EasyChair Preprint

№ 5239

New Safety Concepts for Autonomous Mobile Machines

Timo Malm, Risto Tiusanen, Eetu Heikkilä, Toni Ahonen and Janne Sarsama

March 30, 2021

New safety concepts for autonomous mobile machines

Abstract: Autonomous mobile machines are becoming more common in specific applications. Technologies have developed a lot, but full autonomy has not yet been reached in various outdoor environments. Driverless cars have driven tens of millions documented kilometers and there is already some experience. Safety measures of driverless cars rely on onboard safety sensors and intelligence, which can maintain safety in various conditions. In addition, traffic rules are essential, since collisions can be inevitable, if someone violates the rules. Autonomous mobile machines have also perception and positioning sensors, but quite often safety assurance is based on fleet management and area access control systems. The access to the autonomous area is usually limited when the area is in automated mode. The complete autonomous mobile machine system contains many kinds of subsystems related e.g. to perception, positioning, access control and fleet control. A failure of a subsystem can be hazardous unless safety measures of the subsystems are well integrated and interlocked with each other.

Keywords: safety, autonomous, mobile machine

Authors: Timo Malm, VTT, Finland, timo.malm@vtt.fi
Risto Tiusanen, VTT, Finland, risto.tiusanen@vtt.fi
Eetu Heikkilä, VTT, Finland, eetu.heikkila@vtt.fi
Toni Ahonen, VTT, Finland, toni.ahonen@vtt.fi
Janne Sarsama, VTT, Finland, janne.sarsama@vtt.fi

1 Introduction

Many kinds of autonomous ground vehicles are becoming more common as new technical solutions are applied more and more successfully. Driverless cars have been featured and they have already tens of millions kilometers documented driving. Autonomous mobile machines have been successful in some specific applications related e.g. to agriculture, ports and mines. There are already some standards for autonomous systems, which shows that the associated technological fields are expecting increase in autonomy. However, so far, autonomous mobile machines have been applied in limited applications and the final steps to full autonomy need to be done.

2 Autonomy concept

There are several concepts and terms for autonomous ground vehicles in different applications. The following terms are applied commonly to refer autonomous vehicles: driverless cars, unmanned ground vehicles (UGV), driverless industrial trucks, autonomous machines, highly automated agricultural machines, autonomous mobile robots and automated guided vehicles (AGV). The mixed terminology indicates that there are many fields of development in terms of autonomous systems and they point out different significance.

There are also several levels for autonomy from manual to conditionally automated and furthermore autonomous operation. The Society of Automotive Engineers (SAE) has six levels of autonomy from 0 to 5, which are dedicated to cars, but are applicable for mobile machines too. The levels are [1]: No Automation (0), Driver Assistance (1), Partial Automation (2), Conditional Automation (3), High Automation (4) and Full Automation (5). In level 5, autonomy is applicable in all conditions and in level 4 autonomy is applicable in specific conditions. The level of automation shows also how responsibility of the system is shared between driver and automation. Currently, level 5 has not yet been achieved, since in all autonomous mobile vehicles there are conditions, when autonomy is not applied.

Currently autonomous mobile machine systems are typically fenced and there are access control systems to control traffic in specific areas. Fleet management system can control autonomous machines and prevent their collisions with each other. In comparison with driverless cars, the fleet management system enables many safety features and safety performance level d (PL d) [2] can be achieved without compromising speed. When collision avoidance is based on onboard sensors, then the applied speed must be adequately low to ensure stopping before collision.

3 Standards and requirements

There are standards which consider properties or functions related to autonomous systems. Such standards are related to functional safety of the (control) system. Three standards related to autonomous mobile systems show different approaches to autonomy. Autonomous earth moving machine standard (ISO 17757:2019) [3] shows a model of a complete autonomous system, which has central control to monitor individual machines and persons. Although the background of the standard is earth moving machinery and mining, according to the standard, it is applicable in other kinds of worksites too. Driverless industrial truck standard (ISO 3691-4:2020) [4] gives examples of different levels of isolation and safety functions with functional safety requirements. Highly automated agricultural machine standard (ISO 18497:2018) [5] gives information about onboard safety systems of autonomous machines.

Sensors for human and object detection are critical in outdoors autonomous mobile machine systems. Earlier there have been standards only for indoors sensor systems, but now IEC TS 62998-1:2019 [6] and IEC TR 62998-2:2020 [7] have been published. These standards (actually technical specification and technical report) give guidelines for applying sensors in outdoor conditions, how to define limits for use, how to apply sensor fusion for improving detection capability and safety performance class. The examples are related mainly to laser scanners and radars. The idea is, typically, that the integrator of the sensor system defines all the capabilities and limits of the system.

