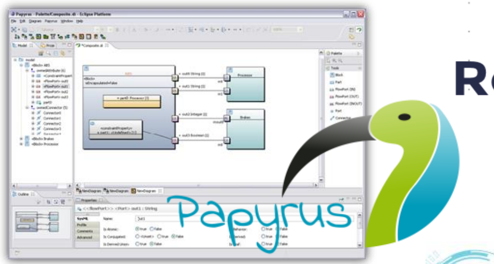
Papyrus4Robotics Example

Matteo Morelli (CEA)

Community Workshop 12th September 2018

Papyrus(4Robotics)

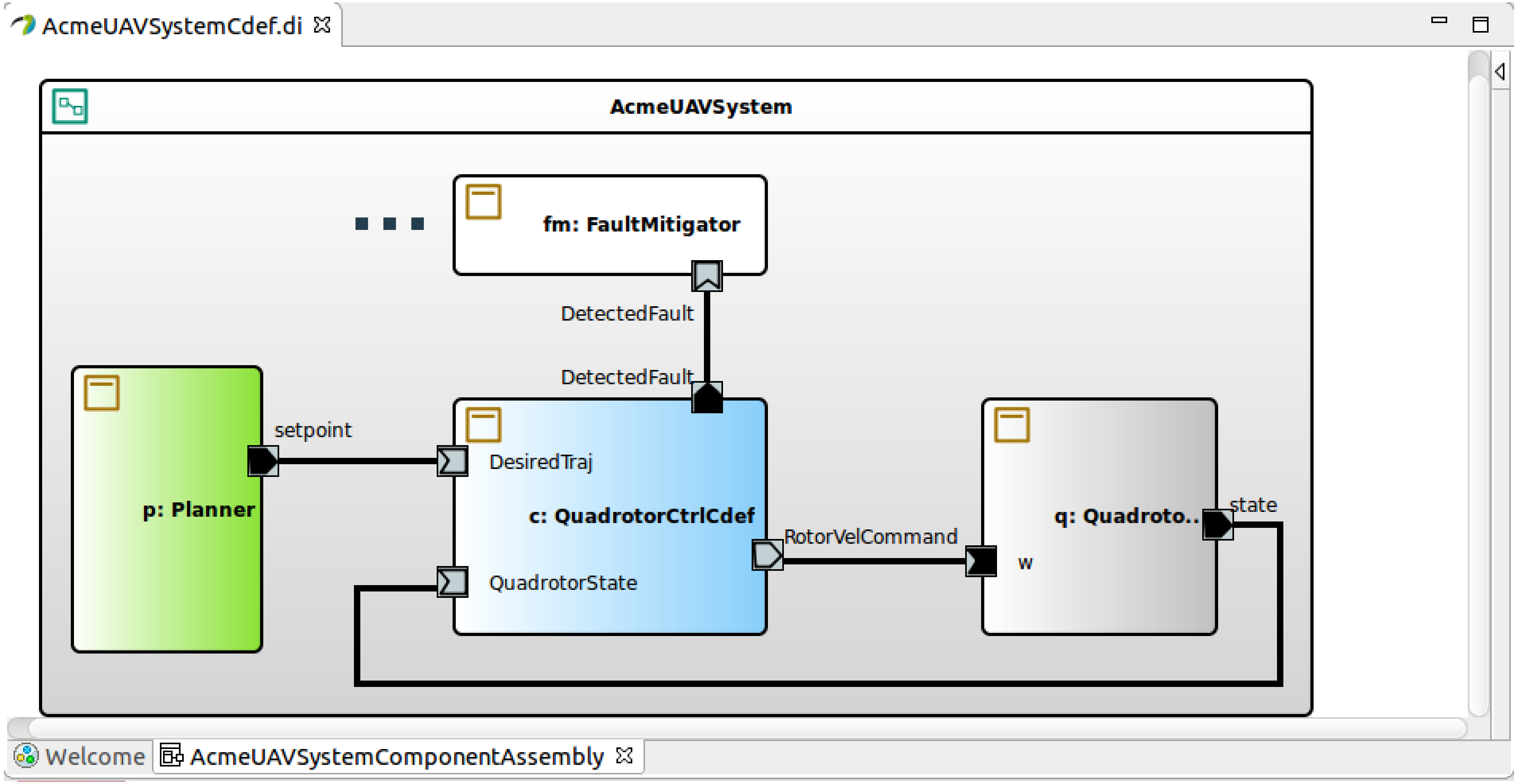
- ***Papyrus***
  - One-liners
    - ***industrial-grade open source Model-Based Engineering tool***
    - ***Standard based (UML, fUML, SysML, MARTE, FMI 2.0, …)***
    - ***Customizable to address domain-specific concerns (model explorer, diagram notation and style, properties views, palette,…)***
  - Get started: https://www.eclipse.org/papyrus/documentation.html
  - More on successful use-case stories: https://www.eclipse.org/papyrus/testimonials.html
  - Papyrus Industry Consortium: https://www.polarsys.org/papyrus-ic/about



- ***Papyrus4Robotics***—customization of Papyrus for the robotics domain
  - feature a **RobMoSys-aligned modeling front-end** and a collection of ***DSLs and tools*** for thorough assessment of multiple design criteria (functional V&V, safety, performance, …)
  - https://robmosys.eu/wiki/baseline:environment_tools:papyrus4robotics

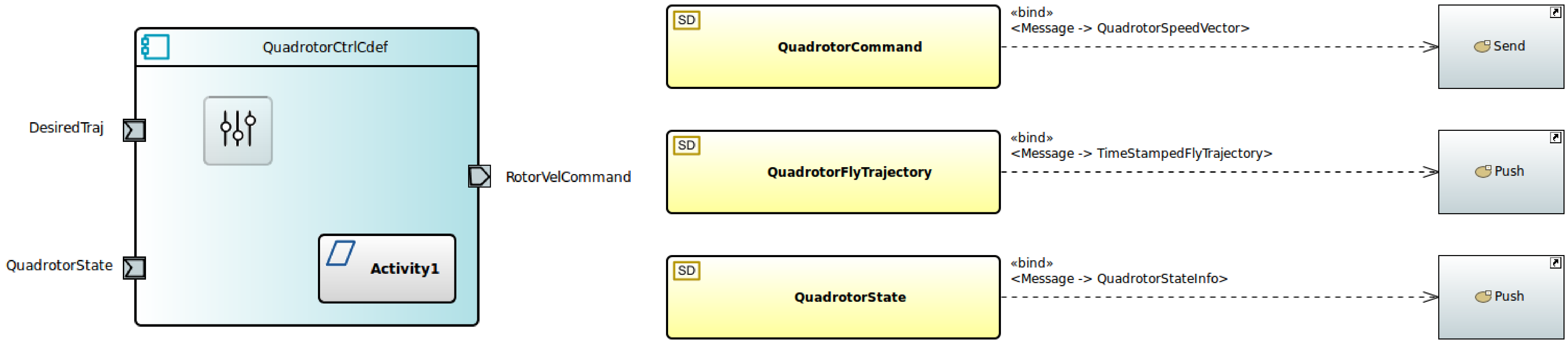
Focus of the talk

- A system builder has just built the component-based architecture for his specific use-case: area monitoring against intrusions using a UAV quadrotor
- How he did it? What is (roughly) the work behind the QuadrotorCtrl component he selected?



