RobMoSys

Eclipse-Based RobMoSys Tooling: Papyrus4Robotics

Huascar Espinoza, CEA

Tutorial at ACM / IEEE 21st Int. Conf. On Model Driven Engineering Languages and Systems (MODELS)

Copenhagen, 16.10.2018

https://robmosys.eu
https://discourse.robmosys.eu

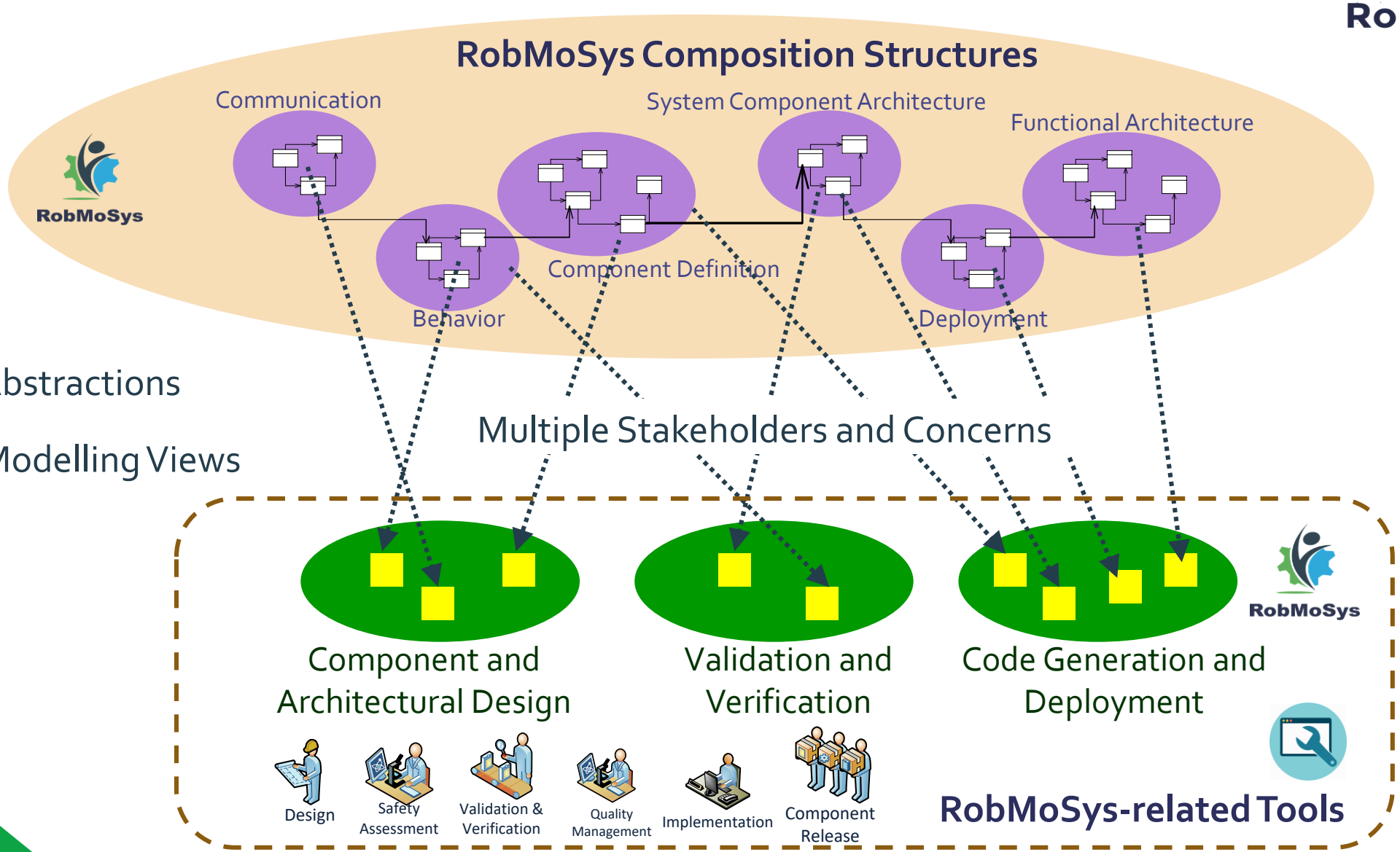
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732410.

cea · Hochschule Ulm University of Applied Sciences · KU LEUVEN · Technische Universität München · COMAU · PAL ROBOTICS · SIEMENS · EUnited Robotics European Robotics Association · eclipse

RobMoSys

Papyrus4Robotics Toolchain

RobMoSys Model-Driven Approach

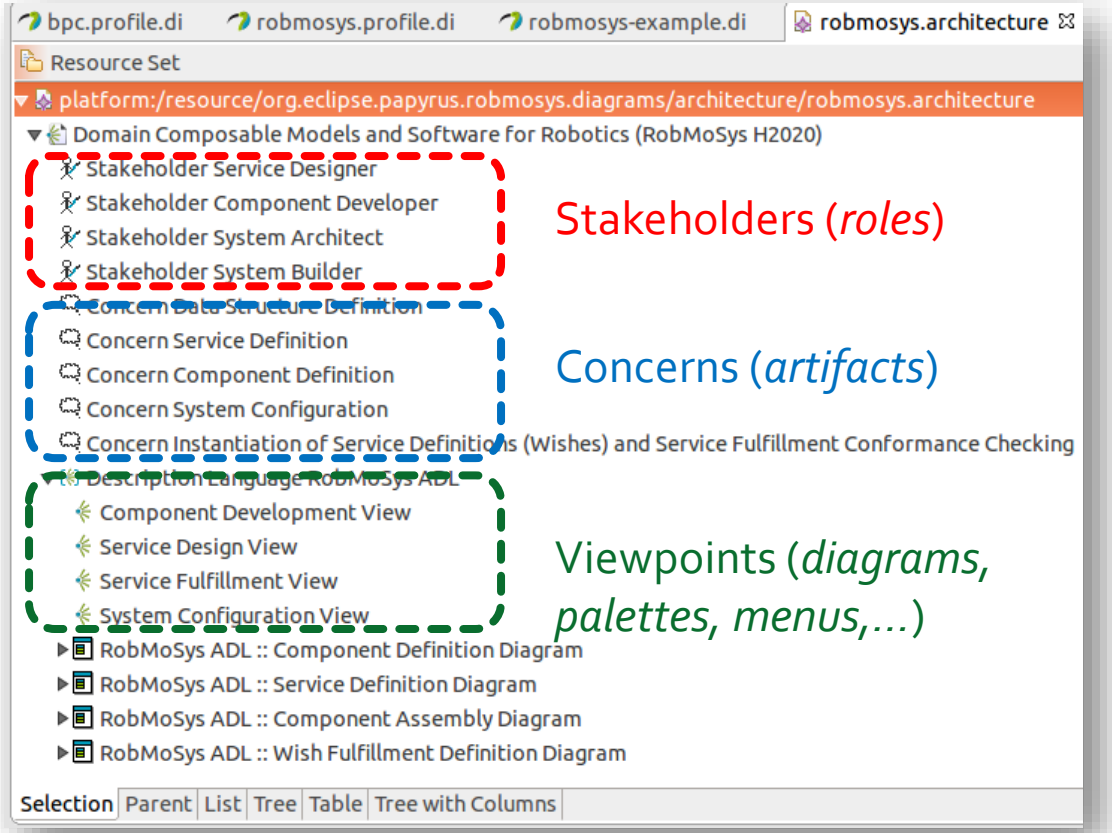


Viewpoints in Papyrus (1/2)

