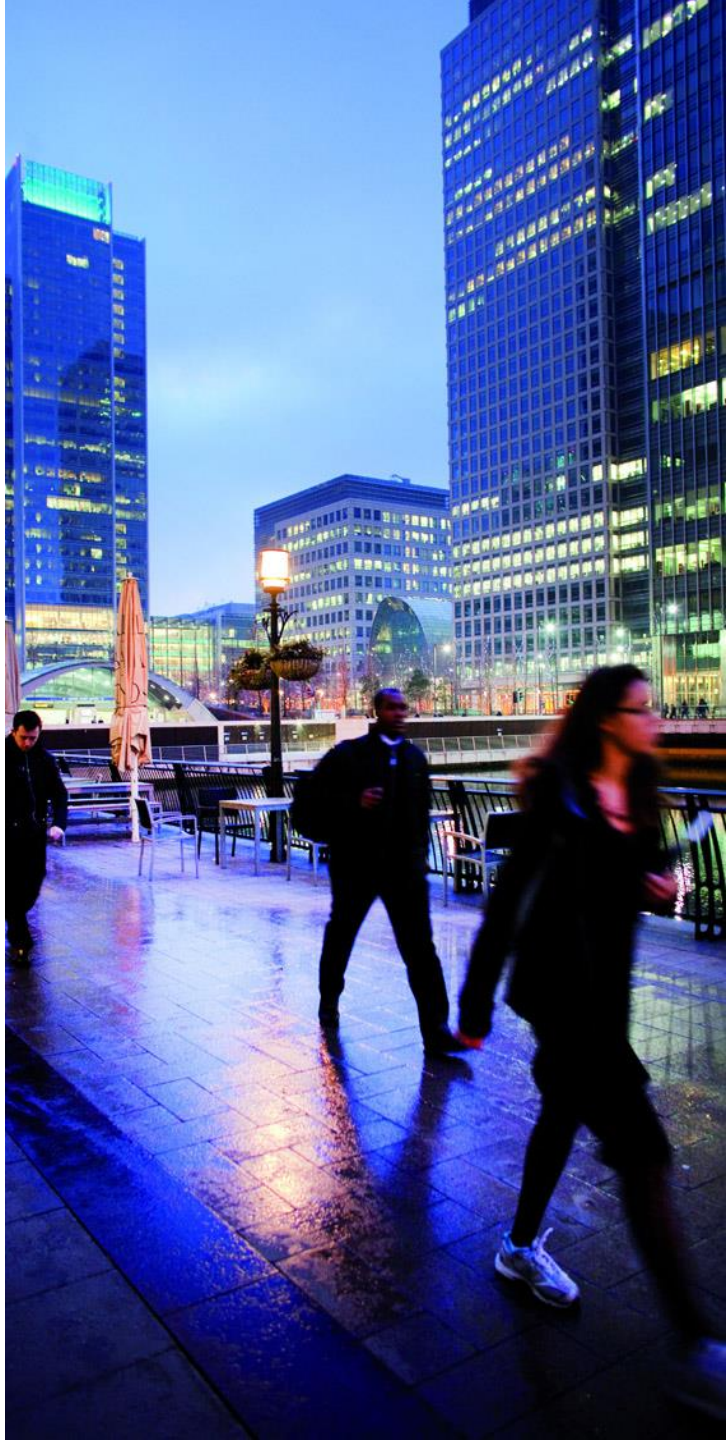
Ingénierie Système Assistée par la Modélisation et la Simulation (ou la Vérification Formelle)

FormReq21
28 Mai 2021

Thuy NGUYEN
thuy.apt@orange.fr



Qui Suis-Je ?

- **Retraité d'EDF R&D à partir du 1er Juin 2021**
- **Expérience professionnelle**
  - Logiciel et systèmes programmés
    - Compilateurs, systèmes temps réel distribués, logiciels de CAO et CFAO, ...
  - Depuis 1994 à EDF : systèmes de contrôle-commande (CC) importants pour la sûreté
    - Vérification formelle, normes internationales, FPGA, architectures globales
    - Retour d'expérience : l'inadéquation des exigences cause plus d'incidents que les erreurs de programmation
- **Depuis 2007, pour mieux garantir l'adéquation des exigences des systèmes de contrôle-commande :**

  Ingénierie des systèmes socio-techniques et cyber-physiques, et des systèmes de systèmes

  (*centrales électriques, réseaux énergétiques nationaux ou continentaux*)

  assistée par la modélisation (formelle) et la simulation

  tout au long du cycle de vie

  depuis les phases conceptuelles d'avant-projet jusqu'à l'exploitation et le démantèlement

Mes Travaux et Réflexions en Cours

- **Peu satisfait des méthodes en vogue**
  - SysML, use cases, ... : peu simulables, peu rigoureux ➔ difficulté à traiter en détail les grands systèmes critiques
  - Les systèmes physiques ne sont pas des logiciels
  - Peu d'attention portée sur le fond et l'adéquation des exigences
    - Qui contiennent presque toujours des erreurs, avec parfois des conséquences catastrophiques
  - Pour les systèmes physiques, l'ingénierie des exigences est inséparable de la conception
    - Qui consiste à placer des exigences sur les sous-systèmes
  - La couverture du cycle de vie est souvent factice
    - Modèles ne servant qu'une petite partie du cycle de vie et non tenus à jour
- **BASAALT (Behaviour Analysis and Simulation All Along Life Time) : une méthode d'ingénierie système focalisée sur les aspects dynamiques des systèmes**
- **FORM-L (FOrmal Requirements Modelling Language) : un langage de modélisation en support de BASAALT**
- **Environnements de justification (Justification Frameworks) : pour structurer les chaines de raisonnement mélant aspects rigoureux (formalisables) et aspects subjectifs (non formalisables)**
  - Justification des hypothèses et des choix de solution
  - Plus informatifs que de simples liens de traçabilité