INTERNATIONAL STANDARD

ISO 14118

Second edition
2017-12

Safety of machinery — Prevention of unexpected start-up

Sécurité des machines — Prévention de la mise en marche intempestive

Reference number
ISO 14118:2017(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 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 199, *Safety of machinery*.

This second edition cancels and replaces the first edition (ISO 14118:2000), which has been technically revised and contains the following changes:

— the text has been edited to facilitate implementation of this document;

— the Scope has been redefined to exclude the specification of performance levels or safety integrity levels for safety-related parts of control systems;

— Figure 1 has been updated.

Introduction

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

a) type-A standards (basic safety standards) giving basic concepts, principles for design, and general aspects that can be applied to all machinery;

b) type-B standards (generic safety standards) dealing with one safety aspect or one or more type(s) of safeguard 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-hand controls, interlocking devices, pressure sensitive devices, guards);

c) type-C standards (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

This document is a type-B 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 organizations, 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.

Keeping a machine in a stopped condition while persons are present in danger zones is one of the most important conditions of the safe use of machinery and hence, one of the major aims of the machine designer and machine user.

In the past, the concepts of “operating machine” and “stopped machine” were generally unambiguous; a machine was

— operating when its movable elements or some of them were moving;

— stopped when its movable elements were at rest.

Machine automation has made the relationship between “operating” and “moving” on one hand and “stopped” and “at rest” on the other hand, more difficult to define. Automation has also increased the

potential for unexpected start-up and a significant number of hazardous events have occurred where machines, stopped for diagnostic work or corrective actions, started up unexpectedly.

Hazards other than mechanical hazards generated by movable elements (e.g. from a laser beam) also need to be taken into account.

The risk assessment relating to the presence of persons in a danger zone of a stopped machine needs to take into account the probability of an unexpected start-up of the hazard-generating elements.

This document provides machine designers and machinery safety standard technical committees with samples of built-in measures which can be used to prevent unexpected start-up.

Safety of machinery — Prevention of unexpected start-up

1 Scope

This document specifies requirements for designed-in means aimed at preventing unexpected machine start-up (see 3.2) to allow safe human interventions in danger zones (see Annex A).

This document applies to unexpected start-up from all types of energy source, i.e.:

— power supply, e.g. electrical, hydraulic, pneumatic;

— stored energy due to, e.g. gravity, compressed springs;

— external influences, e.g. from wind.

This document does not specify performance levels or safety integrity levels for safety-related parts of control systems. While available means to prevent unexpected start-up are identified, this document does not specify the means for the prevention of unexpected machine start-up for specific machines.

NOTE A type-C standard can define the required means for the prevention of harm arising from unexpected start-up. Otherwise, the requirements for a specific machine need to be determined by risk assessment outside the scope of this document.

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

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

IEC 62061, *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.

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

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

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

3.1
start-up
machine start-up
change from rest to motion or switch-on of a machine or of one of its parts

Note 1 to entry: An example of function other than motion is switch-on of a laser.

3.2
unexpected start-up
unintended start-up
start-up (3.1) which, because of its unexpected nature, generates a risk to persons

Note 1 to entry: This can be caused by, for example:

— a start command which is the result of a failure in or an external influence on the control system;

— a start command generated by inopportune action on a start control or other parts of the machine such as a sensor or a power control element;

— restoration of the power supply after an interruption;

— external/internal influences (gravity, wind, self-ignition in internal combustion engines, etc.) on parts of the machine.

Note 2 to entry: Machine start-up during the normal sequence of an automatic cycle is not unintended, but can be considered as being unexpected from the point of view of the operator. Prevention of hazardous events in this case involves the use of safeguarding measures (see 6.3).

3.3
isolation and energy dissipation
procedure which consists of all of the four following actions:

a) isolating (disconnecting, separating) the machine (or defined parts of the machine) from all power supplies;

b) locking (or otherwise securing), if necessary (for instance, when the operator is not able, from every location he may be at, to check that the power supply remains interrupted), all the isolating units in the "isolated" position;

c) dissipating or restraining (containing) any stored energy which may give rise to a hazard.

Note 1 to entry Energy considered in c) may be stored in e.g. mechanical parts continuing to move through inertia, e.g. backdriving of a ventilation fan, mechanical parts liable to move by gravity, capacitors and accumulators, pressurized fluids and springs.

d) verifying by using a safe working procedure (e.g. by measuring) that the actions taken according to a), b) and c) have produced the desired effect.

