Research Article

Timo Malm*, Risto Tiusanen, Eetu Heikkilä and Janne Sarsama

Safety risk sources of autonomous mobile machines

https://doi.org/10.1515/eng-2022-0377
received May 03, 2021; accepted October 03, 2022

Abstract: Autonomous mobile machines are applied increasingly often in outdoor applications, but only in places, where logistic problems and safety issues are resolvable. Solving safety issues require good hazard identification and risk estimation. The aim of this study is to show which new risks emerge in autonomous mobile machines compared to manual machines. There are new risks, which are valid only in autonomous mobile machines (e.g., related to sensors for situational awareness), and risks, which exist in both machine types, but human presence can make the difference in resolving the situation. Humans can take sophisticated protective measures during an unexpected hazardous situation. Another aim of this work is to give information to designers and assessors to consider risks of their own design. Autonomous mobile machines are complex, and their performance is not always easily predictable. A checklist of risks would help an assessor, but currently, it may be difficult to find a checklist for a specific autonomous mobile machine. The main result of this study is a checklist of new risk sources or hazards of autonomous mobile machines.

Keywords: safety, hazard, risk source, risk, mobile machine, autonomous

*** Corresponding author: Timo Malm,** VTT Technical Research Centre of Finland Ltd, Visiokatu 4, Tampere, Finland, e-mail: timo.malm@vtt.fi
Risto Tiusanen: VTT Technical Research Centre of Finland Ltd, Visiokatu 4, Tampere, Finland, e-mail: risto.tiusanen@vtt.fi
Eetu Heikkilä: VTT Technical Research Centre of Finland Ltd, Visiokatu 4, Tampere, Finland, e-mail: eetu.heikkila@vtt.fi
Janne Sarsama: VTT Technical Research Centre of Finland Ltd, Visiokatu 4, Tampere, Finland, e-mail: janne.sarsama@vtt.fi

1 Introduction

Expectations are currently high for many kinds of autonomous (cars and mobile machines) vehicles [1,2]. Currently, there are some examples where autonomous vehicles operate autonomously most of the time, but in certain work phases human help or remote control is needed. These examples can be found, for example, in traffic (cars), port, and mining environments. However, there is no single agreed definition for the concept of autonomy. In addition to fully autonomous operation, it can refer to various levels of human–machine interaction. To describe these levels, several categorizations have been proposed to structure the levels of autonomy. One of the most widely used categorizations is given in the Society of Automotive Engineers' (SAE's) report [3]. The levels are: no automation (0), diver assistance (1), partial automation (2), conditional automation (3), high automation (4), and full automation (5).

Autonomous cars have been in the frontline of autonomous vehicles research, and history shows some interesting development. Vision guided car was introduced in 1980 (Mercedes Benz) and later lidar, radar, GPS, and computer vision have been used [4]. Sensors and navigation systems have been in cars for a long time, but final steps to autonomous cars (SAE level 5) may be close [5] and most of the cars are assumed to be autonomous by the year 2035 [4]. During the past decade, sensor performance, communication speed, and intelligent algorithms have increased the hopes to have practical driverless vehicles to be used soon in various environments. It is still uncertain about how safely the new inventions in autonomous mobile vehicles can operate in various conditions [6].

Autonomous car in good circumstances remarkable may enable reduction in accidents in the future. [7]. Fatal accidents are often related to human errors (USA over 90%) [6] and therefore there is potential for autonomous vehicles to reduce traffic accidents, when human factor is minimized. However, the elimination of human error does not imply the elimination of machine failure [6].

Many articles have been published related to safety and risks of driverless cars. Therefore, the studies related to driverless cars have been considered as a good reference. Autonomous mobile machines have many similar operational risks as driverless cars, but due to the features and functions of autonomous or semi-autonomous machine systems there are also many different risks. Some typical properties of autonomous mobile machines compared to driverless cars are: they are slower, high-performance level (PL) of sensors and systems is required, they are controlled by central traffic control system, and area access control is often applied to allow access to a specific area, like intersection.

This article focuses on autonomous mobile machines. According to ISO 17757, an autonomous machine is a mobile machine that is intended to operate in autonomous mode during its normal operating cycle [8]. Machines are part of autonomous or semi-autonomous machine systems, which provide infrastructure, supporting systems, command, and control centers that enable the use of the autonomous mode.

In fully autonomous mobile machine systems operating in isolated industrial areas, collision risks can be minimized by preventing persons and conventional vehicles from entering the area where the machines are operating in autonomous mode. In this case, machines are stopped and turned to manual mode when a person enters the area. Risk assessment of such system may be modest, if there are no exceptions for access, since isolation eliminates most of the risks of the autonomous mode.

However, total isolation of an area is not practical and usually there are some tasks inside the automated area. Tasks can be related, for e.g., to supervising operation, switching reefer container on, or minor troubleshooting. There is a need for more open systems, which means that complexity increases and more effort is needed for the safety risk management. Automated guided vehicles (AGVs) used in open indoor environments apply usually on-board safety system, which stops the vehicle before it touches an object or before a hazardous force is generated [9]. For example, safety laser scanners are good for the purpose.

Compared to indoor AGVs, outdoor autonomous mobile machines usually have a higher vehicle speed and their sensors are not capable to operate well enough in all rough environmental conditions. Reliable detection range of sensors is not always long enough [10]. Functional safety requirements (safety integrity level (SIL)/PL) of sensors are often not met (without additional measures) and sensors cannot detect longer distance objects behind corners or obstacles (not needed in short distance perception in indoor applications). In addition to single sensors or perception systems, a more advanced safety system is thus applied [8], which may include subsystems, like, area access control systems, safe navigation, safe traffic control, safe communication between fleet control and autonomous machines, and on-board safety sensors.

The aim of this article is to present new safety risk sources related to autonomous mobile machines applied in industrial outdoor environments in autonomous mode. We address the need to understand the effects on risks at the transition from conventional machines to automated functions and even to autonomous systems. It is important to understand what kinds of risk sources need to be considered, and how to identify the relevant hazards in each case.

In addition to direct safety risks of autonomous mobile machines, there are also new reliability risks, which may have an indirect relation to safety. The focus in this article is on risk sources, which are new compared to corresponding conventional machines and which can be associated with collision or other events with severe consequences. This article focuses on autonomous mobile machines associated with autonomy levels 3 and 4 [3]. As a result, checklists are presented in Tables 1 and 2 to give ideas to find risk sources of outdoor autonomous mobile machines used in environments like factory yards, ports, or mines.

This article has been written in a multi-disciplinary research project. The overall project objectives include a variety of research themes supporting the development of automated operations. The work presented in the current article specifically addresses the safety engineering research theme in autonomous systems.