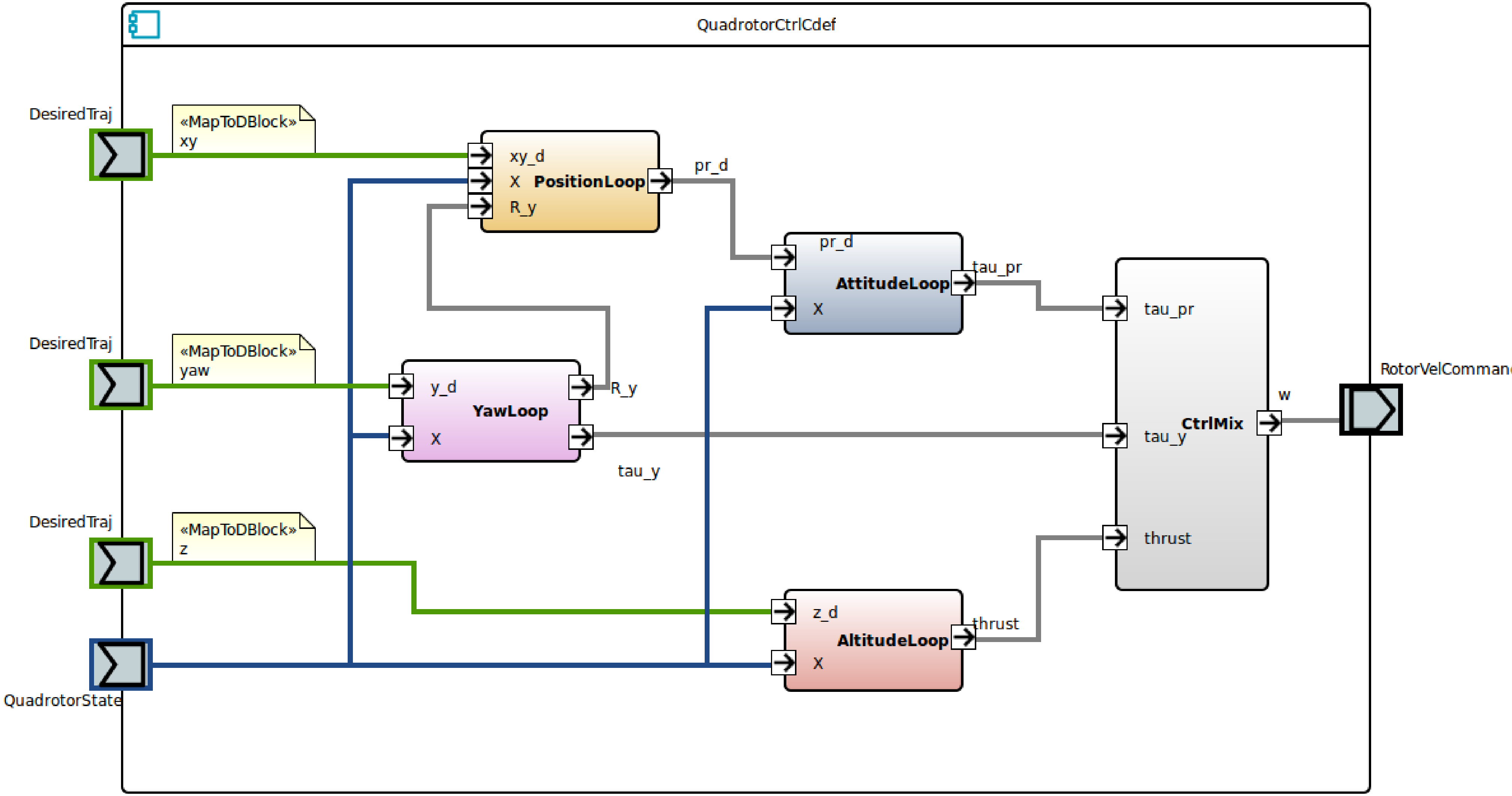
Component Development

- QuadrotorCtrl, part 1 : ComponentDefinition, ports, services



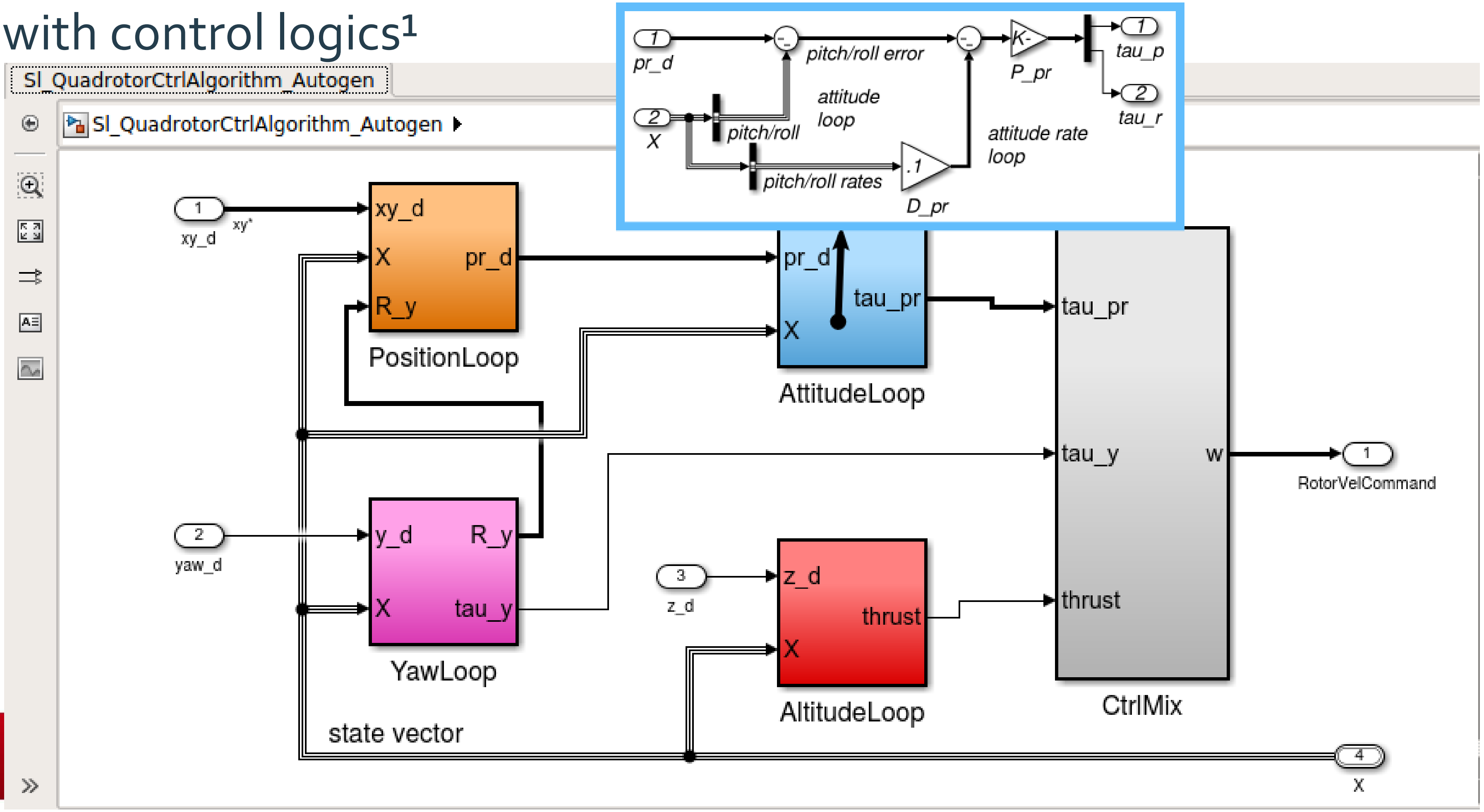
Component Development (cont'd)