A new kind of approach to situational awareness is described in draft ISO/TR 22053:2021 Safeguarding supportive system [8]. Originally the technical report is made for integrated manufacturing systems, but it can be useful for other applications too. The technical report describes how the safeguarding supportive system can be applied, for example, to authentication, authorization, releasing of guard locking device, restarting and message delivering. Depending on the criticality of the applied function, there can be safety requirements for the device. The related safety measures can be, for example, access rights for specific persons, position information of the device (person) or user information about the next task. The safeguarding supportive system can be part of safety system, which controls position and access of all objects. Such system would have to fulfill specific PL (Performance Level) requirements of ISO 13849-1 [2], however in machinery sector there are not yet such systems, or at least they are rare.

4 Risks and accidents

New technologies such as novel sensors for perception and positioning, navigation systems and artificial intelligence are applied in conjunction to ensure safety. There is still uncertainty regarding how safely the systems can operate in all conditions. Taeihagh and Lim have reported 2019 that driverless cars have had minor accidents in California about every 67 000 km [9] and according to Wikipedia (“List of self-driving car fatalities”) [10] there have been at least 5 fatalities around the world. The systems are not yet perfect and therefore more research is needed to integrate and interlock the systems to operate safely even if one part of the system fails.

Compared to cars, autonomous mobile machine systems have usually a different approach to minimize collision hazards. The systems are typically fenced and there are access control systems to control traffic in specific areas. Fleet management system can control autonomous machines and prevent their collisions with each other. In comparison with autonomous cars, the fleet management system enables many safety features and safety performance level d (PL d according to ISO 13849-1) can be achieved without compromising speed. The risks of completely closed autonomous machine systems, where there are no persons inside the autonomous operating zone in autonomous mode, differ from driverless cars and indoors automated guided vehicles (AGV). The most emerging risks of autonomous mobile machine systems are related to access control systems and navigation.

However, in many autonomous mobile machine applications there is a need to have open automated systems, where workers can enter more flexibly. The target, especially in large systems, is to avoid fences and allow at least a limited access to the automated area. This means that sensors need to be onboard the machines and they have to create the situational awareness which enables collision avoidance. When collision avoidance is based on onboard sensors, the applied speed must be adequately slow to ensure stopping before collision.

One problem with outdoors sensors is that it is difficult to detect objects in heavy rain or fog. Another problem is that the machine wobbles, when it moves and therefore sensors are not directed close to the ground and most of the sensors have a blind spot near the ground - a person lying on the ground cannot be detected with sensors. For the onboard protective sensors in outdoors applications, there are conditions, when an object cannot be detected. These risks of inadequate performance need to be defined and the unsafe conditions declared in order to avoid such conditions. The risks must be controlled, for example, by measuring visibility or the amount of rainfall.

5 Safety concepts

Fig. 1 shows an example of an autonomous mobile system, which includes autonomous operating zone, monitored manned machines, monitored persons and autonomous mobile machines. Unmonitored machines and persons are outside the autonomous operating zone. Vehicles and persons can enter the autonomous operating zone when it is safe. There are several means to establish safe operation, like, changing operating mode or dividing autonomous area into several zones with their own area access control systems. The figure shows also systems, which are typical onboard the autonomous mobile machines, and systems/objects, which are operating inside the autonomous area or beside it. According to ISO 17757:2019 each machine or person operating at the automated area shall be monitored or escorted by monitored person or vehicle, but the risk assessment may change the solution. Unauthorized access needs to be deterred anyway [3].

Fig. 2 shows the protective measures, which are applied in autonomous mobile machine systems. The described protective measures are:

- Rules for the autonomous area; these can include specific traffic rules, but there can also areas for persons only and restricted areas,
- Isolated areas, which have access control; this includes, for example, fences, light curtains, doors, gates and locks.
- Safe separation distance; the separation distance can be achieved by using onboard sensors or comparing position information of objects.

Safety measures of autonomous mobile machines can be divided also according to the place of the safety measure:

- Fleet management and supervisory system, which gives tasks and keeps the machines in permitted area and prevents impacts, with other automated machines or stationary objects.
- Area access controls, which can permit persons and machines to enter a specific area. The complete automated area can be divided into several areas, which have their own access control system.
- Rules of the system, which declares where machines and humans may move and on which conditions.
- Onboard safety system, which monitors neighborhood and maintains safety by applying relevant safety functions (e.g. stop or reduced speed command).