This article is structured as follows: Introduction describes how autonomous vehicles (cars and mobile machines) are getting more common and the similar safety challenges they all have. Introduction defines the autonomous mobile machines, which are under consideration here. Section 2 describes the applied methods and references, which give ideas regarding risk sources of autonomous mobile machines. Section 3 describes terminology, risk parameters, the phase when hazard identification is made, and a typical autonomous mobile machine system. Section 4 describes the risk sources related to the autonomous mobile machine. Section 5 (discussion) points out specific features of the autonomous mobile machine system hazards.

2 Materials, methods, and previous research

2.1 Materials and methods

The current study included an analysis of standards for risk source identification, literature review, a compilation

Table 1: Change in hazards, when conventional mobile machine is turned to autonomous

Hazard type	Relevance, conventional/autonomous comparison
Mechanical hazards related to the basic operation of the machine [9,20]	Similar in autonomous/semi-autonomous and conventional systems. After an accident or incident, hazard mitigation (severity) or prevention of additional hazards can be difficult for autonomous mobile machine systems, if there is no person at the place of the event. The situation can be related to other hazards too
Braking failure [9]	Autonomous vehicles do not usually have a driver, during a brake failure, the driver might be able to drive to a direction where the damages are small. Autonomous mobile machine tries to follow the determined route and currently there is no artificial intelligence, which could choose between consequences due to liability, ethical, and technical issues
Falling objects [9]	Autonomous mobile machines do not always have sensors to detect fallen load. The fallen load at a wrong place can cause additional hazards to other machines or bystanders
Gravity [9]	The autonomous mobile machine could be stopped in a position where stability is not optimal
Electrical hazards	Moving close to live electricity needs to be prevented in adequate manner
Thermal hazards	Autonomous mobile machine could be stopped in position, where it can overheat

of findings from recent projects, and merging the results. The findings from projects refer to numerous risk assessments compiled by VTT related to container handling machines at ports, mining machines, and forest machines.

Design science is a research approach that "is focused on problem solving" [11]. This research approach has been selected for the study based on our observation that there is a practical need to formalize our understanding of the risk factors in order to effectively exploit them in the risk management for autonomous mobile machine development.

2.2 Literature review and previous research

The standards related to autonomous mobile machines have been researched to find hazards, which are new to conventional mobile machines. Currently there are no generic standards for autonomous mobile machines, but there are some for specific branches of technologies, which show the requirements of driverless/autonomous/unmanned/highly automated mobile machines. In addition, the terminology in references is partly different. Standard ISO 12100 has been studied, since it shows general checklists of hazards related to machinery and risk assessment procedure. The "Earth-moving machinery and mining standard" [8] present requirements especially for fleet control and concept of complete autonomous machine fleet. The Industrial truck standard [9] presents, among others, specific functional safety requirements and concepts for closed structure (isolated) autonomous systems. The "Agricultural machinery and tractors" standard [12] presents ideas and risks related to on-board systems. These three autonomous mobile machine standards give different perspectives to autonomous systems and they complete each other. These standards have lists of hazards, and the relevant hazards are listed in Table 1 or Table 2. The literature related to autonomous cars is described since the technology on-board car is very advanced and much researched area, and there are some statistics related to autonomous car accidents. There are also some studies, which show that new technologies bring new risks.

Standard ISO 17757:2019 "Earth-moving machinery and mining — Autonomous and semi-autonomous machine system safety" was published in 2019 [8]. It gives an overall frame for outdoor autonomous machine systems and shows a list of significant hazards. The standard points out, especially, the autonomous system and fleet control level risks. Many earth-moving machinery hazards have a generic nature and they can also be applied for other autonomous mobile machine fleets or systems.

Standard ISO 3691-4 "Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems" was published in 2020 [9]. The standard gives requirements for indoor industrial trucks (also called AGVs or autonomous mobile robots) and their on-board systems and safety functions. In addition, the standard describes different operating zones (operating hazard zone, restricted zone, and confined zone), which can have different access rules and safety requirements. Some requirements of the standard are difficult to apply for outdoor systems. For example, according to the standard, typically, the maximum speed in a restricted area for a truck is 1.2 m/s. This is suitable for indoor use, but for many outdoor mobile machines, the

Table 2: Autonomous operation failures and related risk sources

Risk source	Description (operation failure, conditions, requirements)
1. Lack of situational awareness: fire, collision, vibration [8]	The machine does not have the necessary ability to detect fire, vibrations, or a major failure/collision (as humans could) and activate protection system and minimize consequences. It needs to be considered whether technical means are needed to detect unusual performance of the machine, which could lead to more severe hazards
2. Area access control fails [8]	If area access control fails to prevent unauthorized personnel or equipment to enter the autonomous operating zone, there can be collision and other hazards
3. Autonomous operating mode begins unexpectedly [8]	If autonomous operating mode starts up although not all starting conditions are fulfilled, there is a hazard. A single human error should not be able to cause the change to autonomous mode. The start-up should only be possible to initiate from a safe position [8]
4. Incomplete or improper system updates and changes in programming, improper road design, area demarcation and failure in digital terrain map [8,31]	In case of failure, autonomous mobile machine can cause a hazard by entering forbidden or occupied area. The failure can be related, for e.g., to incomplete communication, failed acknowledgement, or poor integration or synchronization with other systems. Communication message failures to be considered [31] include: repetition (block other messages, no new messages), deletion, insertion, re-sequencing, corruption, delay, and masquerade (message mimics other type of message)
5. Cybersecurity risk [8]	Malicious attack of the system or single machine may enable hazardous movements of autonomous mobile machines
6. Procedure in emergency situation [8]	To minimize risks, emergency situation may require quick egress for persons through a normally closed autonomous area. Area access control may, normally, prevent access to the autonomous operating zone, but in emergency situations, entrance may be accepted to avoid additional risks
7. Failing lockout process [8,27]	Lockout process may fail, if it is realized only through standard software. Failed lockout can allow unexpected movements of the system. Physical device is required for lockout. This can be related to adequate PL
8. Navigation failure, operation control failure [8]	Inaccurate position or orientation information can cause false movements of the autonomous mobile machine Incompatible coordinate systems, imprecise navigation control, poor planning, or an inaccurate digital terrain map can cause hazardous movements of the autonomous mobile machine. In addition, the navigation algorithm can fail Latency in receiving data from the fleet control or sensor failures can cause hazardous situation In addition, speed control can fail and cause, for example, inadequate stopping distance, stability problems, or driving control problems due to poor terrain or steep curves Malfunction of the mobile machine can also cause hazards outside of the autonomous operating zone
9. Machine steering control failure [8,32,27]	Machine steering control failure can cause movements toward wrong direction. Failing to fulfil the steering requirements can be an indirect risk source. The requirements of steering control depend on the machine type and, among others, maximum speed. At slow speed, the mobile machine can be stopped to maintain safety. At high speed, the steering performance should be maintained until the speed is low enough for stopping without guaranteed steering. The performance during a failure requires cooperation between primary steering, possible secondary steering, and brakes. The complete function should be according to relevant PL