- Part 2: algorithm (WiP) and parameters



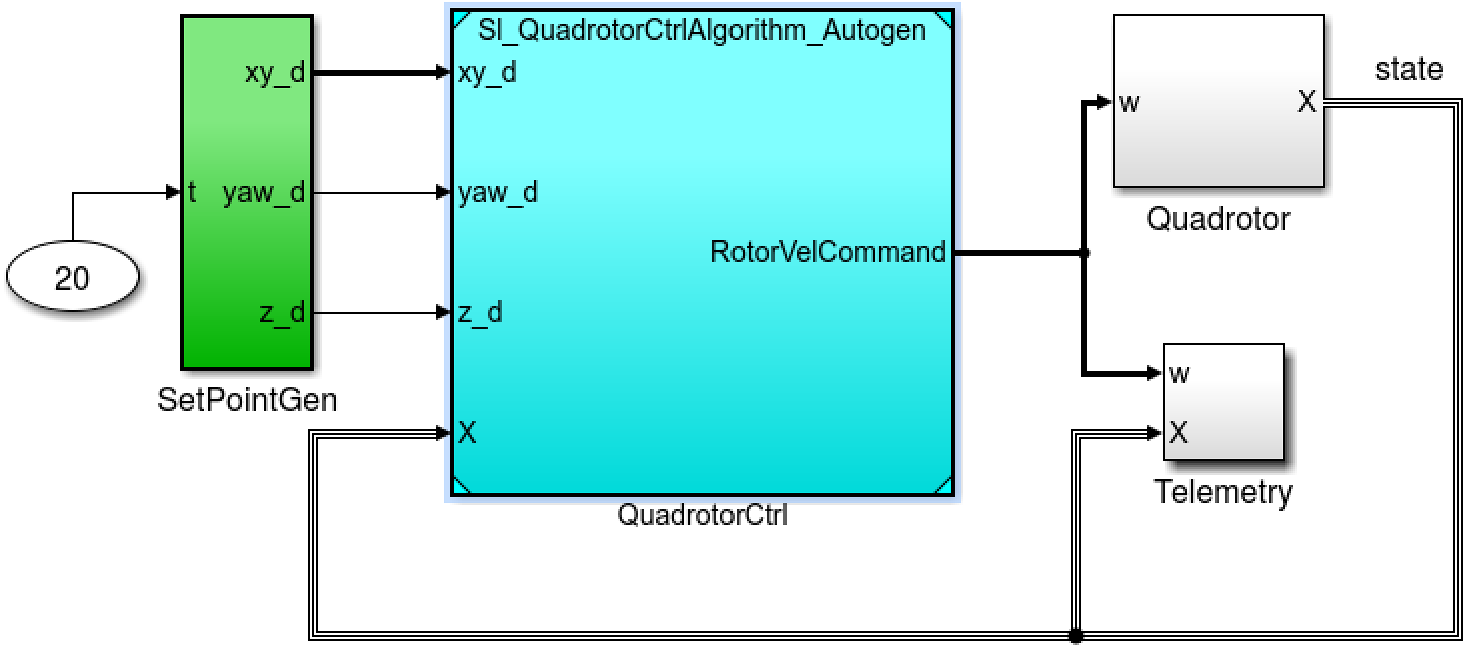
Validation by Simulation (1/2)

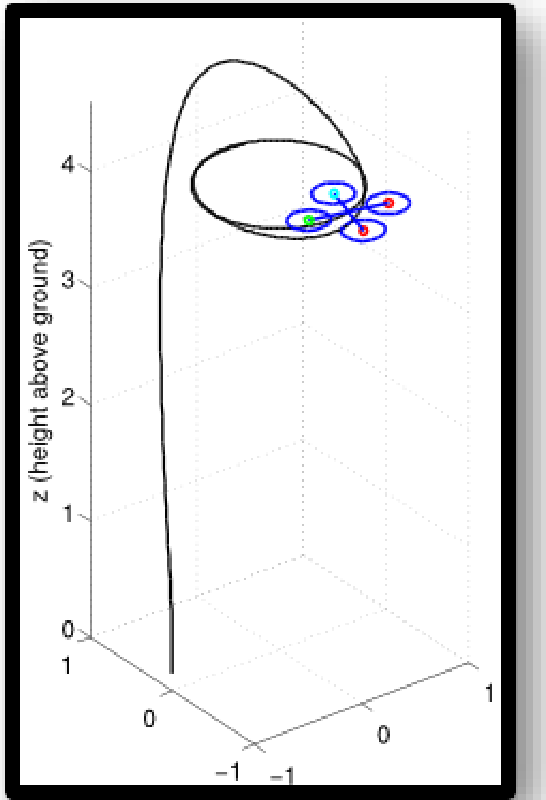
- Fast transition between system definition and simulation models for the verification of performances against requirements
- Algorithm structure and parameters are generated; the control expert fills the functions with control logics[1]



Validation by Simulation (2/2)

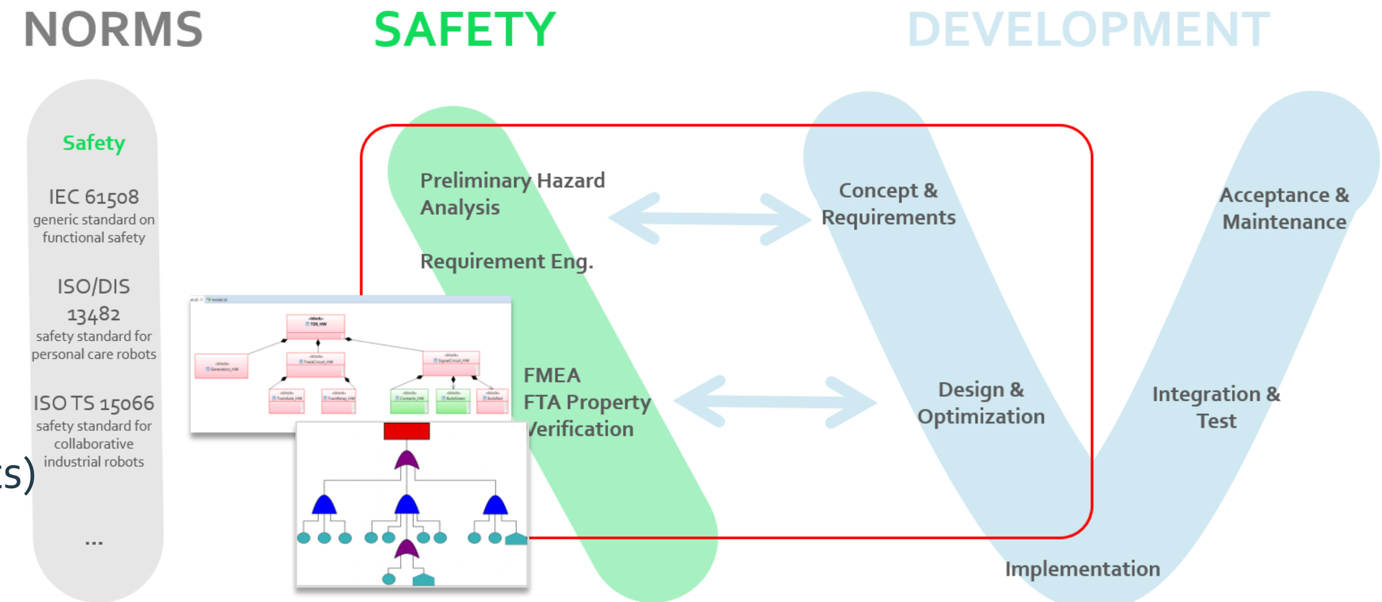
- The generated algorithm is instantiated in a test model as ModelReference block
- The control engineers validate/refine the algorithm against different quadrotor dynamics and under different scenarios





Safety Analysis with Papyrus4Robotics

- ***Rationale***
  - demonstrating conformance to safety standards can become a functional and legal requirement for robot technology to be put in operation
  - Papyrus links architecture descriptions with dedicated concepts for safety analysis
- **Integrated approach** to address safety concerns in the early phases of design
  - Hazard Analysis
  - Failure Mode & Effect Analysis
  - Fault Tree Analysis
  - Property Verification
  - Safety Guidelines
    - *ISO-DIS 13482*
      (Safety of Personal Care Robots)



RobMoSys

cea · Hochschule Ulm · KU LEUVEN · TUM · COMAU · PAL ROBOTICS · SIEMENS · EUnited Robotics · eclipse

Model-based Safety Analysis (FMEA)

- FMEA Analysis context, definition of FMEA table and failure modes[2]
  → effects and their criticality (automatically computed)

Project Explorer | Model Explorer

- «ComponentDefinitionModel, SModel» QuadrotorCtrl
  - «SSafetyArtifacts» SafetyArtifacts
    - «SFMEA» FMEA
      - «SBlockFMEA» QuadrotorCtrlCdef
        - FMEAActuatorFMOscillMode
        - FMEAActuatorFMDeadband
        - FMEAActuatorFMFloatSurf
        - Table FMEATable0
  - «ComponentDefinition, SBlock» QuadrotorCtrlCdef
  - *«EPackage, ModelLibrary» UML Primitive Types*
  - *«ModelLibrary» Ecore Primitive Types*

QuadrotorCtrlCdef.di

		A	B	C	D	E
		Name	Description	Causes	Local Effects	System Effects
0	FMEAActuatorFMOscillMode	FMEAActuatorFMOscillMode	Actuator oscillatory mode	Software bug; faulted RxMux	Limited pitch control; Induce...	LOM, LOV
1	FMEAActuatorFMDeadband	FMEAActuatorFMDeadband	Actuator increased deadban...	Damaged servo driveshaft	Slow actuator dynamics; Lim...	LOM
2	FMEAActuatorFMFloatSurf	FMEAActuatorFMFloatSurf	Actuator floating surface	Broken linkage; Broken servo...	Limited pitch control; LOC	LOM, LOV

Welcome | QuadrotorCtrlCdef_ESFArchitectureDiagram0 | FMEATable0

...