RobMoSys

Aligned to ISO 42010

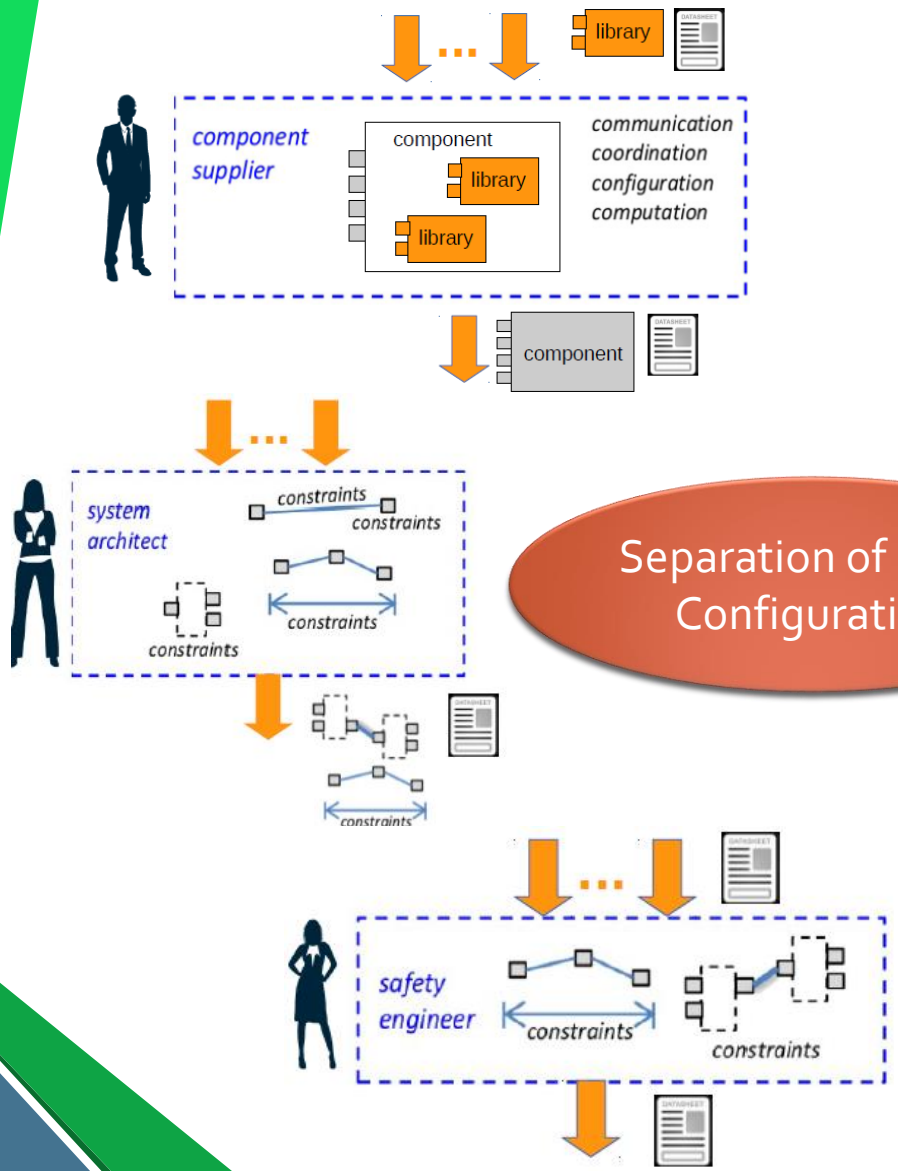
RobMoSys (Papyrus) Architecture Framework



Stakeholders (*roles*)

Concerns (*artifacts*)

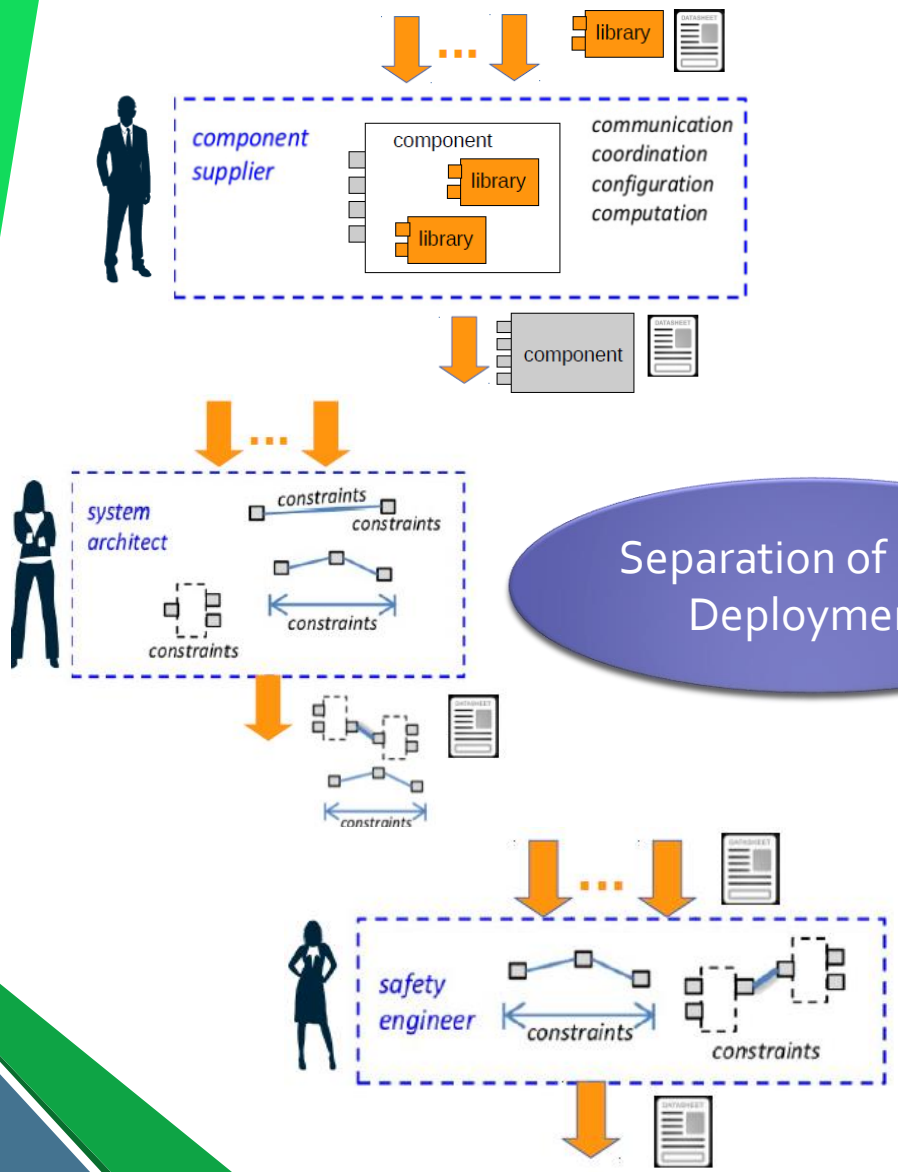
Viewpoints (*diagrams, palettes, menus,…*)



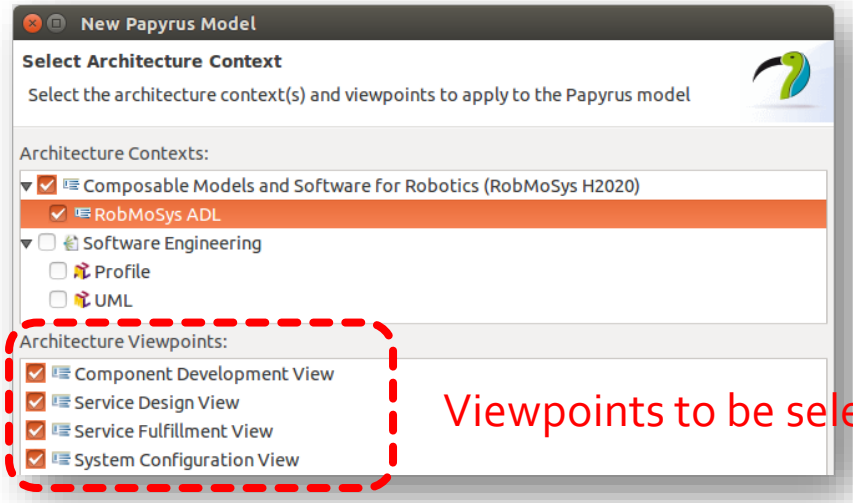
Separation of Roles Configuration

Viewpoints in Papyrus (2/2)

