VTT Technical Research Centre of Finland

An overview of current safety requirements for autonomous machines-review of standards

Tiusanen, Risto; Malm, Timo; Ronkainen, Ari

Published in:
Open Engineering

DOI:
10.1515/eng-2020-0074

Published: 01/01/2020

Document Version
Publisher's final version

Research Article

Risto Tiusanen*, Timo Malm, and Ari Ronkainen

An overview of current safety requirements for autonomous machines – review of standards

https://doi.org/10.1515/eng-2020-0074
Received Nov 01, 2019; accepted Apr 19, 2020

Abstract: The development of automated work machine systems towards autonomous operation is proceeding rapidly in different industrial sectors. The aim of the study was to explore the current situation and possible differences in standardization supporting the development in different industrial sectors. The existing ISO and IEC standards and work items related to autonomous machinery were reviewed as well as activities in international industry groups regarding automation and autonomy of machinery.

In general, the current standards are made mostly for machine manufacturers, but the views or responsibilities at worksite level are not considered. Three different approaches for safety concepts for different operating conditions were identified. One of them relies on onboard safety systems including sensor and perception systems for indoor applications. One guides to separate and isolate the autonomously operating machinery and to use access control to the autonomous operating zone. The third one is relying mainly on the machine operator's ability to understand the situation and to react correctly according to the available information.

From technology point of view there seems to be a gap between the safety requirements set in standards and the state of the art in currently available technology.

Keywords: autonomous work machine, standard, safety concept, safety requirement

1 Introduction

Automatic work machine systems are used widely in different industrial sectors. So far, automated machines have been operating in closed areas outdoors (*e.g.* in ports and in mines). On the other hand, automated

forklift trucks and AGV systems have long been used inside factories and warehouses.

The first international safety standards have recently been published for automated work machine systems. The ISO 17757 standard [1] defines requirements for autonomous or semiautonomous earth moving machinery and mining machinery systems. The key point in this standard is that the requirements are defined from a system-level perspective. The ISO 18497 standard [2] for highly automated agricultural machines defines requirements for automation systems applied in agricultural machinery and tractors. The safety standard for driverless industrial trucks, ISO 3691-4 [3], in turn, defines the requirements for unmanned forklifts, AGVs and associated systems.

VTT Technical Research Centre of Finland Ltd (VTT) and Natural Resources Institute Finland (Luke) conducted the study on safety requirements for autonomous machinery in 2018 assigned by FIMA ry (Forum for Intelligent Machines ry). The purpose of the study was to obtain an overview of safety requirements for commercial non-road vehicles in different industries. The aim of the work was to explore the current situation in different industrial sectors and to study what they have in common and where there are differences.

2 Terms automated and autonomous

When discussing about autonomous machinery the term autonomous should be defined to share the common understanding what it really means in this context. The term Automated that is widely used has been defined so that when an automated equipment or automated system is automated it is made to operate by machines or computers in order to reduce the work done by humans [4].

For road vehicles an autonomous mode has been defined to be 'the status of vehicle operation where technology that is a combination of hardware and software, remote and/or on-board, performs the dynamic driving

***Corresponding Author: Risto Tiusanen:** VTT Technical research centre of Finland Ltd Tampere, Finland; Email: risto.tiusanen@vtt.fi
Timo Malm: VTT Technical research centre of Finland Ltd Tampere, Finland
Ari Ronkainen: Natural Resources Institute Finland (Luke), Finland

task, with or without a natural person actively supervising the autonomous technology's performance of the dynamic driving task' [5]. An autonomous road vehicle 'is operating or driving in autonomous mode when it is operated or driven with the autonomous technology engaged' [5].

In the mobile work-machine sector, ISO 17757 defines terms autonomous operation and autonomous machine as follows [1]:

Autonomous operation is 'the mode of operation in which a mobile machine performs all machine safety-critical and earth-moving or mining functions related to its defined operations without operator interaction. The operator could provide destination or navigation input, but is not needed to assert control during the defined operation.'

Autonomous machine is 'a mobile machine that is intended to operate in autonomous mode during its normal operating cycle'.

In practice, the terminology is still very varied. Terms 'Driverless', 'Unmanned', 'Highly Automated', etc. are used in articles and in standards.

