Experimental Infrastructure Towards Ubiquitously Safe Robotic Systems using RobMoSys

The eITUS project is one of the six Integrated Technical Projects (ITPs) that has been selected from the **RobMoSys** first open call.

eITUS aims at creating a basic experimental infrastructure (models, software and tools) that enables robotic development stakeholders to **assure system safety** both at design time, using analysis and simulation-based techniques, and at run time, using safety monitoring algorithms.

Nowadays, safety is a becoming a crucial property of robotic systems. ISO 12100, ISO 13849 and IEC 62061 are some of the most accepted safety standards in robotics, covering aspects such as functional safety.

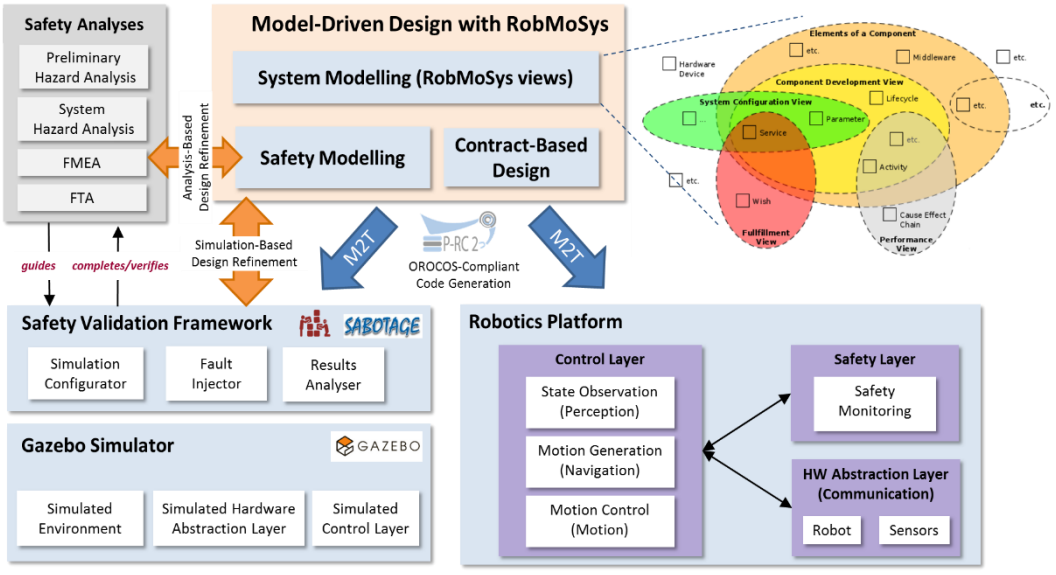
eITUS builds on concepts and tools for the **Model-based design** for safe-aware compositional robotic systems and **Safety Validation** of Robotics Systems during early design phases by means of simulation-based fault injection techniques.

Benefits

- **Standardization of models and interfaces:** eITUS standardizes safety nomenclature such as the definition of FMEAs or failure modes.
- **Certifiable system:** eITUS helps on developing and delivering safety analyses in a formal way, by creating FMEA and Fault Injection tests. Safety artefacts such as FMEA are totally required to proceed to the certification of safe robotics system.
- **Simplifying Usability and Integration:** eITUS integrates safety analysis views with fault injection simulations in a simple and transparent way.
- **Re-usable:** eITUS supports the modelling of reusable domain- and application-specific safety analyses assets.
- **Easy-of use:** eITUS provides an easy way to model safety related aspects and integrate them in the development flow. eITUS supports the separation of roles and views by defining a safety engineer responsible for the FMEA view completion.

Main objectives

- **Model-based design for safe-aware compositional robotic systems**
  - Extension of the RobMoSys metamodel to include safety concerns and support contract-based design.
  - Tools to generate ROS/OROCOS compliant code to run on real demonstration systems.
  - Creation of run-time monitors for safety assessment. By providing formal safety specifications, monitors can be automatically generated and incorporated in the system to ensure the safety of robots.
- **Safety Validation of Robotics Systems during early design phases**
  - Development of a tool enabling an early safety assessment of robotics systems, starting from the Sabotage simulation-based fault injection framework.
  - Use of fault injection simulations for testing the architecture´s robustness and to perform an early dependability/safety validation. The area of Fault Injection is mainly concerned with simulation-based analysis of a system's safety or its dependability properties.
  - Integration of Sabotage and Gazebo for robot dynamics and environment simulation with the RobMoSys design platform. Further investigation in the possible integration to model-based safety analysis tools such as SOPHIA.



eITUS integrates existing technologies from three EU projects:

