Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

« Actualisation de l'Etat de l'art des méthodes et outils innovants pour la modélisation des systèmes complexes »

Projet de l'IMdR n°P20-1

Copyright IMdR – Décembre 2022

Chefs de Projet :
Mme Carole Duval, EDF
M André Lannoy, IMdR

Contractant :
APSYS

APSYS
AUGMENTED TRUST

L'Institut pour la Maîtrise des Risques remercie :

- **Mme Carole Duval (EDF) et M André Lannoy (IMdR)**, qui ont codirigé cette étude,
- **les sociétés** qui ont souscrit à ce projet et **leurs collaborateurs** qui ont participé à sa réalisation :

Mme Carole Duval
Mme Mouna Rifi
M Mohamed Hibti

M Florent Brissaud

M Albin Tarisse

M Jean Caire

- l'équipe du contractant **APSYS** représentée par :

M Emmanuel Arbarétier
M Julien Niol
M Jérôme Fiquet

SYNTHESE DU PROJET

1. INTRODUCTION

Ce document constitue la synthèse du projet P20-1 : **" Actualisation de l'Etat de l'art des méthodes et outils innovants pour la modélisation des systèmes complexes**

2. RÉSULTATS DES TRAVAUX

Le projet P11-4 de l'IMdR, réalisé par APSYS en 2012, dressait un état de l'art sur les différentes méthodes et outils pour mener à bien des analyses de sûreté de fonctionnement de systèmes complexes.

Aujourd'hui, sur l'impulsion du GTR « Innovation en Rupture Transversale – Modélisation des Systèmes Complexes », l'IMdR a souhaité lancer le projet P20-1 consistant en une mise à jour de l'état de l'art du projet P11-4 afin d'y intégrer des nouvelles méthodes/outils choisis en fonction de leur apport spécifique et innovant à l'état de l'art des processus d'analyse de la complexité des systèmes et des approches de maîtrise des risques associées: l'actualisation de ce référentiel est décrite dans ce qui suit.

L'IMdR a donc émis une consultation pour sélectionner une société de service spécialisée en Sûreté de fonctionnement et en modélisation de systèmes complexes et c'est la société AIRBUS PROTECT qui a été mandatée pour mettre en œuvre ce projet, en collaboration avec quatre partenaires EdF, INERIS, GRT GAZ et RATP.

L'analyse du besoin auprès des partenaires cités précédemment a mis en évidence entre autres les limites suivantes, du point de vue des démarches classiques d'analyse des systèmes complexes et de maîtrise des risques globaux:

- il est difficile de contrôler l'exhaustivité des interactions conditionnant le comportement souhaité ou non souhaité d'un système, même lorsque cette exigence d'exhaustivité est ramenée à une notion de complétude ;
- les approches d'Analyse Fonctionnelle et Dysfonctionnelle permettent de cibler les flux d'interaction ou de dépendance qui ont un sens par rapport aux finalités du concepteur, mais ils ne couvrent pas la totalité des flux d'interaction potentiels susceptibles par exemple de contribuer à la production de situations dangereuses ;
- ces analyses descendantes ou ascendantes, suivant le niveau d'avancement des projets auxquels elles s'intègrent, reposent sur la mise en œuvre de logiques de découpages, et l'utilisation de langages de modélisation qui ont peine à appréhender des points de vue de granularité hétérogènes, tout en garantissant une cohérence absolue ;
- la juxtaposition, voire l'intrication de composantes de natures extrêmement diverses : technologique, hardware ou software, humaine, organisationnelle, environnementale laisse peu présager de la réussite de modélisations "unifiées" intégrant ces couches de natures différentes, qu'on voudrait soumettre à des référentiels formels, syntaxiques et sémantiques communs.

En réponse à ces verrous, il a été décidé de compléter le référentiel des méthodes innovantes par les techniques suivantes :

- *Spirops* ou l'utilisation de bases de règles expertes pour procéder à des décisions complexes dans un contexte incertain
- *Linkurious* ou le traitement massif des réseaux de connexion pour anticiper des situations de fraude ou de malveillance dans un contexte de cyber sécurité
- *DC Brain* ou l'utilisation de réseaux de neurones convolutifs pour optimiser des réseaux de distribution logistique
- *Maze*, nouveau cadre d'analyse projet pour des programmes complexes, longs et coûteux avec des enjeux organisationnels sensibles

- Les outils à base de graphes / réseaux et toutes les mathématiques de mesure de complexité de réseaux pour mettre en évidence les faiblesses des systèmes
- La numérisation d'un organisme vivant comme ce qui a été appliqué au « *ver elegans* » pour développer des miroirs ou maquettes virtuelles « fidèles » de la réalité, sur lesquelles pouvoir conduire des expérimentations
- *ALL4TEC* ou la théorie des cliques afin d'échantillonner des univers de cas d'usage infinis
- *STAMP*, méthode d'analyse des risques globaux et transversaux permettant d'avoir une couverture la plus large possible des modes d'exposition d'un système aux risques quelle que soit sa phase de cycle de vie ou quel que soit son contexte opérationnel
- La Logique Linéaire offrant un cadre d'analyse, de démonstration voire de preuve formelle des plus riches concernant les propriétés d'un logiciel critique…

Afin de décider de mettre en œuvre concrètement telle ou telle méthode pour en confronter les promesses théoriques aux difficultés de mise en œuvre pratique, il a été décidé d'explorer le domaine des sciences du vivant et d'y examiner les modalités d'utilisation d'outils de modélisation ou de simulation appliquées par les principaux acteurs, afin de recueillir d'éventuelles pistes de réflexion à l'usage des industriels.