4 General measures to prevent unexpected start-up

4.1 General

A risk assessment in accordance with ISO 12100 shall be performed to identify the required measures to prevent unexpected start-up.

NOTE Measures to prevent unexpected start-up of specific machinery can be specified in a type-C standard. The machine manufacturer is responsible for the suitability of measures identified by risk assessment.

The necessary procedures to prevent unexpected start-up including energy dissipation or restraint (containment) and verification method if necessary, shall be described in the instruction handbook of the machine and/or in warnings on the machine itself. The instructions should be provided with respect to each;

— source of energy;

— means;

— task (see Annex A);

— level (see Figure 1).

4.2 Manual measures for isolation and energy dissipation

Machines shall be provided with manually operated devices for isolation of energy supplies and energy dissipation (see Clause 5), considering the required task to be performed with the machine, e.g. maintenance, work on power circuits and decommissioning.

4.3 Other means to prevent unexpected (unintended) start-up

If the use of manual isolation and energy dissipation is not appropriate for frequent short interventions, the designer shall provide additional automatic controlled functions (see Clause 6) to prevent unexpected start-up.

NOTE 1 Examples of tasks which can require the presence of persons in danger zones are given in Annex A.

The designer should determine as completely as possible the different machine operating and stopping modes and the need for the presence of persons in danger zones. Appropriate safety measures can then be provided. These measures are intended to prevent operators from being induced to use hazardous operating modes and hazardous intervention techniques caused by technical difficulties in the use of the machine.

4.4 Signalling and warning (delayed start)

When required by the risk assessment, an audible and/or visible warning signal and delayed start shall be provided as a means to prevent injury from the unexpected start-up of machinery.

The warning signal shall be audible and/or visual to alert exposed person(s) of the impending start-up. The duration of the warning signal and the period of time corresponding to the delayed start-up shall last long enough to enable the persons either to leave the danger zone before the machine starts or to prevent the machine starting, e.g. by actuating an emergency stop device.

A warning signal and delayed start-up shall be provided when all danger zones cannot be seen from the operator control station or when the presence of persons in danger zones cannot be detected or excluded.

Where applicable, machinery should provide an indication of different states related to start-up, e.g. “waiting for a start command”, “waiting for material”, “power on”, etc.

5 Isolation and energy dissipation

5.1 Prevention of unexpected start-up upon restoration of any power supplies

Risks need to be considered where it is expected that the restoration or start-up after the energy dissipation or interruption could lead to unexpected movements.

Where necessary, (an) appropriate measure(s) to prevent it shall be taken.

5.2 Devices for isolation from power supplies

5.2.1 Isolation devices shall:

— ensure a reliable disconnection or separation from the energy source;

— have a reliable mechanical link between the manual control and the isolating element(s);

— be equipped with clear and unambiguous identification of the state of the isolation device which corresponds to each position of its manual control (actuator).

NOTE 1 For electrical equipment, a supply disconnecting (isolating) device complying with IEC 60204-1:2016, 5.3 meets this requirement.

NOTE 2 Plug and socket systems (for electrical supplies) or their pneumatic, hydraulic or mechanical equivalents, are examples of isolating devices with which it is possible to achieve a visible and reliable discontinuity in the power supply circuits. For electrical plug/socket combinations, see IEC 60204-1:2016, 5.3.2 e) and 5.3.3.

NOTE 3 For hydraulic and pneumatic equipment; see also ISO 4413:2010, 5.4.7.2.1 and ISO 4414:2010, 5.2.8.

5.2.2 The location and number of isolation devices will be determined by risk assessment while taking into account the configuration of the machine, the need for the presence of persons in danger zones and the task to be performed. Each isolation device shall be readily identifiable as to which machine or part of it, it isolates (e.g. by durable marking where necessary).

Isolation of only part of a machine shall not create a hazard due to operation of other parts of the machine.

NOTE 1 For electrical equipment of machinery, see also IEC 60204-1:2016, 5.4.

NOTE 2 For large machinery where it is necessary to have access to individual parts of a machine, separate additional isolation devices can be required.

NOTE 3 The location of the isolating device can be either at the place of the intervention or along the access route.

5.2.3 When, during isolation of the machine, certain circuits have to remain connected to their power supply in order, e.g. to hold parts, protect information or provide local lighting, additional means [e.g. permanent warning label(s)] shall be provided to ensure operator safety.

