DRAFT INTERNATIONAL STANDARD
ISO/DIS 22166-1

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

Voting begins on: **2019-10-28**

Voting terminates on: **2020-01-20**

Robotics — Modularity for service robots —

Part 1: General requirements

ICS: 25.040.30

Reference number
ISO/DIS 22166-1:2019(E)

Contents

Foreword

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

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

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

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

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

This document was prepared by Technical Committee ISO/TC 299, *Robotics*.

Introduction

This International Standard has been developed to cope with the rapidly evolving service robotics sector. At present this robotics market covers many small and niche sectors for which it is difficult to develop the specific and wide-ranging components needed. The market sizes and applications are expected to grow significantly, and the number and range of their functions are also increasing. To enable wide-spread and interoperable development of service robots, a common approach for building service robots is needed. This Standard lays out such common requirements.

On one side, the manufacturer-dependent architectural approaches currently adopted for designing service robots makes design and development difficult and substitution and reuse of modules in upgrading robot products is virtually impossible. On the other side, the research community has developed a vast knowledge base in robot modular design and continues to develop new methods for realising modular approaches, but none have the widespread appeal needed to make significant impact. In these conditions, it is not feasible for the service robotics sector to produce the quality products needed at the prices demanded by the markets and new approaches are urgently needed to help the markets evolve to meet the global challenges.

An international standard on robot modularity and robot component interoperability focusing on main issues of safety, connectivity (from both hardware and software perspectives) and functionality is pivotal to change the service robotics landscape and speed up the development of the new service robot market sectors. The robot modularity issues in this international standard are classified into the issues related to basic and composite modules, basic modules with hardware and/or software aspects. Requirements and guidelines are formulated so that module-based design approaches can be realised allowing application specific service robots and robot systems meeting customer's requirements to be easily configured. The issues are classified into (a) safety and security, and (b) interoperability guidelines. In addition, the open modular approach realised should enable modules to be easily substituted by other modules having the same interface specifications but perhaps with enhanced functionalities as needed.

Safety requirements specified in existing safety standards (e.g. ISO 13482, ISO 10218-1, ISO 10218-2, ISO TS 15066) shall be applied on the system level as well as on the level of a single module. Security issues are also important when adopting an open modularity approaches and hence have been included in this standard (e.g. to align with emerging IEC TC44 and IEC TC65 security related work projects).

The standard contains design and functionality requirements for robot modules to ensure safe and secure operation of such modules and robots built from those modules. It presents design guidelines for building inter-operable robot modules to ensure effective connectivity and correct functionality in line with published standards (e.g. IEC 62443 series). This international standard does not specify the technical implementation of a modular framework. It is intended to provide the necessary guidelines to framework designers, to define a modular framework according to their needs. In view of this, the International Standard, uses the following verbal forms:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates a permission;

— "can" indicates a possibility or a capability.

The safety guidelines at the module level of this International Standard are formulated to ensure compliance with the C-type standards for robot system safety.

Future editions and parts of this family of International Standards are intended to include more specific requirements on particular types of robot modules, e.g., basic and composite modules with hardware and/or software aspects, and for particular types of service robots, e.g., mobile servant robots, physical assistant robots, person carrier robots, and service robots in professional environments.

Title (Robotics — Modularity for service robots — Part 1: General requirements)

1 Scope

This International Standard presents guidelines on the specification of modular frameworks, on open modular design and on the integration of modules for realising service robots in various environments, including personal and professional sectors.

The document is targeted at the following user groups:

- modular service robot framework designers who shall be enabled to specify performant frameworks in an unambiguous way
- module manufacturers who are then able to supply end users or robot integrators as customers
- integrators who are then able to choose applicable modules for building a modular system

This International Standard includes guidelines on how to apply existing safety and security standards to service robot modules.

This International Standard is not a safety standard.

This standard does not apply to robots which are not service robots, although the modularity principles established in this standard can be utilized for these other robots.

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 International Standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 8373: 2012, Robots and robotic devices – Vocabulary

ISO 9409-1:2004, Manipulating industrial robots – Mechanical interfaces – Part 1: Plates

ISO 9409-2:2002, Manipulating industrial robots – Mechanical interfaces – Part 2: Shafts

ISO 10218-1, Robots and robotic devices — Safety requirements for industrial robots— Part 1: Robots

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

ISO 10303 (all parts), Industrial automation systems and integration — Product data representation and exchange

ISO 11593:1996, Manipulating industrial robots – Automatic end-effector exchange systems – Vocabulary and presentation of characteristics

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

ISO 13482, Robots and robotic devices — Safety requirements for personal care robots

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

ISO TS 15066, Robots and robotic devices — Collaborative robots

ISO 19649: 2017, Mobile robots – Vocabulary

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

IEC 60529, Degrees of protection provided by enclosures (IP Code)

IEC/TR 60601-4.1, Medical electrical equipment – Part 4-1: Guidance and interpretation – Medical electrical equipment and medical electrical systems employing a degree of autonomy

IEC 61076-1:2006 Connectors for electronic equipment-Product requirements – Part 1: Generic specification

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1 to 7

IEC 61784-3:2016 Industrial communication networks – Profiles –Part 3: Functional safety fieldbuses – General rules and profile definitions

IEC 61800-5-2, Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

IEC 61984:2008 Connectors – Safety requirements and tests

IEC 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

IEC 62280:2014 Railway applications – Communication, signalling and processing systems –Safety related communication in transmission systems

IEC/TR 62390, Common automation device – Profile guideline

IEC 62443 series of standards on Industrial communication networks - Network and system security

IEC/TR 63074 ED1: Security aspects related to functional safety of safety-related control systems.

