INTERNATIONAL STANDARD

ISO 18497

First edition
2018-11

Agricultural machinery and tractors — Safety of highly automated agricultural machines — Principles for design

Tracteurs et matériels agricoles — Sécurité des machines hautement automatisées — Principes de conception

Reference number
ISO 18497:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 3, *Safety and comfort*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is a type-B1 standard as stated in ISO 12100.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organisations, market surveillance, etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions, organizations for people with special needs);

— service providers, e.g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

The structure of safety standards in the field of machinery is as follows.

— Type-A standards (basis standards) give basic concepts, principles for design, and general aspects that can be applied to machinery.

— Type-B standards (generic safety standards) deal with one or more safety aspects or one or more types of safeguards that can be used across a wide range of machinery:

  — Type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

  — Type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).

— Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

Highly automated agricultural machine operations are an enabling technology. Customer benefits are increased; productivity and increased operator comfort.

Highly automated operation is a departure from traditional machine applications in the agricultural machinery and mobile equipment sectors that up to now required an on-board operator to perform work. Highly automated operations require unique safety considerations.

The objective of this document is to specify principles for the design of highly automated agricultural machine operations to achieve safe operation. Should requirements of this document for highly automated operation be different from those which are stated in a machine-specific standard dealing with highly automated operation, the requirements of the machine-specific standard take precedence over the requirements of this document.

Agricultural machinery and tractors — Safety of highly automated agricultural machines — Principles for design

1 Scope

This document specifies principles for the design of highly automated aspects of highly automated machines and vehicles (e.g. agricultural tractors, tractor implement systems, implements and self-propelled machinery) during agricultural field operations. In addition, it provides guidance on the type of information on safe working practices (including information about residual risks) to be provided by the manufacturer.

The purpose of this document is to assist in the provision of safety requirements, means of verification and information for use to ensure an appropriate level of safety for agricultural and forestry tractors and self-propelled machines with functions allowing highly automated operations (see 3.7).

This document deals with all the significant hazards, hazardous situations and events (as listed in Annex A), relevant to agricultural and forestry tractors and self-propelled machines allowing highly automated field operations when used as intended and under the conditions of misuse foreseeable by the manufacturer during normal operation and service.

NOTE 1 While this document gives principles for the design, verification, validation and provision of information for use of a highly automated agricultural machine (HAAM), the detailed specification of requirements for a specific application will be dependent on the machine and its operating conditions. Therefore, the principles for design given in this document need to be extended for specific HAAM by the use of relevant specific (type-C) standards, when available, or by the manufacturer of the machine using risk assessment. Such additional specification of requirements, for design, verification, validation or information for use are outside the scope of this document.

NOTE 2 Safety requirements for specific machines not related to their highly automated operations can be available in machine-specific type-C standards.

This document is not applicable to:

- forestry applications;
- mobile, semi-mobile or stationary machinery used for farm yard or barn operations;
- operations on public roads including relevant requirements for braking and steering systems.

NOTE 3 With respect to implements (e.g. their specific design, functions) and the communication between tractors and implements, additional risks can be relevant and can require additional measures. Such additional measures are outside the scope of this document and are the responsibility of the manufacturer.

This document is not applicable to agricultural and forestry tractors, tractor implement systems, implements and self-propelled machines which are manufactured before the date of its publication.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3767-1, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Symbols for operator controls and other displays — Part 1: Common symbols*

ISO 3767-2, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Symbols for operator controls and other displays — Part 2: Symbols for agricultural tractors and machinery*

ISO 4254-1, *Agricultural machinery — Safety — Part 1: General requirements*

ISO 7731:2003, *Ergonomics — Danger signals for public and work areas — Auditory danger signals*

ISO 12100, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2015, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

ISO 25119 (all parts), *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems*

ISO 26322-1, *Tractors for agriculture and forestry — Safety — Part 1: Standard tractors*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 4254-1, ISO 12100 and ISO 26322-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
audible alarm
signal that is intended to be detected by the human sense of hearing

3.2
communication
information or data transmitted by a data network

3.3
disabled state
machine state in which *highly automated operation* (3.8) is not allowed

