International Standard

ISO 18497-1

First edition
2024-07

Agricultural machinery and tractors — Safety of partially automated, semi-autonomous and autonomous machinery —

Part 1: Machine design principles and vocabulary

Tracteurs et matériels agricoles — Sécurité des machines partiellement automatisées, semi-autonomes et autonomes —

Partie 1: Principes de conception des machines et vocabulaire

Reference number
ISO 18497-1:2024(en)

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

Published in Switzerland

Contents

Page

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 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 19, *Agricultural electronics*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 144, *Tractors and machinery for agriculture and forestry,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO 18497-1, together with ISO 18497-2, ISO 18497-3 and ISO 18497-4, cancels and replaces ISO 18497:2018, which has been technically revised.

The main changes are as follows:

— machine design principles and vocabulary were made as its own part (i.e. ISO 18497-1) and substantially revised to account for the wide range of functionality and use cases within agricultural machines and tractors.

A list of all parts in the ISO 18497 series can be found on the ISO website.

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 12100:2010.

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.

The purpose of the ISO 18497 series is to establish general design principles for partially automated, semi-autonomous and autonomous (see Clause 3) functions of agricultural machinery and tractors.

Manual non-automated functions are addressed in existing agricultural machinery and tractor safety standards. Due to the potential number of different functions of agricultural machinery and tractors and the mixed type and mode to which these functions can exist, it is necessary to establish general design principles. In this way, the combination, operator location, and types of interaction of these functions can be guided so that further type-C safety standards can be developed consistently and explicitly to address the mitigation of risk of injury to operators and bystanders. This is the primary focus of safety standards. Attempting to specify risk mitigation requirements based on combinations of type and mode of functions alone cannot be accomplished accurately for all agricultural machinery and tractors due to the wide variety of the machinery and variety of functionality.

Therefore, the familiar representation of SAE J3016[1] with six levels of automation was deliberately not chosen as a basis for the ISO 18497 series. It is necessary to develop more specific type-C safety standards,

using the general design principles of this document, to adequately account for the risks of agricultural machinery and tractors used in a specified way with various types of partially automated, semi-autonomous and autonomous functions.

When the requirements of the ISO 18497 series for partially automated, semi-autonomous and autonomous functions of agricultural machinery and tractors are different from those which are stated in a machine-specific type-C standard dealing with partially automated, semi-autonomous and autonomous functions of agricultural machinery and tractors, the requirements of the machine-specific standard take precedence over the requirements of the ISO 18497 series.

Agricultural machinery and tractors — Safety of partially automated, semi-autonomous and autonomous machinery —

Part 1:
Machine design principles and vocabulary

1 Scope

This document specifies principles for the design of agricultural machinery and tractors that are used in agricultural applications and that have partially automated, semi-autonomous and autonomous functions. Additionally, it provides guidance on the type of information to be provided by the manufacturer on safe working practices (including information about residual risks).

The purpose of this document is to assist in the provision of more specific safety requirements, means of verification and information for use to ensure an appropriate level of safety for agricultural machinery and tractors with partially automated, semi-autonomous and autonomous functions used in a specified way.

This document deals with the significant hazards relevant to agricultural machinery and tractors with partially automated, semi-autonomous and autonomous functions when used as intended and under the conditions of misuse reasonably foreseeable by the manufacturer during normal operation and service.

Applicability of the design principles and any additional detailed requirements for design, verification, validation or information for use are outside the scope of this document. When risk assessment concludes that hazards are not significant hazards, the principles of this document do not apply.

NOTE Safety requirements for specific non-automated functions of agricultural machinery and tractors can be available in machine-specific type-C standards.

This document is not applicable to:

— forestry applications;

— operations on public roads including relevant requirements for braking and steering systems.

