# Risk Mitigation Strategies in High Automation

Mario Gleirscher[1]

**Abstract:** The work underlying this presentation is titled "From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case," accepted as a peer-reviewed full technical paper at the "NASA Formal Methods Symposium (NFM 2017)," published in April 2017.[2]

**Keywords:** high automation; autonomous systems; risk analysis; hazard mitigation; safe state; controller design; modelling; planning

## Presentation Abstract

Autonomous machines—mobile, stationary, individual, collective, learning—need mechanisms to anticipate, predict, and mitigate dangerous situations. These mechanisms are required to be highly resilient, secure, and dependable. Increasing autonomy shifts risk ownership towards vendors, hence, raising the demand for such mechanisms to be valid and verified for a large variety of complex operational situations.

However, one of the main problems is that there is only little research on cross-disciplinary and compositional models supporting engineers with the transition from system-level hazard analysis and risk assessment to the design of controllers with risk mitigation strategies, and with the systematic refinement of abstractions of the controlled process towards the details relevant for controller design.

This presentation discusses an analysis and design method for high-level controllers for highly automated or autonomous machines with run-time mechanisms for risk monitoring and mitigation. This method aims at equipping engineers with a way to systematically examine a large number of risk scenarios and encode these scenarios in an action model. This model can then be given an operational semantics to make it suitable for optimal mitigation planning. In support of the planning layer of a machine or a system of machines, from this model it is possible to derive run-time risk monitors as well as controllers for effective handling of such scenarios at run-time.

[1] University of York, Computer Science, Deramore Lane, Heslington, York YO10 5GH, United Kingdom
mario.gleirscher@york.ac.uk

[2] See https://link.springer.com/chapter/10.1007/978-3-319-57288-8_23.

doi:10.18420/se2019-12

Towards these aims, the talk will discuss

(1) a framework for the analysis and specification of high-level controllers capable of run-time risk monitoring and mitigation,

(2) an incremental algorithm for the construction of high-level controller models from incremental inputs of risk analyses, and

(3) possible uses of this method and this algorithm in road vehicle and mobile robotics applications.

The model used in this framework is based on two main concepts, the controlled process and risk: The process model describes the action space of the considered process and the risk model contains information about which of these actions are associated with risk in certain scenarios, and which of these actions might be performed to mitigate such risk in these scenarios.

One of the main tasks of the (safety, systems, or requirements) engineer is to identify and model the process actions, the endangering actions, the mitigation actions, and the foreseeable causal relationships between these actions in each of the considered scenarios.

The method provides guidance for step-wise analysis of endangering actions, the identification of mitigation actions, and, based on these two steps, the modelling of risk mitigation strategies in high automation.

Furthermore, the method supports the composition of mitigation strategies as well as the composition of scenario-specific models. Moreover, the provided algorithm then calculates an operational semantics of the composed model. These semantics can then be used for various checking purposes, for example, consistency and causality checking.

The talk provides a snapshot of the current stage of research of the proposed method and explains the framework using typical examples of risk mitigation in road vehicles. It provides an outlook to the next steps. Further material for this presentation can be found in [Gl17] and [GK17].

## References

[GK17] Gleirscher, Mario; Kugele, Stefan: From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case. In (et al., C. Barrett, ed.): NASA Formal Methods (NFM) – 9th Int. Symp., Proceedings. volume 10227 of LNCS. Springer, Berlin/New York, 2017. https://doi.org/10.1007/978-3-319-57288-8_23.

[Gl17] Gleirscher, Mario: Run-Time Risk Mitigation in Automated Vehicles: A Model for Studying Preparatory Steps. In (Bulwahn, L.; Kamali, M.; Linker, S., eds): First iFM Workshop on Formal Verification of Autonomous Vehicles 2017 (FVAV 2017). EPTCS, 2017. https://doi.org/10.4204/eptcs.257.8.