ExSyn

Explainable Synthesis of Supervisory Controllers

Calvin Terpstra
calvin.terpstra@ru.nl

Supervised by Dennis Hendriks,
Frits Vaandrager and Ivo ter Horst

*How can we increase the **adoption** of **synthesis-based engineering** (**SBE**) and increase the realization of its potential benefits?*

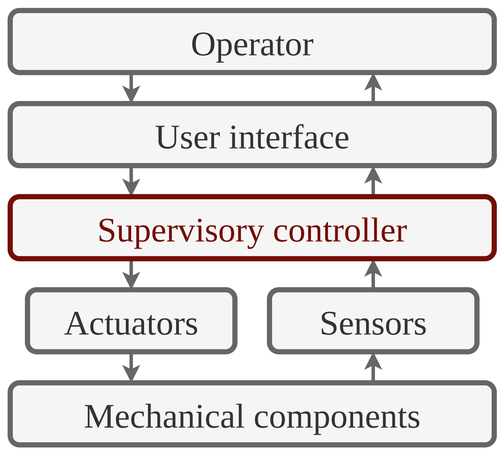
Context

The development of *real-world* supervisory controllers is becoming increasingly complex:

- Performance demands increasing (e.g. parallelization)
- Adaptability to more diverse systems due to system variants and/or evolution of a product family
- Comprehensive robustness to all failures/defects

Leads to downstream problems:

- Larger development efforts and costs
- Longer lead times
- Expertise gap amplifies shortage of skilled engineers



What is **synthesis-based engineering**?

The logical next step in controller engineering.

- Better understanding – focus on **what** the system should do rather than **how** it should to it
- Increased efficiency – highly automated: push-button approach
- Improved quality – correct-by-construction

Engineering approach → / ↓ Development step	Traditional engineering	Model-based engineering	Verification-based engineering	Synthesis-based engineering
Requirements design	Document-based	Document-based	**Model-based (formal)**	Model-based (formal)
Controller design	Document-based	**Model-based (formal)**	Model-based (formal)	**Computer-aided (formal, synthesized)**
Realization in software (implementation code)	Traditional software engineering (coding)	**Code generation (fault-free code)**	Code generation (fault-free code)	Code generation (fault-free code)
Verification (against requirements)	Testing	Testing + model-based testing	**Formal verification (model checking)**	**Correct-by-construction (guaranteed)**
Validation (of requirements)	Testing	Testing + simulation	Testing + simulation	Testing + simulation

Legend: Manual work / Focus | (Semi-)automatic | **Bold: novelty compared to previous approach**

Project Goals

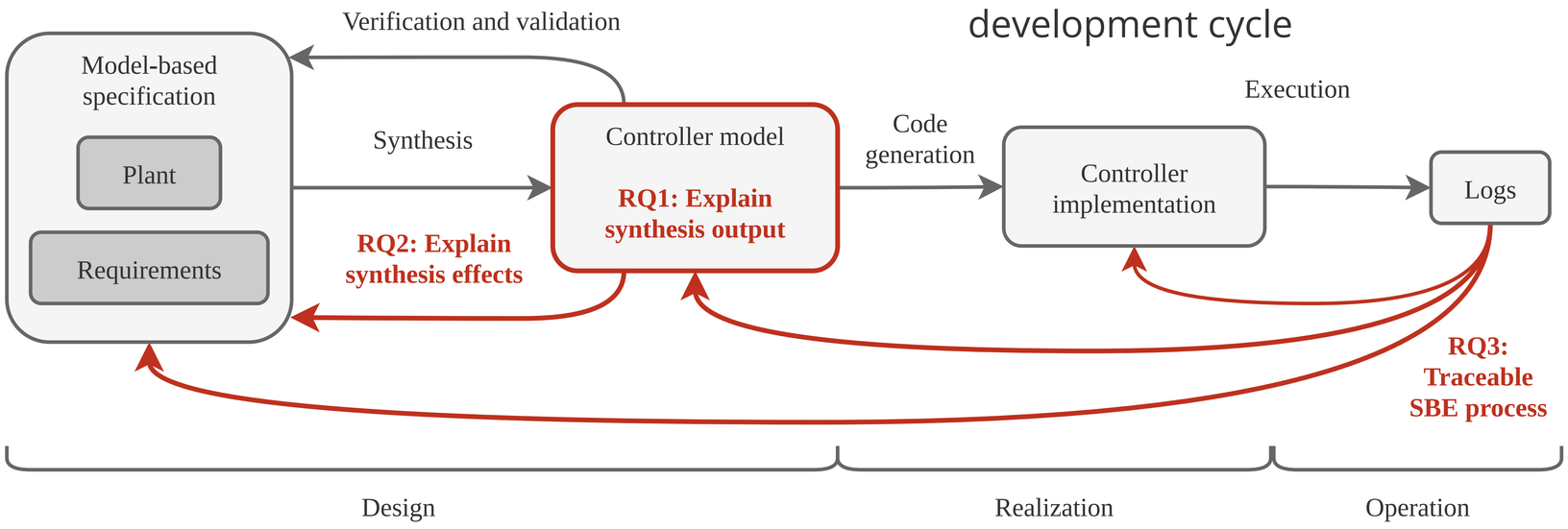
Trust in automation

Engineering efficiency

ExSyn aims to produce:

- Fundamental academic research (2025-2029)
- Algorithm prototypes contributed to the Eclipse ESCET™ open-source project
- Evaluation at industrial scale

Explainable synthesis in the **SBE** development cycle



RQ1: Explain synthesis output

How can the conditions resulting from supervisory controller synthesis be made as compact, readable, and understandable as possible?

- Result of synthesis: extra conditions for the controllable actions
- Simplify conditions to make them more intuitive

RQ2: Explain synthesis effects

How can the effects of synthesis, in terms of restrictions on the control behavior be made as explainable as possible with respect to the plant and requirement specifications?

- Why are the resulting conditions the right conditions?
- Use cause trees to explain causes for the removal of states and transitions

RQ3: Traceable SBE process

How can traceability be improved throughout the SBE process, from execution of the system all the way back to the specified plants and requirements?

- Diagnose issues that occur when supervisory controllers developed through SBE are deployed in the field
- Root cause should be traceable back through the various steps, all the way back to the plants and requirements

Radboud University ASML

The ExSyn project is a collaboration of the Radboud University and ASML. It is partially funded by Holland High Tech, top sector High Tech Systems and Materials (HTSM), with a PPP Innovation subsidy for public/private collaborations on research and development. It is also partially funded by ASML.