RobMoSys

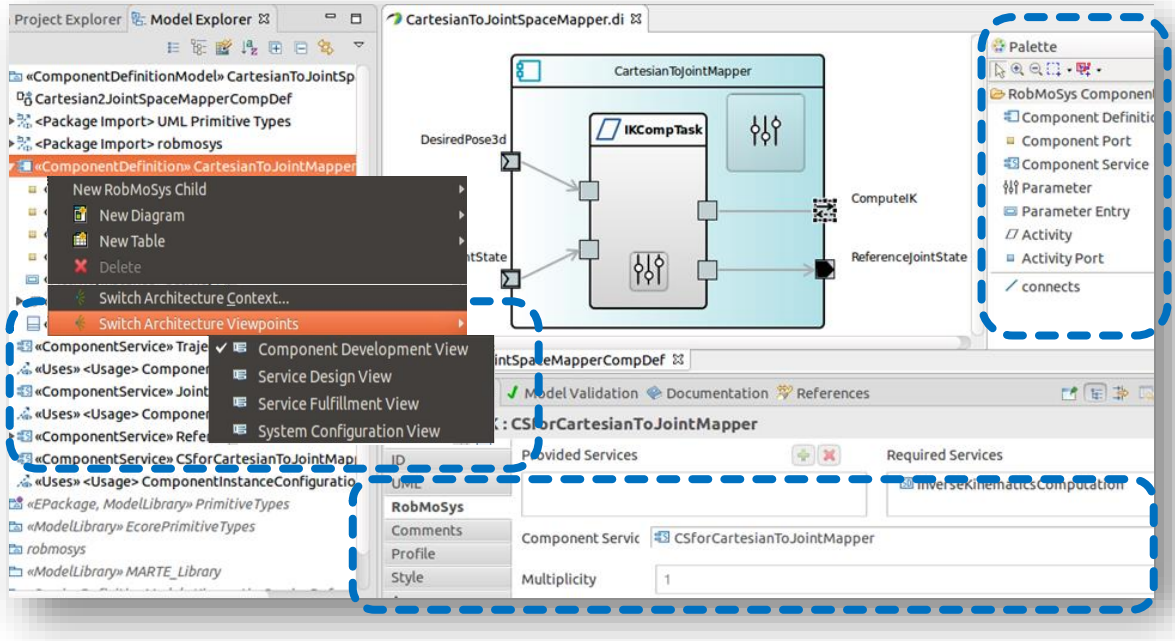


Separation of Roles Deployment



Viewpoints to be selected

Viewpoint-Customized Environment

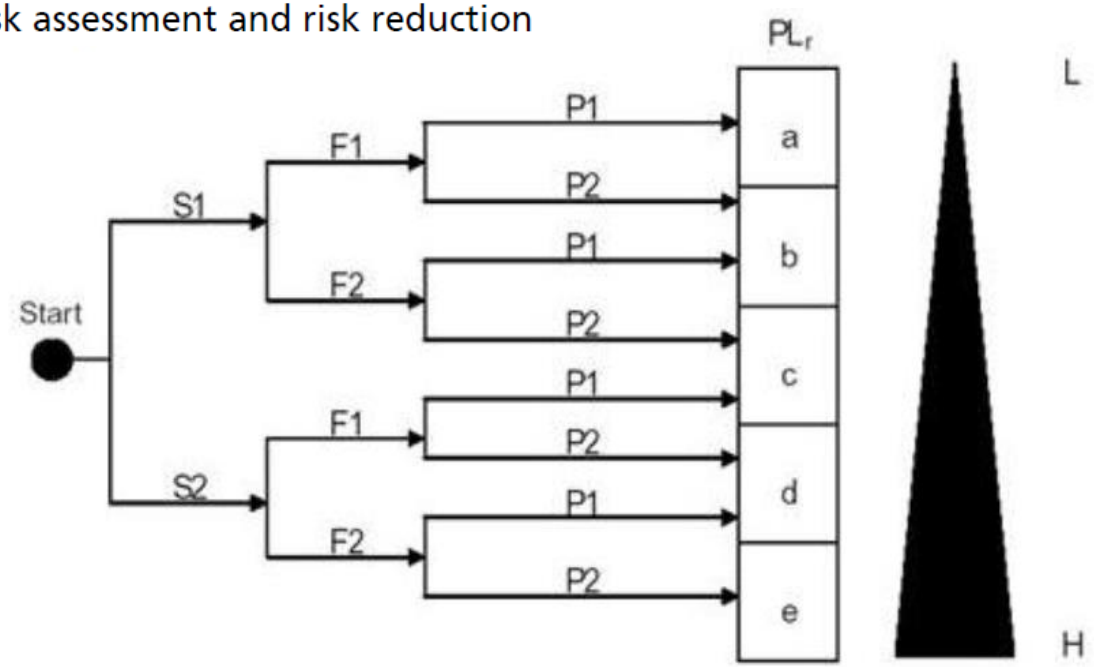


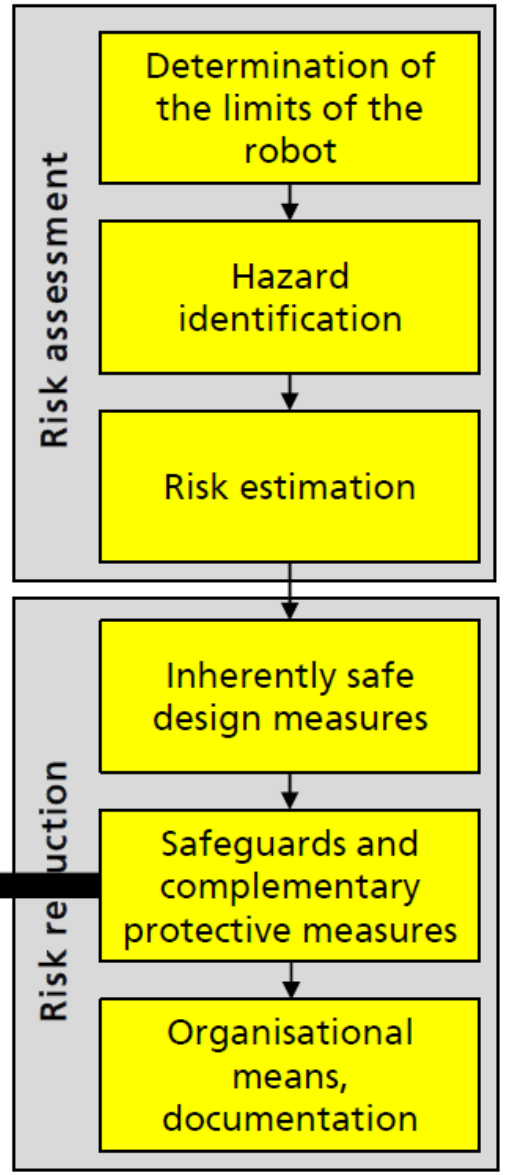
RobMoSys

Safety Analysis with RobMoSys

Applicable Safety Standards in Robotics

ISO 12100 – Safety of machinery – General principles for design – Risk assessment and risk reduction





ISO 13849-1 – Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

RobMoSys

Functional Safety

Electronics, Software

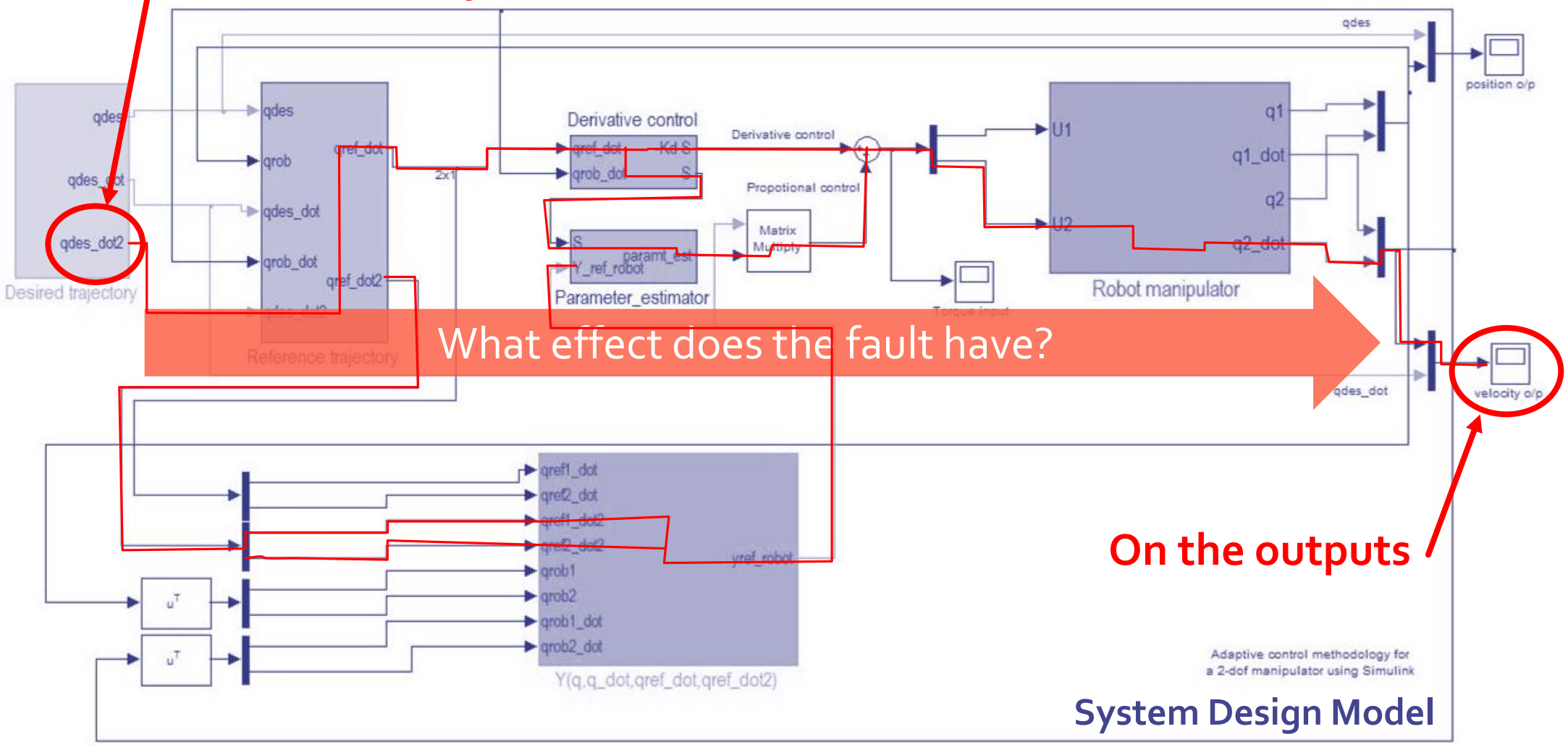
= safety related (part of the) control system

IEC 62061 – Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

RobMoSys

Why Models for Safety Assessment?

