INTERNATIONAL STANDARD

ISO 10218-1

Second edition
2011-07-01

Robots and robotic devices — Safety requirements for industrial robots —

Part 1: Robots

Robots et dispositifs robotiques — Exigences de sécurité pour les robots industriels —

Partie 1: Robots

Reference number
ISO 10218-1:2011(E)

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Hazard identification and risk assessment 6

5 Design requirements and protective measures 7
5.1 General 7
5.2 General requirements 7
5.3 Actuating controls 8
5.4 Safety-related control system performance (hardware/software) 8
5.5 Robot stopping functions 9
5.6 Speed control 11
5.7 Operational modes 11
5.8 Pendant controls 13
5.9 Control of simultaneous motion 15
5.10 Collaborative operation requirements 15
5.11 Singularity protection 16
5.12 Axis limiting 16
5.13 Movement without drive power 18
5.14 Provisions for lifting 18
5.15 Electrical connectors 18

6 Verification and validation of safety requirements and protective measures 19
6.1 General 19
6.2 Verification and validation methods 19
6.3 Required verification and validation 19

7 Information for use 20
7.1 General 20
7.2 Instruction handbook 20
7.3 Marking 21

Annex A (informative) List of significant hazards 23

Annex B (normative) Stopping time and distance metric 28

Annex C (informative) Functional characteristics of three-position enabling device 30

Annex D (informative) Optional features 31

Annex E (informative) Labelling 33

Annex F (normative) Means of verification of the safety requirements and measures 34

Bibliography 43

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 10218-1 was prepared by Technical Committee ISO/TC 184, *Automation systems and integration*, Subcommittee SC 2, *Robots and robotic devices*.

This second edition cancels and replaces the first edition (ISO 10218-1:2006), which has been technically revised. It also incorporates Technical Corrigendum ISO 10218-1:2006/Cor.1:2007.

ISO 10218 consists of the following parts, under the general title *Robots and robotic devices — Safety requirements for industrial robots*:

— *Part 1: Robots*

— *Part 2: Robot systems and integration*

Introduction

ISO 10218 has been created in recognition of the particular hazards that are presented by industrial robots and industrial robot systems.

This part of ISO 10218 is a type-C standard as outlined in ISO 12100.

When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other standards for machines that have been designed and built in accordance with the provisions of the type-C standard.

The machinery concerned and the extent to which hazards, hazardous situations and events are covered are indicated in the Scope of this part of ISO 10218.

Hazards associated with robots are well recognized, but the sources of the hazards are frequently unique to a particular robot system. The number and type(s) of hazard(s) are directly related to the nature of the automation process and the complexity of the installation. The risks associated with these hazards vary with the type of robot used and its purpose, and the way in which it is installed, programmed, operated and maintained.

NOTE Not all of the hazards identified by ISO 10218 apply to every robot, nor will the level of risk associated with a given hazardous situation be the same from robot to robot. Consequently, the safety requirements, or the protective measures, or both, can vary from what is specified in ISO 10218. A risk assessment can be conducted to determine what the protective measures should be.

In recognition of the variable nature of hazards with different uses of industrial robots, ISO 10218 is divided into two parts. This part of ISO 10218 provides guidance for the assurance of safety in the design and construction of the robot. Since safety in the application of industrial robots is influenced by the design and application of the particular robot system integration, ISO 10218-2 provides guidelines for the safeguarding of personnel during robot integration, installation, functional testing, programming, operation, maintenance and repair.

This part of ISO 10218 has been updated based on experience gained in developing the ISO 10218-2 guidance on system and integration requirements, in order to ensure it remains in line with minimum requirements of a harmonized type-C standard for industrial robots. Revised technical requirements include, but are not limited to, definition and requirements for singularity, safeguarding of transmission hazards, power loss requirements, safety-related control circuit performance, addition of a category 2 stopping function, mode selection, power and force limiting requirements, marking, and updated stopping time and distance metric and features.