In this paper, the following abbreviations are used:

- AI = Artificial Intelligence
- AWI = Approved work item
- AGV = Automated Guided Vehicles
- DIS = Draft International Standard
- FDIS = Final Draft International Standard
- IEC = International Electrotechnical Commission
- ISO = International Organization for Standardization
- JWG = A joint subcommittee of the various technical committees
- PAS = Publicly available specification
- PL = Performance Level
- SC = Subcommittee
- TC = Technical Committee
- TS = Technical Specification
- WG = Working group

3 Methods and material

The latest information on safety requirements for the autonomous working machine systems were collected from ISO, IEC and other standards and technical reports from different industrial sectors. The following application areas for machinery were studied: mobile mining machinery, mobile harbor machinery, earthmoving machinery, agricultural machinery, forestry machinery, construction machinery, industrial cranes, industrial trucks and AGVs, and industrial robots.

The work items of the following ISO technical committees (TC) were surveyed:

- TC 127 Earth-moving machinery
- TC 110 Industrial trucks
- TC 82 Mining
- TC 23 Tractors and machinery for agriculture and forestry
- TC 22 Road vehicles
- TC 96 Cranes
- TC 299 Robotics

In addition to that, the work items in two IEC technical committees (TC) were surveyed: TC 44 Safety of machinery – Electro technical aspects, and TC 9 – Electrical equipment and systems for railways.

In the study, two joint workshops with expert from FIMA ry member companies were organized to collect information and experiences from industrial experts involved in the work of the technical committees and to analyze the review results.

From the system development perspective current guidelines for the safety engineering and risk assessment approaches for autonomous machinery were reviewed. An important reference in this regard was ISO 17757 [1], which defines the requirements and principles for the risk assessment process for autonomous earth moving machines and mining machinery systems.

Another important reference was ISO 18497 [2] standard, which defines requirements for automation applied in agricultural machinery and tractors. The third reference in this regard is the standard ISO 3691-4 [3], which defines the requirements for unmanned forklifts, AGVs and associated systems.

Safety requirements set for autonomous transportation and autonomous cars (robot cars) that may be applicable to non-road vehicles (*e.g.* requirements related to automatic driving, automatic navigation, braking, and collision avoidance) were also studied. For road vehicles the IEC 61508's [6] application standard family ISO 26262 [7] is an important reference and guideline.

4 ISO and IEC standards related to autonomous machinery

The following chapters introduce the relevant ISO and IEC standards under study presented by the technical committees in which they have been prepared and published.