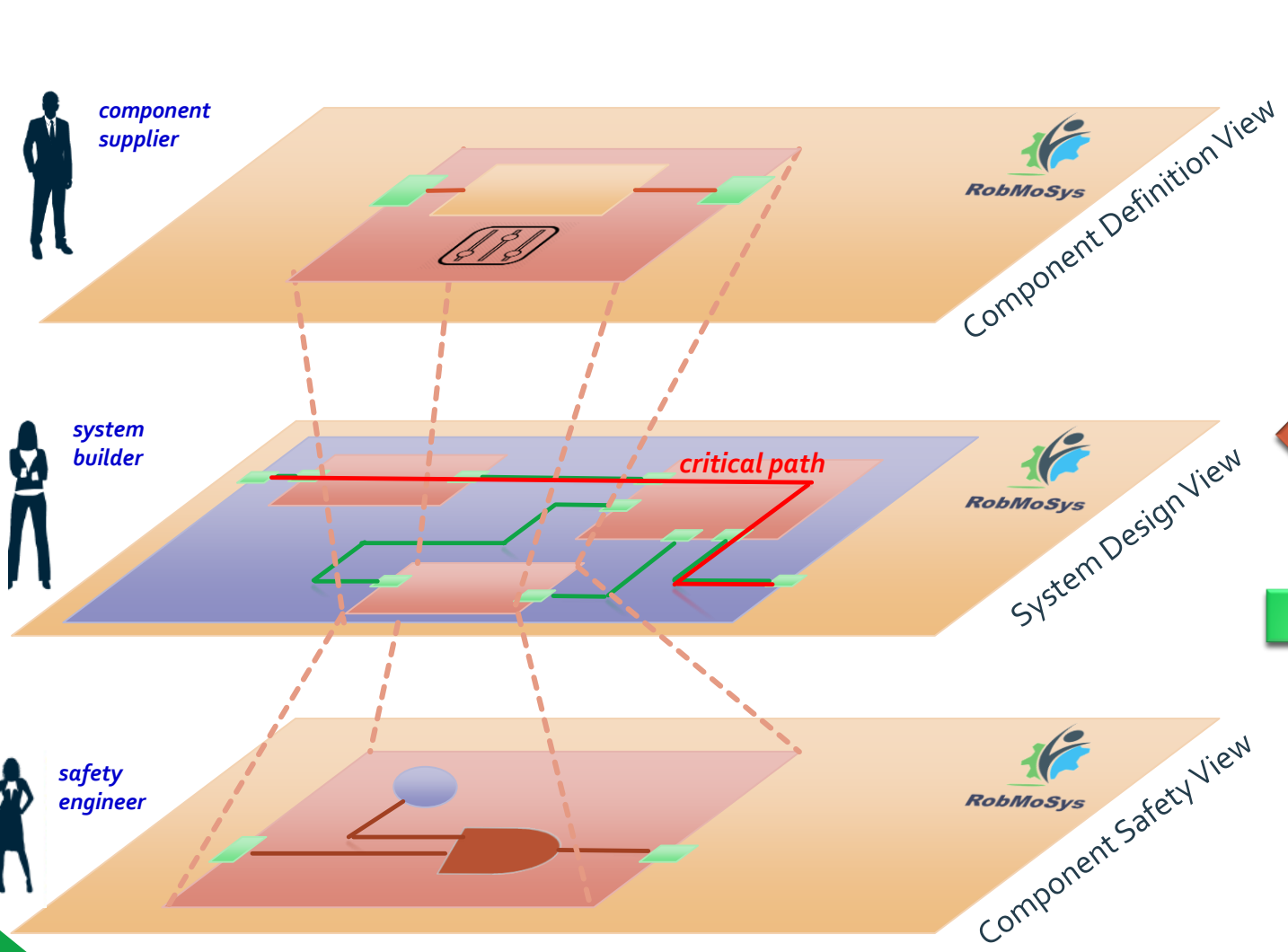
RobMoSys

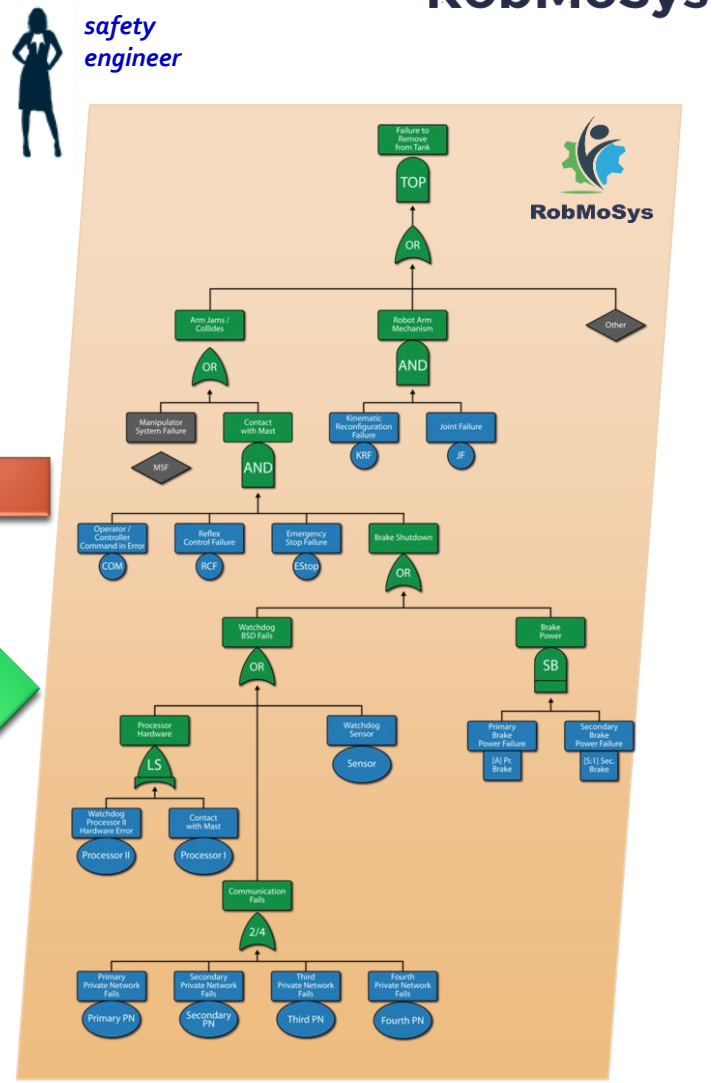


Credits: Yiannis Papadopoulos, University of Hull, U.K

Safety Analysis with RobMoSys

RobMoSys





Fault Tree Analysis (FTA) View

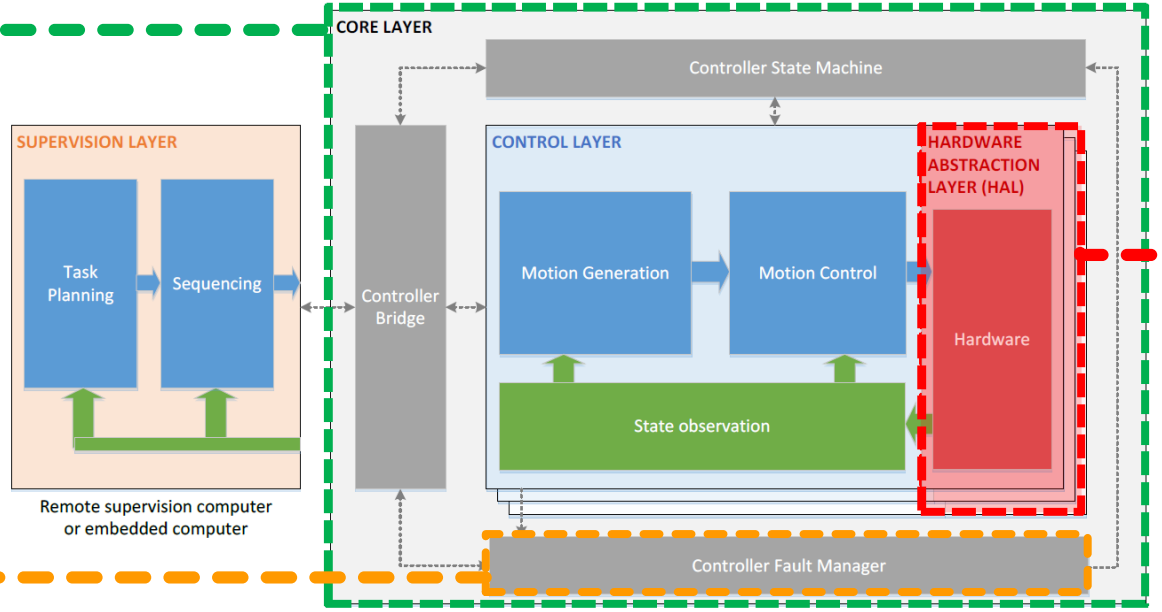
RobMoSys

Safety Analysis Example

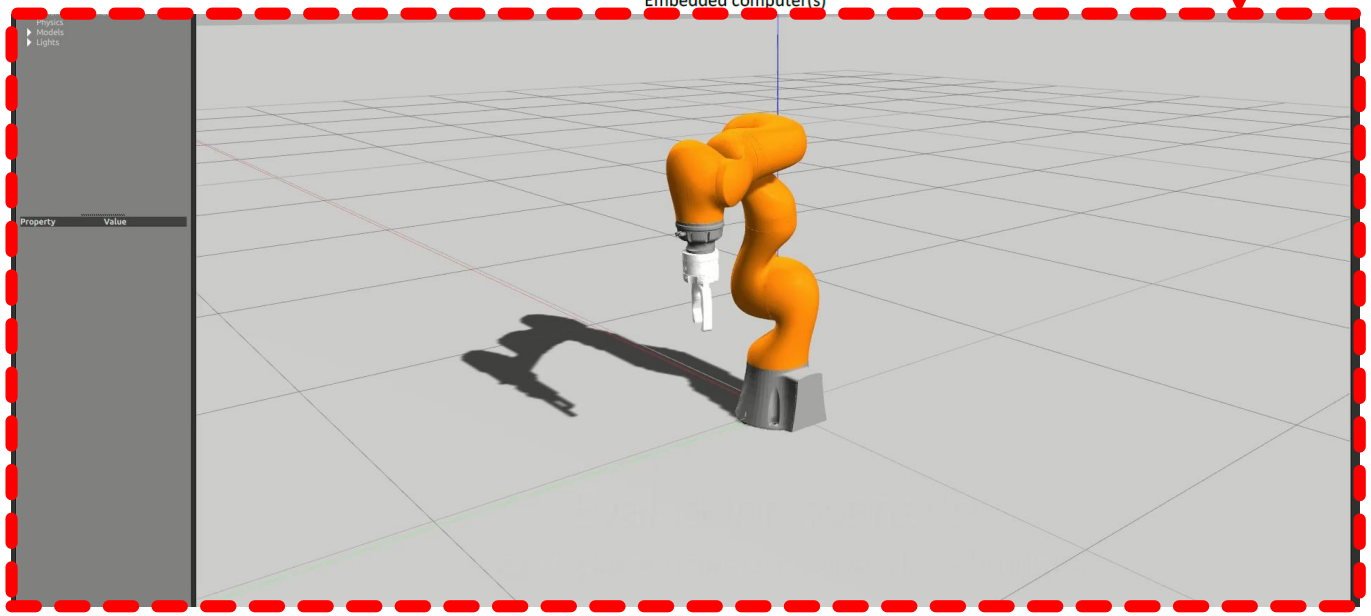
Safety Analysis Use Case Scenario

RobMoSys

- Design of a real-time Cartesian impedance controller, in torque mode.



- Identify the critical faults to be monitored to avoid unintended movements (hazard), that may cause collisions (harm).