3.4
enabled state
machine state in which *highly automated operation* (3.8) is allowed

3.5
guarding system
system that reacts to information received from the *perception system* (3.14) to avoid contact

3.6
hazard zone
area which is a subset of the *warning zone* (3.19) and where if an *obstacle* (3.12) is within that area, then the potential for injury can exist due to movement of the machine or implement

3.7
highly automated agricultural machine
HAAM
mobile vehicle or machine with or without on-board operator allowing *highly automated operation* (3.8)

3.8
highly automated operation
function that is controlled by a control system without direct human input from local or *remote operator* (3.15), does not require an on-board operator for primary control, does or does not include an on-board operator station, and is subject to a *supervisory system* (3.17)

3.9
impaired state
point of degradation where *highly automated operation* (3.8) can no longer be completed safely in the current conditions

3.10
local operator
human in primary control of a machine through the on-board operator controls or through *pendant control* (3.13)

3.11
machine motion control
control of the unshielded highly automated machine components

EXAMPLE Working tools.

3.12
obstacle
object or ground condition which can cause harm, or is harmed, if it comes into contact or collision with the highly automated machinery

3.13
pendant control
wireless or wired hand-held control unit with interfaces to the control system and with only local operation allowed

3.14
perception system
system that gathers and processes information about the environment in which the machine is operating

3.15
remote operator
human who is

— in primary control of a machine through the *supervisory system* (3.17),

— receiving data for the purpose of supervising machine activity, and

— is not on the machine but is located in the field, close to the field, or away from the field

3.16
safe state
operating state of a system with acceptable level of risk for operator or bystander even when the control system fails or partly fails

[SOURCE: ISO 11783-14:2013, 3.10, modified — in the definition, "operating mode" has been changed to "operating state".]

3.17
supervisory system
means to inform the operator responsible for the *highly automated operation* (3.8) about the machine and its operational status

3.18
visual alarm
signal that is intended to be detected by the human sense for sight

3.19
warning zone
area where if an *obstacle* (3.12) is within and no action is taken, then the obstacle might enter the *hazard zone* (3.6)

3.20
wheel motion control
control of the highly automated machine moving with a direction and speed across the ground

4 Safety requirements and protective or risk reduction measures

4.1 General

The highly automated agricultural machine (HAAM) shall comply with the relevant portions of machine-specific safety standards [e.g. ISO 4254 (all relevant parts), ISO 26322 (all relevant parts)] and the safety requirements and protective or risk reduction measures of 4.2 to 4.13. In addition, the HAAM shall be designed according to the principles of ISO 12100 for relevant but not significant hazards which are not dealt with by this document.

Requirements based on the principles for design given in this document may be dependent on the type of machine and the necessary operating conditions. When this applies, the specification of requirements and corresponding verification procedures shall be determined using risk assessment. Machine specific type-C standards, when available, can give machine specific requirements.

NOTE The application of the risk assessment by the manufacturer is relevant for the application of this document in general to develop the given design principles into detailed machine specific requirements. Specific examples are 4.4.2.2.1 (pre-start and total warning time), 4.4.2.6 (safe state), 4.4.2.8 (safe state and duration of loss of communication), 4.4.3.2.1 (pre-start and warning time), 4.4.3.3.1 (pre-start and warning time), 4.4.3.6 (safe state), 4.4.3.9 (time delay and safe state), 4.6, 4.7 and 4.11.3.2 (safe state and enabling subsequent highly automated operation), 4.10 (time delay between loss of communication and safe state), 4.12 (safe state).

4.2 Principles for protection

For ensuring an appropriate level of safety:

- the HAAM shall be provided with a perception system capable of detecting and locating persons or other obstacles relative to the machine;
- the HAAM shall be provided with a perception system capable of locating and positioning the HAAM as required for the operations involved while preventing unintended excursions beyond the boundary of the working area;
- before each movement of the HAAM, it shall be ensured, by the safeguarding system, that there is no obstacle in the hazard zone;
- while performing highly automated operations, the HAAM shall, when an obstacle is detected in or enters the hazard zone, give an audible or visual alarm and enter its defined safe state;
- the HAAM shall be provided with the means to enable a local or remote operator to stop or start highly automated operation;
- the HAAM shall allow adequate supervision by a local or remote operator.