(*Continued*)

Table 2: *Continued*

Risk source	Description (operation failure, conditions, requirements)
10. Stability control [9,27]	In conventional machines, there can be warnings and hazardous movement prevention against falling (e.g., in mobile elevating work platforms). If stability is an issue, then stability control is necessary in autonomous mobile machines too. Stability can also be related to the speed or hoisting performance in curves or exceptional situations. In addition, adequate PL for the function is required
11. Perception of tagged person or machine fails [8,27]	A tag perception failure may enable a person or vehicle to enter a reserved area or a new area does not become reserved when a tagged object enters it. In addition, separation distance to the autonomous machine may become too short. All of these cases can cause a collision. Relevant PL of safety functions should be considered
12. Perception failure of human, machine, or other objects [8,12,26,27,30,33,34]	Perception failure is possible at least due to the following reasons: Sensor hardware, software, or communication failure. The sensors and their functions need to be built according to the defined PL, SIL, and/or type [34]. Physical properties of the sensor (such as detection range, capability in outdoors use, or response time) are not adequate for the purpose due to selection, design failure, or inaccurate calibration. Object position: objects beside larger object, object behind corner or another object, person lying on the ground (detection field is above the person, which cannot be detected), or person leaves a vehicle suddenly. Object surface properties: color similar to background, surface reflects detection beam away, surface absorbs detection ray, object material is transparent to applied detection rays. Object dimensions: object/load dimensions at lower or higher height compared to the detection field, object is small, narrow, long (can reach far from the machine body). Vehicles at crossings or merging paths: fast objects may be undetected, load dimensions exceed the vehicle frame, turning circle difference between front and rear wheels can cause unexpected dimensions. Blind spots: too far, too close, approach direction, obstacles limit visibility, errors in digital terrain map, hole at the ground (negative object), tilting of the vehicle (heavy load, empty tire) cause detection field to rise/lower, inclined ground surface, bumpy ground, sensor misalignment, objects hidden due to restarting of the system, specific/exotic sensor properties. Deliberate or unintentional human actions to avoid detecting sensors. Environmental factors: sunlight, poor lighting on dark, dust, mud, fog, mist, rain, snow, smoke, etc. The system may be unable to detect correctly the environmental conditions (e.g., fog) and therefore fails to observe diminished detection capability. Uneven ground, vibration, tilted vehicle, or impact may cause misalignment of sensors. Sensor signal overflow (saturation) or interference due to multiple similar sensors applied in the same area (sensors interfere with each other).

(*Continued*)

Table 2: *Continued*

Risk source	Description (operation failure, conditions, requirements)
	Other strong signal emitters or reflectors at the site or at other machines can interfere with the sensors. Ability to distinguish persons from other objects (morphological recognition) is diminished due to environment, unusual clothing, unusual posture, and unusual angle from the sensor (e.g., camera). Electromagnetic transponder (tag), ultrasonic transponder or other device positioning, battery condition, latency due to computational load or environment cause diminished detection range.
13. Inability to activate stop or other safety function remotely [31,35]	Message error can cause hazards. Message errors repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade should be considered [31].
14. Lost, delayed, altered, or insufficient data [8]	False data can cause hazards. The failed data can be related to, for e.g., situational awareness information, terrain data, topology changes, commands, insufficient intersection control, machine coordination, traffic control, hazard information, position, planning, tracking, fire protection system, network configuration changes, autonomous machine system configuration changes, environmental issues (e.g., weather), power issues, etc. Altered data may also be related to intentional hacking or jamming (cybersecurity).
15. Autonomous or semi-autonomous machine system (or fleet control) communication failure [8]	Fleet control error can be related to wrong assignment (e.g., coding error), human error, operation is using incorrect/mismatch terrain map/operational area map or incorrect machine parameters (e.g., dimensions).
16. Load handling failure [9]	Load handling failure can be related to, for e.g., false commands, false communication, inadequate accuracy, load imperfection, attached/locked load although it should not, inadequate environmental condition.
17. Automated fueling or charging system failure	Automated fueling of charging can have hazards, which depends on the system. The risk sources need to be found in risk assessment and relevant standards. The risk sources can be related, for example, to overcharging/fueling, flammable fumes, heat, static electricity, live parts, battery management control, positioning, etc.

speed is too low from the productivity perspective. Thus, instead of low speed, system level safety functions like area access control need to be used. The standard shows a generic list of significant on-board hazards and safety functions, including required PLs.

Standard "ISO 18497:2018. Agricultural machinery and tractors — Safety of highly automated agricultural machines" focuses on autonomous tractors and describes among others the risks related to them [12]. The standard focuses on individual tractors, which may have a driver and the described systems are on-board. Many described operations can be related to semi-autonomous or autonomous functions and many risk reduction measures are mutual to them. The presented risks and requirements are related, among others, to perception, guarding system, operational status, and positioning.

Self-driving cars have a long history and apparently, many risk sources are also relevant for autonomous mobile machines. Mobile machines are developed according to Machinery Directive 2006/42/EC [23], while cars have international/European requirements (standards, UNECE) and national rules of the road. Mobile machines typically operate within a restricted area with fleet control applied, whereas cars are driven individually, with much higher speed and with the safety being based on on-board systems. Accidents involving autonomous vehicles [24] have shown that the perception capability and the algorithms used for perception and handling uncertain information are not always adequate [6].

Favarò et Al. described and presented statistics related to autonomous car (self-driving car) studies made in California from 2014 to 2017. One can learn from the described 26 accidents related to autonomous vehicles) [5]. The average accident rate was 1 per 67,000 km (totally travelled 1,750,000 km), but there were differences between different types of autonomous cars. For conventional cars, the value is 1 accident per 800,000 km (over 6 million accidents, but accident definition is presumably narrow). In the autonomous vehicle data, there were no injuries, speed was often about 15 km/h (highest speed 43 km/h), 62% were rear damages (same accidents share of conventional cars was 4%), and front damages 15%. The damaged part of the car is different in autonomous and conventional cars. 23 accidents (88%) happened in intersections. It has been estimated from the reports that the autonomous vehicles caused only 15% of the accidents and half of them were caused by the driver of the autonomous car (in manual mode) [5]. In some cases, the guilty party and human relation to the accident can be difficult to prove. One may conclude that autonomous cars stop promptly at the intersection and someone bumps the rear end of the autonomous car. It does not sound typical case for autonomous machines and it is difficult to conclude much. Anyway, there are collision risks and the intersections are difficult for the autonomous cars, but the accidents have not been severe.

