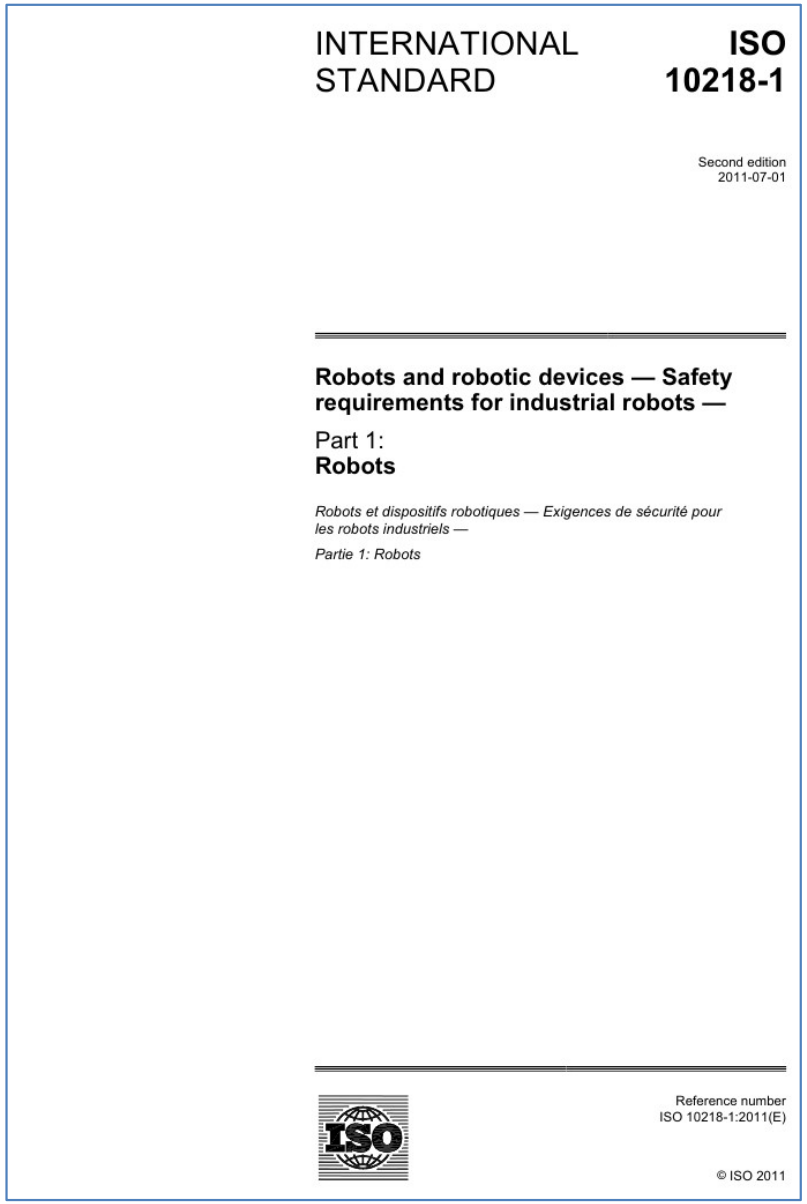
첨단제조 로봇 인증 및 기능안전 대응
ISO/DIS 10218-1:2021 기능안전 개정 동향

KAR 한국로봇산업협회
Korea Association of Robot industry

VERSION

ISO 10218-1:2011



INTERNATIONAL STANDARD

ISO 10218-1

Second edition
2011-07-01

Robots and robotic devices — Safety requirements for industrial robots —

Part 1:
Robots

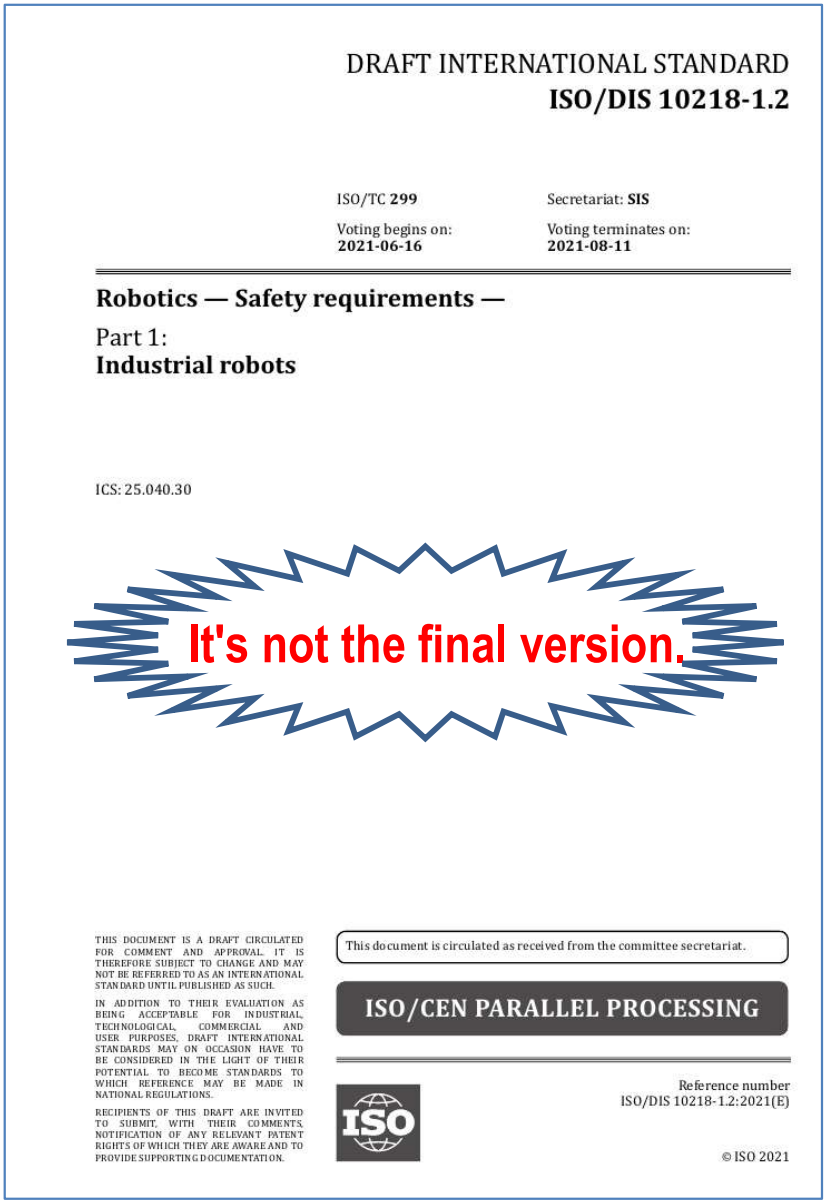
Robots et dispositifs robotiques — Exigences de sécurité pour les robots industriels —

Partie 1: Robots

Reference number
ISO 10218-1:2011(E)

© ISO 2011

ISO/DIS 10218-1:2021



DRAFT INTERNATIONAL STANDARD
ISO/DIS 10218-1.2

ISO/TC **299** Secretariat: **SIS**

Voting begins on:
2021-06-16

Voting terminates on:
2021-08-11

Robotics — Safety requirements —

Part 1:
Industrial robots

ICS: 25.040.30

It's not the final version.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 10218-1.2:2021(E)