This part of ISO 10218 is not applicable to robots that were manufactured prior to its publication date.

Robots and robotic devices — Safety requirements for industrial robots —

Part 1:
Robots

1 Scope

This part of ISO 10218 specifies requirements and guidelines for the inherent safe design, protective measures and information for use of industrial robots. It describes basic hazards associated with robots and provides requirements to eliminate, or adequately reduce, the risks associated with these hazards.

This part of ISO 10218 does not address the robot as a complete machine. Noise emission is generally not considered a significant hazard of the robot alone, and consequently noise is excluded from the scope of this part of ISO 10218.

This part of ISO 10218 does not apply to non-industrial robots, although the safety principles established in ISO 10218 can be utilized for these other robots.

NOTE 1 Examples of non-industrial robot applications include, but are not limited to, undersea, military and space robots, tele-operated manipulators, prosthetics and other aids for the physically impaired, micro-robots (displacement less than 1 mm), surgery or healthcare, and service or consumer products.

NOTE 2 Requirements for robot systems, integration, and installation are covered in ISO 10218-2.

NOTE 3 Additional hazards can be created by specific applications (e.g. welding, laser cutting, machining). These system-related hazards need to be considered during robot design.

2 Normative references

The following referenced documents are indispensable for the application 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 9283:1998, *Manipulating industrial robots — Performance criteria and related test methods*

ISO 10218-2, *Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration*

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

ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 13850, *Safety of machinery — Emergency stop — Principles for design*

IEC 60204-1, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

IEC 62061:2005, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Terms and definitions

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

3.1
actuating control
mechanical mechanism within a control device

EXAMPLE A rod which opens contacts.

3.2
automatic mode
operating mode in which the robot control system operates in accordance with the task programme

[ISO 8373:1994, definition 5.3.8.1]

3.3
automatic operation
state in which the robot is executing its programmed task as intended

NOTE Adapted from ISO 8373:1994, definition 5.5.

3.4
collaborative operation
state in which purposely designed robots work in direct cooperation with a human within a defined workspace

3.5
collaborative workspace
workspace within the safeguarded space where the robot and a human can perform tasks simultaneously during production operation

3.6
drive power
energy source or sources for the robot actuators

3.7
end-effector
device specifically designed for attachment to the mechanical interface to enable the robot to perform its task

EXAMPLE Gripper, nutrunner, welding gun, spray gun.

[ISO 8373:1994, definition 3.11]

3.8
energy source
electrical, mechanical, hydraulic, pneumatic, chemical, thermal, potential, kinetic or other source of power

3.9
hazardous motion
motion that is likely to cause personal physical injury or damage to health

3.10
industrial robot
automatically controlled, reprogrammable multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications

NOTE 1 The industrial robot includes:

— the manipulator, including actuators;

— the controller, including teach pendant and any communication interface (hardware and software).

NOTE 2 This includes any integrated additional axes.

NOTE 3 The following devices are considered industrial robots for the purpose of this part of ISO 10218:

— hand-guided robots;
— the manipulating portions of mobile robots;
— collaborating robots.

NOTE 4 Adapted from ISO 8373:1994, definition 2.6.

3.11
industrial robot system
system comprising:

— industrial robot;
— end-effector(s);
— any machinery, equipment, devices, external auxiliary axes or sensors supporting the robot performing its task

NOTE 1 The robot system requirements, including those for controlling hazards, are contained in ISO 10218-2.

NOTE 2 Adapted from ISO 8373:1994, definition 2.14.

3.12
limiting device
means that restricts the maximum space by stopping or causing to stop all robot motion

3.13
local control
state of the system or portions of the system in which the system is operated from the control panel or pendant of the individual machines only

3.14
manual mode
control state that allows for the direct control by an operator

NOTE 1 Sometimes referred to as teach mode where programme points are set.