4.3 Machine enabling operations

4.3.1 General requirements

The HAAM shall be equipped with a means to enable and disable highly automated operations. The means provided shall be:

- easily identifiable;
- readily accessible by the operator;
- installed on the HAAM or in the cab (if provided) or at the operator station (if provided) or available to the remote operator;
- protected against unintentional actuation.

4.3.2 Labelling and identification

Symbols shall comply with ISO 3767-1 and ISO 3767-2. The HAAM state indicators shall be unambiguous and easily identifiable.

4.3.3 Functional requirements

Available control states shall include highly automated system disabled and highly automated system enabled.

In the disabled state, all highly automated machine operations shall be stopped and disabled. In the enabled state, highly automated operations shall be permitted.

Only the local operator shall be able to enable the highly automated machine.

It shall always be possible to disable the highly automated operation either at the local operator position and, for remote supervision, at the remote operating position.

4.4 Operational procedures

4.4.1 General requirements

It shall not be possible to initiate highly automated operation without the perception system confirming that the hazard zone is obstacle-free. In addition, initiating highly automated operation shall require confirmation by a local operator unless it can be shown by risk assessment that no significant hazards will arise.

When a highly automated operation is stopped (whatever the reason), the procedure for restarting the highly automated operation shall require initiation by the operator.

4.4.2 Automated engine control

4.4.2.1 General

Automated engine control shall only be allowed when highly automated operations are enabled.

Engine start requirements also apply to the engagement of the machine's power source (for example, main contact closing on a battery powered system).

4.4.2.2 Automated engine start

4.4.2.2.1 General

The HAAM shall only allow starting of the engine in response to a request from the operator to start the engine.

Prior to engine cranking an audible alarm shall be initiated and remain active for the duration of the warning period. The delay between initiation of the audible warning and engine cranking and the duration of the warning after engine starting shall be sufficient to avoid exposure to hazards taking into account the charateristics of the machine and its operating environment.

Engine cranking shall only be allowed after the warning period has expired.

The HAAM shall shutdown the engine in response to an obstacle entering the hazard zone surrounding the engine during the warning period or during engine cranking.

In the event that engine cranking stops for more than 1 s, the engine warning period shall be restarted.

If multiple engines are used, the exact alarm sequence of additional engines after the first shall be determined by the manufacturer through a risk assessment.

4.4.2.2.2 Hazard checks

The hazard zone surrounding the engine shall be confirmed to be free of obstacles for the duration of the warning period prior to and during engine cranking and cranking shall stop should an obstacle be detected.

4.4.2.3 Engine running

4.4.2.3.1 General

The HAAM shall shutdown the engine in response to an obstacle entering the hazard zone surrounding the engine while the engine is running.

4.4.2.3.2 Hazard check

The hazard zone surrounding the engine shall be continuously monitored to detect obstacles while the engine is running in highly automated operation.

4.4.2.4 Engine stop

The HAAM shall shutdown the engine in response to a request received from the operator to stop the engine.

4.4.2.5 Engine stall

In the event that the engine stalls, engine starting shall require initiation by the operator.

4.4.2.6 Engine fault

In the event that an engine fault that prevents safe use of the HAAM in accordance with the design specification exists, the HAAM shall enter a defined safe state and highly automated operation of the machine shall be disabled automatically until the fault is rectified.

4.4.2.7 Engine status

Continuous automatic supervision of the engine status shall be provided. Appropriate information shall be available to the operator.

4.4.2.8 Loss of communication

Communication with the supervisory system required to maintain safe operation in accordance with the design specification shall be continuously confirmed. Communication shall be considered lost if no communication happens for a defined periof of time. Should communication be lost, the HAAM shall enter a defined safe state.

4.4.3 Automated motion control

4.4.3.1 General

Automated motion control shall only be allowed when highly automated operations are enabled.

Automated motion control shall apply to wheel motion and machine motion control.