© ISO 2021

목차

ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

Contents

Foreword 4
Introduction 5
1 Scope 1
2 Normative refe 1
3 Terms, definiti 2
3.1 Terms and defi 2
3.1.1 Robot, robot sys 2
3.1.2 Sub-assemblies applications 2
3.1.3 Controls-relatec 2
3.1.4 Program-relatec 2
3.1.5 Power-related 2
3.1.6 Hazard-related. 2
3.1.7 Roles 2
3.1.8 Functional safet 2
3.1.9 Spaces, zones ar 2
3.1.10 Risk reduction r 2
3.1.11 Verification and 2
3.2 Abbreviated te 3
4 Risk Assessme 4
5 Design and pro 4
5.1 Robot design 4
5.1.1 General 4
5.1.2 Materials, mech 4
5.1.3 Handling, lifting 4
5.1.4 Packaging 4
5.1.5 Stability 4
5.1.6 Temperature an 4
5.1.7 Special equipme 4
5.1.8 Position holding 4
5.1.9 Auxiliary axis (a 4
5.1.10 Power loss or ch 4
5.1.11 Component mal 4
5.1.12 Hazardous ener 4
5.1.13 Electrical, pneur 4
5.1.14 Tool centre poir 4
5.1.15 Payload setting. 4
5.1.16 Cybersecurity 4
5.1.17 Robot class 4
5.2 Robot controls 4
5.2.1 General 4
5.2.2 Protection from 4
5.2.3 Singularity 4
5.2.4 Interlocking fun 4
5.2.5 Status indicatio 4
5.2.6 Labelling 4
5.2.7 Single point of c 4
5.2.8 Modes 4
5.2.9 Means of contr 4
5.2.10 Means of initia 4
5.3 Safety functio 4
5.3.1 General 4
5.3.2 Functional safe 4
5.3.3 Performance 4
5.3.4 Failure or fault 4
5.3.5 Parametrizatic 4
5.3.6 Communicatio 4
5.3.7 Electromagnet 4
5.4 Robot stoppir 5
5.4.1 General 5
5.4.2 Emergency sto 5
5.4.3 Protective stop 5
5.4.4 Other stop 5
5.5 Other safety f 5
5.5.1 Start and resta 5
5.5.2 Speed limit(s) 5
5.5.3 Enabling funct 5
5.6 Simultaneous 5
5.7 Limiting robo 5
5.7.1 General 5
5.7.2 Mechanical axi 5
5.7.3 Electro-mecha 5
5.7.4 Soft axis and sp 5
5.7.5 Dynamic limiti 5
5.8 Movement wi 5
5.9 Lasers and las 5
5.10 Capabilities fo 5
5.10.1 General 5
5.10.2 Hand-guided c 5
5.10.3 Speed and sepa 5
5.10.4 Power and forc 5
6 Verification a measures 5
6.1 General 5
6.2 Verification a 5
7 Information f 5
7.1 General 5
7.2 Signals and w 5
7.3 Marking 5
7.4 Signs (pictogr 5
7.5 Instruction ha 5
7.5.1 General 5
7.5.2 Identification 5
7.5.3 Intended use 5
7.5.4 Installation 5
7.5.5 Stopping 5
7.5.6 Commissioning 5
7.5.7 Operation and 5
7.5.8 Singularity 5
7.5.9 Hazardous energy 53
7.5.10 Movement without drive power 54
7.5.11 Cybersecurity 54
7.5.12 Functional safety 54
7.5.13 Teach pendants 57
7.5.14 Integration into a robot system 57
7.5.15 Maintenance 57
7.5.16 Protection against electrical shock 58
7.5.17 Abnormal and emergency situations 58
7.5.18 Handling, lifting and transportation 58
Annex A (informative) List of significant hazards 59
Annex B (informative) Illustrations spaces 63
Annex C (normative) Safety functions 67
Annex D (normative) Required safety function information 71
Annex E (normative) Test methodology for Class I robots – maximum force per manipulator (F_{MPM}) 73
E.1 General 73
E.2 Test methodology for Class I robots 73
Annex F (informative) Symbols 81
Annex G (normative) Means of verification and validation of the design and protective measures 83
Annex H (normative) Stopping time and distance measurement 97
Annex I (informative) Optional features 99
I.1 General 99
I.2 Emergency stop safety function outputs 99
I.3 Enabling device functionality 99
I.4 Mode selection output 99
I.5 Anti-collision sensing 99
I.6 Maintaining path accuracy across all speeds 100
I.7 Optional capabilities 100
I.7.1 Configurable position for as a monitored position safety function 100
I.7.2 Stopping performance safety function(s) or non-safety measurement 100
I.7.3 Real-time interfaces safety function 100
Annex ZA (informative) Relationship between this European Standard and the essential requirements of Directive 2006/42/EC aimed to be covered 101
Bibliography 103

변경 사항

Foreword

This document was prepared by Technical Committee ISO/TC 299, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This third edition cancels and replaces the second edition (ISO 10218-1:2011), which has been technically revised.

The main changes compared to the previous edition are as follows:

- incorporating safety requirements for industrial robots intended for use in collaborative applications (formerly, the content of ISO/TS 15066);
  협업 애플리케이션에 사용하기 위한 산업용 로봇에 대한 안전 요구사항 통합(이전의 ISO/TS 15066 내용)
- clarifying requirements for functional safety;
  기능 안전에 대한 요구사항을 명확히 하는 것
- adding requirements for cybersecurity to the extent that it applies to industrial robot safety.
  산업용 로봇 안전에 적용되는 사이버 보안 요건을 추가.

변경 사항

Introduction

It is important to emphasize that the term "collaborative robot" is not used in ISO this document as only the application can be developed, verified and validated as a collaborative application.
이 문서에서는 "협동 로봇"이라는 용어를 사용하지 않는다는 점을 강조하는 것이 중요합니다.

In addition, the term "collaborative operation" is not used in this document.
또한 이 문서에서는 "협동 작업"이라는 용어를 사용하지 않습니다.

Revisions include the following:
- category 2 stopping functions;
- cybersecurity;
- definitions and abbreviations;
- details within the information for use clause;
- functional safety requirements;
- hand-guided control (HGC) requirements;
- markings;
- mechanical strength and stability requirements;
- mode selection;
- power and force limiting (PFL) requirements to enable collaborative applications;
- power loss requirements;
~~- hand-guided controls (HGC) requirements;~~
- robot classification (Class I and Class II) for functional safety requirements;
- spaces (maximum, restricted) figures shown in Annex B;
- speed and separation monitoring (SSM) requirements to enable collaborative applications;
- test methodology to determine the maximum force per manipulator for Class I robots.

엠에스엔티㈜ 민철휘

목차

ISO 10218-1:2011	ISO/DIS 10218-1:2021
1 Scope	1 Scope
2 Normative references	2 Normative references
3 Terms and definitions	3 Terms, definitions and abbreviations 3.1 Terms and definitions 3.1.1 Robot, robot system, robot application, application 3.1.2 Sub-assemblies and components of robots, robot systems and robot applications 3.1.3 Controls-related 3.1.4 Program-related 3.1.5 Power-related 3.1.6 Hazard-related 3.1.7 Roles 3.1.8 Functional safety-related 3.1.9 Spaces, zones and distances 3.1.10 Risk reduction measures 3.1.11 Verification and validation 3.2 Abbreviated terms
4 Hazard identification and risk assessment	4 Risk Assessment

1. 적용범위

1 Scope

This ISO document specifies requirements for the inherently safe design, protective measures and information for use of robots for an industrial environment.

This ISO document addresses the robot as an incomplete machine.

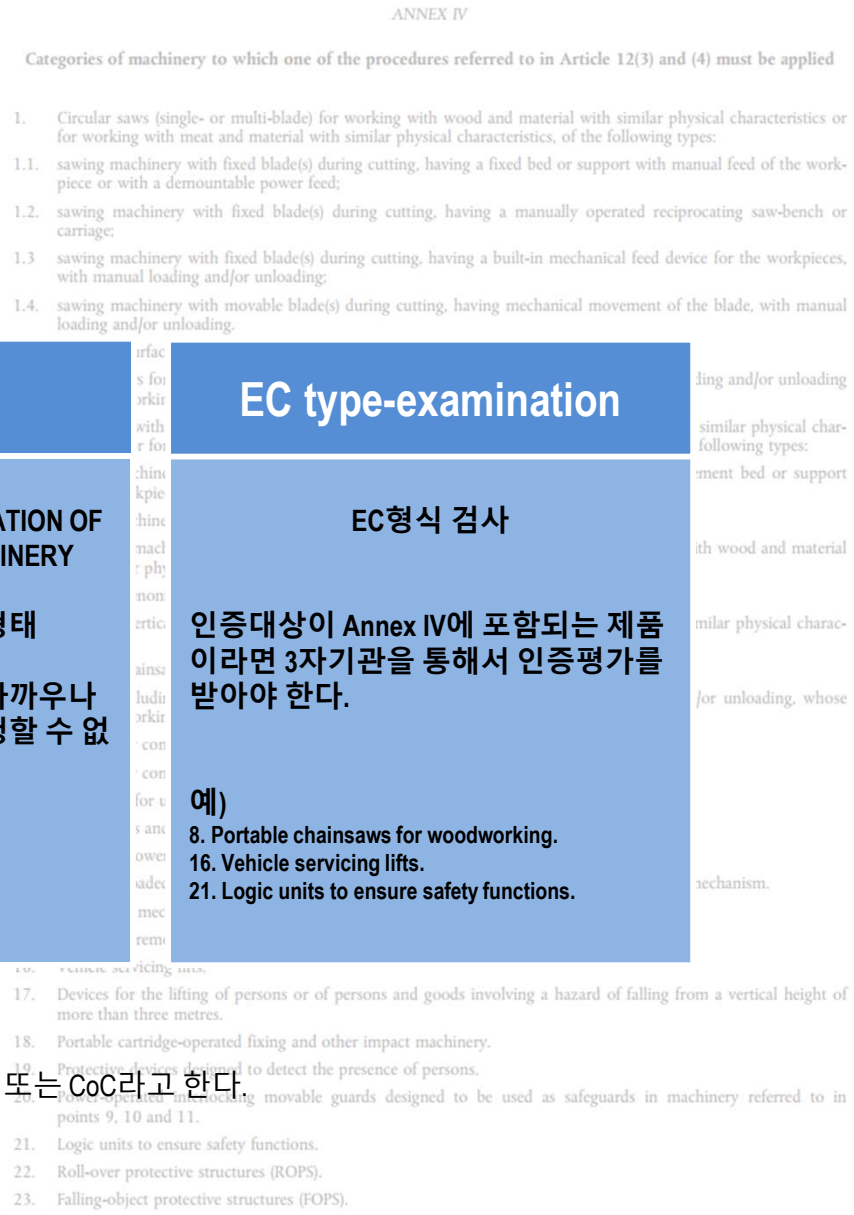
This ISO document is not applicable to the following uses and products:

- underwater;
- Law enforcement;
- military (defence);
- airborne and space robots, including outer space;
- medical robots;
- healthcare robots;
- prosthetics and other aids for the physically impaired
- service robots, which provide a service to a person and as such the public can have access;
- consumer products as this is household use to which the public can have access;
- lifting or transporting people;
- mobile platforms;
- tele-operated manipulators;

CE DoC? DoI? EC Type-examination?