This document is not applicable to agricultural machinery and tractors which are manufactured before the date of its publication, or to systems applied to agricultural machinery and tractors put into use 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 3767-1:2016, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Symbols for operator controls and other displays — Part 1: Common symbols*

ISO 3767-1:2016/Amd 1:2020, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Symbols for operator controls and other displays — Part 1: Common symbols — Amendment 1*

ISO 3767-2:2016, *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 3767-2:2016/Amd 1:2020, *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 — Amendment 1*

ISO 4254-1:2013, *Agricultural machinery — Safety — Part 1: General requirements*

ISO 4254-1:2013/Amd 1:2021, *Agricultural machinery — Safety — Part 1: General requirements – Amendment 1*

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2023, *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 18497-2:2024, *Agricultural machinery and tractors — Safety of partially automated, semi-autonomous and autonomous machinery — Part 2: Design principles for obstacle protective systems*

ISO 18497-3:2024, *Agricultural machinery and tractors — Safety of partially automated, semi-autonomous and autonomous machinery — Part 3: Autonomous operating zones*

ISO 18497-4:2024, *Agricultural machinery and tractors — Safety of partially automated, semi-autonomous and autonomous machinery — Part 4: Verification methods and validation principles*

ISO 25119-1:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

ISO 25119-1:2018/Amd 1:2020, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development — Amendment 1*

ISO 25119-2:2019, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

ISO 25119-3:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software*

ISO 25119-3:2018/Amd 1:2020, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software — Amendment 1*

ISO 25119-4:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes*

ISO 25119-4:2018/Amd 1:2020, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes — Amendment 1*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 4254-1:2013, ISO 4254-1:2013/Amd 1:2021, ISO 12100:2010 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 https://www.electropedia.org/

3.1
manual non-automated
non-automated (3.6) only machine *functions* (3.5) that are intended to operate in *manual mode* (3.9) during all of the machine's *operating cycle* (3.11)

EXAMPLE Implement height above ground controlled manually by the operator.

Note 1 to entry: See Figure 1.

Note 2 to entry: Manual non-automated is not a level or a category of a machine. It is a term only to describe the combination of functions, and modes of functions.

	Manual non-automated (3.1)	Partially automated (3.2)	Semi-autonomous (3.3)	Autonomous (3.4)
Functions (3.5)	Non-automated (3.6)			
		Automated (3.7)		
Modes	Manual mode (3.9)			
			Autonomous mode (3.10)	

Figure 1 — Terms used for combinations of functions and modes

3.2
partially automated
non-automated (3.6) and *automated* (3.7) machine *functions* (3.5) that are intended to operate in *manual mode* (3.9) during all of the machine's *operating cycle* (3.11)

EXAMPLE Implement height above ground maintained automatically to a set point controlled by the operator.

Note 1 to entry: See Figure 1.

Note 2 to entry: Partially automated is not a level or a category of a machine. It is a term only to describe the combination of functions, and modes of functions.

3.3
semi-autonomous
automated (3.7) machine *functions* (3.5) that are intended to operate in *autonomous mode* (3.10) during part of the machine's *operating cycle* (3.11) in addition to *non-automated* (3.6) and automated machine functions that are intended to operate in *manual mode* (3.9) to complete some of the tasks assigned

EXAMPLE 1 Implement height above ground maintained automatically to a set point controlled by the operator in specific conditions, and maintained automatically to a set point controlled by machine without operator interaction during all of the machine's other operating cycles.

EXAMPLE 2 Automated field cultivating machine completing entire operating cycle of field work without operator interaction and also used to complete other operating cycles of field work in specific conditions manually by an operator.

Note 1 to entry: See Figure 1.

Note 2 to entry: Semi-autonomous is not a level or a category of a machine. It is a term only to describe the combination of functions, and modes of functions.

3.4
autonomous
automated (3.7) machine *functions* (3.5) that operate in *autonomous mode* (3.10) during all of the machine's *operating cycle* (3.11)

EXAMPLE 1 Implement height above ground maintained automatically to a set point controlled by the machine without operator interaction during all of the machine's operating cycles.

EXAMPLE 2 Automated field cultivating machine completing all operating cycles of work without operator interaction.

Note 1 to entry: See Figure 1.

Note 2 to entry: Autonomous is not a level or a category of a machine. It is a term only to describe the combination of functions, and modes of functions.

3.5
function
defined activity or behaviour of a machine or a machine system

EXAMPLE Machine propel, steering, braking, lights, 3-point hitch, hydraulic driven unit, implement control (ISOBUS CAN, power-take-off, hydraulic), etc.

3.6
non-automated
technique, method, or system of operating and controlling machine *function(s)* (3.5) by *operator interaction* (3.12)

3.7
automated
technique, method, or system of operating and controlling machine *function(s)* (3.5) by *automatic* (3.8) means

3.8
automatic
process or part of a process when machine *functions* (3.5) follow defined rules

Note 1 to entry: Complex computer functions (e.g. closed loop control, artificial intelligence) can be included in the machine *function* (3.5) following defined rules to accomplish a process or part of a process.