NOTE For electrical circuits, see IEC 60204-1:2016, 5.3.5 and for hydraulic circuits, see ISO 4413:2010, 7.3.2.1.3.

5.3 Locking (securing) devices

The isolation devices shall be capable of being locked or otherwise secured in the “isolated” position.

Locking devices may not be necessary when a plug/socket combination is used and the plug can be kept under immediate supervision of the person present in the danger zone.

Locking devices may include, but are not limited to, one or more of the following:

— facilities to apply one or more padlocks;

— trapped-key interlocking devices (see ISO 14119:2013, B.2), one of the locks of which is associated with the manual control (actuator) of the isolating device;

NOTE For trapped-key interlocking devices requirements, see ISO/TS 19837 and also ISO 14119.

— the use of a personal key(s) which are released from a trapped key interlocking device and retained by a person(s) to prevent a hazardous event, e.g. unexpected start-up;

— lockable housings or enclosures.

5.4 Devices for stored-energy dissipation or restraint (containment)

5.4.1 General

5.4.1.1 Means for stored-energy dissipation or restraint (containment) shall be provided where stored energy can give rise to a hazard.

NOTE Means for stored-energy dissipation can include brakes intended to absorb kinetic energy of moving parts, resistors and relevant circuitry to discharge electrical capacitors, valves or similar devices to depressurize fluidic accumulators (see ISO 4413:2010, 5.4.7.2.1 and ISO 4414:2010, 5.2.8). For discharging of capacitors in machines, see IEC 60204-1:2016, 6.2.4.

5.4.1.2 When dissipation of stored energy would excessively reduce the ability of the machine to be used, additional means shall be incorporated to reliably restrain or contain the remaining stored energy.

5.4.1.3 The devices for energy dissipation or restraint (containment) should be selected and arranged so that:

— dissipation or restraint (containment) results from the isolation of the machine (or relevant part of it);

— the energy dissipation process does not give rise to hazardous situations.

5.4.1.4 The machine shall not be able to be started with dissipation devices activated or restraint devices in place if this generates new hazards. If this is not practicable, warnings and instructions shall be provided in the instruction handbook of the machine and/or in warnings on the machine itself.

5.4.2 Mechanical elements

When mechanical elements can give rise to a hazardous situation:

— by virtue of their mass and position (e.g. unbalanced or raised or in any situation where they could move under the effect of gravity);

— or as a result of the action upon them of spring load (whatever this "spring" is made of);

— mechanical parts continuing to move through inertia.

Means shall be provided to bring them to the lowest energy state (e.g. lowest position or spring-relaxed) either by the usual machine manual controls or by devices specifically designed and identified (marked) for that function.

When the mechanical elements cannot be brought into an intrinsically safe state, they shall be mechanically secured by brakes or mechanical restraint devices as defined in ISO 12100:2010, 3.28.7.

5.4.3 Locking or securing facilities for the restraint (containment) devices

The devices for energy restraint (containment) shall, whenever necessary, be capable of being locked or otherwise secured.

