

Safety and Highly Automated Machinery



Tampere, Finland – often referred to as the "Manchester of the North" and aptly nicknamed "Manse" – is a centre for research into the automation of off-road mobile machinery. This research is being conducted at the University of Tampere in close collaboration with the R&D departments of local machinery manufacturers. There, for the past four years, Marea de Koning, has been conducting research into the safety of highly automated off-road mobile machinery. In this article, Marea provides a summary of her research, where it started and ended.



My initial findings and concerns have been summarised and discussed in a previous publication of this newsletter ("The Innovative Hydraulics and Automation Lab", *Safety Systems* Vol 31 Nos 2 May 2023). Meanwhile, several years later the research – published across five articles (one of which remains in review at the time of writing) – in the form of a PhD dissertation has come to an end.

The objective of my research was threefold:

- To enhance the understanding of where, when, and how automation in off-road mobile machinery exceeds the scope of the Machinery Directive
- to evaluate the implications of forthcoming legislative changes; and
- To identify potential pathways and roadblocks towards safer highly automated off-road mobile machinery

Where the research starts

Off-road mobile machinery, such as those deployed in the construction, mining, forestry, and agricultural sectors, are essential to numerous industries worldwide. Currently, the EU is a world leader in the manufacturing of such machinery, with a turnover of approximately €740 billion annually [1]. This success can be attributed, in part, to the strict safety requirements for machinery entering the market. Manufacturers must demonstrate compliance with the Essential Health and Safety Requirements (EHSR) documented in the Machinery Directive (MD) (Directive 2006/42/EC) via a 'Conformité Européenne' (CE) declaration, which guarantees a baseline level of safety for EU citizens and workers. This protection is vital, as harm – defined as the risk of physical injury, damage to health, or property – is a major concern in workplace safety.

The MD defines machinery as a collection of linked parts or components, at least one of which moves, powered by a non-human or non-animal energy source, and designed for specific functions. The introduction of new digital technologies, such as Artificial Intelligence (AI), Machine Learning (ML), and the Internet of Things (IoT), facilitates higher levels of automation in off-road mobile machinery. These higher levels of automation not only introduce new risks, challenging workplace safety assurance, but have also prompted a change in the machine safety regulatory landscape.

As of January 27th, the MD is to be superseded by a Machinery Regulation (MR) (Regulation 2023/1230). This change broadens the scope of the ESHR and expands the definition of machinery.

“These higher levels of automation not only introduce new risks, challenging workplace safety assurance, but have also prompted a change in the machine safety regulatory landscape”



One of the most significant amendments is the inclusion of software within the overall definition of machinery. More specifically, the definition of machinery has been extended to include "... including those that only lack the software upload intended for the manufacturer's envisioned use"⁶. This update formally acknowledges the role and importance of software in machinery design and operation. Furthermore, the MR specifies that when software performs a safety function and is independently placed on the market, it is classified as a safety component. Such amendments reflect the growing influence of digital solutions on safety, particularly as the level of automation in off-road mobile machinery increases.

Despite existing regulations, fatal and non-fatal accidents in the workplace remain prevalent. In 2022 alone, the EU recorded approximately 3,286 fatalities and 2.97 million non-fatal accidents. Most fatal and non-fatal accidents occur in areas such as mining, manufacturing, forestry/agriculture, or construction sectors. These accidents are often attributed to a loss of control of machinery (e.g., unexpected start-up of an off-road mobile machine or unexpected overextension of a mobile elevating work platform). Human errors such as falling, stumbling, or slipping typically come second [2] [3].

There is a growing concern that accident patterns seen in other fields which integrate higher levels of automation in their systems – such as (mobile) robotics and automotive vehicles – could translate to highly automated off-road mobile machinery. This could potentially exacerbate existing accident rates rather than mitigate them, as is often expected. This concern is one of the reasons the MD has been superseded by the MR.

Nevertheless, adjusting the scope of EHSR to encompass the potential risks of highly automated off-road mobile machinery does not necessarily solve the safety challenges manufacturers now face. Instead, it can be said that it has made the journey to safer highly automated off-road mobile machinery more difficult, as it remains unclear to what extent and to which standards a highly automated off-road mobile machine should comply to conform to the forthcoming MR.

What was contributed

This research contributes by establishing a foundation for understanding safe highly automated off-road mobile machinery by examining the challenges of conforming to standards and achieving compliance. The contribution, presented in [4], is the identification of six key areas where highly automated off-road mobile machinery faces compliance limitations:

- Run-time failures
- Algorithmic failures
- Complex architectural design patterns
- Data-driven intended behaviours
- Integration quality
- Limitations in formal verification

The research continues by identifying lessons learned from related fields facing similar challenges.

⁶ This, in effect, is adding software to the definition of machinery and no longer restricting it to be just physical components.

This contribution found [5], by abstracting lessons learned from similar domains and translating them into the context of highly automated off-road mobile machinery, providing a foundational starting point for understanding its requirements. Building on this, the dissertation makes another contribution found in [6], which examines the transition from the MD to MR. This change has several key implications:

- A directive is now superseded by a regulation
- It explicitly includes software and digital components within the definitions of machinery and safety components
- It introduces additional provisions for highly automated off-road mobile machinery classified as high-risk, requiring autonomous mobile machinery and related products to have control systems capable of performing safety functions independently, even when actions are ordered by using a remote supervisory function; and
- It expands the role of the supervisor, mandating that if the supervisory function is inactive, the automated machinery must not be able to operate, while also requiring the human-machine interface (HMI) to be adapted to the foreseeable characteristics of the operators.

“A recommendation is made for the integration of Safety Reasoning Modules (SRMs) ... intended as a high-level decision-maker. Analysing risks in real-time using sensor data and AI or rule-based logic to adapt responses dynamically.”