Note 2 to entry: *Automatic* (3.8) means are typically accomplished through minimal *operator interaction* (3.12), but can be accomplished without *operator interaction*.

3.9
manual mode
mode of machine operation in which machine *function(s)* (3.5) are controlled by an operator

Note 1 to entry: Manual mode definition infers *operator interaction* (3.12) to accomplish direct or *automatic* (3.8) means by which *non-automated* (3.6) and *automated* (3.7) machine *function(s)* (3.5) are controlled.

3.10
autonomous mode
mode of machine operation in which a machine performs *functions* (3.5) related to its defined tasks without *operator interaction* (3.12)

Note 1 to entry: States of *autonomous mode* (3.10) of a machine may require human interaction, for example: preparing, configuring, setting-up or programming the machine. This type of human interaction is not considered *manual mode* (3.9) or *operator interaction* (3.12) *as the functions* (3.5) of the machine are not involved.

3.11
operating cycle
complete set of tasks carried out within a defined operation

3.12
operator interaction
involvement of an operator to provide information to or control of a machine *function(s)* (3.5)

Note 1 to entry: Examples of operator interaction are: starting, maintaining or stopping machine *function(s)* (3.5); providing exception handling information to a machine, etc.

3.13
hazardous function
defined activity or behaviour of a machine or a machine system which can be a source of harm

Note 1 to entry: A hazardous function is different than a safety function. A safety function (per ISO 12100:2010) is defined as: *function of a machine whose failure can result in an immediate increase of the risk(s)*. Risk(s) (per ISO 12100:2010) is defined as: *combination of the probability of occurrence of harm and the severity of that harm*. Hazardous functions are those functions which are potential sources of harm (e.g. machine propel) in normal operation without failure. Per ISO 12100:2010, risk analysis is required for hazardous functions and risk evaluation to determine if acceptable risk reduction objectives have been achieved.

3.14
obstacle
object or ground condition which can cause harm, or is harmed, if it comes into contact or collision with the machinery

Note 1 to entry: Examples of objects which can cause harm: tree, rock, etc. Examples of objects which can be harmed: persons or animals.

Note 2 to entry: Risk assessment is used to analyse the degree of harm related to an obstacle. Machine specific type-C safety standards may also contain specific protective measures (e.g. reduce speed, change trajectory, etc.) for risk reduction of specific types of obstacles (e.g. persons, animals, etc.).

3.15
obstacle protective system
system that reacts to information received from machine components or systems (e.g. sensors, *perception systems* (3.16), *supervisory systems* (3.17), bumpers) to avoid harmful contact with a person and/or *obstacle* (3.14)

Note 1 to entry: Risk assessment is used to determine the appropriate level of risk reduction achieved by an obstacle protective system. Machine specific type-C safety standards can also contain specific protective measures (e.g. reduce speed, change trajectory, etc.) for risk reduction of specific types of obstacles (e.g. persons, animals, etc.). While avoiding all contact with a person and/or other obstacles is desired in many cases, there can be machine forms that allow for contact which does not cause harm by contact.

3.16
perception system
system that gathers and processes information about the environment in which the machine is operating

3.17
supervisory system
system that has *situational awareness* (3.18) and can take decisions for systems of the machine operation

3.18
situational awareness
machine's computational assimilation of how the machine and the environment are interacting and the context of that interaction from knowledge of the machine state and the environment through the use of a *perception system* (3.16)

3.19
warning zone
area where if an *obstacle* (3.14) is within and no action is taken, then the obstacle might enter the *hazard zone* (3.20)

3.20
hazard zone
area which is a subset of the *warning zone* (3.19) and where if an *obstacle* (3.14) is within that area, then the potential for injury can exist

3.21
autonomous operating zone
designated area in which machines operate in *autonomous mode* (3.10)

