OPPGAVE 9 - FORDYPNINGSPROSJEKT INNENFOR **Safety demonstrations of autonomously controlled and automated systems using simulations**

Revisjon: 3.4.2025

Faglærer: mary.a.lundteigen@ntnu.no. Denne veiledes i hovedsak av PhD student Raffael Wallner som selv jobber med temaet, med støtte fra faglærer.

Kort oppsummert: Foreslått tre alternativer som (i utgangspunktet) *en* student kan velge blant. Oppgaveformuleringen er utformet på engelsk og er knyttet til et spennende 8-årig senter SFI AutoShip ledet fra kybernetikk som skal bidra til økt bruk av autonome fartøy innenfor mange maritime sektorer.

About the specialization topic

In order to put highly automated or autonomous systems into operation, it is necessary to ensure and prove that they comply with today's safety standards. However, a comprehensive formal proof of safety with conventional methods is often not possible due to the complexity of such systems. Furthermore, the operational environment may vary significantly in many different aspects, making it more challenging to limit the scope of formal testing.

An approach to ensure the safety of complex systems is to demonstrate their safe behavior by scenario-based testing in simulations. Therefore, a model or virtual representation of the system and its relevant environment is created and used to test a set of different simulated scenarios. The simulation results are then evaluated with respect to the safety performance of the controller in those scenarios.

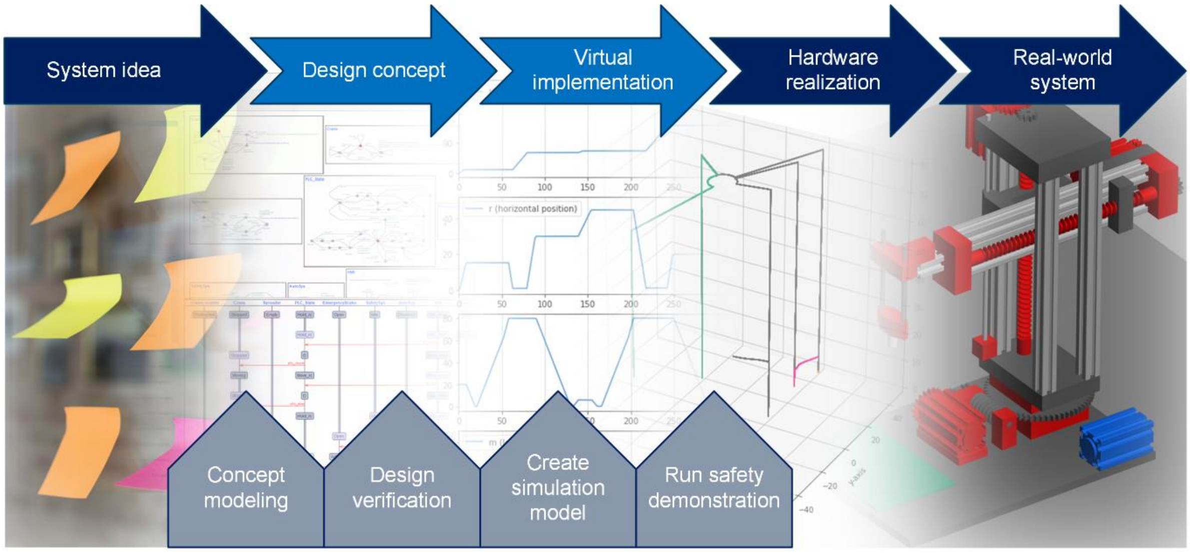

Fig. 1. The project tasks involve the implementation of the conceptual design model and the simulation model, as well as the design verification and safety demonstration using those models.

A currently investigated methodology uses a multi-level simulation approach, combining abstract conceptual simulations using System Modeling Language (SysML) in UPPAAL (https://uppaal.org/) with concrete simulations, e.g., using Python. That methodology requires implementing the system in two environments that, however, complement the design process of complex systems and hence, can be well integrated without adding a lot of extra implementations only for safety assurance. The advantage of this methodology is the possibility to conduct design verification in holistic tests of the system concept in UPPAAL, as well as to investigate more detailed system and component behavior during specific scenarios in concrete simulations.

The work in this specialization project involves the implementation of those simulation models as well as running simulations for safety demonstrations. The exact work content may be open to some adaptations based on the student's expertise.

More about the project work:

This specialization project is for those who are interested in autonomous and automated systems but would like to learn more about what needs to be ensured to make them safe, and how to demonstrate that they comply with safety standards. Although certain tools and project details are given, some adaptations may be discussed based on the student's prior experience and knowledge in certain domains.

Tools/environments:

The necessary or suggested tools used for working on this project are UPPAAL for working on the SysML implementation and the conceptual testing, and Python for the concrete implementation. In case of more expertise in other suitable programming and simulation environments, Python implementation may be replaced with implementations in, e.g., MATLAB, C(++), or similar. That, however, needs to be discussed and may lead to varying levels of support from the supervisors with environment-specific issues.

Use case system:

The suggested use case system is a crane system for partly automated lifting operations at a harbor for container ships. The system shall mainly be operated by a human controller in a remote control room. For long transport distances, the system is equipped with an autopilot that automatically approaches a destination without input from a human operator. It is important that this automatic function operates the crane only outside critical areas close to obstacles or humans. A safety system shall safeguard all crane operations, intervene in case of critical situations, and warn the human operator about hazards.

In case the student has worked extensively with other systems, e.g., ships/Uncrewed Surface Vessels (UAVs) or similar, that allow for an equivalent alternative use case, adaptations may be discussed. As for the simulation environment, there are possible limitations in the supervision.

Main tasks:

- familiarize with simulation frameworks
- familiarize with the use case system
- evaluate system structure and create implementations
- set up and run simulations for the purpose of safety demonstrations