		G	H	I	J	K
		Initial Severity	Initial Occurence	Is Detectable	Initial Detectability	Initial Criticality
0	FMEAActuatorFMOscillMode	9	1	☑	5	45
1	FMEAActuatorFMDeadband	6	1	☑	5	30
2	FMEAActuatorFMFloatSurf	9	4	☑	5	180

Welcome | QuadrotorCtrlCdef_ESFArchitectureDiagram0 | FMEATable0

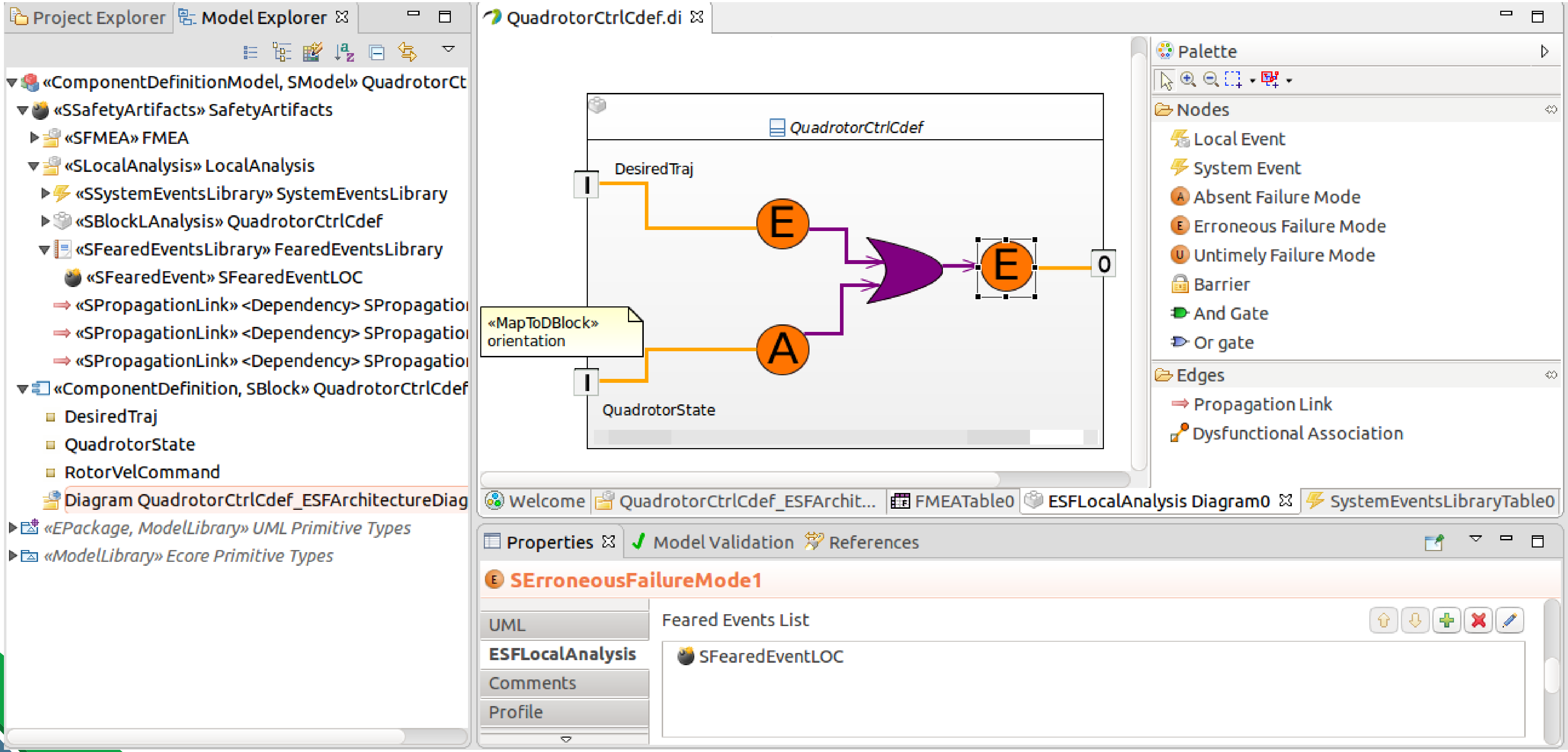
...

Hochschule Ulm

University of Applied Sciences

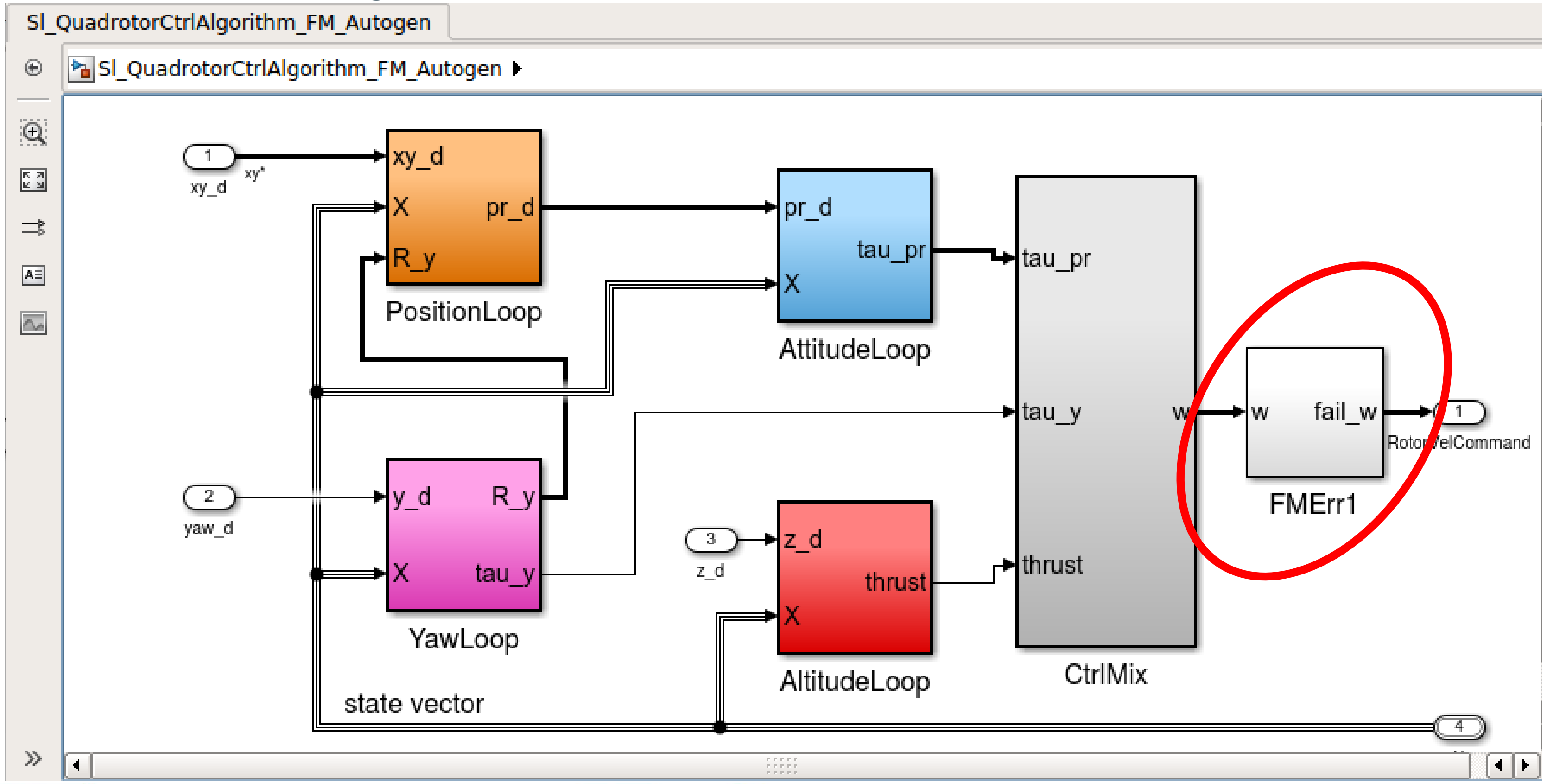
Model-based Safety Analysis (LA)