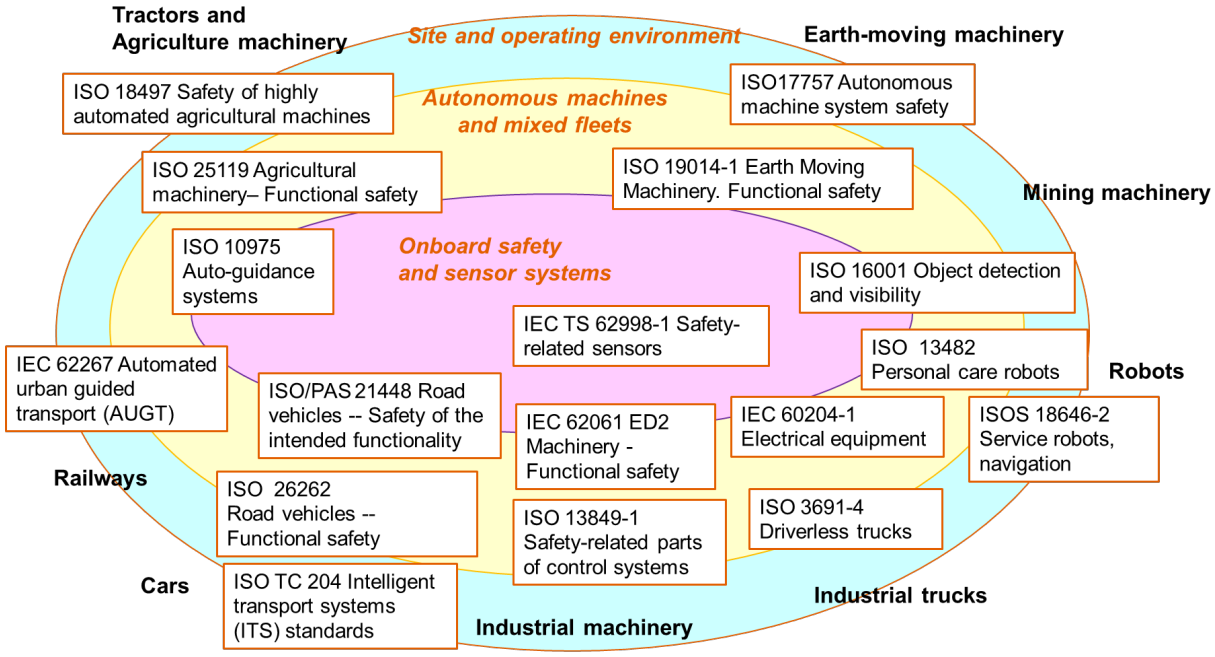

Figure 1: An overview of the current situation in standardization on autonomous machinery.

As a summary an overall picture and status of the most interesting ISO and IEC standards on the context of autonomous machinery is given in Figure 1.

4.1 ISO TC 127 Earth-moving machinery

The scope of ISO TC 127 is standardization of nomenclature, use classification, ratings, technical requirements and test methods, safety requirements, operation, maintenance manual format for earth-moving and related machinery. TC 127 has four subcommittees (SC). SC 1 "Test methods relating to safety and machine performance" has prepared and published the standard ISO 16001 Earth-moving machinery – Object detection systems and visibility aids – Performance requirements and tests [8].

The ISO 16001 specifies general requirements and describes methods for evaluating and testing the performance of object detection systems (ODSs) and visibility aids (VAs) used on earth-moving machines. It covers the following aspects:

- detection or visibility or both of objects including people in the detection zone;
- visual, audible, or both warnings to the operator and if appropriate to the persons in the detection zone;
- operational reliability of the system;
- compatibility and environmental specifications of the system.

Subcommittee SC 2 "Safety, ergonomics and general requirements" has published the standard ISO 19014-1 Earth-moving machinery – Functional safety – Part 1: Methodology to determine safety-related parts of the control system and performance requirements [9]. It replaces ISO 15998:2008 and ISO/TS 15998-2:2012.

Under SC2, the WG 22, which is a joint working group between ISO/TC 127/SC 2 and ISO/TC 82 "Autonomous machine safety", published the first ISO standard on safety of autonomous machinery in 2017. The ISO 17757 Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety [1] provides safety requirements for autonomous machines and semi-autonomous machines used in earth-moving and mining operations, and their autonomous or semi-autonomous machine systems (ASAMS).

Integration of ASAMS into the site planning process is important. ASAMS are complex systems, because of the complexity of the logistic processes themselves, their relation to people, manned operations and the layers of safety that need to be built into them. Supporting infrastructure and operating area requirements should be identified early in the project, as automation systems can have specific needs (*e.g.* fueling facilities, control rooms, communications network). The standard introduces the concept of an autonomous operating zone (AOZ), controlled by the access control system, were monitored manned machines