The year 2016 was a turning point for considering risks of self-driving cars. During 2015, there were only about 20 minor accidents and the fault was attributed to human drivers. During 2016, there was an accident, which was obviously caused by self-driving car. A little bit later, the first fatal accident happened. After that, it has been clear that self-driving cars may cause severe accidents [13]. There have been at least 5 fatalities (2016, 2016, 2018, 2018, and 2019) related to autonomous cars [24].

The recent development of the risk assessment methods for applications of automated systems can be divided into real-time risk assessment methodologies and system design centric methodologies. Large amount of the risk assessment methodologies have been developed for dealing with the complexity of the traffic scenarios and thus for collision avoidance (e.g., [14]). It seems clear that while certain risks are reduced or even eliminated by automation, new risks emerge, as shown for road vehicles automated by Bellet et al. [15]. As stated by Zio [16], risk assessments need to take into account the new challenges posed by the rapid innovations and changes experienced. System-theoretic models have been applied for the analysis of autonomous vessels [17,18] to support the design. Based on the findings of these studies, it is argued that previous methods are limited in their capabilities to address the systemic nature of the targets and thus the interactions between system parts accordingly and that the methods require data, which do not yet exist. Furthermore, it can be argued that we need to learn more about the risk types of autonomous systems in order to support the analysis of the complex systems.

3 Definitions and limitations of the study

3.1 Risk sources and hazards

The focus of this article is on new risk sources and hazards related to autonomous mobile machines. Risk source is an element, which alone or in combination has the potential to give rise to risk [19]. The definition is wider than the definition of hazard, which is associated with harm (physical injury or damage to health). Both the risk source and hazard are applied in this article. Risk source is also applied to depict an accident where no persons are present (e.g., collision of two unmanned vehicles). Hazard is defined in ISO 12100:2010 as potential source of harm [20]. It can have qualifier like collision hazard, it can be continuously present (e.g., rotating wheel), it can appear unexpectedly (crushing hazard as a consequence of unexpected start-up), or there can be ejection as a consequence of breakage or mobile machine can fall as a consequence of acceleration/deceleration [20]. Hazard qualifier can be a factor, which gives more information about the details of a risk source. The new hazards discussed here are typically not relevant for conventional mobile machines.

3.2 Risk parameters

Risk can be defined in many ways and it depends on domain (industry, trade, safety, security, etc.). Aven and Renn [21] presented over ten definitions of risk. According to ISO 12100, risk is a combination of the probability of occurrence of harm and the severity of harm [20]. When related to the safety of machinery, the risk is related to negative impact and the function between probability and severity is not defined (not always multiplication, for e.g., if the parameters are logarithmic). When there are given values for severity, it is difficult to define is the function linear, logarithmic or

something else. It is not easy to compare different severities, like does 1 fatality equal to 10 broken arms or 100 bruises or should the factors be something else. According to ISO 12100, probability of occurrence is a function of occurrence of a hazardous event and technical and human possibilities to avoid or limit the harm [20]. In many cases, uncertainty instead of probability can open a wider view to the risk concept [21]. In the earth-moving machinery sector associated with Machinery Performance Level assignment [22], the following risk elements are applied: severity, exposure to hazardous event (as %), and possibility to avoid harm, which is divided into alternate controls, awareness of hazard, ability to react, and controllability. These factors show that elements like awareness and controllability are important, which are not mentioned for general machinery risk elements [20,27]. Obviously, these elements are originally relevant for conventional mobile machines and for autonomous mobile machines, these elements may require more explanations. For example, how to describe situational awareness of a control system. In upper level, risk parameters are easy to define, like severity and probability, but detailed analysis requires more precise risk parameter specification, which may be applied on case-by-case basis. Risk parameters also show some risk sources to be considered.

3.3 Risk assessment and hazards

Machinery Directive 2006/42/EC [23] and ISO 12100:2010 [20] require risk assessment for manufacturers, but a specific method is not defined. According to Work Equipment Directive 2009/104/EC [25], user organization also needs to do risk assessment.

In functional safety standards SIL [26] and PL [27] assignment processes, the risk assessment is used to identify and determine risk levels associated with safety-related control systems. The determined levels (PL or SIL) can be associated with requirements. In PL and SIL assignment processes, the risks under control are limited to safety functions and not all hazards are considered. PL and SIL can be considered as an agreement of how much effort is needed to minimize the risk under control, and in assignment phase, a hazard may be dropped out, if the risk is low or not related to safety functions. However, not all risks are related to safety functions associated with PL or SIL. The hazard identification is done before PL or SIL assignment, and therefore the assignment does not usually help hazard identification, but the parameters described in functional safety standards may give additional information about the hazards and their properties.

According to ISO 12100:2010 [20], hazard identification is a part of risk assessment process and it can be made when the scope and limits of the system to be analyzed are defined. Limits may be related, for example, in preventing hazardous use of the system and this has an effect on the hazards that need to be identified. The process of risk assessment is presented in Figure 1.

Hazard identification is probably the most important part of risk assessment, since if a hazard is not identified, then the associated risk is not under control; unless the risk is eliminated by a higher/system level overall

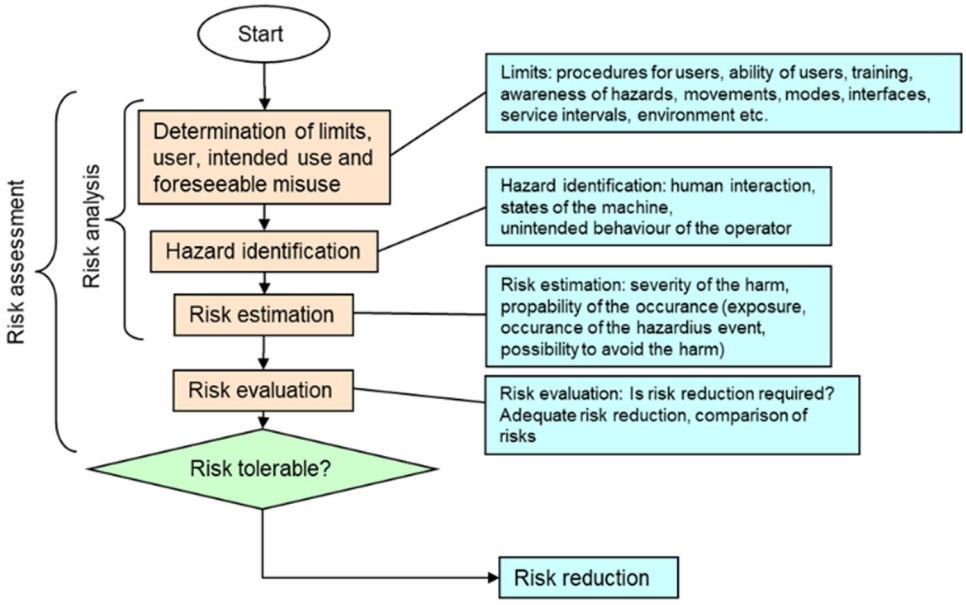

Figure 1: Risk assessment process according to ISO 12100:2010 (modified) [20].