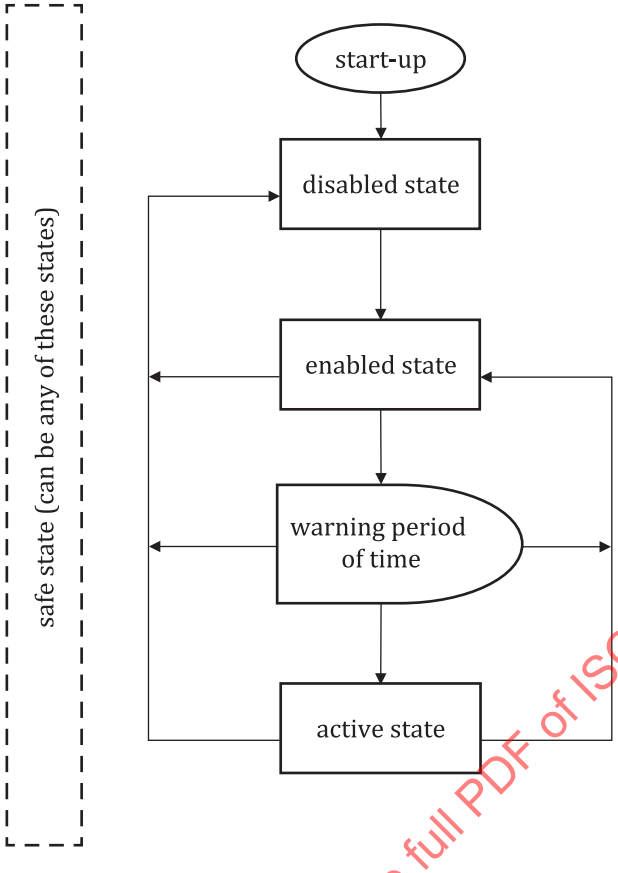

Figure 2 — State flow diagram example

3.22
active state
machine system state in which *partially automated* (3.2), *semi-autonomous* (3.3) *or autonomous* (3.4) *functions* (3.5) are provided

Note 1 to entry: See Figure 2.

3.23
disabled state
machine system state in which *partially automated* (3.2), *semi-autonomous* (3.3) *or autonomous* (3.4) *functions* (3.5) are not allowed

Note 1 to entry: See Figure 2.

3.24
enabled state
machine system state in which *partially automated* (3.2), *semi-autonomous* (3.3) *or autonomous* (3.4) *functions* (3.5) are allowed upon receipt of a valid command or signal

Note 1 to entry: See Figure 2.

3.25
impaired condition
point of degradation where *partially automated* (3.2), *semi-autonomous* (3.3) *or autonomous* (3.4) *functions* (3.5) of the machine systems can no longer be completed safely in the current conditions

3.26
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

Note 1 to entry: See Figure 2.

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

3.27
audible alarm
signal that is intended to be detected by the human sense of hearing

3.28
visual alarm
signal that is intended to be detected by the human sense of sight

3.29
warning period of time
designated period of time to give notice for machine *functions* (3.5) prior to initiation

Note 1 to entry: See Figure 2.

3.30
local operator
human in close proximity with access to machine controls through the *local operator station* (3.31) or through *remote operator station* (3.33) and/or access to machine information through a *notification system* (3.34)

3.31
local operator station
designated location(s) physically on the machine from which the operator provides information to or controls machine *function(s)* (3.5)

3.32
remote operator
human not in close proximity with access to machine controls through *remote operator station* (3.33) and/or access to machine information through a *notification system* (3.34)

3.33
remote operator station
location(s) close to and far away from the machine, but not physically on the machine, from which the operator provides information to or controls machine *function(s)* (3.5)

Note 1 to entry: Remote operator station can be connected to the machine via wire connection.

3.34
notification system
system providing a means to inform the operator about the operational status of the machine *function(s)* (3.5)

3.35
communication
information or data transmitted by a data network

3.36
use case
specific situation in which a product is used

Note 1 to entry: This includes machine type(s), operating conditions, functional ranges, system boundaries and operational design domain.

3.37
start-up
switch-on of a machine or of one of its parts

Note 1 to entry: See Figure 2.

3.38
operational limit
limit of a measurable factor or set of factors that defines the conditions of acceptable system operation

3.39
verification
evaluation of a component or system of the machine to determine if it meets a defined requirement

3.40
validation
assurance that a component or system of the machine meets a defined objective

4 Safety requirements and protective or risk reduction measures

4.1 General

Partially automated, semi-autonomous and autonomous functions (see Figure 1) of agricultural machinery and tractors shall be designed according to the principles of 4.2 for protective or risk reduction measures of significant hazards, as defined in ISO 12100:2010, 3.8.