6 Other measures to prevent unexpected start-up

6.1 Design strategy

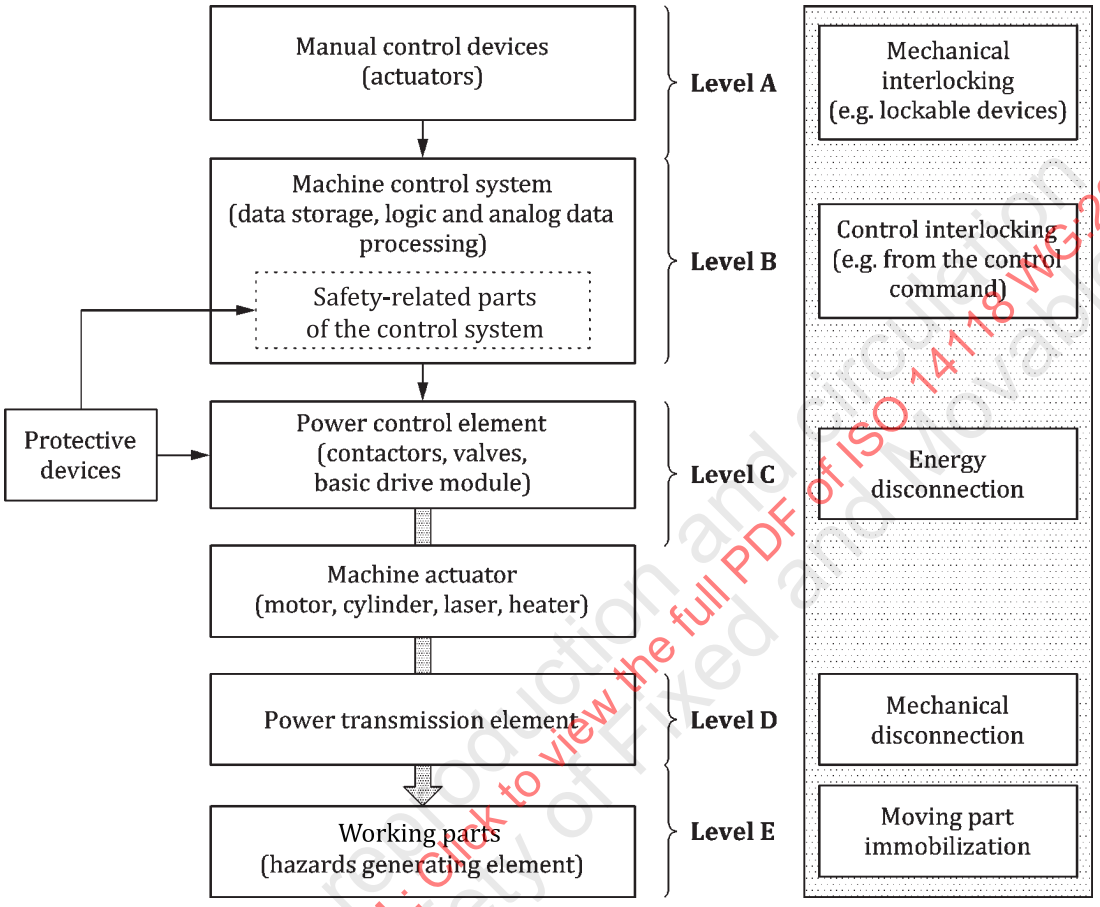
Where the risk assessment shows that isolation and energy dissipation are not appropriate for an intervention (e.g. manual loading/unloading), the following measures necessary to prevent unexpected start-up shall be taken as appropriate:

— measures taken in the control system to prevent the generation of start commands from unintended actuations of a start control device or other parts (e.g. sensors, power control elements), from failures in or from external influences (vibration, shocks, disturbances of the power supply) (see 6.2);

— measures taken at level A, B or C of the machine (see Figure 1) or at mechanical disconnection elements or at moving-parts (immobilization), to prevent unintended start commands resulting in an unexpected start-up (see 6.3);

— measures implemented in the control system to automatically stop the hazard-generating part of the machine before a hazardous event can arise from an unexpected/unintended start-up of this part (see 6.4).

NOTE The selected measures, in most cases, will be a combination of the different measures described in this subclause.



Key

energy (electric, hydraulic, pneumatic, etc.)

usual stop control signal

Figure 1 — Components/devices and application of measures, other than isolation and energy dissipation, to prevent unintended start commands resulting in unexpected start-up

6.2 Measures to prevent unintended generation of start commands

6.2.1 Measures to prevent unintended actuation of manual start controls

Unintended actuation of manual start controls, as well as unexpected results from actuating these devices (e.g. start-up of a machine other than the expected one, initiation of a movement in a wrong direction), shall be prevented by appropriate design, location, protection and marking of manual start controls. The expected results/effects of actions on start controls shall be made clear, e.g. by the use of marking near the control (see also 4.4, paragraph 4), in cases where lack of such information can endanger persons and providing such information is possible.

Where a control device is designed and constructed to perform several different actions, namely, where there is no one-to-one correspondence, the action to be performed shall be clearly displayed and subject to confirmation, where necessary.

NOTE 1 Guidance is given in the IEC 61310 series.

NOTE 2 Other examples of measures to prevent unauthorized/unintended start-up are locking of start manual controls, passwords in programmable control systems.

6.2.2 Design of safety-related parts of the control system

The safety-related parts of the control system (levels A, B and C according to Figure 1) shall be designed in accordance with ISO 13849-1 or IEC 62061.

