UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR ELECTRICAL ENGINEERING IN MEDICINE

Bachelors / Masters Practical Project *or* Bachelor / Masters Thesis

Concept and Implementation of a Control Supervisor

Supervisor & examiner: Prof. Dr. Georg Schildbach

Autonomous systems are currently experiencing an explosive growth, due to the advances in battery technology and an increasing availability of ever more powerful and inexpensive sensors and computational hardware. For many interesting fields of application, however, autonomous systems are subject to **strict safety requirements**. For example, for an automated vehicles or a medical robot, a malfunction can put human health or lives at risk.

Most autonomous systems make use of **advanced control concepts**, such as learning-based control (LBC) [BTA2006] or model predictive control (MPC) [BBM2017]. These algorithms are highly complex, often non-deterministic and/or adaptive, and they are usually designed for a very particular control task. All of this makes the **detection of a malfunction** of the controller a difficult challenge that has received relatively little research attention so far, although it is closely related to fault-tolerant control [BKLS2016].

This project is about the design of a **control supervisor** for **advanced control algorithms**. The goal is to use a general approach, i.e., one that is not tied to a particular type of control algorithm (e.g., LBC, MPC, etc.). The

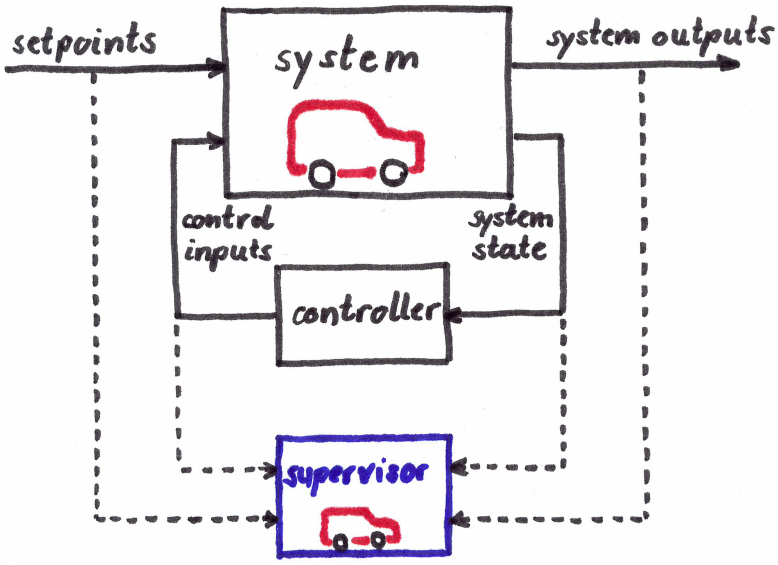

Fig. 1: Architecture of safety-critical system with control supervisor.

supervisor *neither* concerned with determining the **cause of the malfunction** (e.g., software bug, hardware fault, etc.), *nor* with faults that do not lead to a violation of **safety constraints**. Instead, the controller is considered as a black box and the error detection is based solely on **assessing the safety of the control inputs**; see Fig. 1.

For this assessment, the supervisor contains a **model of the controlled system**, as shown in Fig. 1. This model can be used to predict the set of possible trajectories, given the current state of the system and the commanded control inputs. If these trajectories indicate a **possible violation of safety constraints**, the supervisor takes action (e.g., switches off the controller, stops the system, etc.).

This project comprises the **concept design** for a control supervisor as well as its **implementation for an autonomous model car**; see Fig. 2. To this end, a simple controller for trajectory tracking has to be designed. The functionality of the control supervisor is then tested based on the injection of faults into the controller. Here the main safety constraint is for the car not to leave a given corridor, which is constrained by boundaries to the left and to the right. The supervisor is evaluated based on its ability to keep the vehicle safe in the presence of faults in the controller.

Fig. 2: Autonomous model car at the Autonomous Systems Laboratory.

References

[BBM2017] Borrelli, F., Bemporad, A., and Morari, M.: *Predictive Control for Linear and Hybrid Systems*. Cambridge University Press, Cambridge, 2017.

[BTA2006] Bristow, D.A. , Tharayil, M., and Alleyne, A.G.: A Survey on Iterative Learning Control. *IEEE Control Systems Magazine*, 2006.

[BKLS2016] Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M.: *Diagnosis and Fault-Tolerant Control*, 3rd edition. Springer, Berlin, 2016.