BS ISO 22166-1:2021

BSI Standards Publication

Robotics — Modularity for service robots

Part 1: General requirements

Documents
Document Sharing Hub

Full document details: BS ISO 22166-1:2021

National foreword

This British Standard is the UK implementation of ISO 22166-1:2021.

The UK participation in its preparation was entrusted to Technical Committee AMT/10, Robotics.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 580 97834 0

ICS 25.040.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2021.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 22166-1:2021

INTERNATIONAL STANDARD

ISO 22166-1

First edition
2021-02

Robotics — Modularity for service robots —

Part 1: General requirements

Robotique — Modularité des robots de service —

Partie 1: Prescriptions générales

Reference number
ISO 22166-1:2021(E)

Documents
Document Sharing Hub
© ISO 2021

Full document details: BS ISO 22166-1:2021

COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 22166-1:2021

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**
3.1 General terms 2
3.2 Terms related to component 3
3.3 Terms related to module 4
3.4 Terms for classification of modules 6
3.5 Characterization of modules regarding principal function 7

4 General provisions **7**
4.1 General 7
4.2 Generic principles of modularity 8
4.2.1 General 8
4.2.2 Composability 8
4.2.3 Integrability 8
4.2.4 Interoperability 8
4.2.5 Module granularity 8
4.2.6 Platform independence 8
4.2.7 Openness 8
4.2.8 Reusability 9
4.2.9 Safety 9
4.2.10 Security 9
4.3 Abstraction 9
4.4 Electrical interfaces and communication protocols 10
4.5 Interchangeability 11
4.6 Module properties 12
4.6.1 General 12
4.6.2 Module identification 12
4.7 Simulation 12
4.8 Data types for interoperability 13

5 Provisions for safety and security **13**
5.1 General 13
5.2 Robot system level safety 15
5.3 Module level safety 16
5.4 General aspects of security 18
5.5 Steps to design security into a module 19
5.6 Physical security of modules 19
5.7 Cyber security of modules 19

6 Hardware aspects in module design **20**
6.1 General 20
6.2 Requirements and guidance for hardware aspects of modules 21
6.2.1 Mechanical interfaces 21
6.2.2 Interfacing for power supply 24
6.2.3 Other aspects for module description 24

7 Software aspects in module design **25**
7.1 General 25
7.2 Information model 25
7.2.1 General 25
7.2.2 Model for exchange of information among modules 26
7.2.3 Model for access to properties and its access 26
7.2.4 Model for error handling and recovering 27

AVA Documents
Document Sharing Hub

© ISO 2021 – All rights reserved

Full document details: BS ISO 22166-1:2021

7.2.5 Interoperation of software modules ... 28
7.3 Architectural model for software modules ... 29
7.3.1 General ... 29
7.3.2 Requirements for software modules ... 31
7.4 Safety/Security-related requirements for modules with software aspects ... 32
7.4.1 General ... 32
7.4.2 Interaction with safety/security manager modules ... 33

8 Information for use ... 33
8.1 General ... 33
8.2 Markings or Indications ... 34
8.3 Information for users ... 35
8.4 Information for service ... 36

Annex A (informative) **Robot module template ... 37**

Annex B (informative) **Robot module examples ... 39**

Annex C (informative) **Use case examples of modularity for service robots ... 50**

Annex D (informative) **Guidance for testing robot modules ... 62**

Bibliography ... 67

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

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

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

Introduction

This document has been developed for 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 document 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, this document can assist the service robotics manufacturers to produce the quality products at affordable cost 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 module interoperability focusing on main issues of safety, security, 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 document are classified into basic modules with hardware and/or software aspects and composite modules. Requirements and guidelines are formulated so that module-based design approaches can be realised allowing application specific service robots and service 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 has to 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) apply on the system level as well as on the level of a single module. The safety guidelines at the module level of this document are formulated to ensure compliance with the C-type standards for robot system safety. Security issues are also important when adopting an open modularity approaches and hence have been included in this document (e.g. to align with emerging IEC/TC 44 and IEC/TC 65 security related work projects).

Future parts of the ISO 22166 series 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.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

Robotics — Modularity for service robots —

Part 1: General requirements

1 Scope

This document presents requirements and 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 developers who specify performance frameworks in an unambiguous way;

— module designers and/or manufacturers who supply end users or robot integrators;

— service robot integrators who choose applicable modules for building a modular system.

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

This document is not a safety standard.

This document applies specifically to service robots, although the modularity principles presented in this document can be utilized by framework developers, module manufacturers, and module integrators from other fields not necessarily restricted to robotics.

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 9787, *Robots and robotic devices — Coordinate systems and motion nomenclatures*

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

ISO/TR 22100-4, *Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

ISO/IEC 27032, *Information technology — Security techniques — Guidelines for cybersecurity*

IEC 61076-1, *Connectors for electronic equipment-Product requirements — Part 1: Generic specification*

IEC 61984, *Connectors — Safety requirements and tests*

IEC/TS 62443-1-1, *Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models*

IEC 62443-2-1, *Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program*

IEC 62443-3-3, *Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels*

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

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

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

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

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

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

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 accessed in a different and generally more abstract manner

Note 1 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 mechanism that enables connection and disconnection between parts of the system

EXAMPLE Communication, powering, mechanical linking.