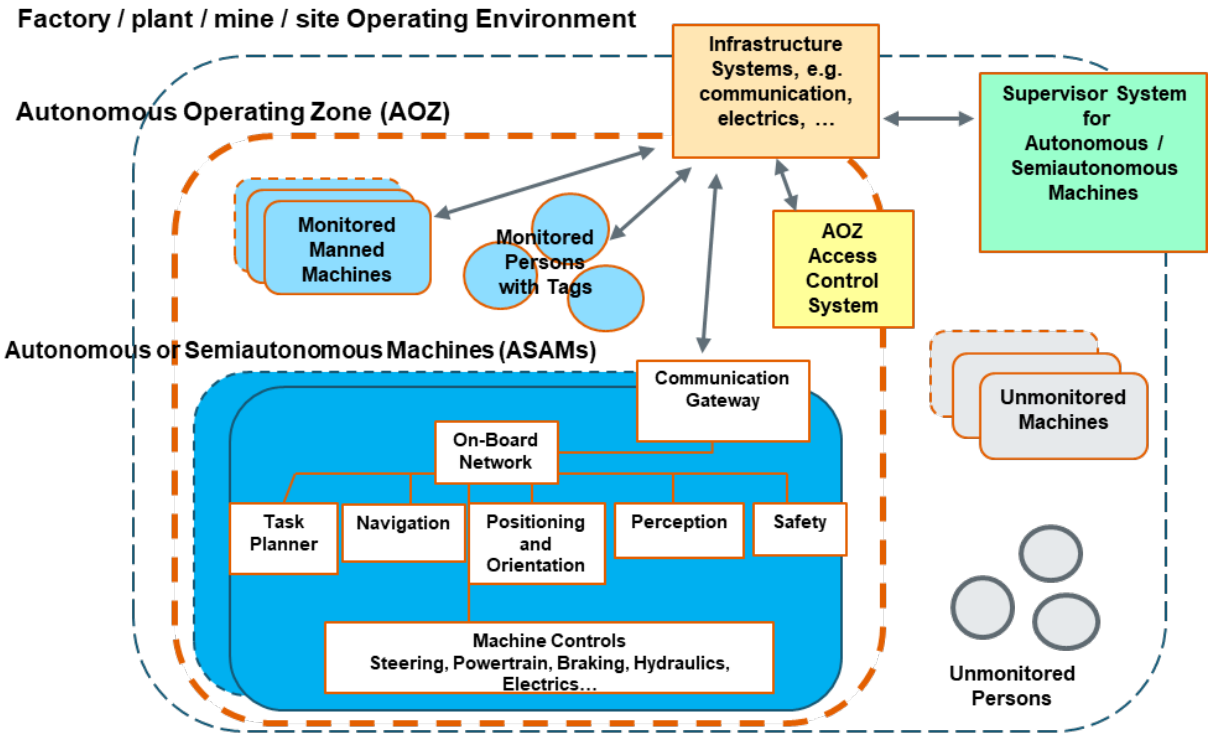

Figure 2: An illustration of the difference between the monitored and un-monitored persons and machinery in relation with the AOZ according to the ASAMS model shown in ISO 17757 [1].

and monitored persons could work at the same time with autonomous machines (Figure 2).

ISO 17757 specifies safety criteria for both the machines and their associated systems and infrastructure, including hardware and software, and provides guidance on safe use in their defined functional environments during the machine and system life cycle.

The standard's risk assessment approach moves towards system safety concepts from individual machinery safety concepts. It gives guidelines how the safety risks should be assessed and how the system safety requirements should be defined in autonomous machinery systems. The approach emphasizes the risks related to the actual operating concepts and actual operating environment at the site and the uncertainties related to the safety related functions and technologies.

4.2 ISO TC 110 Industrial trucks

The scope of ISO TC 110 is standardization in the field of power-operated industrial trucks, hand-operated industrial trucks (including sack trucks, handcarts, and trailers), all types of wheels and castors excluding those with pneumatic tyres and rubber solid tyres for pneumatic tyre rims. TC 110 has five subcommittees. SC 2 "Safety of powered industrial trucks" has recently published ISO 3691-4 Industrial trucks – Safety requirements and verification – Part 4: Driverless industrial trucks and their systems [3].

In the standard driverless truck system is defined to be a combination of one (or more) driverless truck(s) and ancillary components to control and manage the automatic operation of the truck(s). The standard defines "Automatic mode" as an operating mode where no operator intervention is required for operation.

The standard is not limited to indoors applications, but the requirements reflect the history of indoors applications. The standard scope may change or the requirements may become more generic to fit outdoors use.

The standard defines three access zones, which have different requirements. The same system may have all three different zones, depending on the case.

The **operating hazard zone** is a space of the operating zone in which a person can be exposed to a hazard. In this operating hazard zone, the truck speed shall be below 0,3 m/s (no PL d detection) or 0,7-1,2 m/s (clearance and conditions) and shall emit additional audible or visual warnings.

In the **restricted zone** truck speed is limited to 0,3 m/s without personnel detection means in travel direction; or

limited to 1,2 m/s with personnel detection means in travel direction. It is a physically separated space in which only authorized persons are permitted to enter.

The **confined zone** is an enclosed space where only authorized personnel have access after stopping movements of trucks.

The standard describes also required performance levels for safety functions at the normative part of the proposal. Table 1 shows some examples of the required performance levels (PL). According to ISO 13849-1 [10] a performance level (PL) is a discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

In ISO 13849-1, the performance levels are defined in terms of probability of dangerous failure per hour. Five performance levels are set out, from the lowest PL a to the highest PL e with defined ranges of probability of a dangerous failure per hour [10].