Scenario Workflow

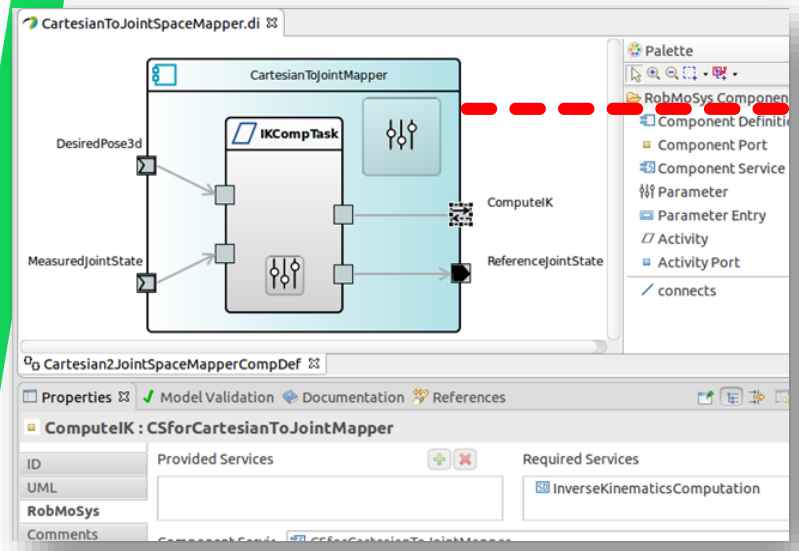
RobMoSys

RobMoSys

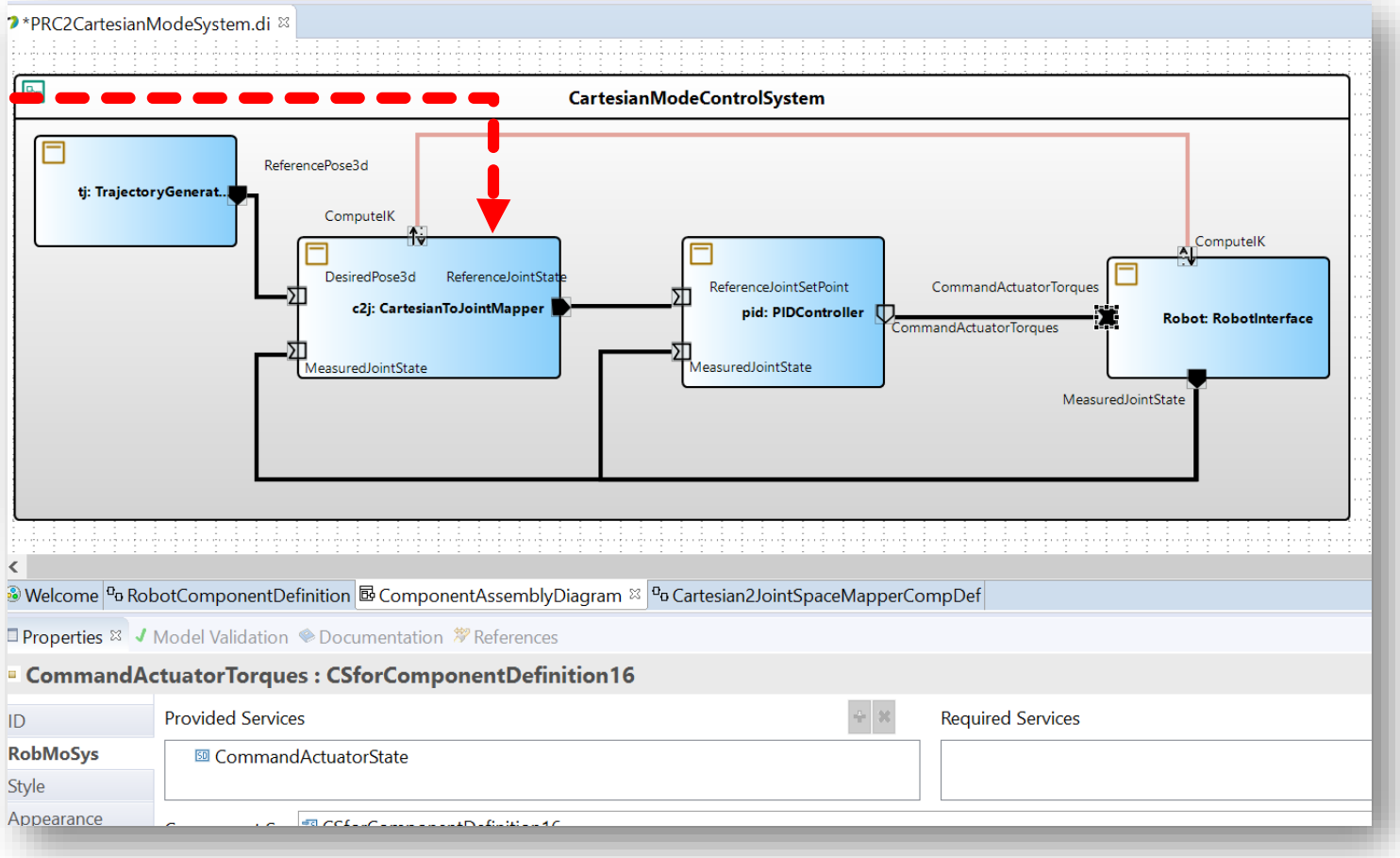
component supplier

system builder

Define System Architecture: Connectors, Service Instantiation, Data exchanged



Define Components: Ports, Services, Parameters, Activities