4.4.3.2 General wheel motion initiation

4.4.3.2.1 General

The HAAM shall only start wheel motion in response to a request from the operator to initiate wheel motion and after confirmation by the perception system that the hazard zone is free of obstacles which need to be avoided.

Prior to wheel motion, an audible alarm shall be initiated and remain active for the duration of the warning period. The delay between initiation of the audible warning and wheel motion and the duration of the warning after wheel motion shall be sufficient to avoid exposure to the hazards concerned taking into account the characteristics of the machine.

Wheel motion shall only be allowed after the warning period has expired.

The HAAM shall abort wheel motion initiation in response to an obstacle entering the hazard zone during the warning period.

Highly automated machine motion may continue during the wheel motion initiation warning period if highly automated machine motion is already active.

4.4.3.2.2 Hazard check

The hazard zone surrounding the machine shall be confirmed to be free of obstacles for the duration of the warning period.

4.4.3.3 General machine motion initiation

4.4.3.3.1 General

The HAAM shall only start machine motion in response to a command initiated by the operator to start machine motion.

Prior to machine motion, an audible alarm shall be initiated and remain active for the duration of the warning period. The delay between initiation of the audible warning and machine motion and the duration of the warning after wheel motion shall be sufficient to avoid exposure to the hazards concerned taking into account the characteristics of the machine.

Machine motion initiation warning periods when highly automated wheel motion is already active can be different to those when highly automated wheel motion is not active.

Machine motion shall only be allowed after the warning period has expired.

The HAAM shall abort machine motion initiation in response to an obstacle entering the hazard zone during the warning period.

Highly automated wheel motion may continue during the machine motion initiation warning period if highly automated machine operation is already fully active.

4.4.3.3.2 Hazard check

The hazard zone surrounding the machine shall be confirmed to be free of obstacles for the duration of the warning period before machine motion initiation.

4.4.3.4 Motion stopping

4.4.3.4.1 General

The HAAM shall stop motion in response to an obstacle entering the hazard zone surrounding the machine.

4.4.3.4.2 Hazard check

The hazard zone surrounding the machine shall be continuously confirmed to be free of obstacles while the machine is moving in highly automated operation.

4.4.3.5 Motion stop

The HAAM shall stop motion in response to a request received from the operator.

4.4.3.6 Impaired motion

In the event that machine motion becomes impaired (e.g. obstacle detected), the machine shall enter a defined safe state. Further motion shall require initiation by the operator.

4.4.3.7 Motion fault

Should a fault occur during highly automated operation, the HAAM shall stop motion automatically and highly automated operation shall be disabled until the fault is rectified.

4.4.3.8 Machine motion status

Continuous automatic supervision of the machine motion status shall be provided and be available to the operator.

4.4.3.9 Loss of communication

Communication with the supervisory system required to maintain safe operation in accordance with the design specification shall be continuously confirmed. Communication shall be considered lost if no communication happens for a defined periof of time. Should communication be lost the HAAM shall enter a defined safe state.

4.5 Machine operational status

System operational status and relevant safety information shall be continuously available to the operator via the supervisory system.

4.6 Overriding of highly automated operation

Deliberate activation of controls for controlling motion functions (e.g. direction control, braking, stopping of hazardous tools) by the on-board or remote operator shall override highly automated operation.

The operator's manual for the machine shall define how to transfer control of the machine from highly automated operation to operator control and from operator control to highly automated operation.

Means (such as key switches, passwords or similar devices) accessible to the local operator shall be provided to reinitiate highly automated operation of the overridden function and to transfer control back to the highly automated function control system.

If no such user interface is practical, the function shall be put in a defined safe state before highly automated operation can be reinstated.

4.7 Remote stopping of highly automated operation

A control to stop highly automated operation shall be provided and shall be easily accessible to the operator at all operating positions.

Actuation of the stop control shall initiate a controlled action to a defined safe state.

4.8 Pendant control

A pendant control shall be provided with HAAM that do not have an operator on-board station.

4.9 Operational speeds of the machine

The machine's maximum operational speed during highly automated operation shall be compatible with the specification of the perception system and shall be given in the operator's manual. The maximum operational speed shall be limited automatically by the control system of the HAAM and shall not exceed the maximum permitted speed specified in the operator's manual.