Machinery Directive 2006/42/EC (MD) : 인증 형태

DoC	DoI	EC type-examination
DECLARATION OF CONFORMITY **기계류에 대한 인증 형태** **기계류란 인간이나 동물의 힘이 직접 가해지지 않는 구동장치에 설치되거나 설치되도록 설계되고, 최소 하나 이상의 이동 가능한 연결부품 또는 구성품으로 구성되어 특정 용도를 위해 연결된 조립체를 의미한다. 외** e.g. ISO 10218-2	**DECLARATION OF INCORPORATION OF PARTLY COMPLETED MACHINERY** **부분품 기계류에 대한 인증 형태** **부분품 기계류란, 기계류에 가까우나 그 자체로는 특정 용도를 수행할 수 없는 조립체를 의미한다.** e.g. ISO 10218-1	**EC형식 검사** **인증대상이 Annex IV에 포함되는 제품이라면 3자기관을 통해서 인증평가를 받아야 한다.** **예)** **8. Portable chainsaws for woodworking.** **16. Vehicle servicing lifts.** **21. Logic units to ensure safety functions.**



ANNEX IV

Categories of machinery to which one of the procedures referred to in Article 12(3) and (4) must be applied

1. Circular saws (single- or multi-blade) for working with wood and material with similar physical characteristics or for working with meat and material with similar physical characteristics, of the following types:
1.1. sawing machinery with fixed blade(s) during cutting, having a fixed bed or support with manual feed of the work-piece or with a demountable power feed;
1.2. sawing machinery with fixed blade(s) during cutting, having a manually operated reciprocating saw-bench or carriage;
1.3 sawing machinery with fixed blade(s) during cutting, having a built-in mechanical feed device for the workpieces, with manual loading and/or unloading;
1.4. sawing machinery with movable blade(s) during cutting, having mechanical movement of the blade, with manual loading and/or unloading.

17. Devices for the lifting of persons or of persons and goods involving a hazard of falling from a vertical height of more than three metres.
18. Portable cartridge-operated fixing and other impact machinery.
19. Protective devices designed to detect the presence of persons.
20. Logic units to ensure safety functions which provide movable guards designed to be used as safeguards in machinery referred to in points 9, 10 and 11.
21. Logic units to ensure safety functions.
22. Roll-over protective structures (ROPS).
23. Falling-object protective structures (FOPS).

Note. 3자 승인기관이 DoC, DoI의 인증을 기관의 승인서를 발행한 것을 AoC 또는 CoC라고 한다.

DoC : Declaration of Conformity

DoI : Declaration Of Incorporation

AoC : Attestation of Conformity

CoC : Certificate of Conformity

2. 참고문헌, 3. 용어, 정의 및 약어

ISO 10218-1:2011

2 Normative references

3 Terms and definitions

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.

ISO/DIS 10218-1:2021

2 Normative references

3 Terms, definitions and abbreviations

[SOURCE: ISO 12100:2010, 3.28.5, modified — Note 1 to entry has been deleted.]

3.1.11 Verification and validation

3.1.11.1
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or *application* (3.1.1.6) have been fulfilled

Note 1 to entry: Validation determines if the specification accomplishes what was intended, e.g. that a specified limit is acceptable for its purpose. Validation includes functional testing.

[SOURCE: ISO 9000:2015, 3.8.13, modified — Note 1 to entry has been added.]

3.1.11.2
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification determines if the design meets its specification, e.g. through review, measurement, analysis, or inspection.

[SOURCE: ISO 9000:2015, 3.8.12, modified — Note 1 to entry has been added.]

3.2 Abbreviated terms

Abbreviated term	Term	
3P	3-position <3-position *enabling device*>	5.2.9.1, 5.5.3.2, 5.5.3.3, Annex C, Annex G
Cat	Category	5.3.3, Annex C, Table D.1
Class	Classification	5.1.17, Table 1, 5.2.8.2.2, 5.2.9.1, 5.3.3, 5.7.1, 5.9.1, h), 7.5.12.7, Annex C, Table C.1, Annex E, Annex G
EMC	Electromagnetic Compatibility	5.3.7, Annex G
EMI	Electromagnetic Interference	5.3.7, Annex A, Annex G
F_{MPM}	Force maximum per manipulator	5.1.17.c), Table 1, Annex E
HFT	Hardware Fault Tolerance	5.3.3, 7.5.12.1, Annex C, Table D.1, Annex G
HGC	Hand-Guided Control	Introduction, 3.1.1.2, 5.2.9.1, 5.5.1.2, 5.10.2, Annex C, Annex G
M	Total mass of moving parts of the manipulator	5.1.17, Table 1
m_L	Effective mass of the payload for the robot application (specified maximum payload of the application)	5.1.17, Table 1

3 용어, 정의 및 약어 – 3.10 산업용 로봇

ISO 10218-1:2011

3.10 industrial robot
automatically controlled, re-programmable 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.

ISO/DIS 10218-1:2021

3.1.1.2 industrial robot, robot
automatically controlled, re-programmable multipurpose manipulator(s), programmable in three or more axes, which can be either fixed in place or fixed to a mobile platform for use in automation applications in an industrial environment

NOTE 1 The industrial robot includes:
– the manipulator(s), including robot actuators controlled by the robot control;
– the robot control;
– the means by which to teach or program the robot, including any communications interface(hardware and software).

NOTE 2 to entry: Industrial robot includes any auxiliary axes that are integrated into the kinematic solution.

NOTE 3 to entry: The following are considered industrial robots;
– the manipulating portions(s) of mobile robots, where a mobile robot consists of a mobile platform with an integrated manipulator or robot
– robots with hand-guided controls(HGC);
– robots with power and force limited (PFL) functionality;
– robots with built-in speed and separation monitoring(SSM) functionality.

robots with hand-guided controls(HGC);

The method consists in allowing the operator to move the robot by hand-operated device to transmit motion commands.

The robot system needs to have the following:

- monitored-speed(5.5.2.2);
- soft axis and space limiting(5.7.4);
- monitored-standstill(5.4.3.3);
- hold-to-run(5.10.2c) and Annex C.

Safety Function

Monitored-speed which monitored-speed shall be capable of being configures during integration in accordance with ISO 10218-2;

robots with built-in speed and separation monitoring(SSM) functionality

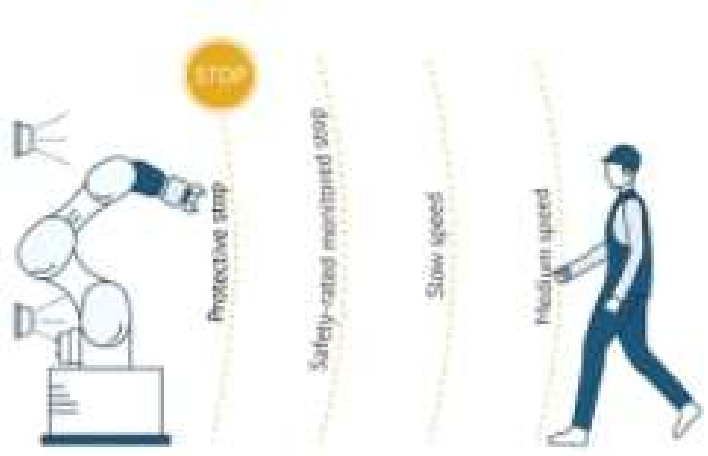
Speed and separation monitoring
: is increasing safety by specifying the minimum protective distance between a robot and an operator.
: the robot and operator may move concurrently within the safeguarded space.