This shift in the EHSR requires machines to perform safety functions autonomously, even when overridden by a supervisor, and mandates supervisory functions in high-risk machinery for event-based intervention, while also emphasising the need to enhance HMIs and prevent machine-determined changes in work rates. This signals a future where the minimum EHSR for off-road mobile machinery prioritises operator well-being and intervention capacity, positioning them as supervisors, either remotely or within the cabin and requires highly automated off-road mobile machinery to be capable of safely reasoning on the behaviour that they are executing.

As such, in [4], a recommendation is made for the integration of Safety Reasoning Modules (SRMs). While a safety function is a predefined mechanism that triggers immediate, fixed responses to hazards – such as a light curtain breach immediately stopping a machine – an SRM is intended as a high-level decision-maker. Analysing risks in real-time using sensor data and AI or rule-based logic to adapt responses dynamically. In safety-critical systems, both the SRM and safety function serve distinct yet complementary roles: the SRM evaluates the need and coordinates safety measures, while safety functions execute them. At the time of writing, one other contribution remains under review. This work evaluated and presented the specifics with respect of the technical design requirements of such an SRM.



Additionally, this dissertation has another contribution found in [7], which proposes a risk-based assessment of supervisor-machine shared decision-making, examining how supervision affects the required level of human engagement, particularly in relation to the machine’s ability to remain aware of and respond to emerging hazards during runtime.

The proposed risk-based assessment of supervisor-machine shared decision-making redefines controllability as the ability of a highly automated off-road machine to prevent harm through timely reactions and the supervisor's event-based intervention. Controllability is then categorized into five Levels of Controllability (LoC), guiding design, verification, and validation to ensure the machine accounts for the supervisor's cognitive limits. This includes Machine Awareness of the Hazard (MAH) – how well the system perceives risks – and Degree of Decision Making (DoDM) – its ability to respond appropriately. The method helps define safety requirements for highly automated off-road machines, ensuring human-in-the-loop solutions where necessary. MAH varies from full hazard awareness to complete unawareness, while DoDM assesses the machine's response capabilities in relation to human reaction times.

Conclusion (Future areas of concern)

That said, many questions remain, particularly about the risk assessment proposal's effectiveness in safety design and whether further adaptations are needed for highly automated off-road machines to address the impact of human supervision. Additionally, it will be necessary to work towards realizing the proposed SRM and assessing its relative effectiveness. Nevertheless, the research presented across multiple peer-reviewed publications and compiled into one dissertation provides a theoretical foundation for safety in highly automated off-road machinery, offering valuable insights for manufacturers, researchers, policymakers, and standards organisations. Its findings support shaping the future of safety in highly automated off-road mobile machinery.

Finally, it is important to highlight how this shift to supervisory roles affects the well-being of operators. For the time being, it appears that supervisors will remain an integral factor in the safety case for event-based intervention if and when the machine fails, despite rigorous efforts by engineers to design robust machines, they do remain responsible for event-based intervention. We should research how machine 'safety by design' practices can evolve to support the needs of humans in supervisory roles to avoid and/or mitigate the negative consequences of long-term supervision on well-being.

The publication of the dissertation and the defence is scheduled for 13th June 2025. It is open to the public and everyone interested can attend. Additionally, it is possible to follow the event via livestream; simply send an email directly to the author, Marea De Koning, at marea.dekoning@gmail.com if interested.

References

- [1] S. Gospodinova, "Commission welcomes political agreement on new rules to ensure the safety of machinery and robots," 15 December 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7741, accessed April 2025.
- [2] E. Union, "Accidents and injuries statistics," 6 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_and_injuries_statistics, accessed April 2025.
- [3] E. Union, "Accidents at work - statistics on causes and circumstances," November 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_at_work_statistics_on_causes_and_circumstances, accessed April 2025.
- [4] A.M.R. de Koning, R. Ghabcheloo, "Machine safety conformance limitations for highly automated and autonomous heavy-duty mobile machinery," in The Future of Safe Systems: Proceedings of the 31st Safety-Critical Systems Symposium (SSS'23) 7-9th February 2023, York, United Kingdom, 2023.
- [5] A.M.R. de Koning, A. Ahonen, N. Strokina, R. Ghabcheloo, "Safety architectures for cyber-physical systems: review of state-of-the-art and outlook for heavy duty mobile machinery," in The Eighteenth Scandinavian International Conference on Fluid Power, SICFP'23, Tampere, Finland, 2023.
- [6] A.M.R. de Koning, A. Ahonen, T. Machado, N. Strokina, T. Minav, R. Ghabcheloo "A comprehensive approach to safety for highly automated off-road machinery under Regulation 2023/1230," Elsevier Journal of Safety Science, vol. 175, 2024.
- [7] A.M.R. de Koning, W.L. brown, T. Minav, R. Ghabcheloo, "Towards Safer Supervisor-Machine Shared Decision-Making for Runtime Hazard Mitigation in Highly Automated Off-road Machinery," in Safety of Industrial Automated Systems – SIAS 2024, Tampere, Finland, 2024.

Image attribution:

Cover Image ID 99960799 © Andrey Salamchev | Dreamstime.com

Tammerkoski ID 275020134 | © Dudlajzov | Dreamstime.com

excavator © IHA lab Tampere University

sunset: © Marea de Koning

Marea de Koning, Functional Safety Expert HULD oy, Finland



Now no longer a newcomer to the field of safety, Marea de Koning, has finished her PhD research in safety for highly automated off-road mobile machinery at Tampere University. Currently, she works as a functional safety expert at HULD oy, consulting on various safety and security related projects. 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 and she remains open to see what the future holds.