solution (e.g., automation inside isolated area). To maximize the probability of identifying hazards, many different risk analysis methods are applied, analyses are made at many levels of detail, and many sources of information, experts, and lists of hazards can be utilized. Current article focuses on the lists of hazards, which are presented in Tables 1 and 2.

3.4 Description of an autonomous mobile machine system

The risk sources in this article are related to new risk sources, which may cause a collision or other major consequence in outdoor autonomous mobile machine applications. The autonomous mobile machines are typically controlled by fleet control, which gives tasks and commands. Typically, there are access control systems, which control the entire area, intersections, and/or specific work areas. The status information of each mobile machine is shared with the fleet control system. Weather conditions, construction work, layout changes, troubleshooting, and traffic at the worksite affect the commands that are given by the fleet control system to the autonomous mobile machines. The autonomous mobile machine drives autonomously up to the defined target or area access control border, where access permission is required. Figure 2 shows an example of autonomous/semiautonomous machine system components.

Figure 3 (modified IEC/TR 62998-2:2020 [28]) shows an example of autonomous mobile machine system. The system consists of three closed and isolated areas with area access control systems. Operation areas 1 and 3 are associated with PL d safety functions (sensors, interlocking devices, and control systems). The detection range of the PL d safety sensor is 4 m and the mobile machine is able to stop within the range due to the slow speed at operation areas 1 and 3. Operation area 2 has lower safety requirements due to low demand rate. The speed is higher and currently (year 2019) there are no PL d certified (type examined) safety detection sensors with detection range more than 4 m [29]. Performance level PL c can be achieved using duplicated PL b sensors with adequate detection range. The safety principles for the sensor fusion are described in technical specification IEC/TS 62998-1:2019 [30] and technical report IEC/TR 62998-2:2020 [28]. A hazard can be realized, for e.g., if one of the duplicated sensors fails or loses the required capability.

Figure 4 shows an example of on-board perception sensors and their detection zones. Here SRS A is PL d certified safety sensor and SRS B sensors fulfil PL b safety requirements. Both the SRS B sensors have longer detection range than required for stop zone B and the other SRS B sensor has even longer detection range than required for speed reduction zone. The sensors are applied according to the zone requirements, in order to fulfil functional safety requirements and to avoid futile perceptions (perception from too far distance). The speed reduction zone fulfils only lower performance level requirements, since the detection capability and performance are not adequate for higher levels. The communication link has both safety-related messages and production-related messages.

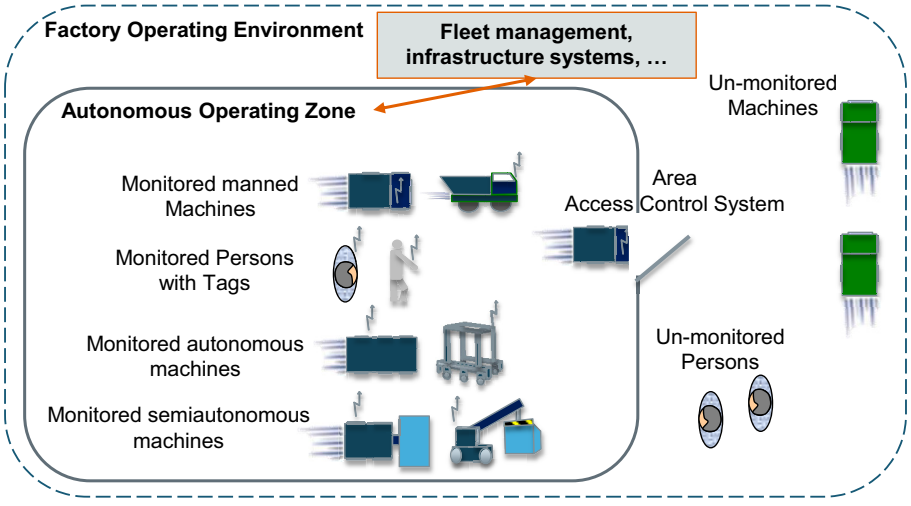

Figure 2: Autonomous/semiautonomous machine system components.

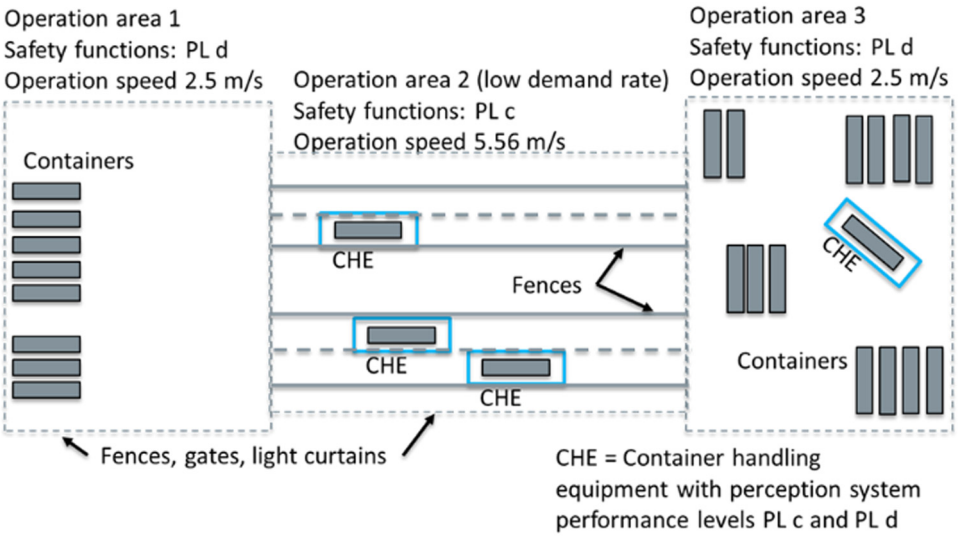

Figure 3: An example of autonomous mobile machine system (modified IEC/TR 62998-2:2020 [28]).