Table 1: Summary of safety functions and their minimum performance levels according to ISO 13849-1 [10].

Function/system	PL
Braking system control	d
Parkin braking system control	c
Overspeed detection	c
Personnel detection system for speed	d
Deactivation of charging systems	b
Control of speed, steering and load handling for stability	c
Warning systems	-
Emergency stop (traction + brake)	c
Person detection system - stop	d

The characteristics of the performance levels b, c and d are described in details in ISO 13849-1 [10].

4.3 ISO TC 82 Mining

The scope of ISO TC 82 is standardization of specifications relating to specialized mining machinery and equipment. ISO TC 82 has recently published ISO 18758-2 Mining and earth-moving machinery – Rock drill rigs and rock reinforcement rigs – Part 2: Safety requirements [11]. It does not give requirements regarding autonomous operation, but in matters relating to autonomy it refers to ISO 17757 [1]. ISO TC 82 Mining has several working groups. But only two subcommittees. JWG 1, the Joint working group between ISO/TC 82 and ISO/TC 127 is working on "Rock drill rigs".

SC 8 is working on "Advanced automated mining systems". Its scope is interesting and matches with the focus of this review: "Standardization in the field of advanced automated and autonomous processes, technologies, equipment, and systems in the mining sector, including both surface and underground mining". The work program of the SC 8 is still open. Its first meeting was in September 2018. From the machine manufacturer's point of view there is a clear need to connect automated and manual machines to the same operating environment. The difficult question is what is the acceptable risk level - the current level of manual operations or zero tolerance?

4.4 ISO TC 23 Tractors and machinery for agriculture and forestry

The scope of ISO TC 23 is on standardization of tractors, machines, systems, implements and their equipment used in agriculture and forestry as well as gardening, landscaping, irrigation and other related areas in which such equipment is used, including electronic / electrical aspects and electronic identification as well as electronic identification of all categories of animals. TC 23 has 11 subcommittees and 5 working groups.

Already over ten years ago TC 23 published the standard ISO 10975 Tractors and machinery for agriculture – Auto-guidance systems for operator-controlled tractors and self-propelled machines – Safety requirements [12]. The standard sets safety requirements for auto-guide systems. Auto-guide systems are systems, which handle the steering of an agricultural tractor, under operator's supervision. The systems can be retrofit systems fitted to steering wheel or built in systems in tractors. They follow and repeat a predefined route.

The standard defines what the system is to do when it encounters faults, loses GPS signal or the controls are manipulated. The standard does not set defined functional safety requirements, but these are to be determined through risk analysis. Common implementations are category 2 designs, according to ISO 13849 [10], and in case of built-in systems usually 1-out-of-2 systems.

The main take away from this standard is the concept, which is quite straightforward. Whenever a fault or user input above a predetermined level is detected, the automatic operation is stopped and the control is transferred back to the operator with sufficient audible and visual warnings.

In 2018 TC 23 published the functional safety standard ISO 25119 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems (parts 1-4) [13]. It is a functional safety standard for machinery and

tractors in agriculture. It alone does not provide new requirements for implementing autonomous machinery. In 2018, TC 23 published also ISO 18497 Agricultural machinery and tractors – Safety of highly automated agricultural machines – Principles for design [2]. The standard specifies requirements for starting the machine, machine movements and tool movements of a highly automated agricultural machine (HAAM). It also specifies a test method for human detection system. A stop function or transferring the control to the operator is required if an error in the perception function is detected. It introduces an Idea of a protective zone around the machine. The zone could be dynamic, relying to the perception system, though it is not yet know how it could be implemented.

The Agricultural Electronics Industry Foundation (AEF) is currently working on Tractor Implement Management (TIM). The TIM is intended to allow agricultural implements to utilize a tractor as a part of their automation control. TIM would allow the agricultural implement to steer the tractor, however, current state-of-the-art requires, that the driver is present.

4.5 ISO TC 22 Road vehicles

The scope of TC 22 is covering all questions of standardization concerning compatibility, interchangeability and safety. TC 22 has 11 subcommittees and 2 advisory groups.