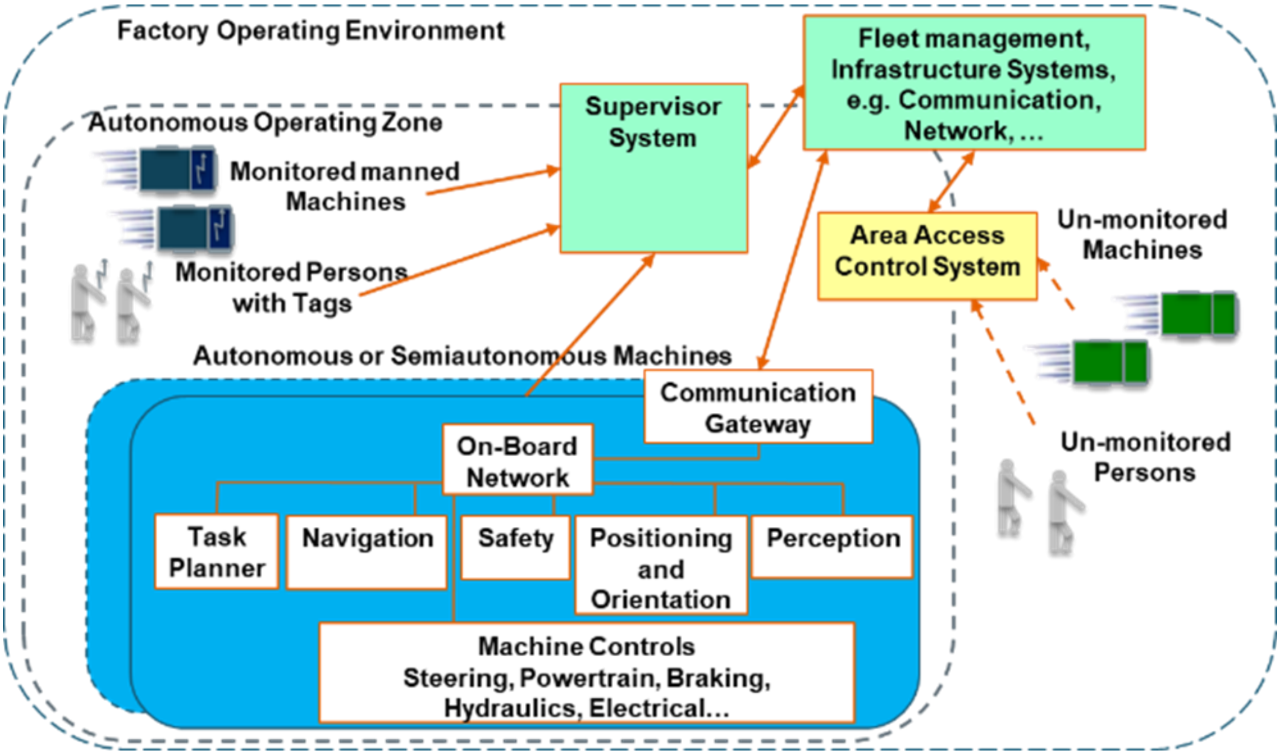
Factory Operating Environment
Autonomous Operating Zone
Monitored manned Machines
Monitored Persons with Tags
Supervisor System
Fleet management, Infrastructure Systems, e.g. Communication, Network, …
Area Access Control System
Un-monitored Machines
Un-monitored Persons
Autonomous or Semiautonomous Machines
Communication Gateway
On-Board Network
Task Planner
Navigation
Safety
Positioning and Orientation
Perception
Machine Controls Steering, Powertrain, Braking, Hydraulics, Electrical…

Fig. 1 Autonomous mobile machine system example according to ISO 17557:2019 (modified).