NOTE 2 Adapted from ISO 8373:1994, definition 5.3.8.2.

3.15
pendant
teach pendant
hand-held unit linked to the control system with which a robot can be programmed or moved

[ISO 8373:1994, definition 5.8]

3.16 Programme

3.16.1
control programme
inherent set of instructions which defines the capabilities, actions, and responses of a robot

NOTE This type of programme is fixed and usually not modified by the user.

[ISO 8373:1994, definition 5.1.2]

3.16.2
task programme
set of instructions for motion and auxiliary functions that define the specific intended task of the robot system

NOTE 1 This type of programme is normally generated by the user.

NOTE 2 An application is a general area of work; a task is specific within the application.

[ISO 8373:1994, definition 5.1.1]

3.16.3
programme verification
execution of a task programme for the purpose of confirming the robot path and process performance

NOTE Verification can include the total path traced by the tool centre point during the execution of a task programme or a segment of the path. The instructions can be executed in a single instruction or continuous instruction sequence. Verification is used in new applications and in fine tuning/editing of existing ones.

3.17
protective stop
type of interruption of operation that allows a cessation of motion for safeguarding purposes and which retains the programme logic to facilitate a restart

3.18
robot actuator
powered mechanism that converts electrical, hydraulic, or pneumatic energy to effect motion

3.19
safety-rated
characterized by having a prescribed safety function with a specified safety-related performance

3.19.1
safety-rated monitored speed
safety-rated function that causes a protective stop when either the Cartesian speed of a point relative to the robot flange (e.g. the TCP), or the speed of one or more axes exceeds a specified limit value

3.19.2
safety-rated reduced speed
safety-rated monitored speed function that limits the robot speed to 250 mm/s or less

NOTE 1 The safety-rated reduced speed limit value is not necessarily the value set in the reduced speed control function.

NOTE 2 The difference between safety-rated monitored speed and safety-rated reduced speed is that safety-rated monitored speed limit can be set to speeds greater than 250 mm/s.

3.19.3
safety-rated soft axis and space limiting
safety-rated soft limit
limit placed on the range of motion of the robot by a software- or firmware-based system having a specified sufficient safety-related performance

NOTE The safety-rated soft limit might be the point where a stop is initiated, or it might ensure that the robot does not move beyond the limit.

3.19.4
safety-rated output
output signal having a specified sufficient safety-related performance

3.19.5
safety-rated zone output
safety-rated output indicating the state of the robot position relative to a safety-rated soft limit

NOTE For example, the robot position can be inside the zone or outside the zone.

3.19.6
safety-rated monitored stop
condition where the robot is stopped with drive power active, while a monitoring system with a specified sufficient safety performance ensures that the robot does not move

3.20
simultaneous motion
motion of two or more robots at the same time under the control of a single control station, and which may be coordinated or may be synchronous using common mathematical correlation

NOTE 1 A teach pendant is an example of a single control station.

NOTE 2 Coordination can be done as master/slave.

3.21
single point of control
ability to operate the robot such that initiation of robot motion is only possible from one source of control and cannot be overridden from another initiation source

3.22
singularity

occurrence whenever the rank of the Jacobian matrix becomes less than full rank

NOTE Mathematically, in a singular configuration, the joint velocity in joint space can become infinite to maintain Cartesian velocity. In actual operation, motions defined in Cartesian space that pass near singularities can produce high axis speeds. These high speeds can be unexpected to an operator.

3.23
reduced speed control
slow speed control
mode of robot motion control where the speed is limited to 250 mm/s or less

NOTE Reduced speed is intended to allow persons sufficient time to either withdraw from the hazardous motion or stop the robot.

3.24
space
three-dimensional volume

3.24.1
maximum space
space which can be swept by the moving parts of the robot as defined by the manufacturer plus the space which can be swept by the end-effector and the workpiece

[ISO 8373:1994, definition 4.8.1]

3.24.2
restricted space
portion of the maximum space restricted by limiting devices that establish limits which will not be exceeded

NOTE Adapted from ISO 8373:1994, definition 4.8.2.

