Spécification formelle de systèmes cyber-physiques et Ingénierie système assistée par la simulation

Thuy Nguyen*[1]

[1]EDF – EDF – France

Résumé

La méthode BASAALT (Behaviour Analysis and Simulation All Along systems Life Time) a été concçue pour aider l'ingénierie des systèmes cyber-physiques et socio-techniques complexes, ainsi que des grands systèmes de systèmes . Elle s'intéresse aux comportements et autres phénomènes dynamiques comme la sûreté de fonctionnement et les coûts d'exploitation, et part du principe que pour pour ce type de systèmes, un support outillé important est nécessaire : comme pour les logiciels, la seule inspection manuelle des modèles ne permet pas de révéler la plupart de leurs défauts, et le test / simulation ou la vérification formelle sont des aides précieuses. Pour cela, les exigences et les solutions doivent être modélisées formellement, dans un langage compréhensible par les personnes impliquées.

FORM-L (FOrmal Requirements Modelling Language) est le langage de modélisation de BASAALT. C'est un langage de contrainte non déterministe qui peut être utilisé dès les phases les plus en amont du cycle de vie et qui permet d'éviter la surspécification inhérente aux langages déterministes.

L'ingénierie des exigences est un aspect important de BASAALT, car l'expérience montre que même pour les systèmes les plus critiques, les exigences sont souvent inadéquates avec parfois des conséquences inacceptables, voire catastrophiques. Il est donc important de ne pas se contenter de la forme et de s'intéresser de près à leur fond et à leur sémantique. Par ailleurs, pour BASAALT, la spécification et la justification des hypothèses sont aussi importantes que la spécification des exigences.

*Intervenant