4 Results

4.1 Safety risk sources of autonomous mobile machines

Conventional and autonomous mobile machines have many similar hazards. However, autonomous functions for mobile machines may change the nature and relevance of different types of risk sources. Table 1 presents how typical mobile machine hazards change when the system is turned to autonomous. The table points out new additional hazards related to autonomy, but these hazards are, typically, not related to functional safety.

Table 2 shows new risk sources related to autonomous mobile machines and especially functional safety. In many cases, the basic hazard can cause collision, but also some other severe events are possible. Risk source reference is mentioned on the left column and description of the hazard or related means to avoid the hazard are on the right column.

Tables 1 and 2 show risk sources of autonomous mobile machines. Risk sources listed in Table 2 are referred as plain numbers. The considered risks are gathered from machine design and risk assessment standard ISO 12100:2010 [20], autonomous earth-moving machine standard ISO 17757:2019 [8], driverless industrial truck standard ISO 3691-4:2020 [9], highly automated agricultural machine standard ISO 18497:2018 [12], sensor standards, and functional safety standards. The standards include many kinds of risk sources, but only those, which can be associated with autonomy, are presented in the tables. The generic hazards, described in standards, have been widened by adding own experiences and discussions with manufacturers of mobile mining machines, container handling machines, and forest machines.

4.2 Analysis of the results

Nearly all the risks in Table 2 are related to inadequate performance of functions realized by control or safety

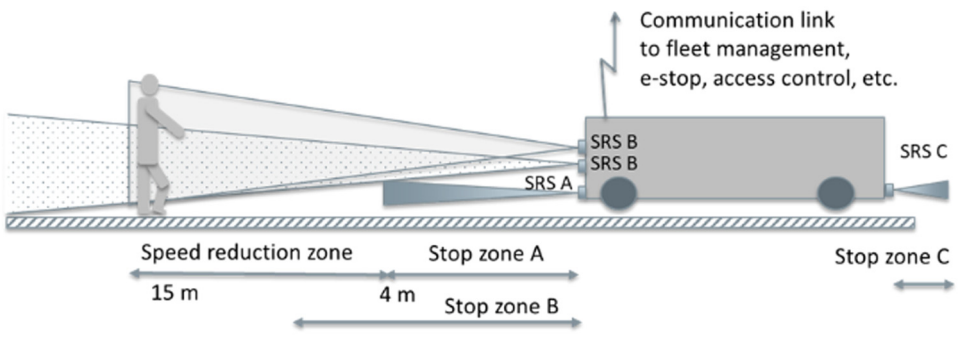

Figure 4: An example of autonomous mobile machine and its on-board perception sensors and their detection zones.

system. Stochastic failures and design failures (including software) cause risks, which need to be controlled according to functional safety requirements (ISO 13849-1 [27]), which include, for e.g., assignment of PL or SIL. If the selected PL is too low, it is a design failure and a hazard is possible. If the PL is adequate, the system suits the environment and the system is applied in designed manner, and a failure should be improbable.

Artificial intelligence (AI) is not mentioned in the tables, but it is associated with requirements of safety functions and their PLs [27], which are relevant to all kinds of control systems. There is an ISO technical report, which considers use of AI, for example, in AGVs [36]. Specific AI failures are not considered here.

Communication related hazards are relevant for autonomous mobile machines, since the current technology cannot usually guarantee safety and productivity of an independent autonomous mobile machine, but communication is needed to provide tasks, commands, safety functions, and situational awareness for the machines (at least 13 and 14 in Table 2). A safe communication system does not deliver false messages and it has specific error handling procedures for delayed, corrupted, and missing messages. However, communication errors may have surprising consequences, which need to be analyzed. More precise information about communication risks and requirements can be found in standard: IEC 61784-3:2021 [35].

Since the safety system and the complete autonomous mobile machine system include so many new subsystems, there are also many new kinds of collision risks compared to conventional mobile machines. One specific issue related to the new subsystems is uncertainty, how much we can trust the new subsystems and certified safety components. Uncertainty means that there is also a potential risk source.

5 Discussion

Increased automation brings new kinds of risks in comparison with conventional vehicles. It is difficult to replace human perception and reasoning capabilities with automation. First, machines do not (yet) have as good perception capabilities (compare 12 in Table 2) as humans do together with many kinds of devices (e.g., speedometer and camera). Humans have excellent vision capabilities and possibilities to sense, for example, vibration, smell, or abnormal steering performance. Second, humans can anticipate situations and do adequately quick decisions to minimize risks in unexpected situations. When looking at the operations of driverless cars, it can be seen that currently human action (disengagement) has been needed (Google/Veimo) about every 1,470 km. General average has been one disengagement per 330 km [5], but it gets better as driverless car teams become more experienced. Not all engagements have been related to a possible accident and the amount of disengagements in the future will be smaller, but human action is needed relatively often [37]. The problem with humans is that, in addition to perception and logical failures, humans intentionally take risks and, in some cases, do not obey rules. In the future, sensors and artificial intelligence are supposed to become in many ways better and less expensive than today. In addition, decision algorithms (which may apply AI) are becoming quicker, more reliable, and more comprehensive to support safe and effective decisions. Both humans and autonomous vehicles have their own advantages and weaknesses from the safety point of view now and in the near future. Safety or control function of autonomous system has replaced human operation at least in items 1, 4, 6, 8, 9, 12, and 16 in Table 2.

The autonomous system needs to consider, to some extent, human errors or unexpected performance in the traffic. This can be related, for example, to disobeying the rules of traffic, performance at the autonomous area, or how to supervise the system. These kinds of risks need to be considered on case-by-case basis and the issue is not specifically mentioned in the tables. Disobeying rules can often lead to an accident.

The safety of autonomous mobile machines is based on many kinds of means, like fences, gates, access control systems (2 in Table 2), communication with fleet control (4, 6, 13, and 14 in Table 2), and on-board sensors (12 in Table 2). The isolated systems without workers at hazardous zone can be currently adequately safe, but there is a need to use more open systems, where humans and conventional machines could move more freely. There are many kinds of risks due to complex combination of systems related to the machines and the fleet control.

If safety is based on on-board safety systems, then also major share of risks is related to them. At this moment, on-board sensors are safe enough for indoor AGVs, which means typically PL d sensors (e.g., type examined laser scanners) as required in driverless industrial truck standard [9]. For outdoor applications, due to high speed and environmental conditions, the machine stopping distance is usually inadequate, if the sensors were the only safety means. Therefore, many additional systems related to, for e.g., fleet control and area access control, are needed. Due to complex safety-related systems,

the large diversity of risk sources will be associated with autonomous mobile machines for some time.

