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

Projet IMdR Complexité CPS – Fiche Projet 24 (FP24)

INTÉRÊT GÉNÉRAL

1. TITRE DU PROJET

Analyse des risques et modélisation des systèmes complexes cyber physiques dans leur environnement pour une meilleure résilience

2. CONTEXTE ET ENJEUX

Les démarches classiques d'analyse des systèmes complexes, systèmes présentant un grand nombre d'éléments, d'interrelations de natures différentes (actions, rétroactions, influences, …), sont majoritairement fondées sur des visions techniques. Elles aboutissent généralement à un traitement par décomposition en sous-problèmes ou sous-systèmes.

Le développement de ces thématiques d'étude dans le domaine industriel amène à se questionner sur les conditions d'application de ces démarches :

- richesse technique et technologique des systèmes complexes, avec une forte hétérogénéité entre ces systèmes, et au sein de leurs constituants ;
- importance de plus en plus forte des interactions, du fait notamment de l'« ouverture » d'un nombre croissant de ces systèmes ;
- évolution rapide et fluctuante de leur environnement d'exploitation ;
- niveau d'assurance (au sens ISO1526 : quelle confiance dans le résultat ?) recherché dans les démonstrations de sécurité (ou plus généralement de maîtrise des risques).

L'expérience acquise sur ces démarches a permis d'en exposer les limites :

- il est difficile de contrôler l'exhaustivité des interactions conditionnant le comportement souhaité ou non souhaité d'un système ;
- les approches d'Analyse Fonctionnelle et Dysfonctionnelle peuvent permettre 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, 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, juridique, sociétale,… rendent difficile la réussite de modélisations "unifiées" intégrant ces couches de natures différentes, qu'on voudrait soumettre à des systèmes de représentation interopérables.

Un précédent projet [1, 2] a permis de mettre à jour un état de l'art des méthodes innovantes capables d'appréhender et de conceptualiser les systèmes complexes, d'en faire l'inventaire, d'identifier leurs lacunes ou incomplétudes.

Il a aussi permis de caractériser les systèmes vivants et de retenir les comportements suivants pour les systèmes industriels même s'il s'agit seulement :

- d'analogies développées du point de vue technique :
  - la résilience par la diversité ; par la multitude des réplications de l'ADN, ses essais-erreurs, le monde du vivant s'adapte aux changements de son environnement ;
  - l'émergence par les interactions entre niveaux ou intra-niveaux ;
  - l'homéostasie, tendance à résister au changement afin de maintenir un environnement interne stable et relativement constant à travers des mécanismes de régulation multi-niveaux et multi-échelles de plus en plus sophistiqués ;
  - l'optimisation des stratégies de reconfiguration, à travers des tentatives répétées de variation et diversification.
- D'algorithmes qui ne représentent qu'une petite partie du comportement du vivant :
  - les colonies de fourmis ;
  - les algorithmes génétiques ;
  - les automates cellulaires ;
  - les réseaux de neurones.

D'autres méthodes ont été considérées dans ce projet comme les réseaux complexes et des méthodes qualitatives comme la méthode d'analyse des dangers STPA (Systems Theoretic Process Analysis) [10] et les cindyniques [11]. Un cas d'usage de production d'Hydrogène vert (dont l'électricité employée lors de l'électrolyse est produite à partir d'une source d'énergie renouvelable) et de sa distribution impliquant son stockage a été traité par une approche intégratrice MBSA [12] pour des enjeux de sécurité, cyber, disponibilité de production et d'impacts environnementaux, complétée par la mise en œuvre de réseaux complexes permettant de mettre en exergue, sans calcul de probabilité, les composants par lesquels transitent des flux maximaux. Ces réseaux permettent d'identifier des composants ou actions clés dans le système, mettant en jeu d'autres éléments par leur défaillance du fait de leur rôle central dans le système, et de détecter ainsi la faible robustesse du système. Cette identification permet d'améliorer la résilience de ces systèmes.

Les perspectives envisagées à la fin du projet [1] conduisent à identifier les objectifs suivants pour ce nouveau projet :

- considérer un système dont la complexité viendrait de l'intégration de risques environnementaux et cyber ;
- prendre en compte un environnement totalement imprévisible en termes de génération de circonstances insidieuses conduisant à un sinistre (cas rencontrés dans les véhicules autonomes et les systèmes dont le software et l'automatisation de nombreux procédés par le biais de contrôleurs informatiques ouvrent la possibilité que le système agisse de manière non sûre par conception, bien que tous ses composants fonctionnent comme attendu) ;
- intégrer la composante humaine avec des actions prévues et imprévues, des variables humaines ;
- mettre en œuvre des techniques de représentation des systèmes complexes à plusieurs niveaux : ex. les réseaux multiplexes ou multicouches [13] qui permettent 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 ;
- spécifier un niveau d'assurance, i.e. un degré de confiance dans les résultats obtenus ;
- identifier les apports de ces techniques par rapport aux approches classiques de modélisation/traitement des risques (MBSE/MBSA). Par exemple, pour la méthode STPA, on pourrait évaluer l'apport d'une analyse du système qui permette de s'assurer qu'il est fonctionnellement sûr en plus d'être robuste aux défaillances matérielles.

3. RÉSULTATS ATTENDUS

Les résultats attendus à la fin du projet sont présentés ci-dessous.