Significant hazards are dependent on the use case of agricultural machinery and tractors with partially automated, semi-autonomous and autonomous functions and shall be determined using a risk assessment according to ISO 12100:2010.

In addition, partially automated, semi-autonomous and autonomous functions of machines shall be designed according to the principles of ISO 12100:2010 for relevant but not significant hazards which are not dealt with by this document. For significant hazards not covered in 4.2, the determination of requirements and corresponding verification procedures shall be done according to ISO 12100:2010.

Specific type-C standards, when available, can give more detailed requirements.

Obstacle protective systems and systems (perception, supervisory or other) to prevent unintended excursions beyond the boundary of the autonomous operating zone shall be designed in accordance with ISO 18497-2:2024 and ISO 18497-3:2024, respectively.

Verification methods of ISO 18497-4:2024 shall be applied to the design principles of 4.2.

4.2 Design principles

4.2.1 General

For ensuring an appropriate level of safety of partially automated, semi-autonomous (when automated machine functions operate in autonomous mode) and autonomous functions of agricultural machinery and tractors, the following protective or risk reduction measures shall be provided in the machine design to reduce significant hazards.

4.2.2 Operator presence

4.2.2.1 Partially automated

An operator presence system shall be provided to detect if an operator is no longer at the local operator station or at the remote operator station.

4.2.2.2 Semi-autonomous and autonomous

a) An operator presence system in autonomous mode of operation shall be provided to detect if an operator is at a local operator station (if equipped).

EXAMPLE 1 Seat switch used to detect if an operator is at the local operator station on a semi-autonomous machine when operating in autonomous mode during part of the machine's operating cycle.

b) An operator presence system in autonomous mode of operation shall be provided to detect if an operator is no longer at the remote operator station (if equipped).

EXAMPLE 2 Activity monitoring by detecting operator interaction with, or acknowledgement of notifications provided on the remote operator station to detect if operator is no longer at the remote operator station for a machine operating in autonomous mode.

4.2.3 Start-up

4.2.3.1 Partially automated

Non-automated and automated hazardous functions shall be in a disabled or neutral state at start-up.

4.2.3.2 Semi-autonomous and autonomous

a) Automated hazardous functions in autonomous mode shall be in a disabled state at start-up.

b) A command from a local operator shall be required to change to an enabled state at start-up in autonomous mode.

EXAMPLE Machine requiring human to setup, power on and confirm autonomous mode settings. Once confirmed, machine enters enabled state (e.g. ready, standby or sleep) of autonomous mode. Upon valid command or signal, machine enters active state in autonomous mode.

4.2.4 States, modes and actions

4.2.4.1 Partially automated

a) Means shall be provided such as contact switches, soft keys or other similar devices, accessible to the operator, for changing states of automated functions.

b) A command from the operator to change to an active state shall be required for automated hazardous functions.

c) Automatic exit of automated hazardous functions from an active state shall be provided under specific conditions (e.g. manual movement of a specific control, lack of sufficient or loss of signal from sensors, indication from operator presence system that operator is no longer present).

d) At standstill, no action initiation shall be provided by automated hazardous functions.

4.2.4.2 Semi-autonomous and autonomous

a) Means shall be provided such as contact switches, soft keys or other similar devices, accessible to the operator, for changing function states and modes.

b) Means shall be provided to change from an active state to a different safe state in autonomous mode of operation from local operator station and/or at the remote operator station.

c) A command from an operator and only by an operator shall be required for initiating hazardous functions in an active state in autonomous mode of operation.

d) A command from a local operator shall be required to change from an enabled state to an active state in autonomous mode of operation involving hazardous functions.

e) Only specific automated hazardous functions shall be provided and allowed when in autonomous mode of operation and in the enabled or active state.

f) A warning period of time shall be provided for hazardous functions prior to initiation in autonomous mode of operation [see 4.2.5.2 b) and 4.2.6.2 b)].

g) A safe state shall be provided automatically in autonomous mode when a person and/or obstacle is detected in or enters the hazard zone of the obstacle protective system (if equipped) and/or under specific conditions (e.g. manual movement of a specific control by local operator, lack of sufficient or loss of signal from sensors, indication from operator presence system that operator is no longer present);

NOTE Use of a supervisory system can be a means to fulfil g).

h) A command from the operator shall be required to re-enter active state or restart functions after change from active state in autonomous mode.