- Local Analysis (LA) consists in linking the failures modes of the block stream output with the failure modes of its input stream (or with internal failures)



Failure Mode Assessment by Simulation

- LA failure modes can be translated to Simulink blocks → effects of LA failure modes can be assessed by simulation → fault detection and mitigation strategies can be designed

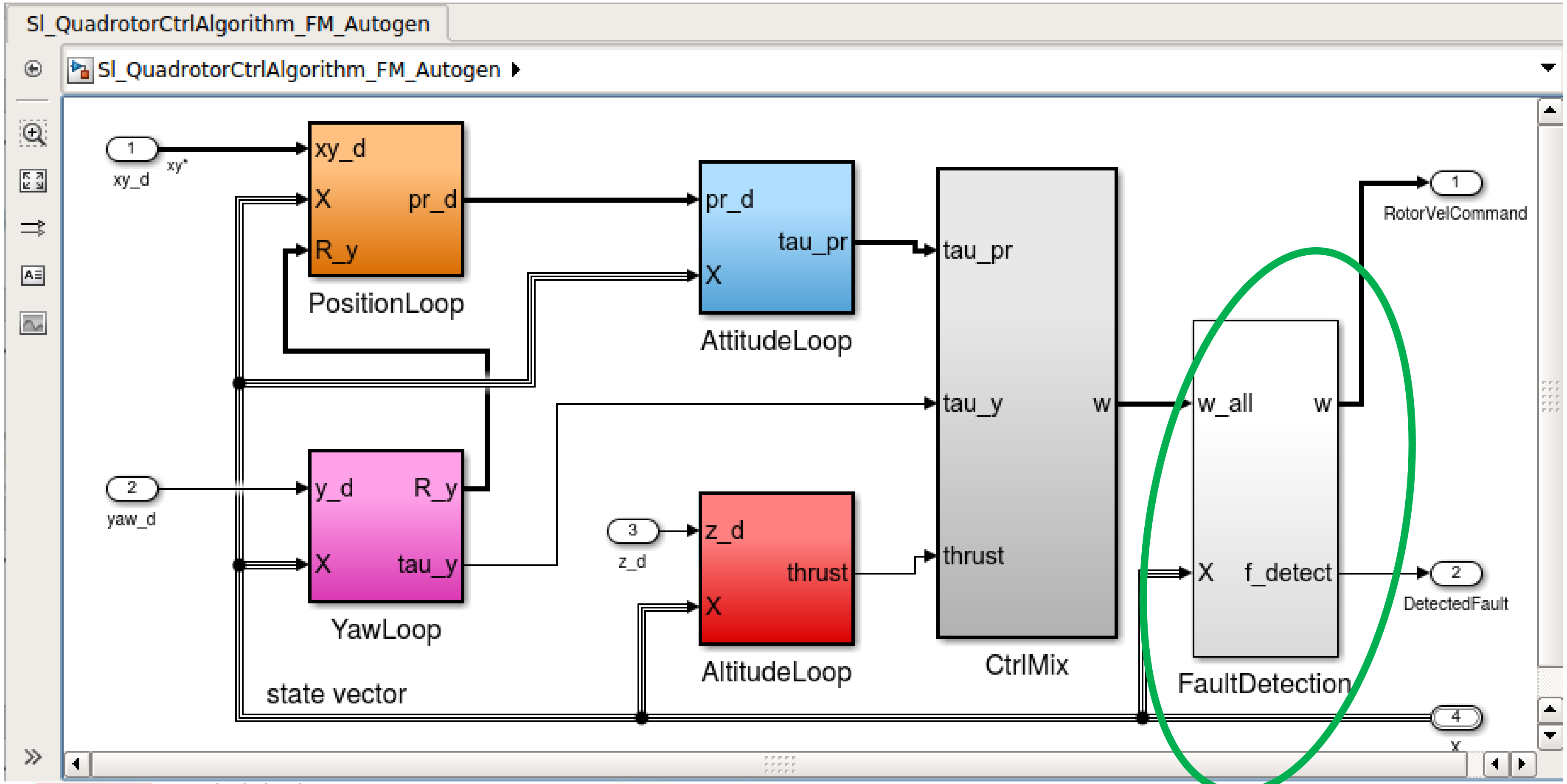


RobMoSys

Hochschule Ulm
KU LEUVEN
TECHNISCHE UNIVERSITÄT MÜNCHEN
COMAU
PAL ROBOTICS
SIEMENS
EUnited Robotics European Robotics Association
eclipse

Failure Mode Assessment by Simulation (cont'd)

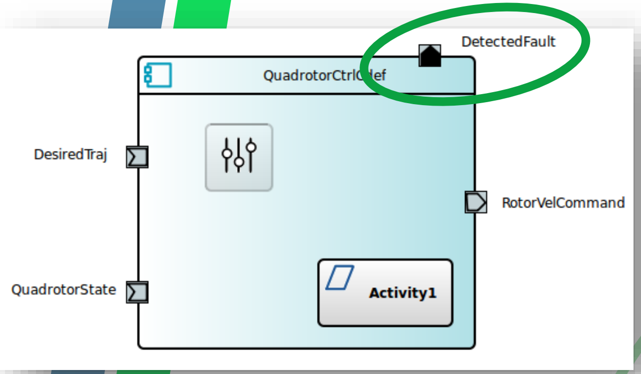
- Safety and control engineers work together to design fault detection and mitigation strategies



Collaborative Workflow between Different Roles

RobMoSys

*Incremental update to **reflect changes made to the other model***



Robotic Component developer

__Models evolve__ (concurrently): __refinements__—add/remove ports, components, connections, change interface types, etc. (can) __occur__ (on both sides)

__Incremental__ on-demand synchronization maintains the __consistency__ between (relevant part of) models—structural and behavioral features of models