Pour cela, AIRBUS PROTECT s'est fait accompagner de deux éminents spécialistes des méthodes de maîtrise de la complexité :

- ***Véronique THOMAS-VASLIN***, Docteur en immunologie, chercheur au CNRS à Paris, a créé en 2008 l'équipe d'Immunologie Intégrative au sein de l'Unité Immunologie, Immunopathologie et Immunothérapie de Sorbonne-Université et de l'INSERM, située sur le campus de la Pitié-Salpêtrière à Paris. Ses recherches l'ont conduite à modéliser et simuler des « systèmes complexes » du monde du vivant ;
- ***Daniel KROB***, ancien professeur de l'Ecole Polytechnique, titulaire de la chaire d'ingénierie des systèmes complexes de 2003 à 2015 et directeur de recherches au CNRS, a créé en 2011 le Centre d'Excellence Sur l'Architecture, le Management et l'Economie des Systèmes (CESAMES).

Cette contribution nous a permis d'élaborer une « Grammaire du Vivant » autour de quatre concepts structurants que sont l'émergence, la résilience, l'homéostasie et la complexité évolutive, définis dans le rapport du projet.

Il est ainsi apparu que le domaine du vivant offre une source inépuisable d'inspiration pour des industriels, en particulier du point de vue de l'émergence, de la résilience et de l'homéostasie, mais aussi du domaine tout à fait spécifique de la complexité évolutive.

Par exemple, certains de ces comportements ont été déjà retenus du monde du vivant pour nos systèmes complexes industriels même s'il s'agit seulement d'analogies développées du point de vue technique :

- La résilience par la diversité,
- L'émergence par les interactions entre niveaux ou intra-niveaux,
- L'homéostasie à travers des mécanismes de régulation de plus en plus sophistiqués.

… et par des outils développés qui ne représentent pourtant qu'une petite partie du comportement du vivant :

- Les colonies de fourmis,
- Les algorithmes génétiques,
- Les automates cellulaires,
- Les réseaux de neurones.

Or, les modèles utilisés par les acteurs des sciences du vivant (par exemple les immunologues) sont proches des modèles réductionnistes ou réductionnistes par morceaux : ils se traduisent souvent par des systèmes d'équations différentielles spéculant sur les trajectoires d'évolutions de populations élémentaires de cellules considérées homogènes.

Ces modèles à l'instar des approches industrielles ne traitent qu'une petite partie de la complexité présentée par les systèmes vivants et sont liés à un grand nombre d'hypothèses simplificatrices.

Compte tenu de ces réflexions, les facteurs de complexité de nos systèmes nous obligent à passer à une vision plus globale et donc à quitter ces modèles réductionnistes qui nous semblent trop limités en termes de couverture des points de vue de la réalité.

Cette réflexion a ainsi ouvert la voie à deux pistes pratiques de développement de cas d'usage.

- La première piste consiste à privilégier des approches intégratrices qui consistent à utiliser des environnements outillés permettant de superposer des points de vue d'analyses de performances très différentes : un cas test simplifié développé à travers une approche MBSA utilisant le langage AltaRica et traitant d'une filière de production d'H2 a permis de traiter des analyses performantielles de sécurité, cyber sécurité, disponibilité opérationnelle de production et sécurité environnementale au sein d'un même référentiels d'outils et de modèles d'ingénierie système.

- La deuxième piste a consisté à mettre en œuvre des outils permettant de simuler des réseaux multiplexés, ce qui permet d'adresser les processus d'interaction entre niveaux et intra-niveaux, qui sont les principaux canaux de propagation et de diffusion des nombreux mécanismes d'émergence, qu'ils soient positifs ou négatifs.

Des séquences d'événements menant à l'atteinte des différents enjeux sécurité et perte de production ont été obtenues avec l'approche MBSA puis par les réseaux complexes.

L'approche MBSA a permis d'obtenir des séquences qui doivent souvent faire l'objet de troncatures, pour des raisons de temps calcul, que ce soit par rapport à des traitements qualitatifs ou quantitatifs, lorsque le modèle est volumineux et que la logique produit des combinatoires trop nombreuses.

Le recours aux modèles sous forme de réseaux représente une alternative susceptible de s'affranchir de ces inconvénients : en effet, à travers la structure de ces derniers, des métriques permettent de mesurer la résilience du système : les composants ressortent, indépendamment de l'aspect quantitatif coûteux en temps calcul.

En effet, les réseaux vont au-delà des coupes minimales en faisant apparaître des défaillances rejetées par la troncature pendant la résolution du modèle MBSA. A la conception, avant le modèle MBSA, ils permettent de vérifier la robustesse du système vis-à-vis des redondances et de la diversification des systèmes de secours en montrant le caractère équilibré du design.

Une piste est d'aller plus loin dans l'exploration de pistes autour du monde du vivant et une autre, d'instruire les réseaux multiplexés capables de traiter les interdépendances entre niveaux et intraniveaux notamment pour l'enjeu des agressions externes et d'origine humaine du type cyber et ceux de la qualité des modèles en excluant les nœuds orphelins, des sous-systèmes incomplets ainsi que les incohérences de modélisation et de visualisation ou communication sur des résultats souvent difficiles à exploiter de manière simple.