- Établissement d'une ontologie des méthodes de traitement des systèmes complexes, basé sur les états de l'art des projets IMdR 11-4 et 20-1. Outre un état des lieux synthétique, il permettra aussi d'identifier les couplages possibles entre elles.
- Construction d'un cas d'application, données nécessaires, structuration. Ce cas mêlera les différentes natures de risques précédemment identifiées : techniques, cyber, humaines, environnementales.
- Evaluation et traitement du cas à l'aide de méthodes différentes : intégratrices (MBSE-MBSA, STPA…), les réseaux multiplexes, les jumeaux numériques.
- Comparaison des résultats. Evaluation du niveau d'assurance. Mise en évidence de l'intérêt et des difficultés.
- Synthèse et perspectives.

Le benchmarking pourra par exemple illustrer les questionnements suivants :

- En quoi ces techniques permettent-elles de visualiser les interdépendances des sous-systèmes/composants vis-à-vis d'un initiateur, sont-elles un moyen de

vérifier la définition des événements indésirables dans les études de fiabilité et d'assurer la qualité des modèles ?

- En quoi contribueraient-elles à la défense en profondeur, source de résilience en choisissant des lignes de défense par exemple ou en vérifiant la robustesse du système vis-à-vis des redondances ou la diversification des systèmes ?
- Comment des réseaux multiplexes ou multicouches pour les agressions et les métriques permettent-ils de retrouver les facteurs d'importance et de garantir la résilience du système ?
- Comment utiliser les jumeaux numériques (agrégation de contenu lié au fonctionnement, dysfonctionnement, à la performance environnementale, à la cyber) pour la validation d'un système autonome dans un environnement à horizon infini dont on caractérisera les niveaux de confiance, les écarts à la réalité ?
- Comment favoriser dans un système des mécanismes d'évolution (notamment en matière logicielle mais aussi en matière d'intégration de nouveaux composants…) améliorant son niveau de robustesse ou sa résilience dans un environnement changeant ou évoluant continuellement ?

4. PROGRAMME DES TRAVAUX

Ce programme est donné à titre indicatif. Il sera bien évidemment précisé dans un cahier des charges, si le projet a un nombre suffisant de souscripteurs, en fonction de leurs besoins.

- **Tâche 1 :** Analyse des besoins des souscripteurs et choix des méthodes outillées à investiguer, établissement d'une ontologie des méthodes pour identifier les couplages possibles entre elles.
- **Tâche 2 :** Choix d'un cas de comparaison des méthodes outillées les plus pertinentes
- Ce cas sera conséquent en termes de nombre et de nature de nœuds, nombre et types de liens d'influence. Il nécessitera des données d'entrée, une expertise pour l'interprétation… Ces informations seront fournies par les souscripteurs qui auront fourni les données ou, à défaut, un exemple fictif pourra être créé ou extrait de la littérature.
- **Tâche 3 :** Traitement du cas

  On s'attachera à appliquer les méthodes et outils issus de la Tâche 1, éventuellement couplés, et à mettre en avant l'apport de ces méthodes et outils par rapport aux méthodes plus classiques, leurs conditions d'utilisation, l'interprétation des résultats et les éventuelles difficultés rencontrées.
- **Tâche 4 :** Analyse critique de l'utilisation des méthodes choisies, exploration des variantes, et des contraintes présentées par les modalités d'implantation, les hypothèses prises en compte et la maîtrise des informations à prendre en compte à l'entrée de la méthode, l'écart à la réalité et le niveau de confiance dans les résultats.

- **Tâche 5 :** Synthèse et identification des insuffisances et incomplétudes pour définir des pistes de développement de méthodes innovantes pour le traitement des systèmes complexes.

5. RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Projet P20-1, « Actualisation de l'Etat de l'art des méthodes et outils innovants pour la modélisation des systèmes complexes et benchmarking », RATP, Ineris, GRT-Gaz, EDF, Airbus Protect, 2022 ; article congrès Lambda-Mu23, 2022, même titre, J. Niol (Airbus Protect), C. Duval, M. Rifi, M. Hibti (EDF-R&D), F. Brissaut (GRT-Gaz), J. Caire (RATP), A. Tarrisse (Ineris)

[2] Atelier « Prise en compte des sciences du vivant dans la modélisation des systèmes complexes », congrès Lambda-Mu 23

[3] Thèse de Mouna Rifi, « Exploration des réseaux complexes pour les études probabilités de sûreté », soutenue en 2019, Paris 13, LIPN

[4] C. Duval, G. Fallet-Fidry, B. Iung, P. Weber and E. Levrat, "A Bayesian network-based integrated risk analysis approach for industrial systems: application to heat sink system and prospects development", Journal of Risk and Reliability, 2012

[5] Le Moigne J.L., « La modélisation des systèmes complexes ». Editions Dunod, 1990

[6] H. Zwirn – « Les systèmes complexes – Mathématiques et biologie ». Odile Jacob Sciences, 2006

[7] Hild D, McEvilley M, Winstead M, "Principles for Trustworthy Design of Cyber-Physical Systems," MITRE Technical Report, MTR210263, June 2021

[8] ISO/IEC 15026: 2013, "Systems and Software Engineering — Systems and Software Assurance"

[9] ISO 21448: 2022, "Road vehicles — Safety of the intended functionality"

[10] Leveson Nancy, "Engineering a Safer World: Systems Thinking Applied to Safety", The MIT Press, décembre 2016

[11] G. Planchette, Livre « Cindyniques, la science du danger : un nouveau souffle », ISTE Editions (30 juin 2022)

[12] Projet IMdR P23-2-MBSA « Rédaction d'un guide de réalisation d'une étude MBSA » lancé en 2023

[13] R. Kanawati, « (PDF) Détection de communautés dans les grands graphes d'interactions (multiplexes) : état de l'art (researchgate.net) », novembre 2013

6. DURÉE

18 mois

7. MONTANT DE LA SOUSCRIPTION

9800 € HT