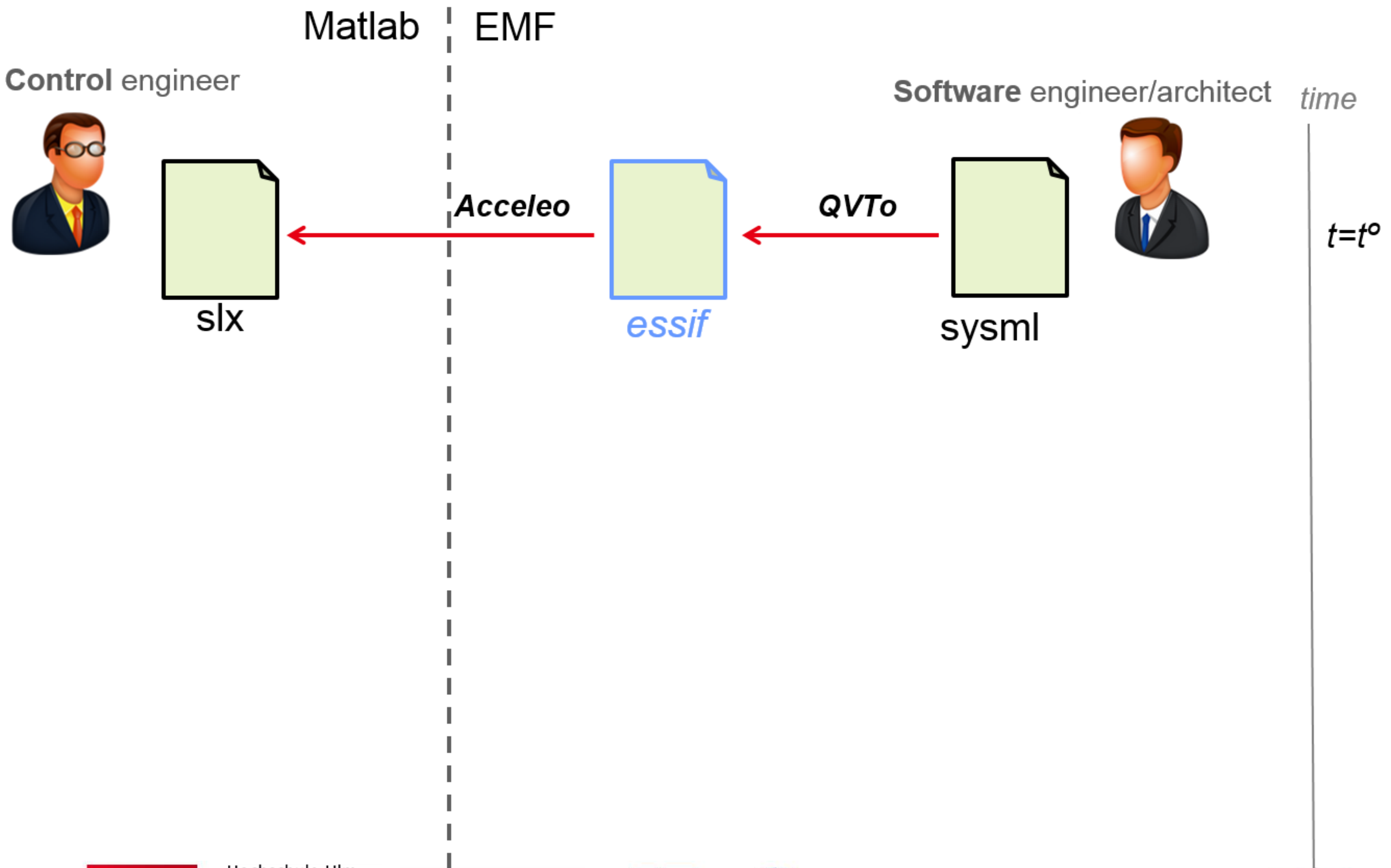
(Incremental update to reflect changes made to the other model)

Control engineer

cea · Hochschule Ulm · KU LEUVEN · TUM Technische Universität München · COMAU · PAL Robotics · SIEMENS · EUnited Robotics European Robotics Association · eclipse

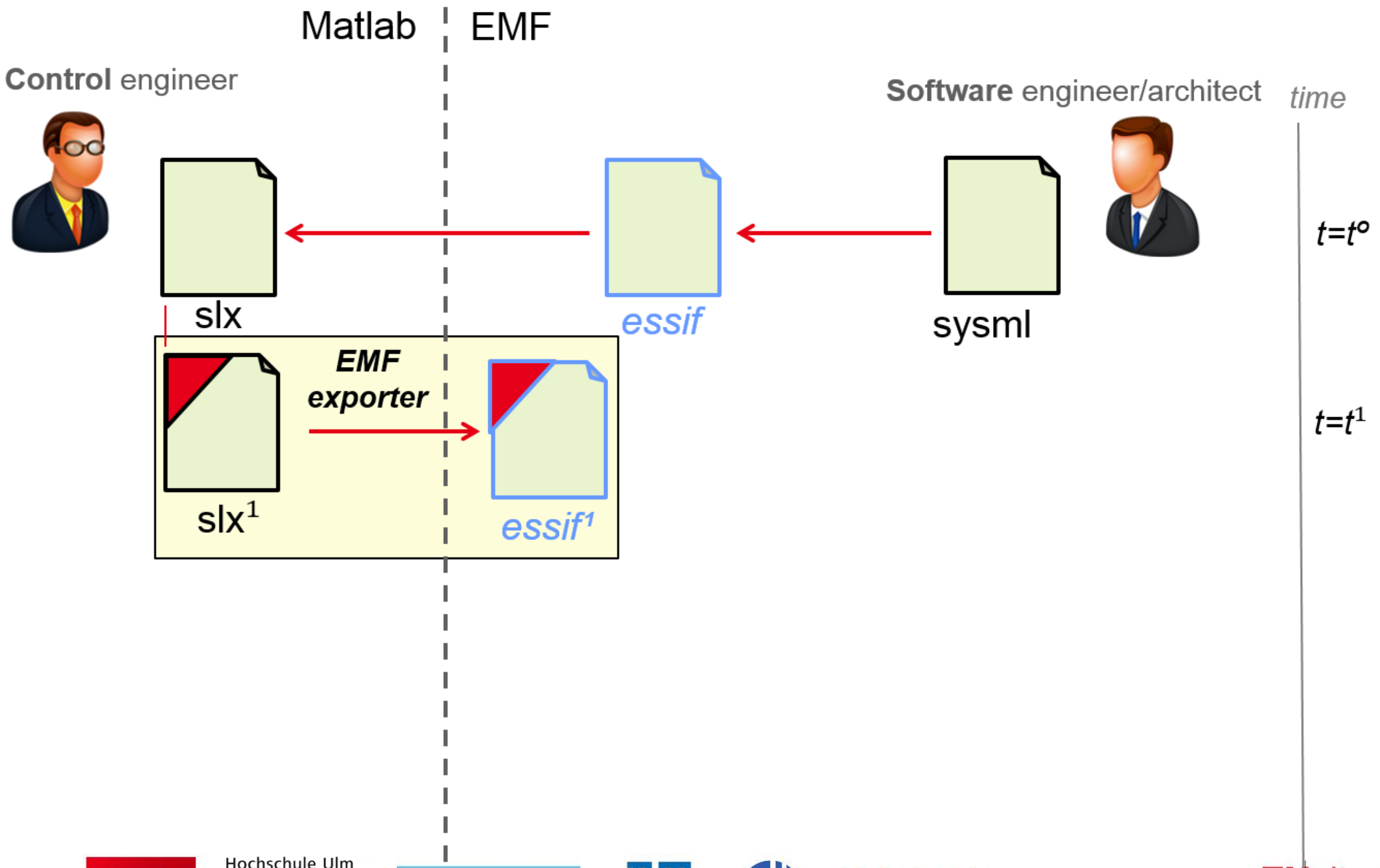
Round-trip engineering

Batch generation of Simulink model from a SysML model of SW systems.