SC 32 is working on "Electrical and electronic components and general system aspects". Functional safety features form an integral part of each automotive product development phase, ranging from the specification, to design, implementation, integration, verification, validation, and production release. In 2018 SC 32 revised the one of the most essential functional safety standard series at the moment ISO 26262 Road vehicles – Functional safety, Parts 1 – 120 [7], which is referenced wide in many other machinery sectors too. The standard is intended to be applied to series production road vehicles.

Last year SC 32 published an interesting document ISO/PAS 21448 Road vehicle – Safety of the intended functionality [14], which gives guidelines for the reliability evaluation of complex, and possibly Artificial Intelligent (AI) based functionalities in road vehicles. It is meant to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms.

The standard extends the conventional functional safety engineering process. It aims to reduce the number of known unsafe and unknown unsafe scenarios, by identifying triggering events and analyzing scenarios and system architecture and properties. Verification and validation of a system according to ISO/PAS 21448 [14] requires a lot of analysis to define a complete verification and validation strategy. The validation is based on evaluation of residual risk, acceptability criteria and in many cases real life testing period. The validation criteria is often based on GAME/GAMAB "Globally at least as good" principle or ALARP "As low as reasonably practicable" principle. The specification is not easy to apply and requires a lot of analysis and testing to gain knowledge needed for validation.

SC 33, which is working on vehicle dynamics and chassis components, has two working groups that have links to autonomous operation. WG 3 works on driver assistance and active safety functions and WG 9 works on test scenario of autonomous driving vehicle.

The advisory group AG 1 "Automated driving ad hoc group" (ADAG) prepares requirements for automated driving.

4.6 IEC TC 44 Safety of machinery – Electrotechnical aspects

The scope of IEC TC 44 is standardization in the field of the application of electro-technical equipment and systems to machinery (including a group of machines working together in a coordinated manner, excluding higher-level systems aspects) not portable by hand while working, but which may include mobile equipment. The equipment covered commences at the point of connection of the electrical supply to the machinery.

Standardization of interfaces (excluding local area networks and fieldbus) between control equipment and the electro-technical equipment of machinery. Standardization of electrotechnical equipment and systems relating to the safeguarding of persons from hazards of the machinery, its associated equipment and the environment. TC 44 also coordinates with ISO all matters concerning the safety of machinery.

In 2016, TC 44 published the sixth version of the IEC 60204-1 [15], which gives the general requirements for all electrical equipment of machinery.

In 2019, TC 44 published IEC TS 62998-1Safety of machinery – Safety-related sensors used for the protection of persons [16]. The revision of IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems [17], is expected to be published 2021. The idea of combining IEC 62061 [17] and ISO 13849-1 [10] has been rejected.

4.7 IEC TC 9 – Electrical equipment and systems for railways

The scope of TC 9 is standardization for the railways field, which includes rolling stock, fixed installations, management systems (including communication, signaling and processing systems) for railway operation, their interfaces and their ecological environment. The standards cover railway networks, metropolitan transport networks (including metros, tramways, trolleybuses and fully automated transport systems) and magnetic levitated transport systems.

The standards relate to systems, components, software, and they will deal with electrical, electronic and mechanical aspects, the latter being limited to items depending on electrical factors. The standards also deal with electromechanical and electronic aspects of power components as well as with electronic hardware and software components.

TC 9 has published already over ten years ago an interesting standard IEC 62267 Railway applications. Automated urban guided transport (AUGT). Safety requirements [18]. Also the technical report IEC TR 62267-2 is relevant to autonomous machinery [19].

IEC 62267 covers high-level safety requirements applicable to automated urban guided transport systems, with driverless or unattended self-propelled trains, operating on an exclusive guideway. Deals with the safety requirements needed to compensate for the absence of a driver or attendant staff who would otherwise be responsible for some or all of train operation functions, depending on the level of automation of the system.

The "guided transport" term means public passenger transport systems whereby the vehicles follow a determined trajectory for all or part of their journey. These usually are, subways, trams, railways providing a regular service or tourist journeys, and intermediate systems such as buses or trolley buses guided by rail or any other non-physical system (optical or magnetic guidance). Urban guided transports usually exclude operations on national rail networks. The standard identifies the relevant stakeholders and assigns each their roles in the system.