3.1.3
electrical interface
combination of connectors and the electrical properties for transmitting power, analogue or digital signals

3.1.4
execution life cycle
finite state machine defining all stages of execution of a part's function

3.1.5
error
discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.1.6
failure
loss of ability to perform as required

[SOURCE: IEC 60050-192:2015, 192-03-01]

3.1.7
fault
inability to perform as required, due to an internal state

[SOURCE: IEC 60050-192:2015, 192-04-01]

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

3.1.8
function
defined objective or characteristic action of a system or component or module

[SOURCE: ISO/IEC/IEEE 24765, 3.1206-5 — modified.]

3.1.9
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]

3.1.10
hardware abstraction layer
HAL
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 1 to entry: The purpose of a HAL is usually so that different module implementations can be accessed through the same software interface.

3.1.11
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 1 to entry: The information model is independent of any specific repository, usage of software aspects, protocol, or platform.

3.1.12
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

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

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

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

3.3 Terms related to module

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

3.3.2
configuration
arrangement of a composite module 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 the term *configuring* (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

Note 1 to entry: Physical interconnection information includes mechanical properties (material, shape, pose, size, forces/torques), electrical and electromagnetic properties, pneumatic and hydraulic properties.

Note 2 to entry: Operational environmental properties include forces, temperature, humidity, vibration and mechanical shock, illumination and noise (sound and electro-magnetic).

3.3.6
infrastructure
structured facilities and resources to support the operation of modules and systems

3.3.7
interface
shared boundary between two or more functional modules, defined by various characteristics pertaining to the functions, signal exchanges, and other characteristics

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.2058, definition 1]

3.3.8
interoperability
capability to communicate, execute programs or transfer data or power among modules or combine modules physically and/or logically in a manner that requires the user to have little or no knowledge of the unique characteristics of the individual modules

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

3.3.9
interchangeability
module property allowing it to be capable of being used to replace another module

Note 1 to entry: Such interchangeability can relate to modules produced by one manufacturer or from different manufacturers.

3.3.10
mechanical interface
physical means of connection with other modules used for the transmission of physical forces and facilitating module function and/or configuring structure

Note 1 to entry: Transmitted physical forces include forces controlled for an intended purpose as part of planned function, and uncontrolled forces both intentional (e.g. structural support) and unintentional (e.g. cushioning).

Note 2 to entry: ISO 8373 uses the term for the mechanical interface between a manipulator and the end-effector. In this document, the term is used in a broader sense, including any mechanical interface between robot modules.

3.3.11
modularity
set of characteristics which allow systems to be separated into discrete modules and recombined

3.3.12
module
component or assembly of components with defined interfaces accompanied with property profiles to facilitate system design, integration, interoperability, and re-use

Note 1 to entry: A module may have both hardware and software aspects. It may consist of other components (hardware and software) or other modules (hardware and software).

Note 2 to entry: This neither requires nor prevents the use of Open Source Software to implement parts or all of the open module's functionalities.

Note 3 to entry: Although an open module is conceptually the opposite of a black module, it is still treated as such a black box module for the purpose of this document, i.e. in a robot system conforming to this document, other modules should only communicate with the open module through its official, manufacturer-specified module interface.

Note 4 to entry: An open module is not necessarily a composite module, nor is a composite module necessarily an open module.

3.3.13
package
set of all software binaries, configuration information and support files necessary for a module with software aspects to function as designed

Note 1 to entry: Packages can depend on other packages.

3.3.14
module property
attribute or characteristic of a module

EXAMPLE A module property for hardware can be the torque of an actuator. A module property for software can be the response time to a new command.

3.3.15
module property profile
catalogue of the values of a sub-set of module properties

3.3.16
quality of service
minimum level of performance of a module's service to other modules connected to it for overall operation as intended

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

3.3.17
reconfiguration
altering the configuration of a modular robot in order to achieve an intended change in the function of the modular robot

3.3.18
reusability
ability to adopt modules, previously designed and produced, to facilitate the development of new modules and robot systems to realise different required functionalities

3.3.19
robot module
module intended to be used as part of a modular robot system

Note 1 to entry: Not all modules used in a modular robot system need to be robot modules, but if the primary intention of a module is use in a modular robot system, then it is a robot module.

Note 2 to entry: Example robot modules are presented in Annex B as being important for service robot modularity.

3.3.20
self-configuration
self-reconfiguration
changing the configuration of a modular robot through an automated process without interaction from outside of the system/subsystem except to initiate the process, if necessary

Note 1 to entry: Typically, mechanical and electrical connections need to be manually (re-)configured, with the automation applying to (re-)configuration of the software aspects.

3.3.21
software aspects
information regarding the external software properties necessary for a module and its interface and the execution life cycle of that module's function

3.4 Terms for classification of modules

3.4.1
basic module
module that is not decomposable into smaller modules

EXAMPLE Basic modules for service robot can be defined as input, processing, output or infrastructure support modules.