4.2.5 Visual indication

4.2.5.1 Partially automated

A visual indicator shall be provided to the operator which shows the current state of the automated functions.

NOTE Visual indicators differ from visual alarms which are specified in 4.3.

4.2.5.2 Semi-autonomous and autonomous

a) A visual alarm shall be provided indicating current state in autonomous mode of operation (see 4.3.2.2).

b) A visual alarm shall be provided prior to, during a warning period of time, during initiation, after starting and during operation of hazardous functions (e.g. drive function) in autonomous mode of operation (see 4.3.2.3).

c) A visual alarm shall be provided indicating manual mode of operation for semi-autonomous machines not equipped with a local operator station (see 4.3.2.4).

EXAMPLE Machine without local operator station using a visual alarm to indicate operation in manual mode instead of autonomous mode.

d) A visual alarm shall be provided when a person and/or obstacle is detected in or enters, at a minimum, the hazard zone of the obstacle protective system (if equipped) in autonomous mode of operation (see 4.3.2.5).

4.2.6 Audible indication

4.2.6.1 Partially automated

An audible indicator shall be provided to the operator which sounds when automated functions enter or leave the active state.

NOTE Audible indicators differ from audible alarms which are specified in 4.3.

4.2.6.2 Semi-autonomous and autonomous

a) An audible alarm shall be provided when entering states in autonomous mode of operation (see 4.3.3.2);

b) An audible alarm shall be provided prior to, during a warning period of time, during initiation and after starting of hazardous functions (e.g. drive function) in autonomous mode of operation (see 4.3.3.3);

c) An audible alarm shall be provided prior to, during initiation and after starting of hazardous functions (e.g. drive function) in manual mode of operation for semi-autonomous machines not equipped with a local operator station (see 4.3.3.4);

EXAMPLE Machine without local operator station using an audible alarm to indicate operation in manual mode instead of autonomous mode.

d) An audible alarm shall be provided when a person and/or obstacle is detected in or enters, at a minimum, the hazard zone of the obstacle protective system (if equipped) in autonomous mode of operation (see 4.3.3.5).

4.2.7 Obstacle protective system

4.2.7.1 Partially automated

a) An obstacle protective system shall be provided for hazardous automated functions.

b) Non-automated and automated hazardous functions shall only be provided and allowed when the obstacle protective system is in an active state.

4.2.7.2 Semi-autonomous and autonomous

a) An obstacle protective system shall be provided in autonomous mode of operation:

— that ensures, before action of specific hazardous functions, that there is no person and/or obstacle in the relative hazard zone of the hazardous function;

— that ensures automatically maintaining a safe state during initiation and operation of specific hazardous functions when a person and/or obstacle is detected in or enters the relative hazard zone of the hazardous function;

— that is compatible with the maximum operational speed of specific hazardous functions to ensure adequate responsiveness when a person and/or obstacle is detected in or enters the relative hazard zone of the hazardous function;

— that ensures adequate detection of a person and/or obstacles within or entering boundary of the defined warning zone of the hazardous function;

b) Hazardous functions in autonomous mode of operation shall only be provided and allowed when the obstacle protective system is in an active state.

4.2.8 Operating zone (semi-autonomous and autonomous)

a) Means, such as a perception system, shall be provided in autonomous mode of operation to prevent unintended excursions beyond the boundary of the autonomous operating zone.

b) The means provided in a) shall be compatible with the maximum operational speed of the machine in autonomous mode of operation.

c) Hazardous functions in autonomous mode of operation shall only be provided and allowed when the defined autonomous operating zone is ensured and the machine is within the autonomous operating zone.

4.2.9 Monitoring

4.2.9.1 Partially automated

See 4.2.5.1 and 4.2.6.1.

4.2.9.2 Semi-autonomous and autonomous

a) A notification system shall be provided to allow adequate monitoring of the machine and specific functions by an operator.

b) Automatic change from an active state or enabled state to a different safe state shall be provided in autonomous mode when loss of communication (for a defined period of time) between the notification system and the machine.