The safety is mainly managed through controlling access to guideway and monitoring the guideway. This is done by isolating the guideway and monitoring the access to guideway. For railway stations there are requirements for systems in station platforms and for controlling people flow. There are also requirements for monitoring the operation of an AUGT and for operational rules for the transport system including rescue and maintenance operations.

IEC 62267 standard was supplemented in 2011 with IEC TR 62267-2 Railway applications - Automated urban guided transport (AUGT) – Safety requirements – Part 2: Hazard analysis at top system level [19]. The report provides a non-normative generic hazard analysis at top system level conducted for the development of IEC 62267 for Automated Urban Guided Transport (AUGT) systems. This report is applicable to all systems covered by the scope of IEC 62267. This generic hazard analysis can be used for specific AUGT systems to support the necessary activities in lifecycle process following IEC 62278 [20].

IEC 62278 Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS) provides Railway Authorities and railway support industry with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS [20].

Processes for the specification and demonstration of RAMS requirements are the cornerstones of this standard. It aims to promote a common understanding and approach to the management of RAMS. The approach could be applied systematically throughout all phases of the life cycle of a complex machinery application too to develop case specific RAMS requirements and to achieve compliance with these requirements. The systems-level approach defined by this standard facilitates assessment of the RAMS interactions between elements of complex machinery applications.

The standard has been supplemented by several reports. The latest is IEC TR 62278-4 Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 4: RAM risk and RAM life cycle aspects [21].

4.8 ISO TC 299 Robotics

The scope of TC 299 is standardization in the field of robotics, excluding toys and military applications. TC 299 has six working groups and three other advisory or study groups. TC 299 has published a standard ISO 13482:2014 "Robots and robotic devices – Safety requirements for personal care robots" [22] on safety requirements for personal care robots.

It specifies requirements and guidelines for the inherently safe design, protective measures, and information for use of personal care robots, in particular the following three types of personal care robots: mobile servant robot, physical assistant robot and person carrier robot.

The standard describes different areas where robot can be applied: maximum space, restricted space, monitored space, safeguarded space and protective stop space. There are different requirements for each kind of space.

Last year TC 299 published the ISO 18646-2 Robotics – Performance criteria and related test methods for service robots – Part 2: Navigation [23] that sets requirements for navigation of service robots. Other existing standards related to robots and robotic devices that might be interesting are ISO 10218-1 [24], ISO 10218-2 [25] and ISO 19649 [26].

4.9 ISO TC 204 Intelligent transport systems (ITS)

The scope of TC 204 is standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveler information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field.

TC 204 is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work program in this field including the schedule for standards development, taking into account the work of existing international standardization bodies.

TC 204 has 255 published standards and has 84 standards under development in several topics related to intelligent transport systems.

5 Discussion

Many of the standards related to safety requirements for autonomous machine systems are published quite recently and there is not yet much experience with their application. The standards are expected to become more precise as more is learned about the performance of the autonomous systems.

Two main problems in the standardization of safety requirements for autonomous machinery were identified during the survey and workshops. Firstly, there is a gap between the requirements set in standards and the state of the art in technology. As standards expect full compliance, there is no gradual path to develop the system. A fully functioning system is what standards expect and there is no room for trying and learning. There are problems fitting the existing designs to meet the requirements in standards. Secondly, the safety standards are mainly for machine manufacturers. The worksite operators or owners need to be involved in the process of creating an autonomous system and its operating environment. The work process and the worksite should guide the design and implementation of autonomous machinery systems.

5.1 Safety concepts

The systems engineering approach presented in ISO 17757 [1] can be considered to be a good guideline to handle the management of fully autonomous or mixed fleet operation and earth moving machinery. The standard is already widely referenced.

Three approaches for the development of safety concepts for autonomous machinery were identified in the current standardization.

The first approach aims to concepts, where machine carries a sensor system and safety system is contained within a machine. This allows non-separated working areas for humans, machines and autonomous machines to operate in the same area. These concepts are restricted to indoor applications as the sensor systems needed are only fit for indoor use.

The second approach aims to separate and isolate the autonomously operating machinery and control the access to working area and monitor other vehicles or persons in the autonomous operating area. This approach is for machines working in intensive outdoor environment.