Collaborative applications using SSM can use a SPE that detects entrance into a safeguarded space or that monitors the presence of any person.

When a presence-sensing device like a laser scanner or a safety radar, is used to define the detection zones, the size and location of the detection zones shall be set so that the separation distance is maintained, even during detection zone transitions.

The SSM can be provided by the robot controller or by an external protective device, or by a mixture of both.

- reduce robot speed(e.g. down to speed zero); and/or
- change pose(s) and/or trajectory of the robot.
- failure to maintain the separation distance, shall result in, a protective stop.



Speed and separation monitoring

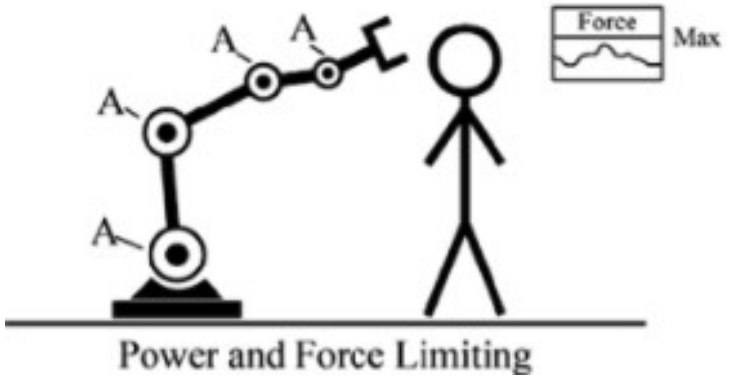
robots with power and force limited (PFL) functionality;

Accomplishing PFL can be by inherently safe design or safety functions.

Where PFL is achieved by inherently safe design, the limits shall be fixed, not adjustable and not configurable.

Where PFL is achieved by safety functions,

a) the power and force limit values shall be adjustable; and
b) power and force limit values shall not be exceeded during operating or when power and force limit values are exceeded, a protective stop shall be initiated; and
c) the following safety functions shall be provided:
   1) monitored-speed (5.5.2.2);
   2) soft axis and space limiting (5.7.4);
   3) monitored standstill (5.4.3.3).



Power and Force Limiting

4. 위험성 평가

ISO 10218-1:2011

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.

ISO/DIS 10218-1:2021

4 Risk Assessment

A robot manufacturer shall perform a risk assessment in accordance with ISO 12100.

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

Note 2 Annex A contains a list of hazards that can be present with robots.

For robot system, robot application and robot cell requirements, see ISO 10218-2:2021.

Annex A
(informative)
List of significant hazards

Table A. 1 provides a list of significant hazards for robots before integration into a system.

Note See ISO 10218-2, Annex A for hazards of the robot system, robot application and robot cell.

Note The list in Table A. 1 is derived from ISO 12100:2010, Table B1.

Table A. 1— List of significant hazards

No.	Type or group	Example of hazards		Corresponding requirement	
		Origin	Potential consequences		
1	Mechanical hazards	— movements (normal or unexpected) of any part of the manipulator(including back) — movements (normal or unexpected) of additional axis — movement of robot parts — rotational motion of any axes — failure of a safety function to perform as expected — loose clothing, long hair — between joints of the manipulator — unintended motion or activation of auxiliary axes unexpected release of potential energy from stored sources	— crushing — shearing — cutting or severing — entanglement — drawing-in or trapping — impact — stabbing or puncture — friction, abrasion — high-pressure fluid/gas injection or ejection	4 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8	Risk assessment Robot design Robot controls Safety functions Robot stopping functions Other safety functions Simultaneous motion Limiting robot motion Movement without drive power
2	Electrical hazards	— contact with live parts — confusion of various voltages — contact with discrete components in the electrical (electronic) circuitry, i.e. capacitors — exposure to arc flash	— electric shock — burn or scald — inhalation of toxic fume — eye damage by electric spark — influence on pacemaker	4 5.1 5.2 5.3	Risk assessment Robot design Robot controls Safety functions
3	Thermal hazards	— hot surfaces — cold surfaces	— burns — fire, explosion — radiation from heat sources — inhalation of toxic fumes — dehydration	4 5.1	Risk assessment Robot design
4	Vibration hazards	— loosening of connections, fasteners, components resulting		4 5.1	Risk assessment Robot design

5. 설계 및 보호 조치 – 5.1 로봇 설계

ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

5 Design and protective measures
5.1 Robot design
5.1.1 General
5.1.2 Materials, mechanical strength and mechanical design
5.1.3 Handling, lifting and transportation
5.1.4 Packaging
5.1.5 Stability
5.1.6 Temperature and fire risks
5.1.7 Special equipment
5.1.8 Position holding
5.1.9 Auxiliary axis (axes)
5.1.10 Power loss or change
5.1.11 Component malfunction
5.1.12 Hazardous energy
5.1.13 Electrical, pneumatic and hydraulic parts
5.1.14 Tool centre point (TCP) setting
5.1.15 Payload setting
5.1.16 Cybersecurity
5.1.17 Robot class

5.3.5 Parametrization of safety functions

ISO/DIS 10218-1:2021

5.1.16 Cybersecurity

A cybersecurity assessment of the robot shall be carried out. If the assessment has identified that a threat can result in (safety) risk(s), measures to support cybersecurity shall be provided.

These measures shall include the means to prevent unauthorized access to the robot, its hardware, software, configuration data and the industrial robot application program.

The means to prevent unauthorized access can include providing the following:

- Ability to disable access to communications ports, e.g. TCP/UDP port;
- Ability to change the TCP/UDP port number, e.g. logical connection;
- Authenticated protection of the safety configuration;
- Ability to change the default usernames and passwords;
- Use of encrypted and authenticated protocols.

Note 1 For further information, see ISO/TR 22100-4:2018.
Note 2 For information and requirements about security of industrial automation and control systems, see IEC 62443 series and IEC TR 63074:2019.

Note. ISO/TR 22100-4:2018 Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects
Note. IEC TR 63074:2019 Safety of machinery - Security aspects related to functional safety of safety-related control systems
Note. IEC 62443 Series Industrial communication networks - Network and system security

