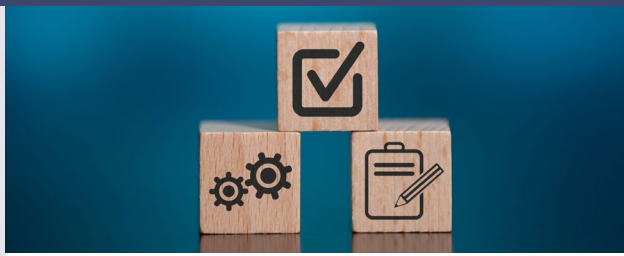
FICHE DOMAINE

Sûreté de fonctionnement

Modéliser et démontrer la sûreté de fonctionnement des systèmes

La complexification des systèmes actuels, liée à une combinaison massive de composants hétérogènes matériels, logiciels et humains, engendre des contraintes fortes sur les différentes dimensions de la sûreté de fonctionnement : la fiabilité et le diagnostic des systèmes, leur disponibilité, leur maintenabilité, leur sûreté et leur sécurité.

Même si ces contraintes sont correctement appréhendées et utilisées dans certains secteurs industriels, les approches actuelles en sûreté de fonctionnement présentent néanmoins des lacunes. D'une part, le couplage des approches de sûreté de fonctionnement et de sécurité est faible. D'autre part, et notamment pour la sûreté matérielle, elles peinent à considérer la dynamique, la structure, ou encore l'hétérogénéité des systèmes qu'elles tentent d'appréhender.



ENJEUX

Les enjeux actuels sont partagés par les différentes filières industrielles. Ils se caractérisent par la définition et la conception de nouvelles méthodes et outils innovants permettant de prendre en compte cette complexification croissante des systèmes, ainsi que les différentes dimensions de la sûreté de fonctionnement.

POSITIONNEMENT DE L'INSTITUT

La sûreté de fonctionnement est au cœur de nombreux projets de R&D de l'IRT SystemX, en particulier dans le domaine de la mobilité autonome ou de l'intelligence artificielle. Dans ce cadre, l'institut apporte des solutions à l'état de l'art et mène des travaux de recherche plus amont adressant trois principaux défis : l'hétérogénéité et la non-stationnarité des systèmes, les approches d'évaluation de la sûreté de fonctionnement allant jusqu'à des approches formelles, et la métrologie de la qualité des études de sûreté de fonctionnement.

EXPERTISES

Sûreté de fonctionnement, sécurité logicielle, MBSA (*Model-Based Safety Analysis*), test, *model-checking*, preuve, homologation, certification, fiabilité, maintenance, diagnostic, pronostic.

Projets illustratifs

Projet 3SA

Améliorer la Simulation pour la Sécurité du Système du véhicule Autonome

- Algèbre de processus et ontologies pour les taux de couverture de tests
- Analyse AMDEC (Analyse des Modes de Défaillance, de leurs Effets, et de leur Criticité) des systèmes autonomes
- Modélisation des capteurs et de leurs limitations (caméra, radar, lidar et GNSS, *global navigation satellite systems*)

Projet PST

Augmenter la Performance des Systèmes de Transport par un meilleur couplage des outils de simulation, de conception logicielle et des plateformes d'exécution

- Amélioration des performances fonctionnelles et non fonctionnelles des composants d'un système
- Réutilisation des modélisations des composants pour de nouvelles conceptions

Projet SAM

Concevoir un environnement de démonstration de la Sécurité et de l'Acceptabilité de la Mobilité autonome

- Méthodologie de démonstration de la sécurité de systèmes automatisés
- Partage des éléments de preuve avec les autorités de réglementation et d'homologation
- Evaluation de l'acceptabilité et des bénéfices sociétaux

Projet RTI

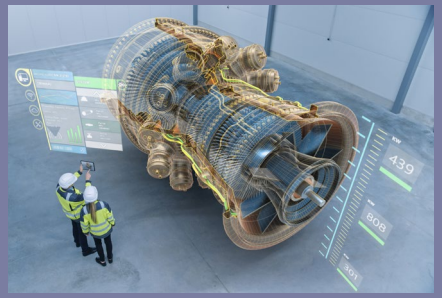
Assurer la Résilience du Transport Intelligent

