KIT
Karlsruher Institut für Technologie

Case Study:
Provably Safe Neural Control of Cooling Towers

Master's Thesis

Background. Recently, it has been investigated whether NNs can be used to control the behavior of cooling towers at CERN's LHC [2]. This is desirable in principle, as NNs can represent complex, efficient control strategies as a (comparatively) efficient computation. However, to put such NNs into practice, it is paramount to ensure their safety, e.g. to prevent overheating.

Recent work at KIT has investigated both how heating/cooling systems can be formalized in differential dynamic logic (dL) and how control envelopes formalized in dL can be used for NN verification [4].

Task. In this work, we want to investigate how dL results for cooling systems and switched systems can be leveraged to (dis)prove the safety of the NNs proposed by Lopez-Miguel *et al.* [2]. Prior work proposes a switched system formulation [1] for the considered cooling system, which could also be formalized in dL [3]. This raises the question to what degree the NN verification approach VerSAILLE [4] is directly applicable to switched systems or what changes are required in this case. The task for this Master's thesis would be to formalize the given system in KeYmaera X and to subsequently (dis)prove the safety of the NN Control System given in [2]. If necessary, further safe NNs could be trained.

Stichworte: Differential Dynamic Logic, Switched Systems, Neural Network Verification, Cyber-Physical Systems

Referenzen

[1] Faiq Ghawash et al. "Optimal Control of Induced Draft Cooling Tower using Mixed Integer Programming". In: *IEEE Conference on Control Technology and Applications, CCTA 2021, San Diego, CA, USA, August 9-11, 2021*. IEEE, 2021, pp. 214–219. DOI: 10.1109/CCTA48906.2021.9658627.

[2] Ignacio D. Lopez-Miguel et al. "Verification of Neural Networks Meets PLC Code: An LHC Cooling Tower Control System at CERN". In: *Engineering Applications of Neural Networks - 24th International Conference, EAAAI/EANN 2023, León, Spain, June 14-17, 2023, Proceedings*. Ed. by Lazaros Iliadis et al. Vol. 1826. Communications in Computer and Information Science. Springer, 2023, pp. 420–432. DOI: 10.1007/978-3-031-34204-2_35.

[3] Yong Kiam Tan et al. "Switched Systems as Hybrid Programs". In: *7th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2021, Brussels, Belgium, July 7-9, 2021*. Ed. by Raphaël M. Jungers et al. Vol. 54. IFAC-PapersOnLine 5. Elsevier, 2021, pp. 247–252. DOI: 10.1016/j.ifacol.2021.08.506.

[4] Samuel Teuber et al. "Provably Safe Neural Network Controllers via Differential Dynamic Logic". In: *Advances in Neural Information Processing Systems*. Ed. by A. Globerson et al. Curran Associates, Inc., 2024. DOI: 10.48550/arXiv.2402.10998.

Betreuung:

Samuel Teuber, teuber@kit.edu, Room 203 (Building 50.34)
Noah Abou El Wafa, noah.abouelwafa@kit.edu, Room 158 (Building 50.34)