INFORMATION SHEET

Safety

Modelling and demonstrating the dependability of systems

The massive combination of heterogeneous components (hardware, software, human) induces strong constraints, and then increases the system's complexity. It occurs on the various dimensions of dependability: reliability, diagnosis, availability, maintainability, safety and security.

Whilst these constraints are correctly understood and used for some industrial sectors, current dependability approaches nevertheless have shortcomings.

On the one hand, the coupling of safety and security approaches is weak. On the other hand, and in particular for hardware systems, they struggle to consider their dynamics, their structures or their heterogeneities.

CHALLENGES

The current challenges are shared by various industrial sectors.. The increasing complexity of systems, as well as the different dimensions of dependability must be assessed with new innovative methods and tools.

POSITIONING OF THE INSTITUTE

Dependability is the focus of many of IRT SystemX's R&D projects, particularly in the field of autonomous mobility and artificial intelligence. In this context, the institute provides state of the art solutions and carries out more upstream research works addressing three main challenges: how to handle heterogeneity and non-stationarity of systems? How to assess dependability including formal approaches? How to improve the metrology of dependability studies?

EXPERTISE

Dependability, software safety, MBSA (Model-Based Safety Assessment), testing, model-checking, formal proof, certification, reliability, maintenance, diagnosis, prognosis

Projects in this field

Projet 3SA

Improving Simulation for Autonomous Vehicle System Safety

- Process algebra and ontologies for test coverage rates
- FMEA (Failure Modes and Effects Analysis) of autonomous systems
- Modelling of sensors and their limitations (camera, radar, lidar and GNSS, global navigation satellite systems)

PST project

Increasing the Performance of Transport Systems through better coupling of simulation tools, software design and execution platforms

- Improving the functional and non-functional performance of system components
- Reuse of component models for new designs

SÉCURITÉ ACCEPTABILITÉ MOBILITÉ AUTONOME

SAM project

Designing a Demonstration Environment for Safety and Acceptability of Autonomous Mobility

- Methodology for demonstrating the safety of automated systems
- Sharing evidence with regulatory and approval authorities
- Evaluation of acceptability and societal benefits

RTI project

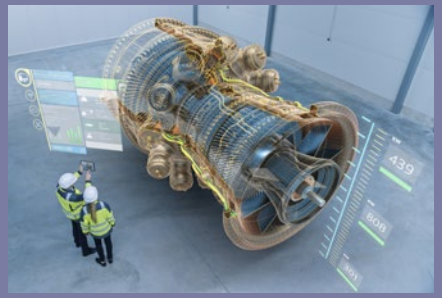
Ensuring Resilience in Intelligent Transport

- Analysis of correlations between cybersecurity studies and safety studies
- Behavioural modelling tool for the validation of the robustness of control and defence algorithms
- Application to autonomous cars and autonomous drone fleets

Roadmap

SCIENTIFIC AND TECHNOLOGICAL CHALLENGES	RELATED RESEARCH FIELDS
Safety analysis of non-stationary and heterogeneous systems	• Systems of systems and autonomous systems • Cyber-physical systems (asynchronous/synchronous, real-time, embedded, local or distributed) • Security protocol
Methods and tools for assessing the dependability	• Combining cyber security and safety • Smart validation of autonomous systems • Verification (model checking, test case generation, deductive verification) • Behavioural modelling
Metrology of the quality of dependability studies	• Homologation/certification • Automation of proposals for solutions to optimise dependability (redundancy, reliability improvement, maintenance strategies, etc.) • Interpretability and reliability of results in the field of artificial intelligence • Models consistency / synchronisation

Platforms and demonstrators



OPENALTARICA

Platform for the evaluation of the dependability of complex systems

- Considering the dynamic behaviour of systems
- Panel of assessment tools

Target of IRT SystemX publications in this field (HAL collection)

● JOURNALS

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

● CONFERENCES

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)

Safety

ACADEMIC PARTNERS

RESEARCH GROUPS AND SCHOLARLY ORGANIZATIONS

INDUSTRIAL PARTNERS

ABOUT IRT SYSTEMX

SystemX is a technological research institute (IRT) with expertise in the fields of analysis, modelling, simulation and decision support for complex systems. As the only IRT dedicated to digital systems engineering, it coordinates partnership research projects, bringing together academics and industry in a multi-sector perspective. Together, they work to solve major scientific and technological problems in four priority application sectors: Mobility and Autonomous Transport, Industry of the Future, Defence and Security, Environment and Sustainable Development.

Through use-case oriented projects, SystemX's research engineers respond to the major societal and technological challenges of our time, and thus contribute to the acceleration of the digital transformation of industries, services and territories.

Located at the Paris-Saclay plateau and in Lyon, SystemX was created in 2012 as part of the future investment programme.

IN THE TEAMS

15 engineers-researchers

6 PhD projects
4 defended

(September 2021)

CONTACTS

Team leader
Mohamed Tlig
mohamed.tlig@irt-systemx.fr

Head of scientific research
Michel Batteux
michel.batteux@irt-systemx.fr

www.irt-systemx.fr/en/

@IRTSystemX

IRT SystemX