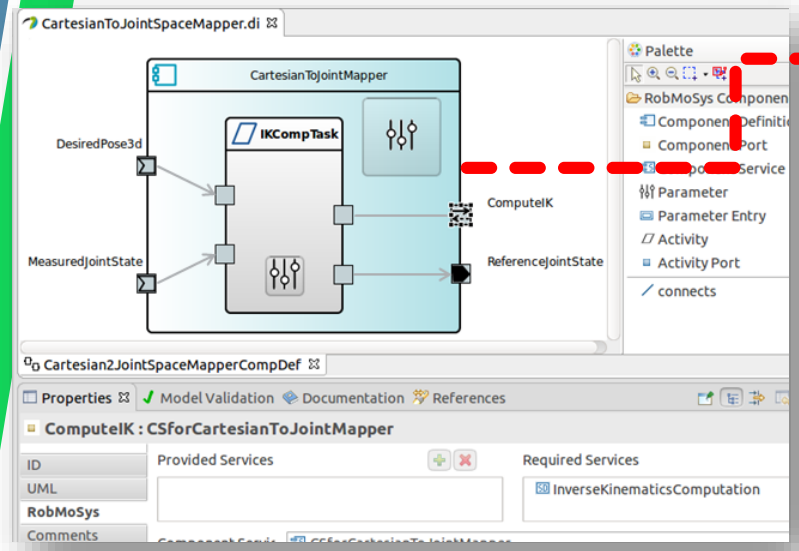


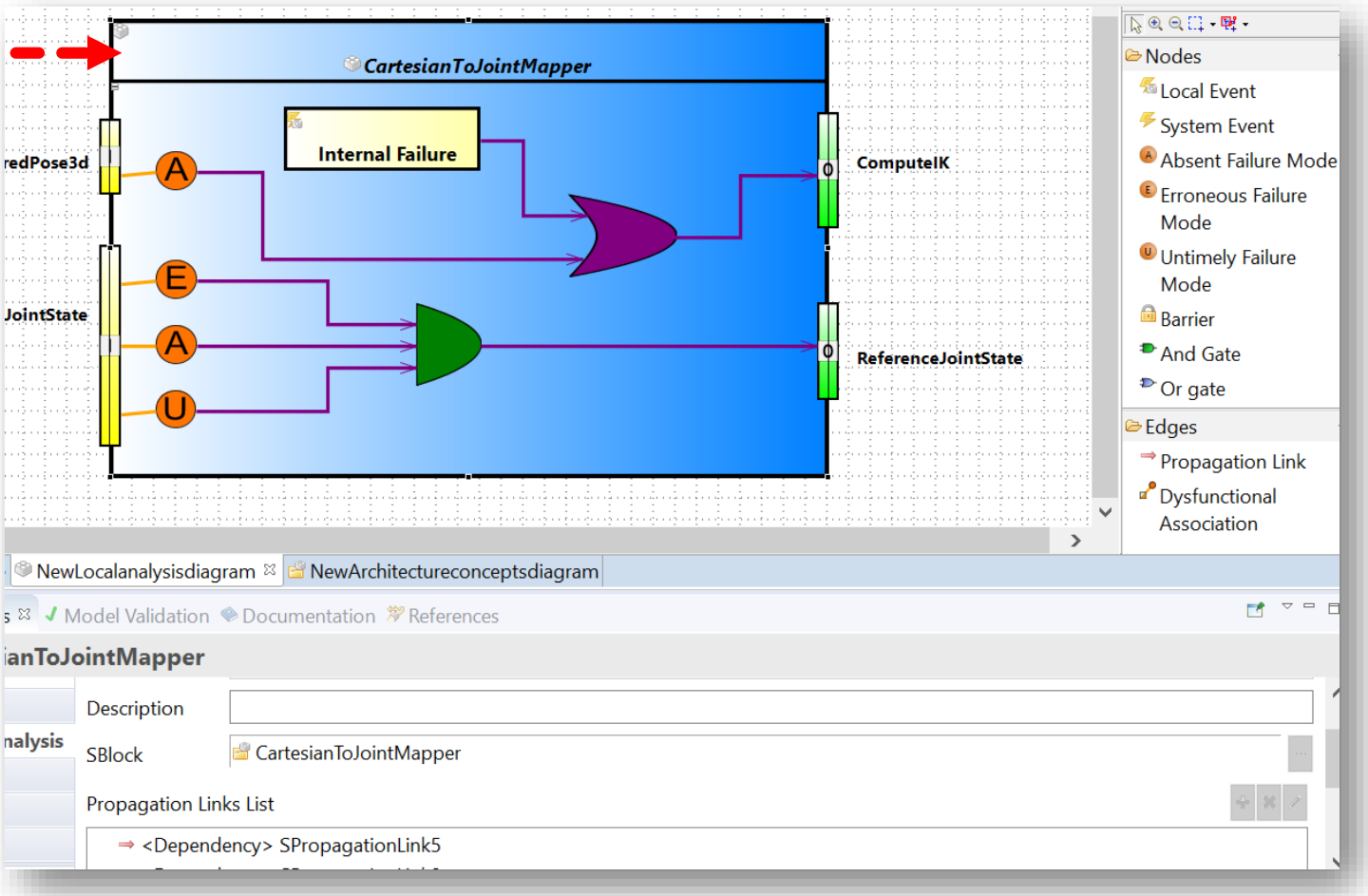
RobMoSys

component supplier

safety engineer

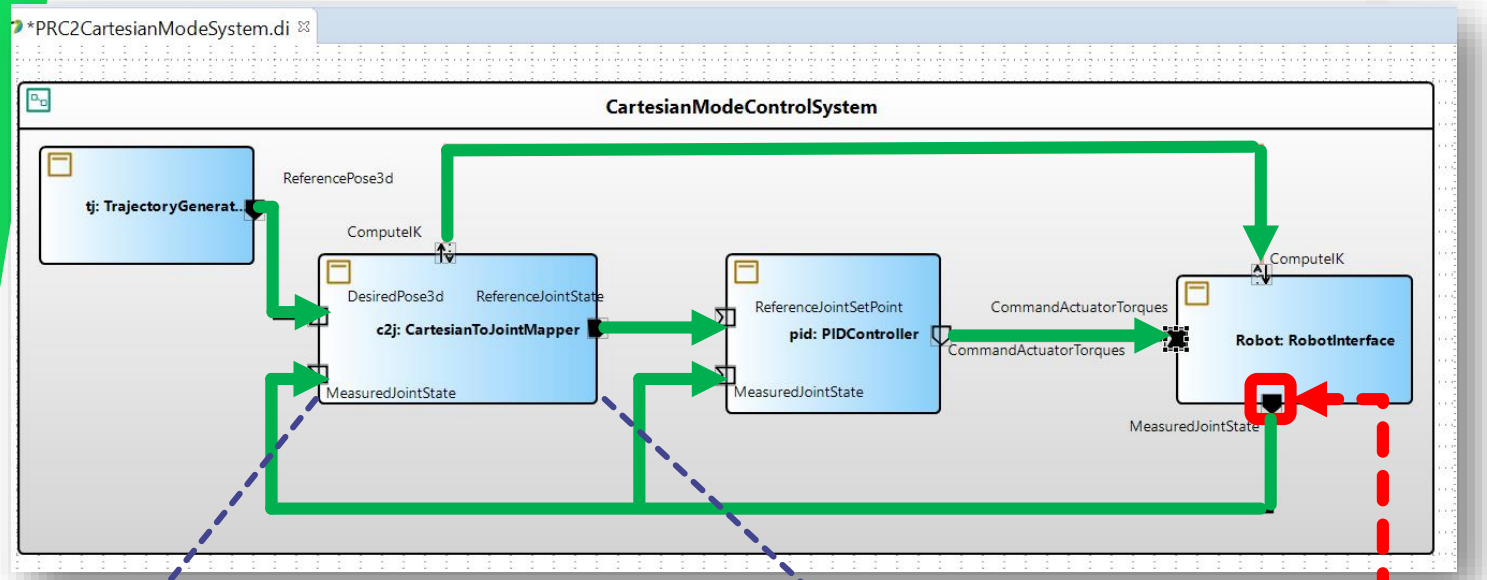
Associate failure modes to ports, internal failures, propagation links, and barriers