The third approach aims to rely on monitoring by the operator. Here the concepts might include some sensing solutions to detect hazardous situations. When a problematic situation is detected, the operation could be stopped and the control is transferred to local or remote operator. The approach relies heavily on the operator's ability to understand the situation and to react correctly. The approach is suitable to working environments where there is low activity and low likelihood of hazardous situation and where there is enough time to alert the operator and transfer responsibility.

5.2 Performance requirements for perception systems

A major challenge in the development of autonomous mobile machinery is and has been the requirements for sensor systems for detecting humans.

As the major risks associated with autonomous mobile work machinery are associated with collision between a

machine and a human, because of machine, tool or payload movement, it is therefore necessary to identify humans. The currently available sensors have the problem that as they fail they will not detect a human. The failure is in most cases caused by various environmental reasons. In addition, sensors have some limits beyond of which they are unable to operate. Unfortunately, these limits are not often clear, but the sensor's capability deteriorates gradually as conditions get worse.

As the mobile work machinery is heavy, collisions with the machinery pose the risk of serious injury and death, which leads to requirements for PL d (ref. to ISO 13849) for safety related parts of the control system. The target PL is d, but the conditions are not defined for outdoor use. The varying conditions in outdoor are the main source of failures in sensors. Currently there are no standard definitions for the outdoor conditions. The performance requirements for sensors may include operation in a fog, but without a definition what kind of fog. Fog density and droplet size are important parameters as well as ambient lighting conditions in a foggy environment.

Sensor fusion seems to be a good way to approach in difficult environments, since different sensors have different advantages and the sensors can compensate the weaknesses of other sensors.

Moving to a safe state in autonomous road vehicles means something different from non-road vehicles. Vehicles on the road should maintain their controllability for as long as possible to allow them to move from the traffic to the side of the road. They cannot be stopped in a fault situation such as mobile work machines at a work site can do.

Acknowledgement: VTT and Luke are grateful to all the companies and experts involved in this study of current standardization activities on safety requirements for autonomous machinery. The study was financed by FIMA ry.

References

[1] ISO 17757:2019 Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety
[2] ISO 18497:2018 Agricultural machinery and tractors — Safety of highly automated agricultural machines — Principles for design
[3] ISO 3691-4:2020 Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems
[4] https://dictionary.cambridge.org/dictionary/english/ [cited 29.4.2020]
[5] https://definedterm.com/a/document/10823 [cited 29.4.2020]
[6] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems- Parts 1 – 7.
[7] ISO 26262-1:2011 Road vehicles – Functional safety – Parts 1 - 10
[8] ISO 16001:2017 Earth-moving machinery – Object detection systems and visibility aids – Performance requirements and tests
[9] ISO 19014-1:2018 Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements
[10] ISO 13849-1:2015 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design.
[11] ISO 18758-2:2018 Mining and earth-moving machinery — Rock drill rigs and rock reinforcement rigs — Part 2: Safety requirements.
[12] ISO 10975:2009 Tractors and machinery for agriculture — Autoguidance systems for operator-controlled tractors and self-propelled machines — Safety requirements.
[13] ISO 25119:2018 (parts 1-4) Tractors and machinery for agriculture and forestry – Safety-related parts of control systems.
[14] ISO/PAS 21448:2019 Road vehicles — Safety of the intended functionality
[15] IEC 60204-1:2016 Safety of machinery - Electrical equipment of machines - Part 1: General requirements
[16] IEC TS 62998-1:2019 Safety of machinery - Safety-related sensors used for the protection of persons
[17] IEC 62061:2015 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
[18] IEC 62267:2009 Railway applications. Automated urban guided transport (AUGT). Safety requirements
[19] IEC TR 62267-2:2011 Railway applications - Automated urban guided transport (AUGT) - Safety requirements - Part 2: Hazard analysis at top system level
[20] IEC 62278:2002 Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
[21] IEC TR 62278-4:2016 Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 4: RAM risk and RAM life cycle aspects
[22] ISO 13482:2014 "Robots and robotic devices – Safety requirements for personal care robots"
[23] ISO 18646-2:2019 "Robotics – Performance criteria and related test methods for service robots – Part 2: Navigation"
[24] ISO 10218-1:2011 Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots
[25] ISO 10218-2:2011 Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration
[26] ISO 19649:2017 Mobile robots – Vocabulary