ISO/IEC 7498-1, Information technology – Open systems interconnection – Basic reference model: The basic model

ISO/IEC/IEEE 15288 Systems and software engineering – System life cycle processes

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC Guide 77-1:2008, Guide for specification of product properties and classes – Part 1: Fundamental benefits

ISO/IEC Guide 77-2:2008, Guide for specification of product properties and classes – Part 2: Technical principles and guidance

ISO/IEC Guide 77-3:2008, Guide for specification of product properties and classes – Part 3: Experience gained.

NIST SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

NIST SP 800-154 Guide to Data-Centric System Threat Modelling

NIST SP 800-160 vols 1 and 2 Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.

3 Terms and definitions

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

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

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

For the purposes of this International Standard, the following terms and definitions apply.

3.1. General terms

3.1.1.
abstraction layer
interface to the system that allows some or all of the capabilities of the system to be viewed in a different and generally more abstract manner.

Note to entry: An abstraction layer for a module is the same in the case where the system is the module

3.1.2.
connector
physical link that establishes connection between parts of the system

EXAMPLE: Communication, powering, mechanical linking.

3.1.3.
control signals
signals for altering the state of a receiving module or component in some way

Note to entry: Control signal does not transmit structured data like sensor readings (images, sound, etc.) or other data processed as part of the robots application.

3.1.4.
software communication interface
logical layer in communication with other parts of the system

3.1.5.
electrical interface
connectors and the electrical properties for transmitting power, analogue or digital signals

3.1.6.
execution life cycle
finite state machine defining all stages of execution of a part's function

3.1.7.
error
discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition

[SOURCE IEC 60050 International Electrotechnical Vocabulary 192-03-02]

3.1.8.
failure
loss of ability to perform as required

[SOURCE IEC 60050 International Electrotechnical Vocabulary 192-03-01]

3.1.9.
fault
inability to perform as required, due to an internal state

[SOURCE IEC 60050 International Electrotechnical Vocabulary 192-04-01]

3.1.10.
function
defined objective or characteristic action of a system or component or module

[SOURCE ISO/IEC/IEEE 24765 3.1206-5 (Modified)]

3.1.11.
functional safety
part of the overall safety relating to the equipment under control (EUC) and the EUC control system that depends on the correct functioning of the electrical, electronic and programmable electronic (E/E/PE) safety-related systems and other risk reduction measures

[SOURCE IEC 61508-4:2010, 3.1.12]

3.1.12.
hardware abstraction layer (HAL)
an abstraction layer for a component/module that contains hardware aspects, with the abstraction layer providing control of the component/module via a software interface.

Note to entry: The purpose of a HAL is usually so that different module implementations can be accessed through the same software interface

3.1.13.
information model
abstraction and representation of the entities in a managed environment, their properties, attributes and operations, and the way that they relate to each other.

Note to entry: The information model is independent of any specific repository, usage of software aspects, protocol, or platform.

3.1.14.
software communication interface
logical layer in communication with other parts of the system

3.1.15.
security
combination of confidentiality, integrity, and availability

[SOURCE ISO TR 17522:2015 3.19]

3.2. Terms related to component

3.2.1.
component
part of something that is discrete and identifiable with respect to combining with other parts to produce something larger

[SOURCE: ISO/IEC 24765]

Note 1 to entry: Component can be either software or hardware. Even a component that is mainly software or hardware can be referred to as a software or hardware component respectively.

Note 2 to entry: Component does not need to have any special properties regarding modularity.

Note 3 to entry: Component and module have been used interchangeably in general terms, but to avoid confusion the term module is used to refer to a component that meets the guidelines presented in this International Standard

Note 4 to entry: A module is a component, whereas a component does not need to be a module.

3.2.2.
software component
component whose implementation consists of a computer programmed algorithm

3.2.3.
hardware component
component whose implementation consists of physical elements and possibly any embedded software necessary for its operation

3.3. Terms related to module

Note to entry: Many terms defined in this subclause can also apply to components but for the purposes of this International Standard the definitions are formulated to apply to modules as presented in this standard.

3.3.1.
composability
ability to assemble modules logically and physically (without need for adaptation of the modules or additional interfacing work) using various combinations into new modules

Note to entry: While 'integration' generally implies significant effort, 'composition' generally implies limited to no effort

3.3.2.
configuration
arrangement of a modular service robot in terms of the number and type of modules used, the connections between those modules, and the settings for those modules, in order to achieve the desired functionality of the modular robot as a whole

Note 1 to entry: ISO 8373 also defines (joint) configuration but this is a different concept

Note 2 to entry: This term describes to result of some process, i.e. the state something is in. The process of creating such a state is covered by term 3.3.3

3.3.3.
configuring
setting the number of modules, type of modules, the connections between the modules, and the settings for the modules in order to achieve the desired functionality of a modular service robot as a whole

3.3.4.
granularity
degree to which a robot module can be broken down into separate modules

3.3.5.
hardware aspects
information regarding properties and functions necessary for a module and its physical interconnection and regarding the allowed range of physical properties of the operational environment