IEC 62443 Series

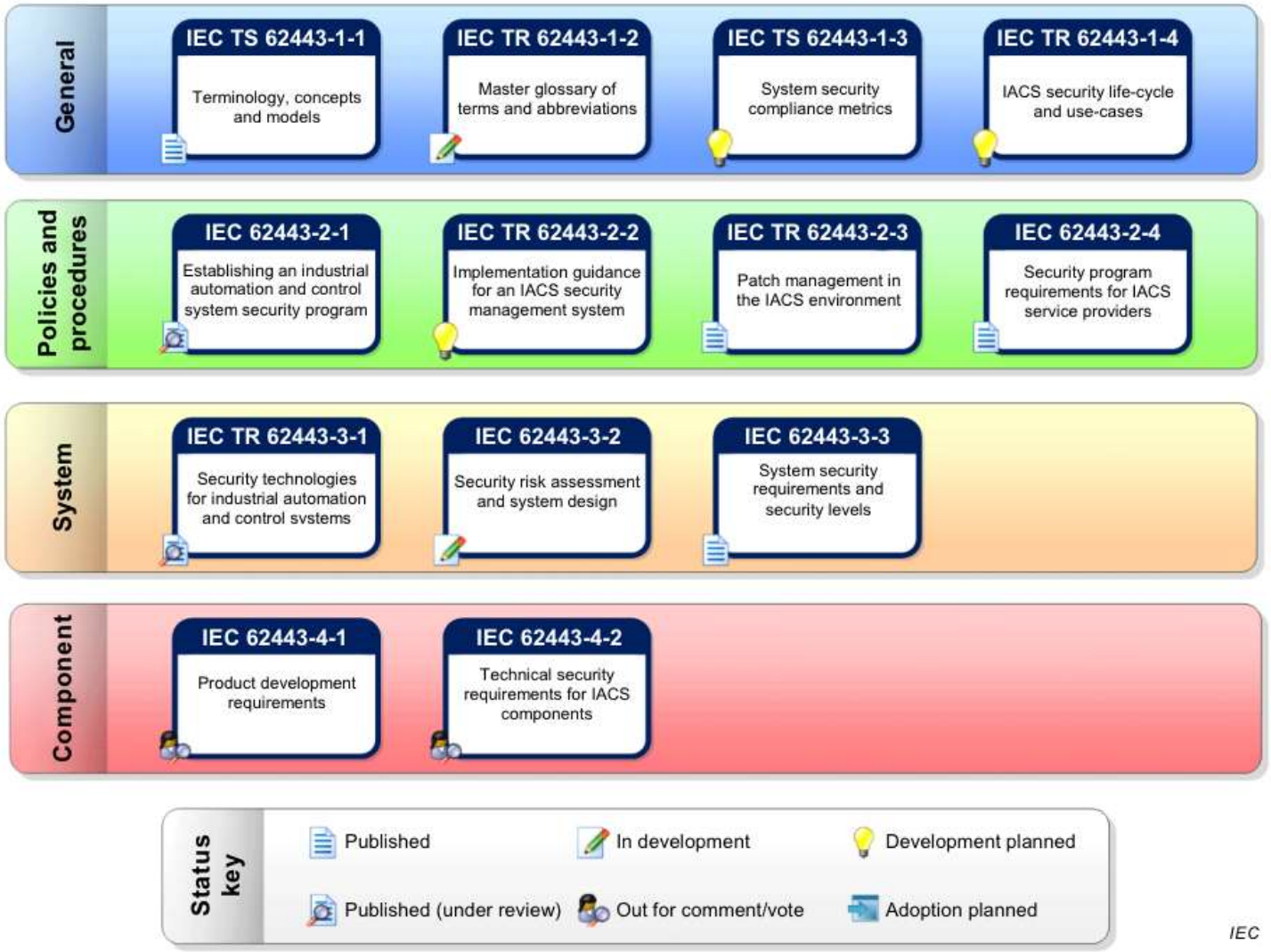


Figure 1 – Parts of the IEC 62443 series

ISO/DIS 10218-1:2021

Table 1: Robot class

Robot Class	Total mass per manipulator (M) [kg]	Maximum force* per manipulator (F_{MPM}) [N]	Maximum speed [mm/s]
I	10 kg and under	50 and under	250 mm/s and under
II	Over 10 kg	Over 50	Over 250 mm/s

NOTES:

M is the total mass of the moving parts of the manipulator.

See Annex E for ***M*** test methodology.

If multiple manipulators are provided, ***M*** is per manipulator.

See reference [65] FP 0317 (Mainz Study)for derivation of the 50 N maximum force per manipulator value **(F_{MPM})**.

* Maximum force is with a manipulator minimum contact area of 0.5cm² [65] .
Reference [65] FP 0317 (Mainz Study): the third quartile of the 29 body parts that were considered (except head and neck) study FP 0317 shows that forces of around 50N are below pain onset independent of pressure (except needles and knives). Therefore, the 50 N limit can be applied as a general borderline between robot class I and II.

Class 1 로봇일 경우 규격에서 요구하는 Safety Fucntion이 제외 or 낮은 등급을 요구한다.

예1) 5.2.8.2.2 Reduced-speed 제외 가능

예2) 5.7 Limiting robot motion 선택사항…

5. 설계 및 보호 조치 – 5.2 로봇 컨트롤

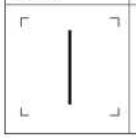
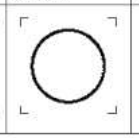
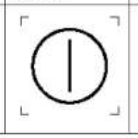
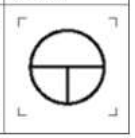
ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

5.2 Robot controls
5.2.1 General
5.2.2 Protection from unexpected start- up
5.2.3 Singularity
5.2.4 Interlocking functions - ISO 14119
5.2.5 Status indication and warning devices
5.2.6 Labelling

Table 2 – Symbols for actuators (Power)

Power			
ON	OFF	ON/OFF (push on-push off)	ON (hold-to-run)
IEC 60417-5007 (2002-10)	IEC 60417-5008 (2002-10)	IEC 60417-5010 (2002-10)	IEC 60417-5011 (2002-10)
			

5.2.7 Single point of control
5.2.7.1 General
5.2.7.2 Direct control
5.2.7.3 External control
5.2.8 Modes
5.2.8.2.1 General
5.2.8.2.2 Reduced-speed
5.2.8.2.3 High-speed
5.2.8.3 Selection, activation and change of the operating mode
5.2.9 Means of controlling the robot
5.2.9.1 General
5.2.10 Means of initiating automatic operation

ISO/DIS 10218-1:2021

5.2.9.3 Cableless or detachable teach pendant(s)

Teach pendants that have no cables connecting to the robot, or where the cable can be detached, the following shall be fulfilled:

a) visual indication shall be provided to show that the teach pendant is active, e.g. at the teach pendant display;
b) visual indication shall be provided to indicate which robot the teach pendant is connected (e.g. at the teach pendant display) at the robot;
c) loss of safety-related communication shall result in a protective stop for all robots being controlled when in manual mode(s).
d) restoration of safety-related communication shall not restart robot motion without a separate deliberate action;
e) their emergency stop device(s) shall be in accordance with ISO 13850:2015, 4.3.8;
f) an unambiguous means shall be provided to connect and disconnect robot control from the teach pendant (e.g. a positive action by the operator);
g) safety-related wireless communication (e.g. radio, infra-red) of teach pendants shall be in accordance with IEC 62745; and
h) a means shall be provided to prevent confusion between active and inactive emergency stop devices, (e.g. stowage or instructions for providing stowage).

4.3.8 When emergency stop devices are installed on detachable or cableless operator control stations (e.g. pluggable portable teaching pendants), at least one emergency stop device shall be permanently available (e.g. in a fixed position) on the machine.

In addition, at least one of the following measures shall be applied to avoid confusion between active and inactive emergency stop devices:

— device colour changing through illumination of the active emergency stop device;

— automatic (self-actuating) covering of inactive emergency stop devices; where this is not practicable, manually-applied covering may be used, provided that the cover remains attached to the operator control stations;

— provision of proper storage for detached or cableless operator control stations.

The instructions for use of the machine shall state, which measure has been applied in order to avoid confusion between active or inactive emergency stop device(s). The correct operation of this measure shall be explained.

Note. IEC 62745:2017 Safety of machinery - Requirements for cableless control systems of machinery

5. 설계 및 보호 조치 – 5.3 안전기능

ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

5.3 Safety functions
5.3.1 General
5.3.2 Functional safety standards
5.3.3 Performance
5.3.4 Failure or fault detection
5.3.5 Parametrization of safety functions
5.3.6 Communications
5.3.7 Electromagnetic compatibility (EMC)

5. 설계 및 보호 조치 – 5.3 안전기능

ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

5.3 Safety functions
5.3.1 General
5.3.3 Performance

The minimum functional safety performance for safety functions shall be at least one of the following:

- Performance Level (PL) d, category 3 architecture in accordance with ISO 13849-1:2015;
or
- Safety Integrity Level (SIL) 2, hardware fault tolerance (HFT) = 1 with a mission time of not less than 20 years, in accordance with IEC 62061:2015;
or
- Performance Level (PL) d or SIL 2, with a PFH D less than 4.43 x 10-7/h.

Note. PFHD average probability of dangerous failure per hour

5. 설계 및 보호 조치 – 5.3 안전기능

ISO 13849-1

Table 2 — Performance levels (PL)

PL	Average probability of dangerous failure per hour (PFH_D) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

Table 4 — Mean time to dangerous failure of each channel ($MTTF_D$)

$MTTF_D$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years

NOTE 1 The choice of the $MTTF_D$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $MTTF_D$ value of each channel less than three years is not expected to be found for real SRP/CS since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $MTTF_D$ value of each channel greater than 100 years is not acceptable because SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_D$ of each channel values to a maximum of 100 years refers to the single channel of the SRP/CS which carries out the safety function. Higher $MTTF_D$ values can be used for single components (see Table D.1).

NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.

Table 5 — Diagnostic coverage (DC)

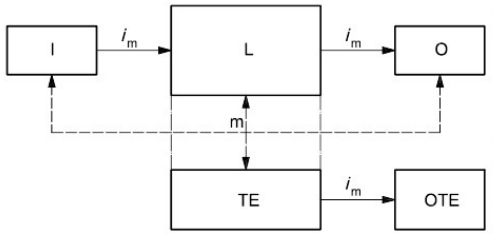
DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g. IEC 61508) dealing with diagnostic coverage of tests. Investigations show that (1 - DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 - DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called "none". A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.

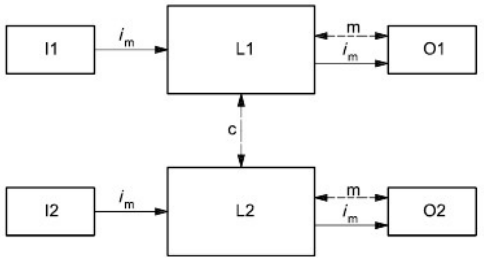
Table 3 — Relationship between performance level (PL) and safety integrity level (SIL)

PL	SIL (IEC 61508–1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3



Key
i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE
Dashed lines represent reasonably practicable fault detection.