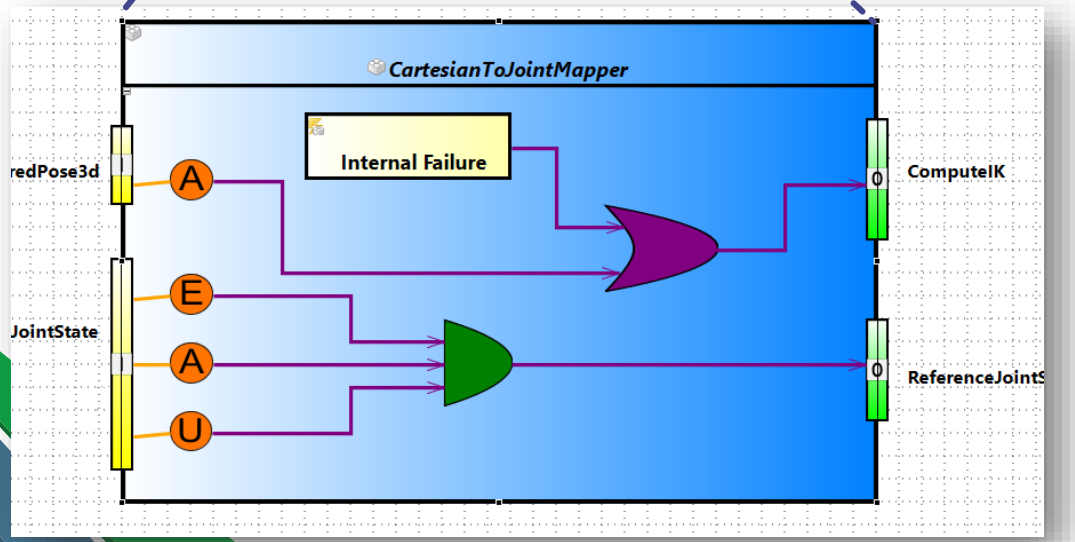




It defined the potential fault propagation inside each component

RobMoSys



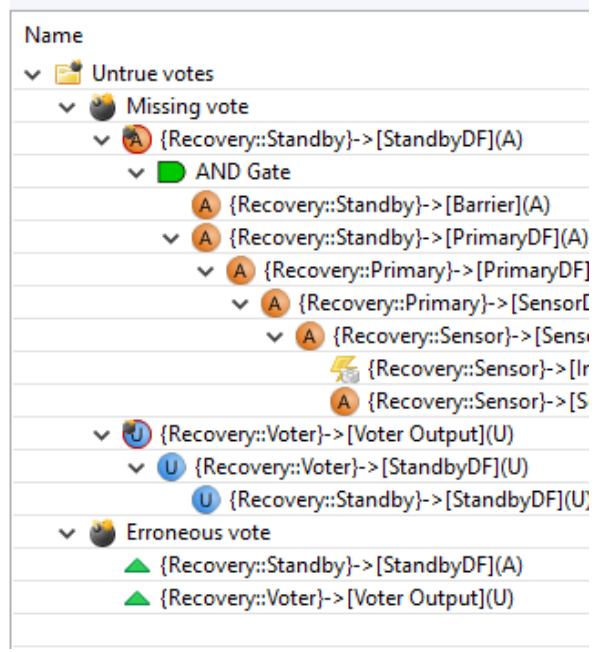


Set to "Top Event"

This defines the (high-level) safety requirement:

"pick & place trajectory speed < 250 mm/s"

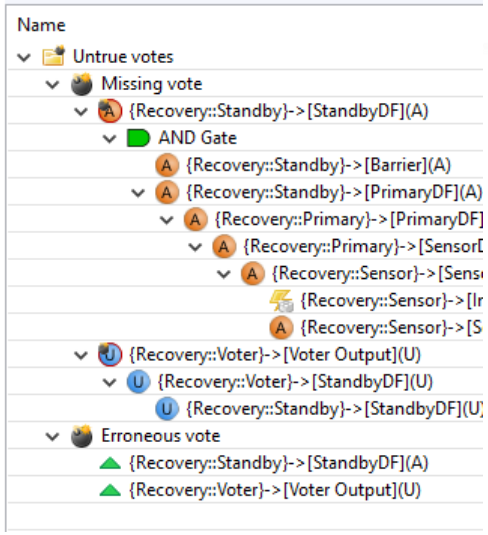
Fault Propagation Tree

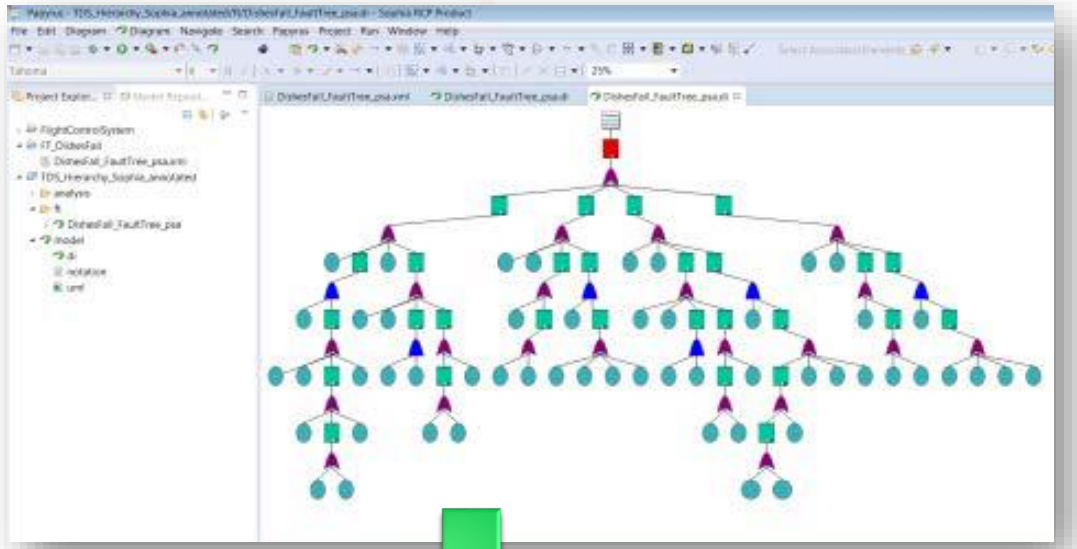


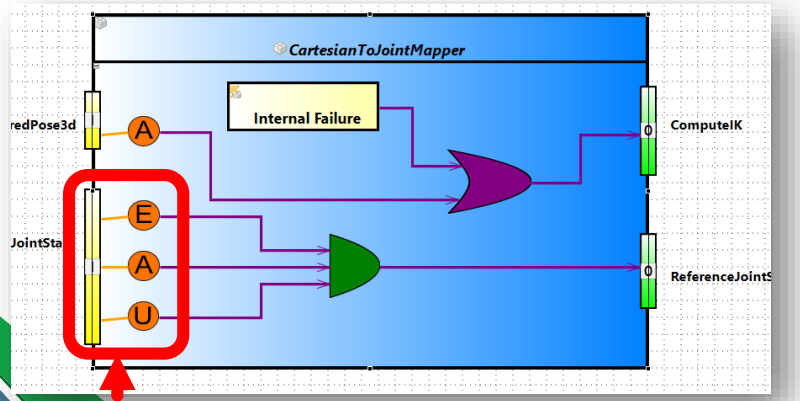
* solver under development

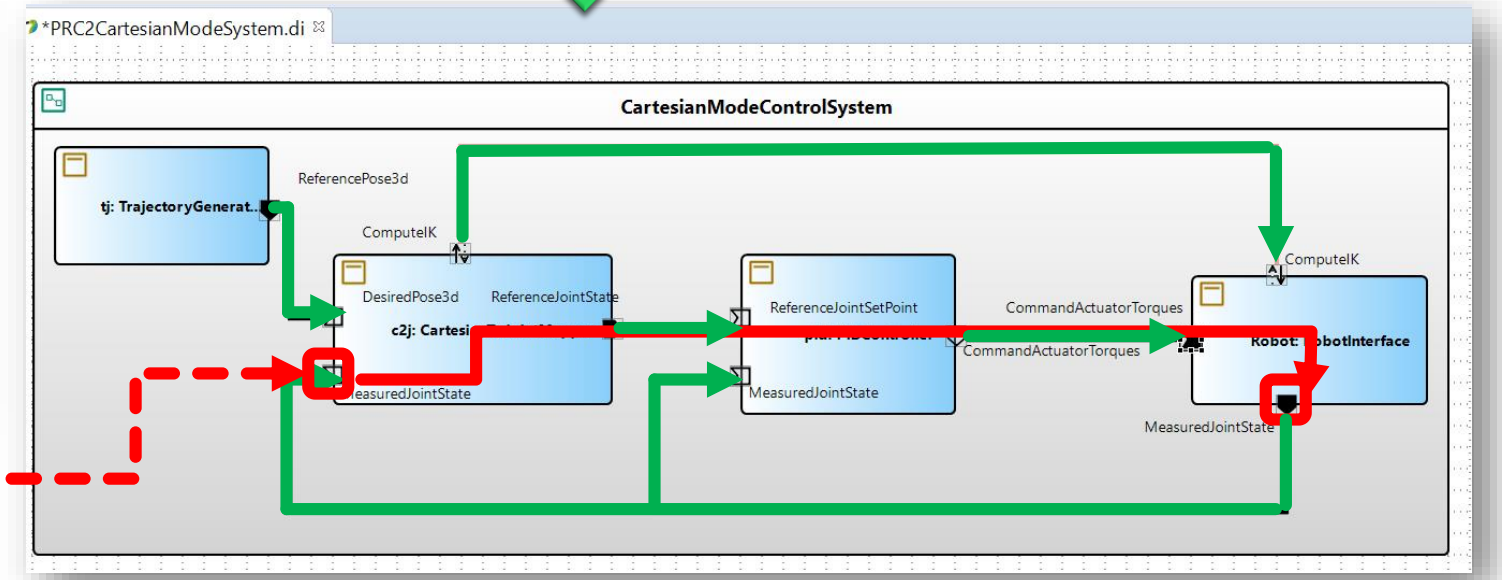
1. 2. 3. **4. Critical Path Identification**