4.10 Communication system

If communication failures prevent the required communication between elements of the highly automated system (monitoring or machine control) and external signals (e.g. GNSS), the system shall enter its defined safe state.

NOTE 1 This requirement is adapted from IEC 60204-1.

The acceptable time duration for communication failures before hazardous motions are stopped shall be dependent on machine application and the use of the information. When this time is exceeded the HAAM shall enter a defined safe state. The time during loss of communication, and defined safe state shall be consistent with maintaining a safe condition in relation to, for example, the maximum permitted travel speed, the extent of the warning and hazard zones, the response time of the object perception system, effectiveness of the guarding and stopping performance.

Communication failures to be taken into account shall include lost, degraded, delayed, misdirected, erroneous, and out-of-sequence communications.

NOTE 2 The following are examples of sources of communication failure: issues affecting network performance in general, network physical or configuration changes, machines added to or taken from the network, noise issues (for example, unintentional jamming, EMC), hardware failures, systemic failures, software defects, network configuration changes, bandwidth limitations, weather-related issues, topography changes, system power issues, intentional hacking, spoofing, or jamming.

4.11 Perception system

4.11.1 General

A perception system capable of detecting, under foreseeable operating conditions, objects in the path of the HAAM, persons approaching the HAAM and the position of the HAAM relative to detected obstacles and the boundary of the warning zone shall be provided. The perception system shall consist of perception sensors, positioning/guidance systems, associated algorithms required for the identification and classification of significant objects relative to the HAAM and the safety related control system for controlling the machine without the need for human intervention.

4.11.2 Possible risk and failure modes

4.11.2.1 The following are examples of reasons for failure to detect an obstacle or late detection of an obstacle :

a) obstacles are occluded due to crops, dust, fog, snow, rain or other obscurants;

b) perception results become unreliable due to poor or intense lighting conditions;

c) uneven ground causes scanning plane to vary, e.g. the laser beam might hit the ground or point to the sky when the vehicle is pitching down or up or tilting side to side;

d) vehicle vibration or motion causes misalignment of sensors;

e) obstacles are moving too fast to be detected;

f) obstacles are too small or do not reflect back in the direction of the receiver, e.g. the reliability of the radar technology depends on the effective radar cross-section of the obstacle to identify it; organic, transparent, or dark obstacles do not reflect, e.g. laser beam or radar signal, or are not detectable by visible light sensor; sound-absorbing obstacles do not reflect sufficient acoustic energy from, for example an ultrasonic sensor;

g) obstacles reflect or emit too much energy and saturate the sensor;

h) obstacles at the same temperature as the environment are not detected by thermal sensor;

i) negative obstacles (holes in the terrain) are not detected;

j) latency may increase due to other applications or computation loading on the processor used for the obstacle detection or classification system;

k) dust or other obscurants on the sensors itself can reduce the sensor field of view;

l) difficult terrain condition (mud, significant slopes, etc.) and body of water are not detected;

m) sensor is moved out of the alignment or blocked by a machine cover or shield not installed correctly for operation.

4.11.2.2 The following are examples of reasons for false detection of non-existent obstacles :

a) dust, fog, snow, rain or other obscurants reflecting sufficient energy to be classified as an obstacle;

b) material on the transmitter or receiver is erroneously detected as obstacles.

4.11.2.3 The following are examples of reasons for erroneous location of a detected obstacle or HAAM position:

a) sensor misalignment causes inaccurate position estimate;

b) positioning and orientation system errors (e.g. GNSS error) causing inaccurate machine position or orientation;

c) vibration of the sensor mounting causing sensor motion that is not accounted for by the perception system;

d) dust, fog, snow, rain or obscurants blur the edges of the obstacle or environment;

e) inaccurate sensor calibration or registration;

f) wrong location of obstacle due to multi-path propagation.

4.11.2.4 The following are examples of reasons for misclassification of an obstacle:

a) dust, fog, snow, rain or obscurants blur the edges;

b) inadequate experience, training or validation of the classifier;

c) traversable grass or crops classified as non-traversable obstacle;

d) obstacles are occluded due to crops, dust, fog, snow, rain, or other obscurants.