- Analyse des corrélations entre les études de cybersécurité et les études de sûreté de fonctionnement
- Outil de modélisation comportementale pour la validation de la robustesse des algorithmes de pilotage et de défense
- Application aux voitures autonomes et aux flottes de drones autonomes

Feuille de route

DÉFIS SCIENTIFIQUES ET TECHNOLOGIQUES	VERROUS ASSOCIÉS
Analyse de sûreté de fonctionnement des systèmes non-stationnaires et hétérogènes	• Systèmes de systèmes et systèmes autonomes • Systèmes cyber-physiques (systèmes asynchrones/ synchrones, systèmes temps-réel, systèmes embarqués, locaux ou distribués) • Protocoles de sécurité
Méthodes et outils d'évaluation de la sûreté de fonctionnement	• Combinaison de la cybersécurité et de la sûreté • Validation intelligente des systèmes autonomes • Vérification (*model checking*, génération de cas tests, vérification déductive) • Modélisation comportementale
Métrologie de la qualité des études de sûreté de fonctionnement	• Homologation/certification • Automatisation des propositions de solutions d'optimisation de la sûreté de fonctionnement (redondance, amélioration de la fiabilité, stratégies de maintenance, etc.) • Interprétabilité et fiabilité des résultats dans le domaine de l'intelligence artificielle • Mise en cohérence / synchronisation de modèles

Plateformes et démonstrateurs



OPENALTARICA

Plateforme d'évaluation de la sûreté de fonctionnement des systèmes complexes

- Prise en compte du comportement dynamique des systèmes
- Panel d'outils d'analyse

Cible des publications de l'IRT SystemX dans ce domaine (collection HAL)

● JOURNAUX

Reliability Engineering & System Safety, Journal of Risk and Reliability, International Journal of Critical Computer-Based Systems

● CONFÉRENCES

ESREL (European Safety and Reliability Conference), Lambda-Mu, IMBSA (International Symposium on Model-Based Safety and Assessment), ICSRS (International Conference on System Reliability and Safety), RAMS® (Reliability and Maintainability Symposium), SafeComp (International Conference on Computer Safety, Reliability, and Security), PSAM (Probabilistic Safety Assessment and Management Conference), DSN (Annual IEEE/IFIP International Conference on Dependable Systems and Networks)

Sûreté de fonctionnement

PARTENAIRES ACADÉMIQUES

GROUPEMENTS DE RECHERCHE ET SOCIÉTÉS SAVANTES

PARTENAIRES INDUSTRIELS

À PROPOS DE L'IRT SYSTEMX

SystemX est un institut de recherche technologique (IRT) expert en analyse, modélisation, simulation et aide à la décision pour les systèmes complexes. Seul IRT dédié à l'ingénierie numérique des systèmes, il coordonne des projets de recherche partenariale, réunissant académiques et industriels dans une perspective multi-filière. Ensemble, ils s'appliquent à lever des verrous scientifiques et technologiques majeurs de 4 secteurs applicatifs prioritaires : Mobilité et Transport autonome, Industrie du futur, Défense et Sécurité, Environnement et Développement durable.

Au travers de projets orientés cas d'usage, les ingénieurs-chercheurs de SystemX répondent aux grands enjeux de notre temps, sociétaux et technologiques, et contribuent ainsi à l'accélération de la transformation numérique des industries, des services et des territoires.

Basé sur le plateau de Paris-Saclay et à Lyon, SystemX a été créé en 2012 dans le cadre du programme des investissements d'avenir.

DANS LES ÉQUIPES

15 ingénieurs-chercheurs

6 thèses dont **4** soutenues

(septembre 2021)

CONTACTS

Responsable d'équipe
Mohamed Tlig
mohamed.tlig@irt-systemx.fr

Responsable d'axe scientifique
Michel Batteux
michel.batteux@irt-systemx.fr

www.irt-systemx.fr

@IRTSystemX

IRT SystemX