6.2.3 Selection and location of power control elements

Power control elements (e.g. contactors, valves; see Figure 1) shall be selected and/or applied so that they cannot change their state under the effect of external influences (such as vibration or shocks of the highest intensity) within intended conditions of use or the effect of disturbances of the power supply (such as pressure or voltage fluctuations) within defined limits.

Power control elements shall, if necessary (especially if they can be manually operated), be located in an enclosure to prevent their unauthorized or unintended actuation.

6.3 Measures to maintain stop commands

6.3.1 Principle

Maintained stop commands are introduced, separately or in combination, in the machine at different "levels" (see Figure 1). Depending on the risk assessment, these can be generated either by stop control devices (see 6.3.2) or by protective devices (see 6.3.3). Mechanical disconnection (see 6.3.4) or moving-part immobilization (see 6.3.5) may be used instead of, or in addition to, maintained stop commands.

An unintended start command shall not result in machine start-up if

— it is generated by/in a machine component placed above the level at which a maintained stop command has been introduced (level A, B or C), or

— mechanical disconnection (level D) or moving-part immobilization (level E) has been achieved (see Figure 1).

6.3.2 Maintained stop command generated by a stop control device (level A)

The control system shall be designed so that the stop commands from the stop control device have priority over the start commands. To prevent unexpected (unintended) start-up due to unintended generation of start commands (including those generated within the control system itself), the stop manual control (or the stop control device) can be secured in the OFF/STOP condition. Depending on the risk assessment, securing in the OFF/STOP condition can be achieved by means of:

— a latching-in or key-operated stop control device which applies a maintained stop command until the device is reset manually;

NOTE The emergency stop function cannot be considered as a measure of prevention of unexpected start-up as described in ISO 12100 (see also ISO 13850:2015, 4.1.1.2).

— a lockable selector switch with a reliable and unambiguous indication of position which applies a maintained stop command until the switch is manually reset;

— a lockable cover which, when locked closed, forces the stop manual control into the OFF/STOP condition;

— other means.

Criteria for the design and selection of the securing means suitable for the intended application are:

— unambiguity, i.e. clear and unambiguous indication when the device is in the OFF/STOP condition;

— reliability, as far as the ability of the device to remain in the OFF/STOP condition is concerned.

Where a stop control is provided with a securing device to retain it in the OFF/STOP condition, removal of the securing device shall not by itself cause a start or restart command.

6.3.3 Maintained stop command generated by machine control (level B/C)

To prevent unexpected start-up of a machine (from whatever cause) when a person is in a danger zone, a protective device (according to ISO 12100) or combination of protective devices can be provided. The maintained stop command it generates shall be introduced at the appropriate level (see Figure 1).

NOTE The following International Standards give guidance:

— ISO 12100:2010, 6.3.2;

— ISO 14119, dealing with interlocking devices associated with guards;

— IEC/TS 62046, dealing with use of electro-sensitive devices.

6.3.4 Mechanical disconnection (level D; see Figure 1)

Mechanical disconnecting devices, e.g. clutches, shall be designed, selected and used and where necessary, monitored, so that the separation from machine actuators is ensured.

6.3.5 Moving-part immobilization (level E; see Figure 1)

When a moving part is immobilized by means of a mechanical restraint device (see, for example, ISO 12100:2010, 3.28.7), e.g. a wedge, spindle, strut, scotch, which is an integral part of the machine, the mechanical strength of this mechanical restraint device shall be sufficient to withstand the expected forces resulting from the start-up of the machine.

6.4 Automatic monitoring of the safe state (stopped condition) during a category 2 stop

If other measures to prevent unexpected start-up are not practicable as the result of the risk assessment, one method is to monitor the stopped condition during a stop category 2 as defined in IEC 60204-1. If this monitoring function detects that there is arising movement, it shall initiate a stop category 0. Additional measures may also be required (e.g. mechanical brakes).

The parts of the control system that perform the monitoring function shall be considered as safety related.

7 Design requirements for verification

7.1 General

The machine and the isolation and energy dissipation or restraint (containment) devices shall be designed, selected and arranged so that reliable verification of the effectiveness of the isolation and energy dissipation or restraint (containment) can be carried out.

The verification procedure to ensure the effectiveness of the isolation, energy dissipation and restraint (containment) measures shall not impair correct operation. For example, while relieving and measuring the pressure between energy isolating device and the equipment being worked on gives an indication that stored pressure has been released, pressure could still be retained in an accumulator.

