **Construction des modèles dynamiques de SdF transparente pour le concepteur en avant-vente**
  - Absence d'expertise pour la construction de tels modèles,
  - Nécessité d'évaluer plusieurs architectures candidates.

État de l'art

Méthodes analytiques

Diagramme de fiabilité, arbre de défaillances *approches non compatibles avec la prise en compte des aspects dynamiques des architectures et de leurs performances.*

Chaine de Markov
analyses analytiques limitées à des distributions exponentielles et problème d'explosion sur des architectures industrielles

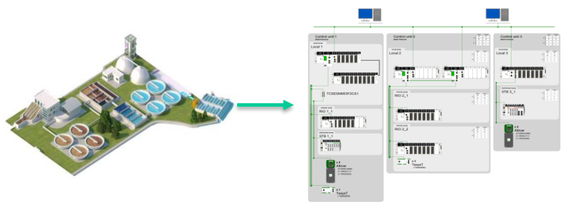
Méthodes par simulation

Réseaux de Petri (RdP) colorés et stochastiques
Modularité et hiérarchie, possibilité de définir des composants d'architecture génériques et paramétrables.
Simulation de Monte Carlo (MC) et évaluation statistique des indicateurs de SdF

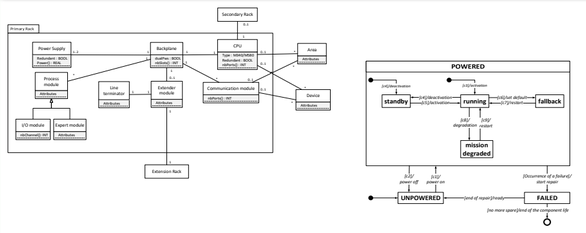
Approche proposée

- Spécification du besoin et des architectures sous forme de modèles UML (diagrammes d'états, de classe et de séquence),
- Instanciation automatique d'un modèle dynamique en RdP colorés et stochastiques à partir :
  - d'une bibliothèque de composants d'architecture RdP paramétrables et réutilisables regroupés en famille (CPU, module d'alimentation, support, module de communication, module d'entrée-sortie, …),
  - de la description d'une architecture donnée et de règles d'instanciation définies en UML.
- Evaluation des performances obtenues par simulation MC et une estimation statistique post-simulation.

Description informelle architecture candidate

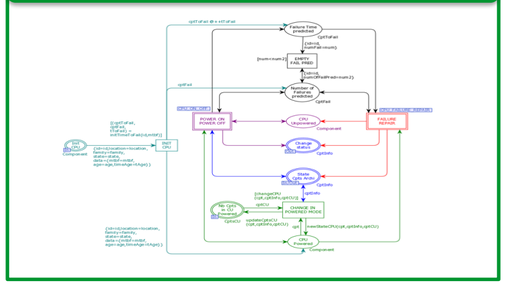


Diagrammes UML spécifications architecture

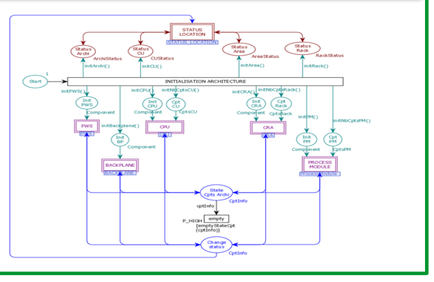


Instanciation automatique

Modèle RdP composants architecture

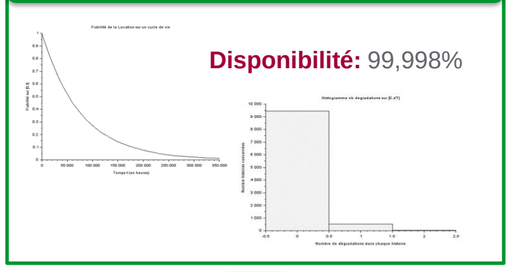


Modèle RdP structure architecture



Simulation de Monte Carlo

Performances SdF architecture



Prise de décision

Validation de l'architecture ou préconisation de modification

Perspectives des travaux

- Intégration des phénomènes induits par le contexte d'usage et le vieillissement
- Calculs de facteurs d'importance relatif à l'impact des composants sur la disponibilité de l'architecture
- Intégration de l'approche dans les outils Schneider Electric

Publications

- G. Boyer, J.F Pétin, N. Brînzei, J. Camerini, and M. Ndiaye (2019). Toward generation of dependability assessment models for industrial control system, *Information and Digital Technologies 2019, IDT 2019*, Slovakia, pp 40-49.
- G. Boyer, N. Brînzei, P. Do and J. Pétin, "Reliability modelling and assessment by joint consideration of Petri nets and gamma deterioration processes," *2017 2nd International Conference on System Reliability and Safety (ICSRS)*, Milan, 2017, pp. 57-61.