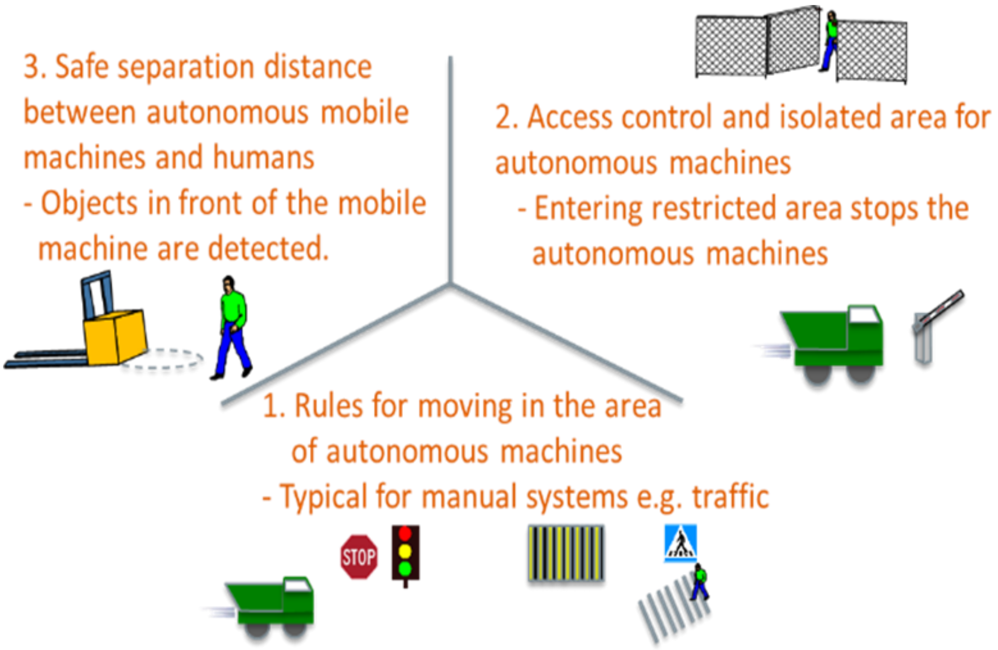
3. Safe separation distance between autonomous mobile machines and humans
- Objects in front of the mobile machine are detected.
2. Access control and isolated area for autonomous machines
- Entering restricted area stops the autonomous machines
1. Rules for moving in the area of autonomous machines
- Typical for manual systems e.g. traffic
STOP

Fig. 2.Approaches to ensure safety in an autonomous area.

If the system has many mobile machines and the paths intersect often, fleet management system can be necessary. The path conflicts and priorities of machines are difficult to handle using only onboard intelligence.

Area access control allows persons and machines to enter safely into the specified area. This can allow high speeds in the system, since no unknown objects are supposed to be in the controlled area.

Rules of the autonomous system can be an inexpensive way to control safety of the autonomous area. However, according to three-step method presented at ISO 12100, information (or rules) may not be used to replace inherently safe design methods or safeguarding [11]. Rules give information, for example, about lanes inside system, forbidden areas, walkways, and priorities. There can be also traffic signs, traffic lights, and voice signals. In the future, situational awareness can be a versatile system, which has all the rules and situation information integrated.

In autonomous mobile machines, onboard safety systems are applied to detect objects, which are beside the autonomous mobile machine in a hazardous position. Safety of driverless cars is typically based on onboard safety system, which detects objects that can cause collision hazard. Typical sensors for object detection are laser scanners, lidars, radars and tactile sensors. Cameras are common in cars. Onboard object detection sensors are necessary, when an object moves in front of the machine unexpectedly i.e. fleet management does not have the information.

The autonomous mobile machines are controlled and monitored by fleet management, supervisory and area access control systems, which are essential part of the autonomous system safety. If autonomous area could be isolated totally and no persons were allowed to enter the automated area in automated mode, then most of the hazards inside the area can be under control. However, usually it is not practical to prevent the access completely, but the conditions when the entrance is safe, need to be arranged.

Fig. 3 shows an outline of a container handling terminal, which has three different operating areas. This example resembles the example presented in IEC TS 62998-1, but it has some more options to describe different kinds of safety measures [6]. On the left operation area 1 has almost all the time only autonomous vehicles, speed is moderate (5 m/s) and human entrance turns the operating areas 1 and 2 into manual mode. The transfer area 2 has almost all the time only autonomous vehicles and the speed is high (7 m/s). Operation area 3 may have manual machines and persons at the area. The speed (2,5 m/s) is low in order to guarantee adequate stopping distance for the autonomous mobile machine to avoid collisions. Persons may walk only at marked areas and manual vehicles only in dedicated areas and lanes when the operating area is in autonomous mode. The complete area has peripheral guards (fences or light curtains) and access control system to control the manual traffic.