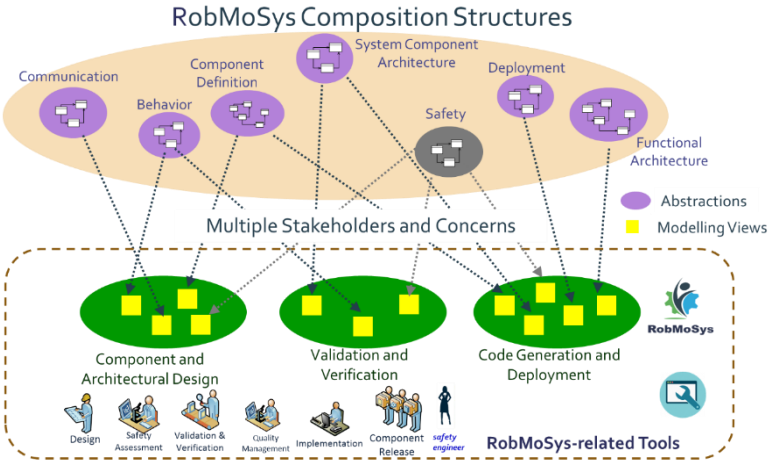
- **RobMoSys** provides the core technologies for modelling robotics systems using the different metamodels underlying the RobMoSys views.
- **P-RC2** provides a framework for the functional design of the robot controller with component development and system configuration views.
- **AMASS** provides the metamodeling backbone for safety validation.

Safety Analysis with RobMoSys

Functional safety is the aspect of safety that aims to avoid unacceptable risks. The system should be designed to properly handle likely human errors, hardware failures and operational/environmental stress. The safety analysis and validation steps are fundamental aspects to perform the safety assessment.

Some of the commonly used risk assessment methods are Preliminary Hazard Analysis, Hazard Operability Analysis, Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Furthermore, Fault Injection simulations complete these analyses by finding unexpected hazards and verifying the implemented safety mechanisms.

eITUS broadens the RobMoSys ecosystem by considering safety aspects, such as the development of a **Safety view** and the introduction of a new role called **Safety Engineer.**

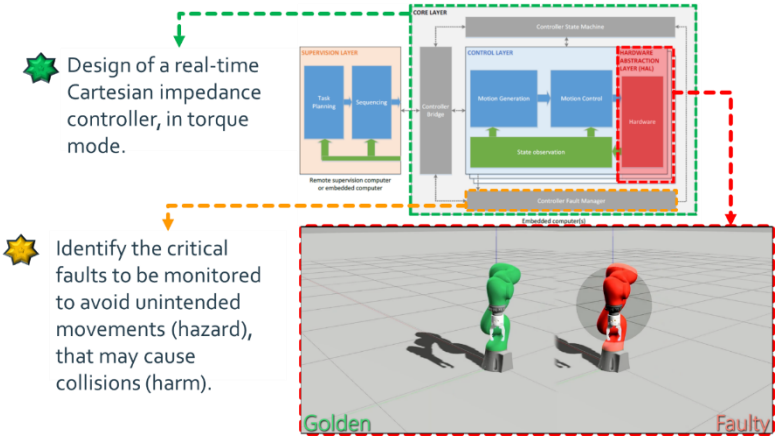


Safety Analysis Use Case Scenario

The 'Safety Assessment of Robotics Systems Using Fault Injection in RobMoSys' scenario shows how to perform safety analysis in the context of **RobMoSys** by using and extending the **Papyrus4Robotics** toolchain and **Gazebo** with Safety concepts and Safety Analysis (FMEA and Fault Injection). **Model-based design** combined with a **simulation-based fault injection** technique and a **virtual robot** poses as a promising solution for an early safety assessment of robotics systems.

The use case is designed in Gazebo by using a Cartesian Mode Control System. Then, the Safety Engineer determines the component failure modes in the **FMEA view.** The **Fault Injection view** allows to set up, configure, execute and analyse the simulation results. First, the Golden system is modelled, and its simulations are executed. Then, based on the system model and the robotics scenario, the **fault injection policy** is defined (faults location, time, duration and model). The original system model is modified though the **fault injector script** according to the fault list. Out of the faulty models, the deployed code is generated, and the simulations are run.

Finally, the comparation of the obtained simulation traces with respect to the Golden ones allows determining if a sufficient level of safety has been reached.



eITUS RobMoSys ITP

Mar 2018 - Mar 2019

Web: https://robmosys.eu/e-itus/
Twitter: @eITUS_ITP
Coordinator: Tecnalia Research & Innovation
Contact: Garazi Juez (garazi.juez@tecnalia.com)

Partners

tecnalia Inspiring Business

AKÉO + PLUS SMART TECHNOLOGIES & ROBOTICS

cea