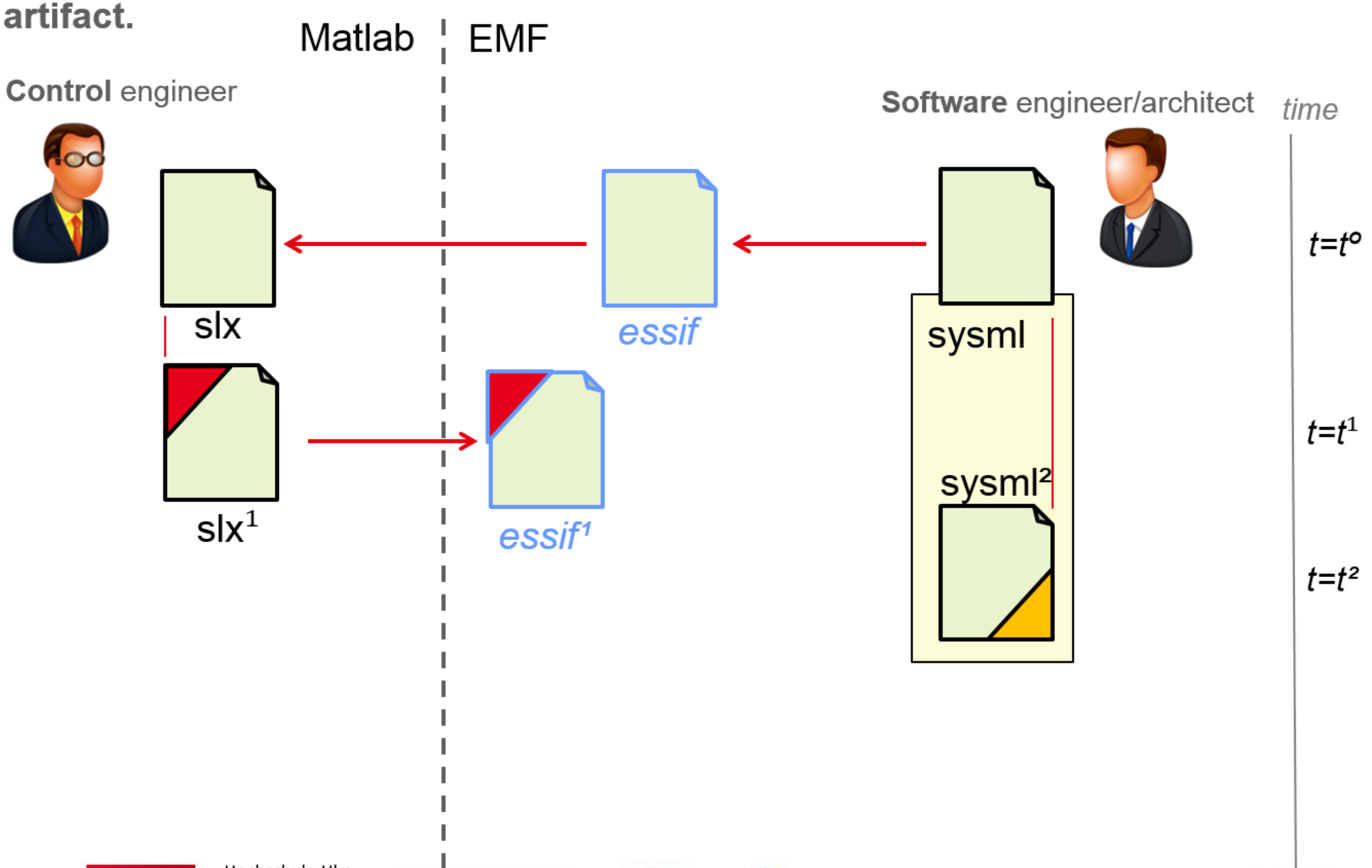
Round-trip engineering

Evolution of Simulink model and generation of synchronization artifact.



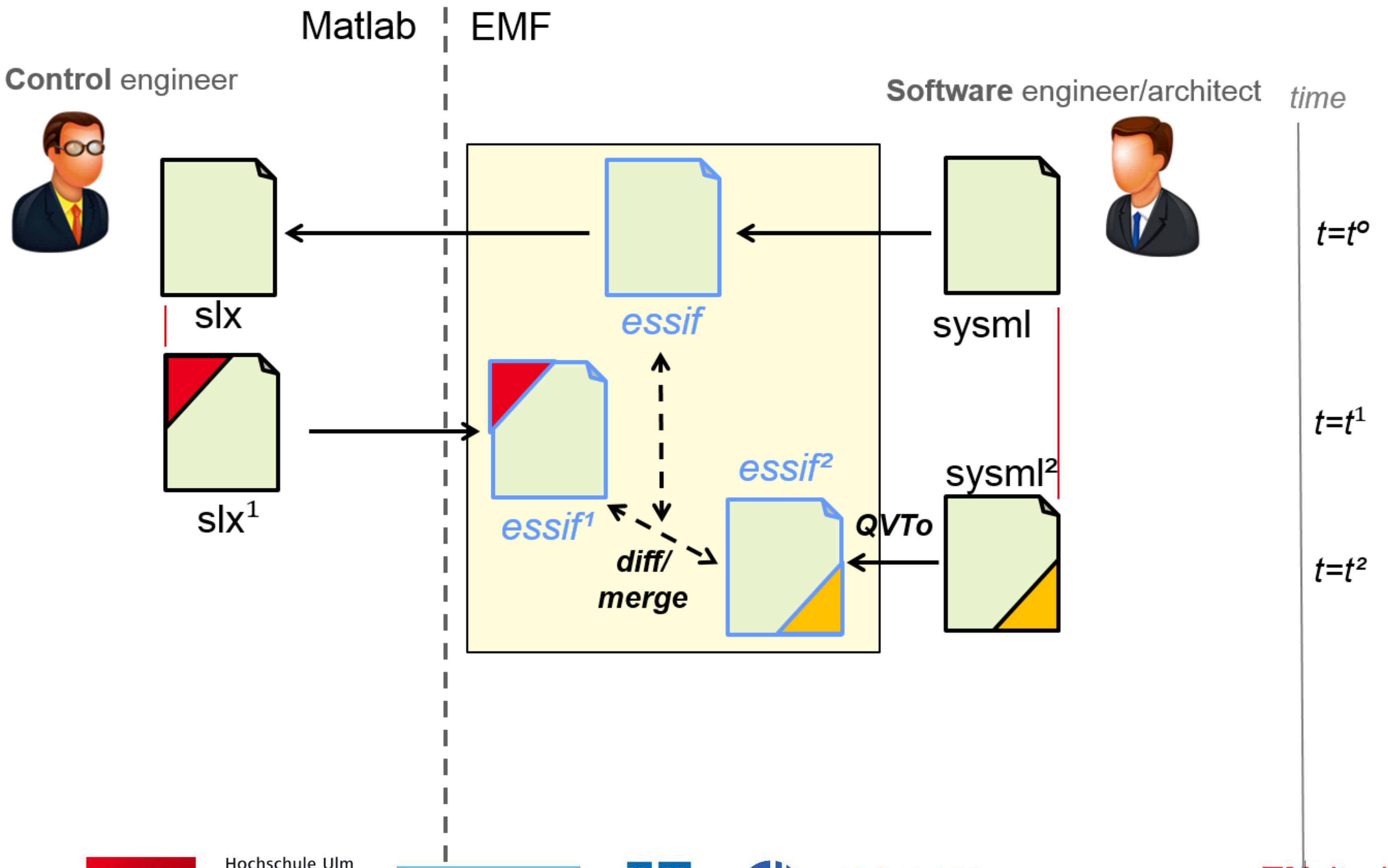
Round-trip engineering

Evolution of SysML model; preparation to the generation of the synchroniz. artifact.