Perception failures (12 in Table 2) are important in applications where autonomous mobile machine safety relies on on-board perception. Outdoor applications may have environmental or other conditions, when perception is unreliable. Therefore, additional means are required to ensure safety. When using additional means, a single failure does not necessarily lead to danger, since there is another system to ensure safety. It may be difficult from the analysis point of view to find out which exception or failure is actually hazardous and which is only potentially hazardous. If a specific detection sensor, like camera (EPO European Inventor Finalists for automotive sector 2019), would be adequately safe in the near future, it would change the risk sources considerably. Cameras have a long detection range, objects beside large objects can be detected, and the safety is based on software and AI, but adequate purity of the lenses, object colors, adequate lighting, and the safety of algorithms (or AI) need to be considered.

Communication systems are becoming increasingly important for safety measures. In the future, it is possible that all objects communicate with each other and give information about their position, path intention, and stopping distance. Such information needs to have high integrity (no unintentional changes) and high availability and the communication needs to be fast. Communication systems can take much responsibility of safety, but then also risks related to failures and errors become relevant (13 and 14 in Table 2). There have been high hopes related to, for example, 5G, which could solve many safety issues due its high speed and connectivity.

It has been said that human is responsible for 90% of the car accidents [6]. Since human is not much involved in autonomous (self-driving) vehicles, how much do the accident rate drop, or does it? Who is a safer driver, human or control system? In ordinary cars, humans do steering, acceleration, deceleration, and braking with the help of actuators. It may look obvious that human is the main risk. What happens to overall risk when all of these functions are operated by control systems? Nowadays, difficult parts of driving are still operated by humans and so, only the well-defined cases can be autonomous. For example, Google (Veimo) autonomous cars have had about 0.68 disengagements per 1000 km [37]. Disengagement means that the driver needs to be alert and capable of taking control of the vehicle. The reasons for disengagements were system failure 56.1%, driver initiated 26.57%, road infrastructure 9.98%, other road users 5%, construction zones 1.55%, and weather 0.8% [37]. Apparently, the disengagement number will be lower in the future (at least in similar roads). It sounds that humans take the risky phases of the nearly autonomous mobile machines. Recognition errors, decision errors, and performance errors have been related to humans, but what happens, if the tasks are given to control systems. Autonomous machine errors would include large variety of additional errors or risks (Tables 1 and 2). It is currently difficult to have a generic conclusion, who is the safer driver in the near future: human or control system? [38].

Liability risk is not considered here specifically, but actually, autonomous mobile machine systems have often many stakeholders, like machine manufacturer, control system supplier, logistics operator, software provider, software operator, and user. Since there are so many stakeholders, it may be difficult to define the liable stakeholder of a specific risk. Undefined liability is a risk and it may cause new risks, if nobody is considering risks of other stakeholders. The liability risk can be related to any item of Table 1 or Table 2, but items 4 (infrastructure information), 5 (cybersecurity), and 6 (informing about emergency situation) of Table 2 are often related to two or more stakeholders. Taeihagh and Lim [6] point out that liability issues related to autonomous vehicles are difficult to solve completely, since often, there are so many parties involved. Liability issues can be related, for example, to accidents, design or manufacturing failures, practical and moral reputation, insurance, trade, and legal issues. One problem is that liability is different in different countries and currently the liability legislation related to automated vehicles is developing only currently. A specific risk may be huge from one stakeholder's point of view, but small from another stakeholder's point of view [6]. Since the liability issues are so complex, it may be a good strategy to consider other risks also than those related to only own design.

Cybersecurity is a risk source mentioned in Table 2 (5). A malicious attack can cause hazardous situation, like collision. Earlier, cybersecurity has not been such an important factor, since the systems and communication have been relatively individual and closed. Therefore, attack would have needed special knowledge of the system, vicinity, and resources. Nowadays, there are more communication systems, they are becoming more open and standardized and therefore there are more challenges to keep cybersecurity issues in adequate level. Cybersecurity risks for automation are considered more detailed in IEC 62443 standard family: "Industrial communication networks. Network and system security."

Collision is often the main consequence of a wrong movement, which furthermore, can be associated with

risk sources, although if there are no persons at an automated operating area, the probability of a harm is very small. Also, other consequences can be associated with autonomy, like stability problems (10 of Table 2) and load handling problems (16 in Table 2), which are relevant, but not so common for all kinds of mobile machines.

Checklists for finding risk sources are presented in Tables 1 and 2. The tables intend to be comprehensive and generic, but it means that in some cases, the risk sources are described in generic level, which allows some technology variations. However, each application is unique and there may be special autonomy-related risks, which are not mentioned in the tables. Technologies are developing and there will be new kinds of risk sources.

New technological features are developed continuously. The new features can be applied to better safety or effectiveness. For example, increasing the velocity would often mean more severe risks and better effectiveness, but yet overall safety level can be the same.

6 Conclusion

Outdoor autonomous mobile machines require more safety features and devices to ensure safety than driverless cars (dedicated to on-board intelligent systems), indoor AGVs, or manual mobile machines. Autonomous mobile machine systems also include supervisory systems. like safety-related fleet control and area access control systems. Although the safety measures are intended to provide better safety, they also initiate new risk sources. Since there are so many safety-related systems, the amount of potential risk sources is also big. Table 2 shows 17 risk source groups, which are related to functional safety or control systems. In addition, Table 1 shows risk sources, which are relevant in manual machines too, but due to autonomy, they have changed.

It is possible to learn from the accidents related to driverless cars, since there are millions of documented kilometers. The accidents of driverless cars are concentrated on intersections. Currently intersection control is mentioned in standards ISO 17757:2019 [8] and ISO 3691-4:2020 [9], but risks or safety measures are not described. It is possible that autonomous mobile machine accidents also occur at intersections, but currently we do not know that due to inadequate statistics. In some cases, intersection accidents can be associated with area access control risks (2 in Table 2), but special consideration of intersection risks is needed in any case. Another observation related to driverless cars is that the most common accident is when the conventional car contacts the rear end of the driverless car. This kind of accident is also possible for autonomous mobile machines, but the main reason for such accidents have been careless manual driving. Large share of manual driving accidents indicates that manual driving needs to be considered carefully as a risk source inside the automated areas. Manual driving can be associated, in some cases, to risk related to area access control (2 in Table 2).