3.24.3
safeguarded space
space defined by the perimeter safeguarding

3.25
teach
teach programming
task programming
programming of the task performed by

a) manually leading the robot end-effector; or

b) manually leading a mechanical simulating device; or

c) using a teach pendant to step the robot through the desired positions

NOTE Adapted from ISO 8373:1994, definition 5.2.3.

3.26
tool centre point
TCP
point defined for a given application with regard to the mechanical interface coordinate system

[ISO 8373:1994, definition 4.9]

3.27
user
entity that uses robots and is responsible for the personnel associated with the robot operation

4 Hazard identification and risk assessment

Annex A contains a list of hazards that can be present with robots. A hazard analysis shall be carried out to identify any further hazards that may be present.

A risk assessment shall be carried out on those hazards identified in the hazard identification. This risk assessment shall give particular consideration to:

a) the intended operations of the robot, including teaching, maintenance, setting and cleaning;

b) unexpected start-up;

c) access by personnel from all directions;

d) reasonably foreseeable misuse of the robot;

e) the effect of failure in the control system; and

f) where necessary, the hazards associated with the specific robot application.

Risks shall be eliminated or reduced first by design or by substitution, then by safeguarding and other complementary measures. Any residual risks shall then be reduced by other measures (e.g. warnings, signs, training).

The requirements contained in Clause 5 derive from the iterative process consisting of applying safeguarding measures that are described in ISO 12100 to the hazards identified in Annex A.

NOTE 1 ISO 12100 provides requirements and guidance in performing hazard identification and risk reduction.

NOTE 2 Hazard identification and risk assessment requirements for robot systems, integration, and installation are covered in ISO 10218-2.

5 Design requirements and protective measures

5.1 General

The robot shall be designed in accordance with the principles of ISO 12100 for relevant hazards. Significant hazards, such as sharp edges, are not dealt with by this part of ISO 10218.

Robots shall be designed and constructed to comply with the requirements in 5.2 to 5.15.

5.2 General requirements

5.2.1 Power transmission components

Exposure to hazards caused by components such as motor shafts, gears, drive belts, or linkages which are not protected by integral covers (e.g. panel over a gear box) shall be prevented either by fixed guards or movable guards. The fixing systems of the fixed guards which are intended to be removed for routine service actions shall remain attached to the machine or the guard. Movable guards shall be interlocked with the hazardous movements in such a way that the hazardous machine functions cease before they can be reached. The safety-related control system performance of an interlocking system shall conform to the requirements of 5.4.

5.2.2 Power loss or change

Loss of, or variations in power shall not result in a hazard.

Re-initiation of power shall not lead to any motion.

Robots shall be designed and constructed so that loss or change of electrical, hydraulic, pneumatic or vacuum power does not result in a hazard. If hazards exist that are not protected by design, then other protective measures shall be taken to protect against those hazards. Unprotected hazards of the expected use shall be identified in the information for use.

NOTE See IEC 60204-1 for electrical power supply requirements.

5.2.3 Component malfunction

Robot components shall be designed, constructed, secured, or contained so that hazards caused by breaking or loosening, or releasing stored energy are minimized.

5.2.4 Sources of energy

A means of isolating any hazardous energy source to the robot shall be provided. This means shall be provided with capability of locking or otherwise securing in the de-energized position.

5.2.5 Stored energy

A means shall be provided for the controlled release of stored hazardous energy. A label shall be affixed to identify the stored energy hazard.

NOTE Stored energy can occur in air and hydraulic pressure accumulators, capacitors, batteries, springs, counterbalances, flywheels, etc.

5.2.6 Electromagnetic compatibility (EMC)

The design and construction of the robot shall prevent hazardous motion or situations due to the expected effects of electromagnetic interference (EMI), radio frequency interference (RFI) and electrostatic discharge (ESD).

