

The Innovative Hydraulics and Automation Lab



Marea de Koning discusses the safety assurance challenges of highly automated heavy-duty mobile machinery, often operating in harsh environments, such as construction and mining sites. She introduces her research aimed at addressing these issues through safe logic-driven decision making and describes the role the Innovative Hydraulics and Automation Laboratory plays in supporting those objectives.

The fourth industrial revolution is characterised by the emergence of smart cyber-physical systems (CPSs) that integrate various levels of automation, such as heavy-duty mobile machinery (HDMM), robotic systems, and automotive vehicles. These CPSs require behaviours with higher levels of automation, perception, and cognition not only to execute their functions but also to ensure the safety of their intended behaviour. This necessitates the integration of numerous sensors, actuators, deterministic, probabilistic, and data-driven elements to interrelate with each other, resulting in complex architectures where hidden flaws can lead to death or serious injuries to humans, severe damage to the machine, or environmental harm, i.e., safety-critical situations.

In light of technological advances facilitated by the integration of autonomous capabilities in HDMM, safety is of a growing concern. With operators being phased out from full control of the machines, it is necessary to determine a method that harnesses the advantages of automation while ensuring adequate levels of safe and logic-driven decision making by the machine.



Tampere University and the Innovative Hydraulics and Automation Laboratory

Tampere University (Tampereen yliopisto) was established on 1st January 2019 through a merger between Tampere University and Tampere University of Technology. Along with TAMK – Tampere University of Applied Sciences, this constitutes the higher education community of the Tampere area [1]. Within the Department of Automation Technology and Mechanical Engineering (ATME), the Laboratory of Innovative Hydraulics and Automation (IHA) conducts interdisciplinary research in the field of fluid power and automation, bridging theory and practice in close collaboration with industry.

IHA provides excellent facilities for practical research, including the campus area testing ground. This area has several instrumented HDMMs enclosed within a 4,000m² working area for excavating, with different surfaces ranging from gravel to asphalt and a hill with three slopes ranging up to about 18 degrees [2]. Within IHA, the Autonomous Mobile Machines Research group, led by Prof. Reza Ghabcheloo, the Zonal Hydraulics and Hybrid Technology Research group, led by Prof. Tatiana Minav, and the Heavy-Duty Robotics Research group, led by Prof. Jouni Mattila, conduct practical and relevant research based on solid theoretical grounding in the application areas of HDMM and heavy-duty robotics. Our research focus is determined to face emerging challenges with the goal of developing innovative solutions, methods, tools, and processes to build energy-efficient autonomous behaviours in a short time and at lower costs that are generic, modular, and transferable.

Safety Limitations in varying levels of HDMM automation

The increase in levels of automation integrated in machinery exceeds the scope of available safety assurance guidelines, limiting the market placement of highly automated HDMM within the European Economic Area (EEA), as compliance with regulatory requirements cannot be guaranteed. For example, the existing legislation on safety in HDMM does not consider limited or no operator control for safety assurance purposes, revealing limitations for manufacturers in justifying sufficient integration of adequate risk reduction efforts.

Increasing the automated capabilities of a HDMM to a level where it becomes responsible for the correct execution of its tasks, it consequently assumes the responsibility of safety. When a machine becomes responsible for safety it must become aware of the environment it operates in, this requires a significant and reliable level of perception and safe logic-driven decision making. Additionally, HDMM operates in harsh environments, such as construction sites or mining sites, providing unique challenges for system architecture and interoperability of safety functions.

The integration of complex systems supplied by multiple vendors can make interoperability and safety across components difficult. Ensuring that all of the different subsystems work together effectively and reliably requires thoughtful design, integration, validation and testing.

“Existing legislation on safety in heavy-duty mobile machinery does not consider limited or no operator control for safety assurance purposes.”

Compliant Safety Assurance for Automated HDMM

As a result of these concerns, my research aims to find a balance between higher levels of automation in HDMM while simultaneously ensuring adequate risk reduction of safety-critical situations. The ability of a highly automated HDMM to adequately avoid harm through timely reactions of the safety-related control systems requires the integration of high levels of safe logic-driven decision making. The cognitive awareness of a HDMM influencing its decision-making capacity necessitates a significant number of sensors, conventional deterministic software logic, and probabilistic modules such as machine learning and data-driven methods. Furthermore, ensuring the risk reduction efforts are sufficient in relation to the level of automation and operator engagement requires an understanding of EU machine safety legislation.

Ensuring safety compliance of a HDMM becomes challenging when it is capable of executing functionalities based on its own discernment, assuming all task conditions are met. The HDMM's ability to discern the safety of the actions it plans to execute heavily depends on its perception of the environment it operates in. However, the inherent complexity of the HDMM's operating environment significantly increases the risk of known hazardous situations and also opens up the possibility of previously unforeseen hazardous situations emerging. Thereby exceeding the scope of the minimum health and safety requirements as established in EU directive 2006/42/EC.

Through analysis of Directive 2006/42/EC and harmonized machine safety standards it can be concluded that limitations with the machine safety argument emerge throughout the machine safety development lifecycle and can be summarised in six concrete limitations [3]:

- run-time failures
- algorithmic failures
- convoluted architectural design patterns
- data-driven intended behaviour
- quality integration
- formal verification limitations

In addressing the limitation of convoluted architectural design patterns, the current trend is to integrate safety through a separate monitoring layer encompassing intricate fault-handling modules, thereby increasing the overall fault tolerance of the HDMM.

Currently, there are no tangible guidelines available for the safety architectural design patterns of higher complexity. Therefore, my current objective is to determine these design objectives and integrate them into a highly automated HDMM available within IHA.

By providing a physical realisation of safety assurances for highly automated HDMM, I aim to derive a method for future realisations of appropriate risk reduction techniques in highly automated HDMM.

References

- [1] Tampere University, "Tampere University Home." <https://www.tuni.fi/en> Accessed May 2023.
- [2] IHA, "Innovative Hydraulics and Automation". <https://research.tuni.fi/iha/research/autonomous-off-road-machines/> Accessed May 2023.
- [3] AMR de Koning. and Reza Ghabcheloo, "Machine safety conformance limitations for highly automated and autonomous heavy-duty mobile machinery" published in "The Future of Safe Systems: Proceedings of the Thirty First Safety-Critical Systems Symposium". <https://scsc.uk/scsc-179> SCSC, York, UK, 2023.

Image Attribution

Images are the copyright of the Innovative Hydraulics and Automation unit of Tampere University, Finland.

Marea de Koning, Doctoral researcher, Tampere University, Finland.

Marea de Koning is a newcomer to the field of safety engineering. She is a doctoral researcher from Tampere University in Finland within the field of safety for autonomous heavy-duty mobile machinery. Her background comes from a bachelor's degree in embedded software development and a master's degree in industrial engineering received from the Netherlands and Germany respectively. Her aim is to contribute to the advancement of autonomous technologies, by ensuring that these systems can be deployed safely.

The author retains copyright of this article.