Figure 10 — Designated architecture for category 2

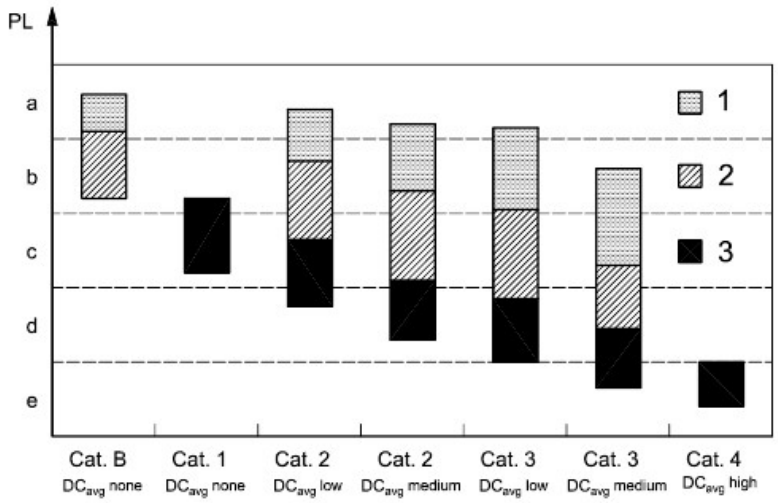


Key
i_m interconnecting means
c cross monitoring
I1, I2 input device, e.g. sensor
L1, L2 logic
m monitoring
$O1, O_2$ output device, e.g. main contactor
Dashed lines represent reasonably practicable fault detection.

Figure 11 — Designated architecture for category 3

5. 설계 및 보호 조치 – 5.3 안전기능

ISO 13849-1



Key

PL performance level

1 $MTTF_D$ of each channel = low

2 $MTTF_D$ of each channel = medium

3 $MTTF_D$ of each channel = high

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL

Table 6 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	1	2	2	3	3	4
DC_{avg}	none	none	low	medium	low	medium	high
$MTTF_D$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

possible, but very hard!

IEC 62061

Table 3 – Safety integrity levels: target failure values for SRCFs

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 7 – Probability of dangerous failure

Category	Hardware fault tolerance	DC	PFH_D threshold values (per hour) that can be claimed for the subsystem
	It is assumed that subsystems with the stated category have the characteristics given below.		PFH_D ($MTTF_{subsystem}$, T_{test}, DC) (See Note 1)
1	0	0 %	To be provided by supplier or use generic data (see Annex D)
2	0	60 % – 90 %	$\geq 10^{-6}$
3	1	60 % – 90 %	$\geq 2 \times 10^{-7}$
4	>1	60 % – 90 %	$\geq 3 \times 10^{-8}$
	1	> 90 %	$\geq 3 \times 10^{-8}$

NOTE 1 The PFH_D threshold value is a function of the subsystem MTTF (to be derived by the subsystem manufacturer or from relevant component data handbooks), test/check cycle time as specified in the safety requirements specification (this information is also required for subsystem validation in accordance with ISO 13849-2, 3.5) and the diagnostic coverage as shown in this table (these values are based on the requirements of the categories described in ISO 13849-1).

NOTE 2 Category B in accordance with ISO 13849-1 cannot be considered sufficient to achieve SIL 1.

5. 설계 및 보호 조치 – 5.3 안전기능

ISO/DIS 10218-1:2021

52 **Annex C**
53 (normative)
54 **Safety functions**

55 Table C.1 details the robot safety functions that shall be in accordance with 5.3.3, except Class I
56 robot (5.1.17) safety functions which may be at least PLb or SIL 1. Table C.2 contains the safety
57 functions which may be provided with different functional safety performance.

58 Note The robot application can require safety function(s) meeting PLe (Cat 3 or Cat 4) or SIL 3
59 (HFT 1).

70 **Table C. 1 — Robo**

Clause	Mandatory OR Conditional OR Optional[1]	Safety Function Name	Possible Ti
5.1.8	**Optional**	**position holding**	Robot powe the rol
5.2.4	**Conditional** if interlocking functions are provided	**interlocking**	Opening or re [e.g
5.2.8.2.1	**Mandatory**	**manual mode, general**	Change of mo
5.2.8.2.2	**Mandatory** for Class II robots	**manual mode, reduced-speed**	Manual mod se
5.2.8.2.3	**Conditional** required for high-speed manual mode	**manual mode, high-speed**	Manual mode,
5.2.8.3	**Conditional** required if there is a change in active risk reduction with mode activation	**mode activation**	Activation of
5.4.3	**Mandatory**	**protective stop**	Internal safet Actuation of a which is co protecti
5.4.3.3	**Conditional** required for • HGC (5.10.2) without PFL • PFL by safety functions (5.10.4) • Simultaneous motion (5.6)	**monitored standstill**	Triggering of a protective command, th fu

Clause	Mandatory OR Conditional OR Optional[1]	Safety Function Name	Possible Triggering Event	Intended Re
5.5.1.1	**Mandatory**	**start interlock**	Energy supply is switched on OR After an interruption and restoration of power	No motion until there is
5.5.1.2	**Mandatory**	**restart interlock**	Change of mode (5.5.2.2) OR After a protective stop while in manual mode	No motion until there is
5.5.2.1	**Mandatory**	**reduced-speed**	Selecting manual mode	Protective stop (5.4.3) i exceeded Prevent the robot from limit by slowing or stopp stop) before the limit
5.5.2.2	**Conditional** required for • HGC (5.10.2) • PFL by safety functions (5.10.4) • See also Position holding (5.1.8)	**monitored-speed**	Robot exceeds the configured limit. Continuous monitoring until reaching the point where a stop shall be initiated so that the configured limit will not be exceeded	Protective stop (5.4.3) i exceeded Prevent the robot from limit by slowing or stopp stop) before the limit
5.5.3	**Mandatory**	**enabling device function**	Release or compression of the 3P enabling device	Stop and prevent robot operation of other pro hazards are controlled
5.6	**Conditional** Required for simultaneous control	**restriction of robot selection**	Selection of robots to be under simultaneous control	Only robots in the same selected for simultan AND Any robot not selected monitored stan
5.7.3	**Conditional** required if this is the means of axis limiting	**electro-mechanical axis limiting**	Exceed the limit Reach the point where a stop shall be initiated so that the limit will not be exceeded	Protective stop Protective stop
5.7.4	**Conditional** required for • HGC (5.10.2) • PFL (5.10.4) by safety functions	**soft axis and space limiting**	Exceed the limit. Not exceed the limit(s) Reach the point where a stop shall be initiated so that the limit will not be exceeded	Protective stop (Prevent the robot from exceeding the set limit by slowing or protective stop (5.4.3)
5.7.5	**Optional**	**dynamic limiting**	Exceed the limit. Not exceed the limit(s) Reach the point where a stop shall be initiated so that the limit will not be exceeded	Protective stop (5.4.3) Prevent the robot from exceeding the set limit by slowing or a protective stop (5.4.3)
5.10.2	**Conditional** required for robots with HGC	**hold-to-run control**	Release of hold-to-run control device	Protective stop (5.4.3)

Clause	Mandatory OR Conditional OR Optional[1]	Safety Function Name	Possible Triggering Event	Intended Result
5.10.3	**Conditional** required for robots with SSM safety functions/ capabilities	**speed and separation monitoring (SSM)**	Position of the human relative to the robot is such that the robot will not be able to stop before coming in contact with the human	Change robot speed (e.g. down to speed zero) Change pose(s) and/or trajectory of the robot
5.10.4	**Conditional** required for PFL robots by safety functions	**monitored power and force limiting**	Exceeds the set limit(s) Monitors to prevent exceeding the limit(s)	**One or more of the following:** • Protective Stop (5.4.3) . • Stop the robot, then move to a position where the limit is not exceeded. Then, cause a protective stop (5.4.3)or a monitored standstill (5.4.3.3) • Stop the robot, hold position (monitored standstill). It is permitted for the robot to automatically go into a force and torque-free state
5.1.8 5.4.3.3 Annex I.7.1	**Optional**	**monitored position**	Protective device, manual control device, safety function Robot is in a Category 2 stop (monitored standstill) at the configured position	**All of the following:** 1) Robot moves to configured position within specified time; 2) Monitored standstill (5.4.3.3); 3) Robot does not move from the configured position. Optionally, a safety output changes state. Robot does not move from the configured position
7.5.5 Annex H Annex I I.7.2	**Optional**	**stopping time limiting**	Exceed the limit. Reach the point where a stop shall be initiated so that the limit shalll not be exceeded	Protective stop (5.4.3) Prevent the robot from exceeding the set limit by slowing the robot or by a protective stop (5.4.3)
7.5.5 Annex H Annex I I.7.2	**Optional**	**stopping distance limiting**	Exceeding the limit. Reach the point where a stop shall be initiated so that the limit shall not be exceeded	Protective stop (5.4.3) Prevent the robot from exceeding the set limit by slowing the robot or by a protective stop (5.4.3)

1 Mandatory: shall be provided.
Conditional: shall be provided if certain conditions are met according to referenced clause
Optional: not required and can be provided as an option.