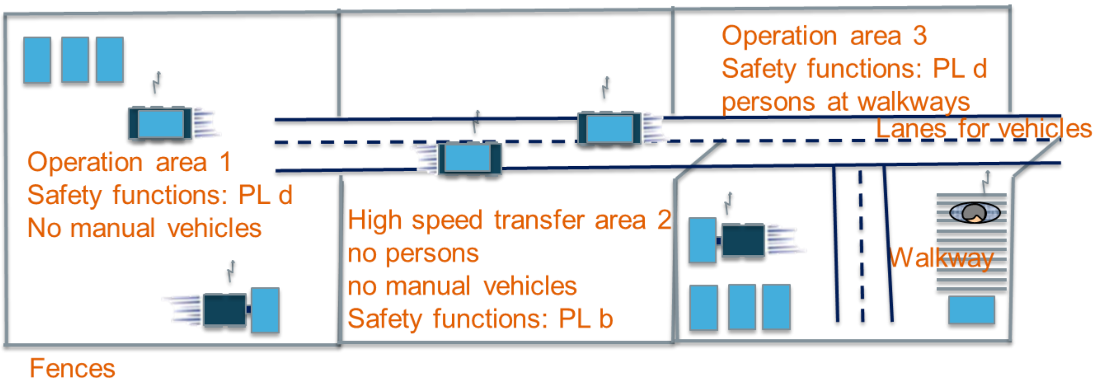

Fig. 3. Container handling terminal with three different operating areas.

6 Discussion

Three approaches to ensure safety are presented in this article:

- rules for autonomous area,
- safe separation distance between autonomous mobile machine and other objects and
- isolation of autonomous mobile machines.

Currently all the approaches are needed in most of the autonomous mobile machine systems. Rules are often the easiest and most economical way to control safety. Especially rare unsafe exceptions are often controlled using rules and information.

There are high hopes in controlling safety using onboard object detecting systems. However, currently there are not many type examined safety sensors and the reliable (accepted) detection range is only 4 m. Apparently, the detection range will increase in the future, but it can be a limiting factor for applications. Perhaps even a bigger challenge can be blind spots of detection. This is related, for example, to objects having low height, objects beside large object, objects coming behind a corner and poor detection conditions (e.g. rain).

Isolation of the autonomous mobile machine system is currently a clear way to achieve high performance level (PL d) for safety functions and relatively high speed of mobile machines. Humans are usually not in danger, if there are no persons inside the autonomous operating zone. However, there are risks, for example, related to control/navigation errors, which cause an autonomous mobile machine running or falling through a fence. The problem with total isolation of an autonomous mobile system is that usually there are exceptions when the system is not turned to manual mode and yet a person needs to go inside the system. There can be specific access rights, monitoring of the persons and safe walkways, which may be adequate measures to ensure safety, when the exceptions are relatively rare.

Situational awareness can be related to the information that the autonomous mobile machine utilizes and/or a person utilizes. The possibilities to use situational awareness have increased, since mobile phones/devices enable large variety of information to be delivered to the user and from user to the system. There is also a standard technical report related to safeguarding supportive systems.

The speed of an autonomous mobile machine is an important safety-related factor. There are two basic approaches to control speed and safety:

- peripheral guards and area access control; this enable also high speed inside the automated area.
- object detection system to stop the machine before a collision to an object; speed needs to be slowed down in order to stop the machine quickly enough.

Of course, there are also other means and means can be combined to achieve adequate safety level. Depending on the case, safety measures can increase productivity, but on the other hand high speed nearly always increase risks. In practice, safety measures are combined to optimize productivity, safety and flexibility of the system.

Acknowledgements

Research on safety engineering methodology for autonomous machinery systems has been done in VTT in a national co-innovation project AUTOPORT (https://autoport.fi/). financed by Business Finland, VTT and participating companies.

References

[1] SAE J3016_201806. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. 2018.

[2] SFS-EN ISO 13849-1:2015. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design. 193 p.

[3] ISO 17757:2019. Earth-moving machinery and mining — Autonomous and semiautonomous machine system safety. 36.

[4] ISO 3691-4:2020. Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems. 84.

[5] ISO 18497:2018. Agricultural machinery and tractors — Safety of highly automated agricultural machines — Principles for design. 18.

[6] IEC TS 62998-1:2019 Safety of machinery - Safety-related sensors used for the protection of persons

[7] IEC TR 62998-2:2020 Safety of machinery - Part 2: Examples of application

[8] ISO TR 22053:2021 Safety of machinery. Safeguarding supportive system. 10 p.

[9] Taeihagh, A & Lim, H. S. M,. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks, Transport Reviews, 2019. 39:1, 103-128, DOI: 10.1080/01441647.2018.1494640.

[10] Wikipedia a. List of self-driving car fatalities. Retrieved 16.9.2020. https://en.wikipedia.org/wiki/List_of_self-driving_car_fatalities.

[11] ISO 12100:2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. 77.