4.11.2.5 In addition, interference between the following examples can occur:

a) sensors;

b) sensors and communication systems;

c) sensors and electromagnetic signal in the environment (e.g. solar radiation and GNSS, 5 GHz radar and Wi-Fi router).

4.11.3 Fault management

4.11.3.1 General

Faults due to reliability issues (as a result of a hardware failure in the system) and malfunction due to conceptual or software issues (e.g. whether or not the system is functioning as intended under a no-fault condition in a variety of environmental parameters) shall not result in a dangerous condition.

Fault management and performance shall be verified by testing of the perception system in accordance with 4.11.3.2 and 4.11.3.3.

4.11.3.2 Behaviour of the obstacle detection system in a fault condition

The reliability of the perception system shall be subject to an assessment according to ISO 25119 (all parts) or an equivalent functional safety standard [e.g. ISO 13849 (all parts) or IEC 61508].

All fault conditions of the perception systems shall be identified. The required PL or SIL shall be determined taking into account all foreseeable fault conditions, hazards arising from the use of the HAAM during a fault condition, the foreseeable severity of harm and the probability of harm taking into account the likely presence of bystanders and the ability of bystanders to avoid the hazard. Upon detection of a residual hazardous fault condition, the HAAM shall enter a defined safe state.

4.11.3.3 Behaviour of the perception system in a no-fault condition

4.11.3.3.1 The system shall function as intended under the conditions and constraints foreseeable during operation including foreseeable misuse. Limitations of the perception system shall be described in the operator's manual.

4.11.3.3.2 These limitations could be environmental parameters, such as sun radiation, darkness, fog, temperature, all kinds of atmospheric precipitation and conditions, terrain irregularities and weed or bush-infected areas.

4.11.3.3.3 These limitations could be obstacle-related parameters, such as too small dimensions, a too fast obstacle moving speed, or poor reflection properties.

4.11.3.3.4 These limitations could be HAAM, related parameters, such as misalignment of the sensor(s), a too high operating speed, dirt on the sensor, too high vibrations or a too high computation demand for the processor.

4.11.3.3.5 If the confidence level of the sensors for the perception system falls below the minimum performance threshold required for safe operation, the HAAM shall initiate safe state. A diagnostic system of the HAAM shall indicate and record the reason why the safe state has been initiated. For HAAM with on-board operator the initiation of a safe state can be replaced by an audible warning if risk assessment shows this to be sufficient.

4.12 Safeguarding system

The safeguarding system shall

— give a warning, for example by an audible or visual alarm, if an obstacle (e.g. person or animal) is identified in the warning zone, and

— stop all highly automated functions and the machine shall enter its defined safe state (travelling and working functions) if an obstacle is identified in the hazard zone.

4.13 Visual and audible alarms

4.13.1 Visual alarm

If provided, a visual alarm detectable by persons in the vicinity of the HAAM shall be given continuously when highly automated operation is selected.

The following modes of operation and conditions of the HAAM shall be indicated visually at all positions for operator control:

— highly automated operation selected (amber);

— highly automated operation suspended following object detection or malfunction (green);

— remote operator manual control (green);

— error mode initiated (red).

When highly automated operation is suspended because of object detection or a malfunction, appropriate additional warnings shall be given to indicate the cause.

The meanings of the indications and any action to be taken shall be described in the operator's manual.

Diagnostics shall be provided for visual warnings and indications (e.g. start-up function test, circuit current measurement).

NOTE 1 Local regulations can have specific colours for visual warnings and indications.

NOTE 2 Information for persons in the vicinity of HAAM is still subject to further investigations and will be amended in the future revision.

4.13.2 Audible alarm

The alarm spectral characteristics shall comply with the requirements of ISO 7731:2003, 6.3.

Temporal characteristics shall comply with the requirements of ISO 7731:2003, 6.4.1. The maximum repetition frequency shall not exceed 2 Hz. The on-interval of the alarm should be equal to the off-interval of the alarm within 20 %.