ISO/DIS 10218-1:2021

5.3 Safety functions

5.3.5 Parametrization of safety functions

Note Correct operation of safety function is based on proper and reliable setting of a safety-related parameter(s) used in the safety function(s), especially for safety-related application software.

5.3.6 Communications

Table 2: Robot network – countermeasure requirements

Transmission Category	Repetition	Deletion	Insertion	Resequence	Corruption	Delay	Masquerade
1	+	+	+	+	++	+	-
2	++	++	++	+	++	++	-
3	++	++	++	++	++	++	++

NOTE The term: "masquerade" means that the true source of a message is not correctly identified. For example, a message from a non-safety element is incorrectly identified as a message from a safety element. [Source: IEC 61508-2:2010, 7.4.11.1]

Key

-	Threat can be neglected.
+	Threat exists, but rare; weak countermeasures sufficient.
++	Threat exists; strong countermeasures required.

IEC 61784-3

Table 1 – Overview of the effectiveness of the various measures on the possible errors

Communication errors	Safety measures							
	Sequence number (see 5.4.2)	Time stamp (see 5.4.3)	Time expectation (see 5.4.4)	Connection authentication (see 5.4.5)	Feedback message (see 5.4.6)	Data integrity assurance (see 5.4.7)	Redundancy with cross checking (see 5.4.8)	Different data integrity assurance systems (see 5.4.9)
Corruption (see 5.3.2)					X [d]	X	Only for serial bus [c]	
Unintended repetition (see 5.3.3)	X	X					X	
Incorrect sequence (see 5.3.4)	X	X					X	
Loss (see 5.3.5)	X				X		X	
Unacceptable delay (see 5.3.6)		X	X [b]					
Insertion (see 5.3.7)	X			X [a]	X		X	
Masquerade (see 5.3.8)				X	X			X
Addressing (see 5.3.9)				X				

Note. IEC 61784-3 Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

5. 설계 및 보호 조치 – 5.4 로봇 정지 기능

ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

5.4 Robot stopping functions
5.4.1 General
5.4.2 Emergency stop
5.4.3 Protective stop
5.4.4 Other stop

5.5 Other safety functions
5.5.1 Start and restart interlocking
5.5.2 Speed limit(s) monitoring
5.5.3 Enabling function

5.6 Simultaneous motion

5. 설계 및 보호 조치 – 5.4 로봇 정지 기능

ISO 10218-1:2011

5.5 Robot stopping functions
5.5.1 General

Table 1 — Comparison of emergency and protective stops

Parameter	Emergency stop	Protective stop
Location of initiation means	Operator has quick, unobstructed access	For protective devices, the location is determined by the minimum (safe) distance formulas described in ISO 13855
Initiation	Manual	Manual, automatic or may be automatically initiated by a safety-related function
Safety-related control system performance	Shall meet performance requirement in 5.4	Shall meet performance requirement in 5.4
Reset	Manual only	Manual or automatic
Use frequency	Infrequent	Variable; from every operation to infrequent
Purpose	Emergency	Safeguarding or risk reduction
Effect	Remove energy sources to all hazards	Safely control the safeguarded hazard(s)

ISO/DIS 10218-1:2021

5.4 Robot stopping functions
5.4.1 General

5

Table 1 — Comparison of the stop functions

Parameter	Other stop	Emergency stop	Protective stop
Purpose	Stopping, on/off	Emergency	Safeguarding
Effect	Stop the robot or its hazardous functions, then remove energy to actuators	Remove energy sources to all hazards	Safely control the safeguarded hazard(s) in accordance with either 5.4.3.1 (protective stop, general) or 5.4.3.3 (monitored standstill safety function)
Initiation	Manual	Manual	Manual, automatic or may be automatically initiated by a safety function
Stop category in accordance with IEC 60204-1	0 or 1	0 or 1	0, 1 or **2**
Safety-related control system performance	Not required	See performance requirement in Annex C.2	See performance requirement in 5.3.
Reset	Not appliable	Manual only	Manual or automatic *Can vary with each safety function that initiates a protective stop*
Use frequency	Frequent	Infrequent	Variable: from on-going (i.e. internal robot safety functions) to infrequent

5. 설계 및 보호 조치 – 5.7 로봇 모션 제한, 5.8 구동 전원 없이 이동, 5.9 레이저 및 레이저 장비, 5.10 협업 애플리케이션을 위한 기능

ISO 10218-1:2011

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

ISO/DIS 10218-1:2021

5.7 Limiting robot motion
5.7.1 General
5.7.2 Mechanical axis limiting devices
5.7.3 Electro-mechanical axis limiting devices
5.7.4 Soft axis and space limiting
5.7.5 Dynamic limiting

5.8 Movement without drive power

5.9 Lasers and laser equipment

5.10 Capabilities for collaborative applications
5.10.1 General
5.10.2 Hand-guided controls (HGC)
5.10.3 Speed and separation monitoring (SSM)
5.10.4 Power and force limiting (PFL) by inherent design or safety function(s)

6. 안전 요구 사항 및 보호 조치의 검증

ISO 10218-1:2011

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

Annex F
(normative)

Means of verification of the safety requirements and measures

Table F.1 lists specific performance requirements that are identified as essential to the safety of the robot that shall be verified or validated, or both.

See 6.3 for notes on using this table.

Table F.1 — Means of verification of the safety requirements and measures

Subclause	Applicable safety requirements and/or measures	Verification and/or validation method (see 6.2)						
		A	B	C	D	E	F	G
5.2	**General requirements**							
5.2.1	Fixed or moveable guards are installed to prevent exposure to hazards such as shafts, gears, drive belts, or linkages	X			X			
5.2.1	Fixed guards intended to be removed for routine service have captive hardware		X					X
5.2.1	Movable guards are interlocked with the hazardous movements in such a way that the hazardous movements come to a stop before the hazards can be reached		X	X	X	X		
5.2.1	The safety-related control system performance of an interlocking system conforms to 5.4					X		
5.2.2	Loss of, or unstable power does not result in a hazard		X		X	X		
5.2.2	Re-initiation of power does not initiate motion		X		X	X		
5.2.2	Loss or change of electrical, hydraulic, pneumatic or vacuum power does not result in a hazard		X		X			
5.2.2	Additional protective measures are taken to protect against hazards not protected by design	X						X
5.2.2	Unprotected hazards of the expected use are identified in the information for use						X	X
5.2.3	Robot components are designed, constructed, secured, or contained so that hazards caused by breaking or loosening, or releasing stored energy are minimized	X	X		X			
5.2.4	Capability to lock or secure in the de-energized position isolated hazardous energy to the robot	X	X	X		X		
5.2.5	Means provided for the controlled release of stored hazardous energy		X			X		X
5.2.5	A label is affixed to identify the stored energy hazard	X						
5.2.6	Expected effects of electromagnetic interference (EMI), radio frequency interference (RFI) and electrostatic discharge (ESD) do not initiate hazardous motion		X	X		X		
5.2.7	The robot electrical equipment is designed and constructed in accordance with the relevant requirements of IEC 60204-1	X	X			X		X

ISO/DIS 10218-1:2021

6 Verification and validation of safety requirements and protective measures
6.1 General
6.2 Verification and validation .

Annex G
(normative)
Means of verification and validation of the design and protective measures

Table G.1 lists specific performance requirements that shall be verified or validated, or both. Table G.1 lists acceptable methods for verification, validation or both of each listed requirements from Clause 5.

Verification and validation, in accordance with Clause 5, shall be performed using one or more of the below methods.

A visual inspection;

B practical test(s);

C measurement;

D observation during operation;

E review of schematics, circuit diagrams and design material;

F review of risk assessment;

G review of specifications and information for use.