4.2.10 Faults and failures

4.2.10.1 General

The machine design with partially automated, semi-autonomous and autonomous hazardous functions shall comply with ISO 25119-1:2018, ISO 25119-1:2018/Amd 1:2020, ISO 25119-2:2019, ISO 25119-3:2018, ISO 25119-3:2018/Amd 1:2020, ISO 25119-4:2018 and ISO 25119-4:2018/Amd 1:2020, or ISO 13849-1:2023 and ISO 13849-2:2012.

Use of a supervisory system can be a means to detect and take action from faults and failures.

Diagnostics shall be provided for visual and audible alarm (e.g. start-up function test, circuit current measurement). It also shall be provided that under fault conditions of the visual and audible alarm, the operator be notified of the fault and further autonomous mode of operation shall not be possible until the fault is rectified.

For software and data that are critical for safety, measures and methods shall be provided to minimize accidental or intentional corruptions from external sources (e.g. cyber-attacks or perturbations).

NOTE See References [3] and [4] for more information regarding cybersecurity.

Protection from faults and failures of the power supply for partially automated, semi-autonomous and autonomous functions shall be provided.

4.2.10.2 Communication failures

Systems shall be provided with means to allow only intentional and safe communications. Functional safety standards (see 4.2.10.1) shall be applied for communication failures.

If communication failures prevent the required communication between system elements (e.g. GNSS and the supervisory system) of partially automated, semi-autonomous and autonomous hazardous functions, the system shall enter a safe state.

The acceptable time duration for communication failures before hazardous functions are stopped shall be dependent on the application and the use of the information. When this time is exceeded, the hazardous functions shall enter a safe state. The time between a communication failure and entering a 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 obstacle protective system, effectiveness of the guarding and stopping performance.

NOTE 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 (e.g. unintentional jamming, EMC), hardware failures, systemic failures, software defects, network configuration changes, bandwidth limitations, weather-related issues, changes in topography, system power issues, intentional hacking, spoofing or jamming.

4.2.10.3 Partially automated

Automatically enter a safe state shall be provided if faults due to failures cause an impaired condition for automated hazardous functions.

4.2.10.4 Semi-autonomous and autonomous

a) Automatically exit from autonomous mode and enter a defined safe state shall be provided when faults due to failures cause an impaired condition for hazardous functions operating in autonomous mode.

NOTE 1 Use of a supervisory system can be a means to fulfil a).

b) Automatically change from an active state to a different safe state shall be provided in autonomous mode of operation when specific hazardous functions are unable to complete initiation sequence commands.

NOTE 2 Automatically restarting initiation sequence commands for specific hazardous functions with a given warning period of time, etc. is dependent on risk assessments.

NOTE 3 Use of a supervisory system can be a means to fulfil b).

4.3 Visual and audible alarms

4.3.1 General

Means shall be provided such as contact switches, soft keys or other similar devices, accessible to the operator, for checking the operation of visual and audible alarms.

4.3.2 Visual alarm (semi-autonomous and autonomous)

4.3.2.1 General

The requirements of 4.3.2 shall be followed unless prohibited by local regulations for visual warnings and indications.

If provided, a visual alarm shall be detectable by local operators and bystanders in the vicinity that can lead to a risk to safe machine operation.

4.3.2.2 State in autonomous mode of operation

The visual alarm shall use the following colours to indicate the current state in autonomous mode of operation:

— white (power on and disabled state);

NOTE 1 Significant hazards can exist when the source of power is non-audible or not clearly evident.

EXAMPLE White colour visual alarm used to indicate when power is switched on, but all functions are in a disabled state for a battery powered machine.

— blue-green (enabled or active state);

NOTE 2 Blue-green x,y based colour boundaries according to CIE 1931 of ISO/CIE 11664-1:2019[5]:

x	y
0,013	0,494
0,200	0,400
0,200	0,320
0,040	0,320

— red or blue (error).

NOTE 3 Local regulations can prohibit specific colours for visual warnings and indications, therefore either red or blue colour is specified.

Only the white visual alarm colour shall be given continuously without flashing in the power on and disabled state. The white visual alarm colour source shall not be used in other states of autonomous mode of operation except to momentarily:

— indicate prior to, during a warning period of time and during initiation of hazardous functions in autonomous mode of operation (see 4.3.2.3); and/or