NOTE See IEC 61000 for design information.

5.2.7 Electrical equipment

The robot electrical equipment shall be designed and constructed in accordance with the relevant requirements of IEC 60204-1.

5.3 Actuating controls

5.3.1 General

Actuating controls that initiate power or motion shall be designed and constructed to meet the performance criteria mentioned in 5.3.2 to 5.3.5.

5.3.2 Protection from unintended operation

Actuating controls shall be constructed or located so as to prevent unintended operation. For example, appropriately designed push-buttons or key selector switches in appropriate locations can be used.

5.3.3 Status indication

The status of the actuating controls shall be clearly indicated, e.g. power on, fault detected, automatic operation.

If an indicator light is used, it shall be suitable for its installed location and its colour shall meet the requirements of IEC 60204-1.

5.3.4 Labelling

Actuating controls shall be labelled to clearly indicate their function.

5.3.5 Single point of control

The robot control system shall be designed and constructed so that when the robot is placed under local pendant control or other teaching device control, initiation of robot motion or change of local control selection from any other source is prevented.

5.4 Safety-related control system performance (hardware/software)

5.4.1 General

Safety-related control systems (electric, hydraulic, pneumatic and software) shall comply with 5.4.2, unless the results of the risk assessment determine that an alternative performance criterion as described in 5.4.3 is appropriate. The safety-related control system performance of the robot and any furnished equipment shall be clearly stated in the information for use.

NOTE 1 Safety-related control systems can also be called SRP/CS (safety-related parts of control systems).

For the purposes of this part of ISO 10218, safety-related control system performance is stated as:

— Performance Levels (PL) and categories as described in ISO 13849-1:2006, 4.5.1;

— Safety Integrity Levels (SIL) and hardware fault tolerance requirements as described in IEC 62061:2005, 5.2.4.

Those two standards address functional safety using similar but different methods. Requirements in those standards should be used for the respective safety-related control systems for which they are intended. The designer may choose to use either of the two standards. The data and criteria necessary to determine the safety-related control system performance shall be included in the information for use.

NOTE 2 The comparison with ISO 13849-1 and IEC 62061 is described in ISO/TR 23849.

Other standards offering alternative performance requirements, such as the term “control reliability” used in North America, may also be used. When using these alternative standards to design safety-related control systems, an equivalent level of risk reduction shall be achieved.

Any failure of the safety-related control system shall result in a stop category 0 or 1 in accordance with IEC 60204-1.

5.4.2 Performance requirement

Safety-related parts of control systems shall be designed so that they comply with PL=d with structure category 3 as described in ISO 13849-1:2006, or so that they comply with SIL 2 with a hardware fault tolerance of 1 with a proof test interval of not less than 20 years, as described in IEC 62061:2005.

This means in particular:

a) a single fault in any of these parts does not lead to the loss of the safety function;

b) whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function;

c) when the single fault occurs, the safety function is always performed and a safe state shall be maintained until the detected fault is corrected; and

d) all reasonably foreseeable faults shall be detected.

The requirements a) to d) are considered to be equivalent to structure category 3 as described in ISO 13849-1:2006.

NOTE The requirement of single fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output and a hazardous situation at the machine.

5.4.3 Other control system performance criteria

The results of a comprehensive risk assessment performed on the robot and its intended application may determine that a safety-related control system performance other than that stated in 5.4.2 is warranted for the application.

Selection of one of these other safety-related performance criteria shall be specifically identified, and appropriate limitations and cautions shall be included in the information for use provided with the affected equipment.

5.5 Robot stopping functions

5.5.1 General

Every robot shall have a protective stop function and an independent emergency stop function. These functions shall have provision for the connection of external protective devices. Optionally, an emergency stop output signal may be provided. Table 1 shows a comparison of the emergency stop and protective stop functions.