Table G. 1 — Means of verification and validation of the design requirements and protective measures in Clause 5

Clause	Applicable design requirements and/or protective measures	Method						
		A	B	C	D	E	F	G
5.1	**Robot Design**							
5.1.1	In accordance with the principles of ISO 12100 for identified hazards				X		X	X
5.1.2	**Materials, mechanical strength, and mechanical design**							
5.1.2.1	Failures due to fatigue and wear do not lead to a hazardous situation for intended lifecycle	X	X	X	X			X
5.1.2.2	**Materials**							
5.1.2.2	Appropriate for the intended use		X	X				X
5.1.2.2	Do not endanger persons' safety or health				X		X	
5.1.2.2	Are non-toxic in all reasonably foreseeable conditions of use		X	X				X
5.1.2.2	Are not prone to brittle fracture, excessive deformation, or emission of toxic or flammable fumes		X	X				X
5.1.2.2	Retain their properties in the reasonably foreseeable range of climatic and workplace conditions, including temperature variations or sudden changes	X	X	X	X			X
5.1.2.1	Where fluids are used, machinery is designed and constructed to prevent risks due to filling, use, recovery or draining		X	X			X	X

7. 사용 정보

ISO 10218-1:2011

7 Information for use
7.1 General
7.2 Instruction handbook
7.3 Marking

ISO/DIS 10218-1:2021

7 Information for use
7.1 General
7.2 Signals and warning devices
7.3 Marking
7.4 Signs (pictograms) and written warnings
7.5 Instruction handbook
- 7.5.1 General
- 7.5.2 Identification
- 7.5.3 Intended use
- 7.5.4 Installation
- 7.5.5 Stopping
- 7.5.6 Commissioning and programming
- 7.5.7 Operation and setting
- 7.5.8 Singularity
- 7.5.9 Hazardous energy
- 7.5.10 Movement without drive power
- 7.5.11 Cybersecurity
- 7.5.12 Functional safety
- 7.5.13 Teach pendants
- 7.5.14 Integration into a robot system
- 7.5.15 Maintenance
- 7.5.16 Protection against electrical shock
- 7.5.17 Abnormal and emergency situations
- 7.5.18 Handling, lifting and transportation

7.5.12.1 General

7.5.12.2 Software and safety-related parametrization of software

The following information about safety-related parametrization of software shall be provided:

a) how safety parameters are secured;

b) safety functions affected by manually set parameters, such as payload, TCP;

c) what robot safety function(s) are included in the identifier (e.g. checksum);

d) how to view and document the settings and parameters;

7.5.12.3 Response time of safety functions

7. 사용 정보 - 7.5 Instruction handbook - 7.5.12 기능안전

7.5.12.4 Stop functions including emergency stop

For all stop functions, the stop category (i.e. category 0, 1 or 2) in accordance with IEC 60204-1 shall be provided.

7.5.12.5 External inputs & outputs

Information about the specification of each external input and output provided and the fault detection measures implemented as well as instructions for the provision of external fault detection means if required

7.5.12.6 Operating modes

Instructions and warnings that the reduced-speed manual mode tasks should, where practicable, be performed with all operators outside the safeguarded space

7.5.12.7 Enabling device(s)

7.5.12.8 Axis limiting

Axis limiting capabilities (e.g. mechanical limiting, electro-mechanical limiting, soft axis and space limiting safety function(s)) and how to use these capabilities shall be described and provided.

7.5.12.9 Position holding device(s)

b) description of the holding capability (5.1.8) including:

- the maximum distance of movement(s) when the position holding device is engaged;
- instructions for how to test the movement.

ANNEX

ISO 10218-1:2011

Annex A (informative) List of significant hazards
Annex B (normative) Stopping time and distance metric
Annex C (informative) Functional characteristics of three-position enabling device
Annex D (informative) Optional features
Annex E (informative) Labelling
Annex F (normative) Means of verification of the safety requirements and measures

ISO/DIS 10218-1:2021

Annex A (informative) List of significant hazards
Annex B (informative) Illustrations spaces
Annex C (normative) Safety functions
Annex D (normative) Required safety function information
Annex E (normative) Test methodology for Class I robots – maximum force per manipulator (FMPM)
Annex F (informative) Symbols
Annex G (normative) Means of verification and validation of the design and protective measures
Annex H (normative) Stopping time and distance measurement
Annex I (informative) Optional features
Annex ZA (informative) Relationship between this European Standard and the essential requirements of Directive 2006/42/EC aimed to be covered

Annex D (normative) Required safety function information - Safety Function Information Table

Annex D
(normative)
Required safety function information

The safety function information shall be provided in accordance with Clause 7.5.11. Table D. 1 is an example format that can be used to present the information for each safety function. More information may be provided.

Table D. 1 — Safety function information example

Clause # *if applicable*	Included in Checksum	Safety function name	Active in mode(s)	Triggering event	Span-of-control	Intended result	Stop Category & description, *if applicable* *See NOTE 2*	Intended result *Reaction on detected fault in safety function* *See NOTE 3*	Reset required *See NOTE 4*	Assumptions & Conditions of use *See NOTE 5*	Diagnostic Coverage	Functional safety performance See NOTE 1		PFH_D	Response time(s), Test rate *See NOTE 6*
												PL and Category	SIL and HFT		
Example: *5.4.3.1*	*Yes*	*Protective stop or "safeguard stop"*	*Configurable: ALL modes or only Automatic mode*	*internal safety function or external protective device*	*robot*	*Monitored standstill*	*Stop Category 2*	*Robot stops. While stopping trajectory is maintained. Upon stopping, a monitored standstill occurs.*	***configurable**: automatic or manual reset **Reset** at teach pendant or by use of an external input*	*1) external protective device fulfills same functional safety requirements 2) dual inputs*	*medium*	*PLd, Cat 3*	*----*	*1.20E-07 without external protective device*	*Time to stop depends on stopping time safety function setting*

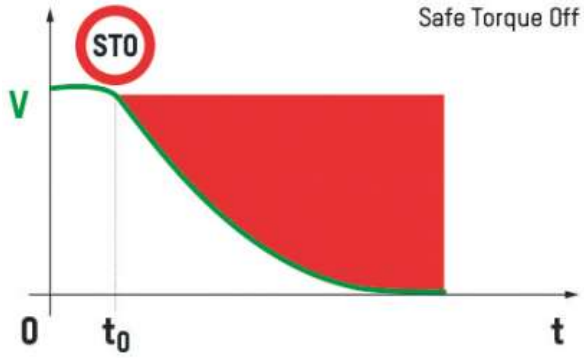
NOTES
1. In accordance with either ISO 13849-1 or IEC 62061
2. Stop category according IEC 60204-1. If applicable, as described in IEC 61850-5-2.
3. For example, inhibit restart. See 5.3.4 for Failure or fault detection.
4. Example: Where is the reset? Is the reset is manual or automatic.
5. Assumptions: N_{op}, shared outputs, fault exclusion, and any resulting installation requirements that lessen a fault…
   Conditions of use: configuration parameters, maximum activation frequency, diagnostics tests…
6. Describe applicable response time(s), test rate(s) or both.

결론

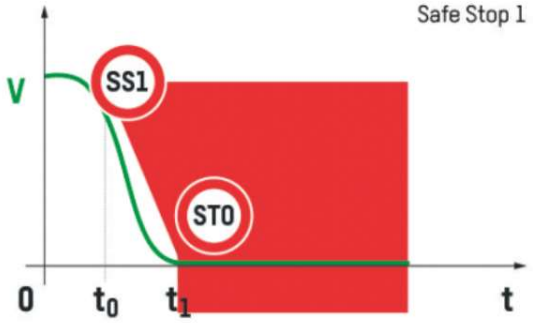
제조사에서 제공하는 Robot Function이 Safety Function일 경우 규격 요구사항을 만족해야 한다.(Annex C)

STO(SBC)를 제외한 대부분의 Safety Function이 Software 관련 되어 있으며 따라서 Software 평가에 대한 검토가 필요하다.

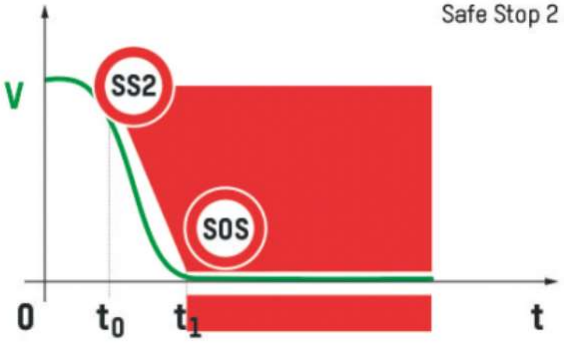
참고자료



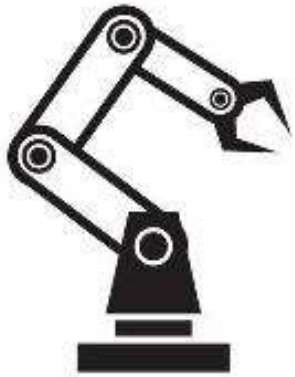
Stop Category 0 :
Machine Actuators의 즉각적인 전원차단에 의해 정지



Stop Category 1 :
Machine Actuators의 전원이 공급된 상태에서 기계가 정지 후 전원이 차단



Stop Category 2 :
Machine Actuators의 전원인 인가된 상태에서 정지



감사합니다

Robot System Safety