RobMoSys





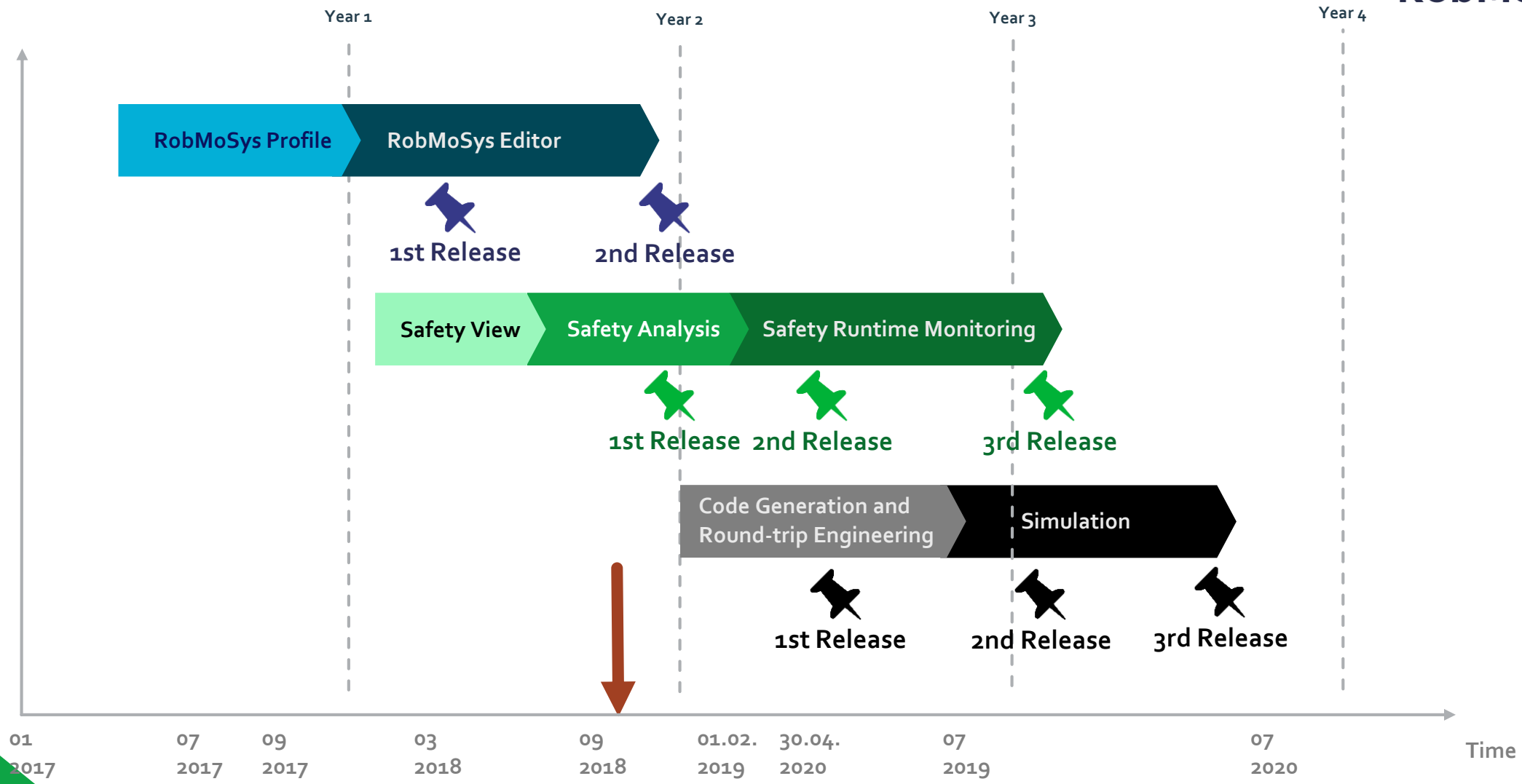




Faults that must be monitored and mitigated

Papyrus4Robotics Roadmap

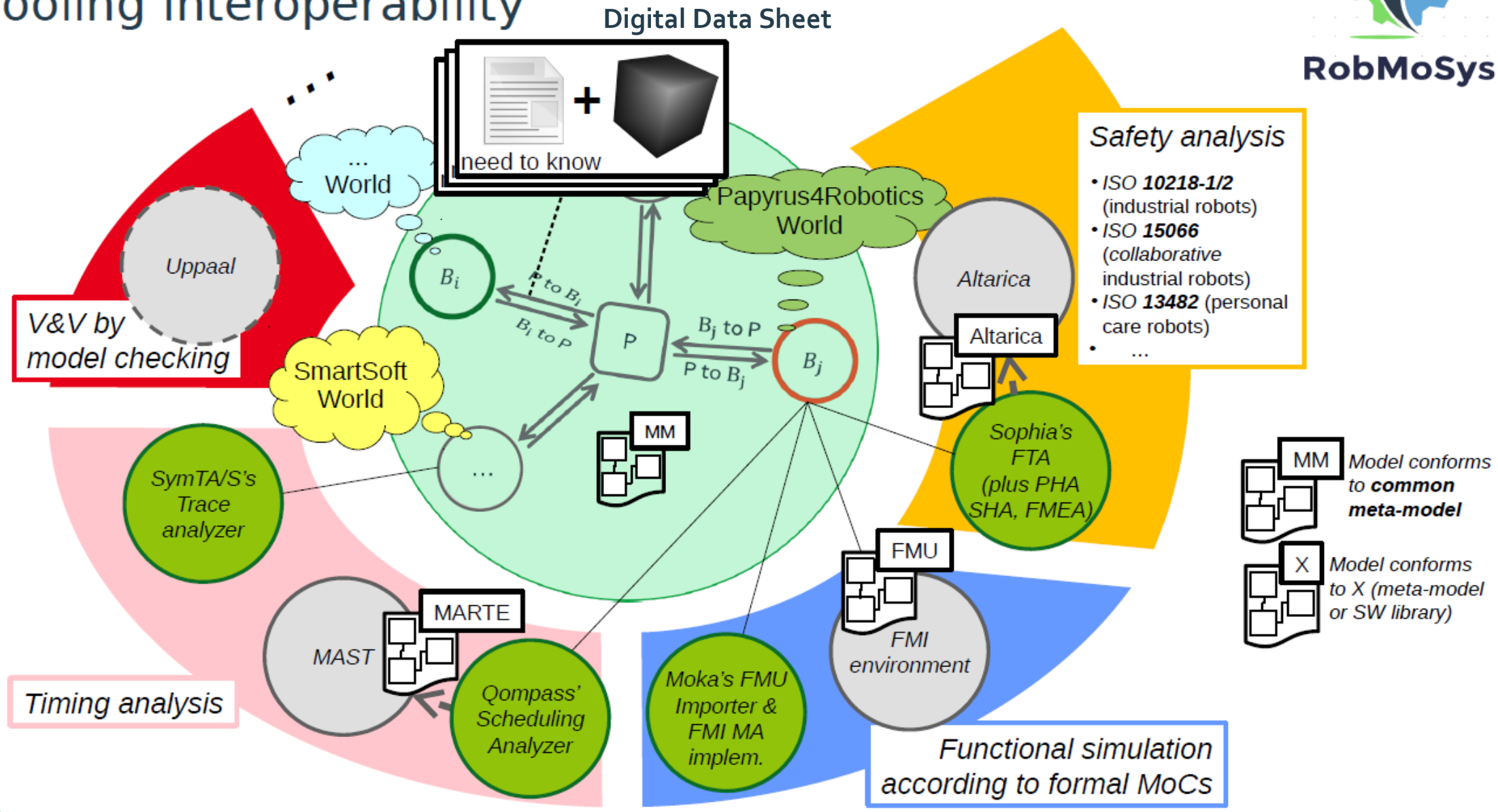
RobMoSys



RobMoSys

Thanks!
Questions?

Tooling Interoperability



RobMoSys

Ambition of Creating Models