Checklist of risk sources related to autonomous mobile machines is presented in this article to help finding new risk sources of autonomous mobile machines. The checklist does not describe risks in detail, but it is intended to be comprehensive in device level. However, the checklist may not be too long to be practical, there are many kinds of different applications and, in addition, new technologies are developed continuously and therefore risk sources for all kinds of autonomous mobile applications cannot be presented. The checklist gives ideas for risk assessment to identify new risk sources.

Acknowledgements: Research on safety engineering methods and safety requirement management in autonomous machinery systems has been done and is ongoing in Finland in a national co-innovation project financed by Business Finland, VTT, and participating companies.

Conflict of interest: Authors state no conflict of interest.

References

[1] Burkacky O, Deichmann H, Stein JP. Automotive software and electronics 2030. McKinsey & Co; 2019. p. 48.
[2] Ramsey M, Arnott M, Davenport J. Forecast analysis: Autonomous vehicle net additions, internet of things, worldwide. Gartner, Inc; 2019.
[3] SAE J3016_201806. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles; 2018.
[4] Bimbraw K. Autonomous cars: past, present and future: a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology. Proceedings of the 12th International Conference on Informatics in Control, Automation and Robotics (ICINCO-2015); 2015. p. 191–8. ISBN: 978-989-758-122-9.
[5] Favarò FM, Nader N, Eurich SO, Tripp M, Varadaraju N. Examining accident reports involving autonomous vehicles in California. PLoS ONE. 2017;12(9):e0184952. doi: 10.1371/journal.pone.0184952.
[6] Taeihagh A, Lim HSM. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transp Rev. 2019;39(1):103–28. doi: 10.1080/01441647.2018.1494640.

[7] Goldin P. 10 Advantages of autonomous vehicles. ITSdigest 20; 2018. https://www.itsdigest.com/10-advantages-autonomous-vehicles.
[8] ISO 17757 2019 2019. Earth-moving machinery and mining — Autonomous and semiautonomous machine system safety. 36.
[9] ISO 3691-4 2020. Industrial trucks — Safety requirements and verification — Part 4: driverless industrial trucks and their systems; 2020. p. 84.
[10] Van Brummelen J, O'Brien M, Gruyer D, Najjaran H. Autonomous vehicle perception: The technology of today and tomorrow. Transp Res Part C. 2018;89:384–406.
[11] March S, Storey V. Design science in the information systems discipline: An introduction to the special issue on design science research. MIS Q. 2008;32(4):725–30.
[12] ISO 18497 2018. Agricultural machinery and tractors — Safety of highly automated agricultural machines — Principles for design; 2018. p. 18.
[13] Nyholm S. The ethics of crashes with self-driving cars: A roadmap, I. Philosophy Compass. 2018;13:e12507. doi: 10.1111/phc3.12507. wileyonlinelibrary.com/journal/phc3.
[14] Katrakazas C, Quddus M, Chen W-H. A new integrated collision risk assessment methodology for 1 autonomous vehicle. Accid Anal & Prev. 2019;127:61–79.
[15] Bellet T, Cunneen M, Mullins M, Murphy F, Pütz F, Spickermann F, et al. From semi to fully autonomous vehicles: New emerging risks and ethico-legal challenges for human-machine interactions. Transportation Research Part F. Elsevier. 2019. p. 153–64.
[16] Zio E. The future of risk assessment. Reliab Eng Syst Saf. 2018;177:176–90.
[17] Wróbel K, Montewka J, Kujala P. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliab Eng Syst Saf. 2018;178:209–24.
[18] Banda O, Kannos S, Goerlandt F, van Gelder P, Bergström M, Kujala P. A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. Reliab Eng Syst Saf. 2019;191:106584.
[19] ISO 31000 2018. Risk management. guidelines; 2018. p. 20.
[20] ISO 12100 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction; 2010. p. 77.
[21] Aven T, Renn O. On risk defined as an event where the outcome is uncertain. J Risk Res. 2009;12(1):1–11. doi: 10.1080/13669870802488883.
[22] ISO 19014-1 2018. Earth-moving machinery. Functional safety. part 1: Methodology to determine safety-related parts of the control system and performance requirements; 2018. p. 24.
[23] Machinery directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending directive 95/16/EC (recast); 2006. p. 63. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri = OJ:L:2006:157:0024:0086:EN:PDF.
[24] Wikipedia a. List of self-driving car fatalities. Retrieved 16.9.2020. https://en.wikipedia.org/wiki/List_of_self-driving_car_fatalities.
[25] Work equipment directive 2009/104/ECequipment directive 2009/104/EC. Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC); 2009. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri = CELEX:32009L0104&from = EN.
[26] IEC 61508-1 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements; 2010. p. 127.
[27] ISO 13849-1 2015. Safety of machinery. Safety-related parts of control systems. part 1: General principles for design;2015. p. 193.
[28] IEC TR 62998-2 2020. Safety of machinery – part 2: Examples of application; 2020. p. 37.
[29] Heikkilä E, Malm T, Tiusanen R, Ahonen T. Safety and dependability of autonomous systems in container terminals: Challenges and research directions. In: Berns K, Helfert M, Gusikhin O, (Eds). VEHITS 2020 - Proceedings of the 6th international conference on vehicle technology and intelligent transport systems. Vol. 1. SciTePress; 2020. p. 528–34. doi: 10.5220/0009472505280534.
[30] IEC TS 62998-1 2019. Safety of machinery – Safety-related sensors used for the protection of persons; 2019. p. 91.
[31] IEC 61508-2 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems; 2010. p. 167.
[32] ISO 5010 2019. Earth-moving machinery — Wheeled machines — Steering requirements; 2019. p. 18.
[33] ISO 16001 2017. Earth-moving machinery. Object detection systems and visibility aids. Performance requirements and tests; 2017. p. 79.
[34] EN 61496-1 2013. Safety of machinery - Electrosensitive protective equipment - part 1: General requirements and tests; 2013. p. 61.
[35] IEC 61784-3:2021. Industrial communication networks - Profiles - part 3: Functional safety fieldbuses; 2021. p. 214.
[36] ISO/TR 22100-5 2021. Safety of machinery — Relationship with ISO 12100 — part 5: Implications of embedded Artificial intelligence-machine learning; 2021. p. 12.
[37] Dixit VV, Chand S, Nair DJ. Autonomous vehicles: Disengagements, accidents and reaction times. PLoS ONE. 2016;11(12):e0168054. doi: 10.1371/journal.pone.0168054.
[38] Cunneen M, Mullins M, Murphy F. Autonomous vehicles and embedded artificial intelligence: The challenges of framing machine driving decisions. Appl Artif Intell. 2019;33(8):706–31. doi: 10.1080/08839514.2019.1600301.