Diagnostics shall be provided (for example, start-up function test, circuit current measurement). Under fault conditions of the audible alarms the operator shall be notified of the fault and further highly automated operation shall not be possible until the fault is rectified.

5 Verification and validation of the safety requirements and protective or risk reduction measures

5.1 General

The verification and validation methods of ISO 13849 (all parts) or ISO 25119 (all parts) shall be applied to the HAAM. Prior to the validation of the design of the safety-related part of a control system (SRP/CS), or the combination of SRP/CS providing the safety function, the requirements specification for the safety function shall be verified to ensure suitability and completeness for its intended use, as described in ISO 13849-2:2012, Clause 7.

5.2 Verification methods

Compliance with the principles for design and information for use of this document shall be verified in accordance with one or a combination of the following methods as appropriate taking into account any relevant standards for components or specific machines:

a) **Inspection**: Inspecting the condition of the HAAM or equipment and structures, using human senses without any specialized inspection equipment; inspection is typically carried out visually or acoustically when the HAAM is not in operation.

b) **Practical tests**: Testing the HAAM or its equipment under normal and abnormal conditions; functional tests (e.g. fault injection testing), cyclic tests (e.g. endurance testing), performance tests (e.g. braking performance testing).

c) **Measurement**: Evaluate the actual values of HAAM characteristics with specified values or limits.

d) **Simulation**: Results from modelling of the vehicle system operating under simulated operating conditions. Simulations shall be validated and verified against data from practical tests.

e) **Observation during operation**: Inspecting the functions of the HAAM for correct operation under normal and abnormal conditions, e.g. with rated payloads, overloaded situations and under difficult environmental conditions.

f) **Examination of circuit diagrams**: Structured review or walk-through of the design of circuit diagrams (e.g. electrical, hydraulic, pneumatic) and related specifications.

g) **Examination of software**: Structured review or walk-through of the design of software code and related specifications. Code inspection or testing of the software code should follow.

h) **Review of task-based risk assessment**: Structured review or walk-through of the risk analysis, risk estimation and relevant documentation.

i) **Examination of layout drawings and relevant documents**: Structured review or walk-through of the design of layout drawings and relevant documents.

5.3 Test object specification

The following defines a test obstacle, intended to represent a seated human that shall meet the following requirements and is used only to achieve repeatable results (see 5.4.2 for additional verification tests):

a) the dimensions given by Figure 1;

b) test obstacle shall be filled with water to represent the composition of the human body;

c) material shall be plastic, e.g. polyethylene with matte surface;

d) the colour shall be olive green with matte surface.

NOTE "Olive green" is specified as 2.5 GY 3.5/3 by the Munsell Colour System.

Dimensions in millimetres

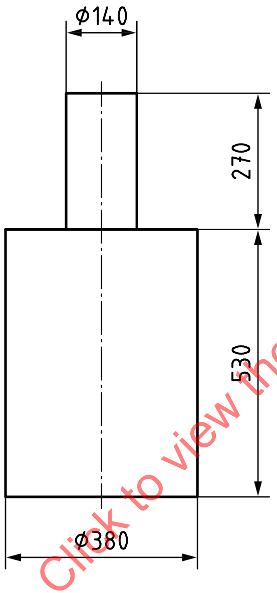

Figure 1 — Test obstacle dimensions

5.4 Verification of minimum performance of the systems perception and safety

5.4.1 As a means for verifying minimum performance requirements of the perception system with regard to obstacle detection, tests shall be performed under the following conditions and the results documented:

a) flat, dry paved area so that traction conditions are consistent and repeatable;

b) at the maximum operating speed of the HAAM achievable for highly automated operation under normal operating conditions;

c) date, time, location and environmental conditions of each test to be documented and recorded (e.g. solar intensity, presence of obscurants);

d) with a test obstacle in accordance with Figure 1 directly in the centre of the path travelled by the HAAM, verify whether the HAAM can detect the test obstacle and stops before making contact with the detected test obstacle;

e) carry out additional tests with the test obstacle located at positions laterally offset from the centre of the path travelled by the HAAM, to verify the capabilities of the safety systems to detect and stop the HAAM or an implement attached to the HAAM would make contact with detected obstruction;