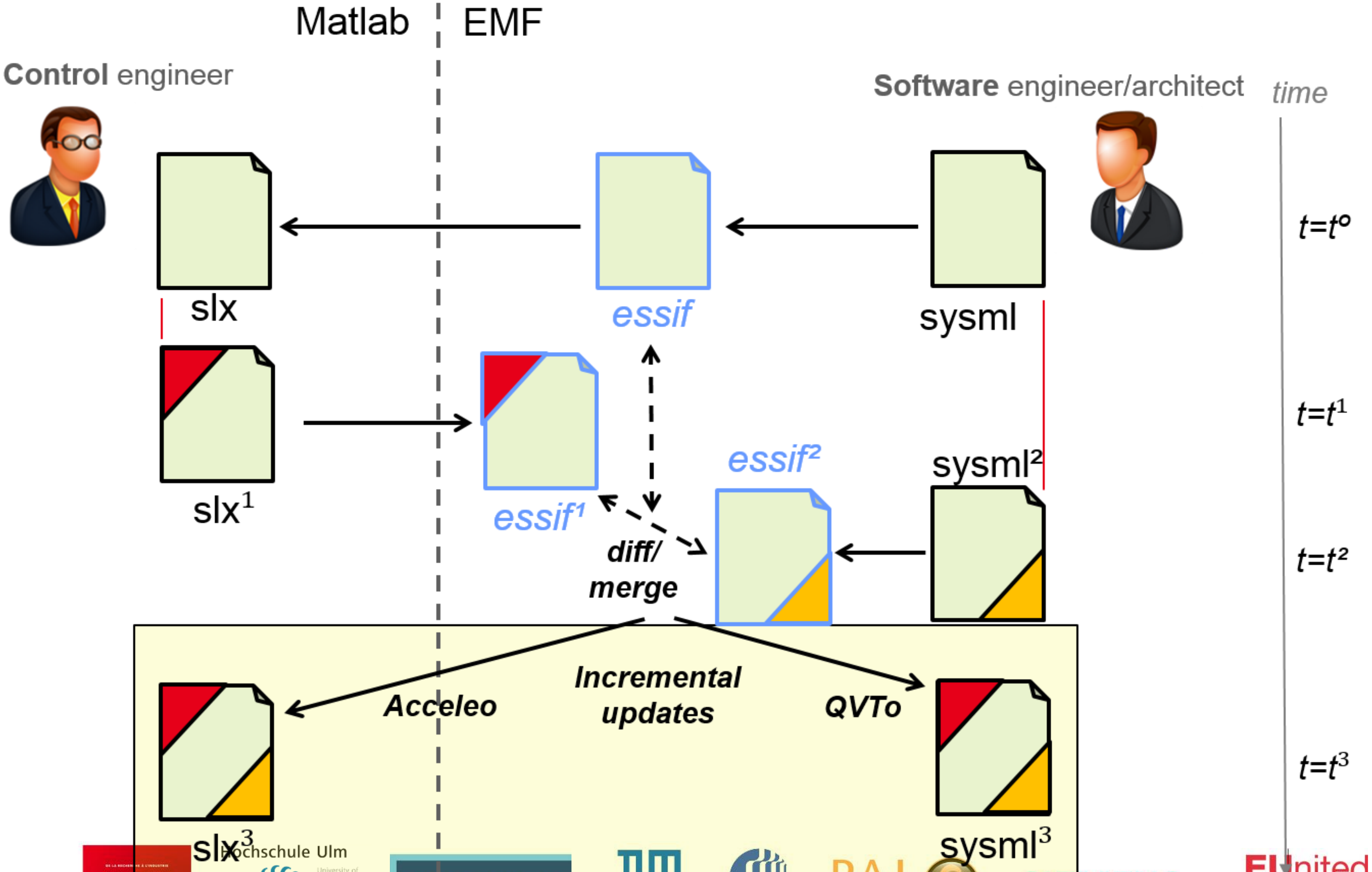
Round-trip engineering

Operation of 3-way comparison process.



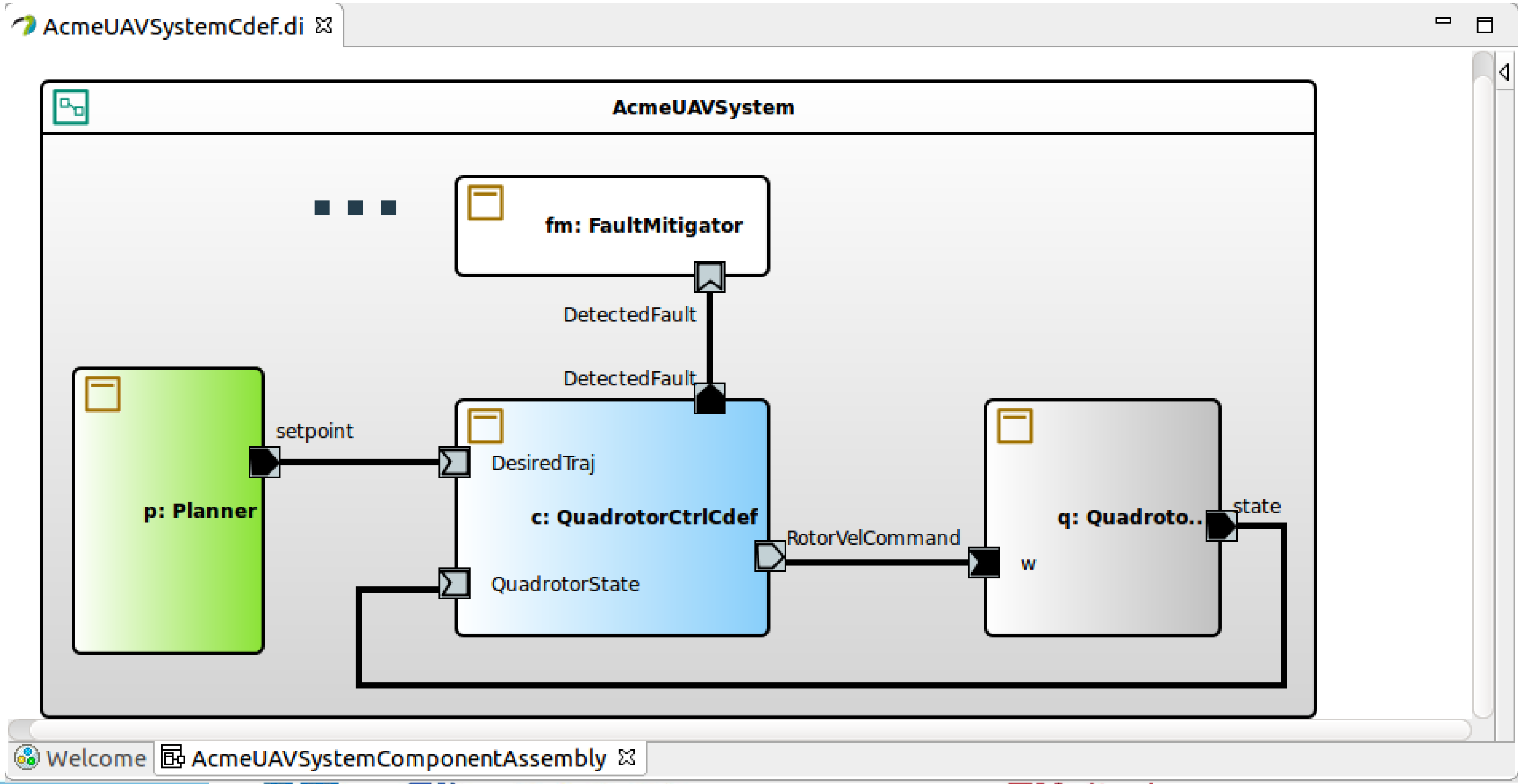
Round-trip engineering

Achieving synchronization through incremental model updates.



That's All For Now

- This is only part of the story: rapid control prototyping and test of QuadrotorCtrl logics, dysfunctional analysis to early address safety concerns (fault detection & mitigation)
- Other paths for a complete story include: interfacing with task-level behavior (for multiple operating modes), performance analysis (how to map functions into threads, deploy using resource reservation schemes), deploy to a concrete target platform, …



RobMoSys

Hochschule Ulm KU LEUVEN TUM SIEMENS eclipse

Recap

- Papyrus4Robotics

  "umbrella framework that collects a set of Papyrus-based DSLs and tools and supports the design of robotic systems in conformance with the RobMoSys approach"

- Support
  - **Fundamental roles** such as **component developer, service designer, system builder, etc.**
  - **Simulation** in Simulink—rapid control prototyping and test; grounds in a formal MoC (logical time, causal, deterministic simulations)
  - Model-Based **safety analysis (FMEA, LA, FTA)**
  - **Integration between roles/views**
- Next version
  - new release coming soon

References

- 1. P.I. Corke, “Robotics, Vision & Control”, Springer 2017, ISBN 978-3-319-54413-7.
- 2. P. Freeman and G. J. Balas, "Actuation failure modes and effects analysis for a small UAV," *2014 American Control Conference*, Portland, OR, 2014, pp. 1292-1297.

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