3.4.2
composite module
module constructed by two or more modules

Note 1 to entry: A module manufacturer can choose to document the internal structure of its composite module including possibly access to internal interfaces or documented procedures to replace some of the built-in modules. However, in any case the composite module for the purpose of the requirements defined in this document is considered as a "black box module".

3.4.3
hardware module
module whose implementation consists purely of physical parts, including mechanical parts, electronic circuits and any software, such as firmware, not externally accessible through the communication interface

Note 1 to entry: A hardware module has hardware aspects. It consists of hardware components.

EXAMPLE 1 A mechanical joint with no electronics contained; its' hardware aspects include its size, the kinematic properties, the mounting plates at both ends, the material, stiffness, maximum allowed force and torque, etc.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

EXAMPLE 2 An enhanced mechanical joint, that includes a microcontroller, software on the controller and motors to control properties such as stiffness, or damping; its' hardware aspects also include the connector for powering the embedded electronics and embedded motors, including specifying voltage and current limits.

3.4.4
software module
module whose implementation consists purely of programmed algorithms

Note 1 to entry: A software module has software aspects. It consists of software components.

3.5 Characterization of modules regarding principal function

3.5.1
actuator module
actuating module
output module whose primary function is to physically move the robot, or alter the world around the robot, in response to instructions from other modules, with the purpose of achieving the robot system's task(s)

3.5.2
communication module
module that exposes communication interfaces to other mediums or provide means of interconnection between modules

Note 1 to entry: Interfaces to other mediums can be via Wi-Fi, mobile network, Ethernet, etc.

3.5.3
computing module
module that provides computing resources for use by software modules

Note 1 to entry: Computing resources are the hardware for executing the software, and can include distributed modules.

3.5.4
infrastructure module
module that provides facilities and resources to support the operation of other modules

Note 1 to entry: Examples of facilities used by other modules include mechanical frames for physical attachment points and cables for communication and power, where cables can be attached to the frame.

Note 2 to entry: Examples of resources used by other modules include power supplies, memory and processors, and communication bridges (or hubs) among inter-robots or the robot and the servers.

3.5.5
sensing module
input module for collecting data about the world around the robot or the state of the robot for use by other modules to support the robot system in performing its task(s)

3.5.6
supervisor module
software module which checks the status of other modules and can control the transition from one state to other state to make the operation sequence of modules proper

4 General provisions

4.1 General

This clause introduces the essential concepts behind the use of modularity in service robotics. For describing these concepts SysML (OMG SysML) should be used, which defines types of diagrams within a general-purpose modelling language for systems engineering applications and which also supports

AVA Documents
Document Sharing Hub

© ISO 2021 – All rights reserved

Full document details: BS ISO 22166-1:2021

specification, analysis, design, verification and validation. Manufacturers should perform verification and validations processes for satisfying the principles of modularity.

4.2 Generic principles of modularity

4.2.1 General

This subclause explains generic principles that a module's design should follow. While these principles are partly presented as recommendations, a module designer shall:

— document whatever modular approach has been chosen; and

— provide all necessary information for integrators to use the module.

These principles can apply generically to modules with hardware or software aspects. In this Clause the term module, unless stated otherwise, is used in its widest sense to refer to basic or composite modules.

4.2.2 Composability

Modules shall be designed in a way that they can be assembled logically and physically into composite modules for performing more sophisticated operations, while maintaining operational and safety requirements. Composing should be possible based on information provided on interfaces so that information of internal structure is not necessary. Modules can be organized in data banks or repositories to make re-use more practicable. This is further discussed in 7.2.2.

4.2.3 Integrability

Hardware aspects and software aspects of modules shall be designed in a way that they can be integrated to form larger systems to perform intended target services or functions. To allow the linking of modules in a reliable manner, appropriate interfaces should be designed. Safety aspects of systems made from modules are discussed in Clause 5.

4.2.4 Interoperability

Modules shall be designed in a way that they can be linked to work with other modules. They should be easy to connect and should allow to share power and data via appropriate connectors. To allow exchange of data, interfacing protocols shall be defined and implemented at appropriate levels, as specified in Clause 7.

4.2.5 Module granularity

The function of modules should be achieved with an appropriate level of granularity in a modular framework: Basic modules and composite modules. Examples of basic modules and composite modules are presented in Annex B.

4.2.6 Platform independence

Modules should be designed in a way that they can be implemented on different service robots or combined with different sets of modules without significant modification. Software modules should be generated in such a way that they should run on different platforms such as embedded computing systems, Linux, Windows or real-time operating systems with minimum modifications. Modules with hardware aspects which are used in different service robot system should be operated on different platforms.

4.2.7 Openness

Openness in this document shall include mechanical and electrical interfaces for modules with hardware aspect and software interfaces among modules should include the following: a defined

© ISO 2021 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO 22166-1:2021

reference architecture consisting of modules with hardware and software aspects, and their design together with their safety, security and testing methods.

The re-use of modules should be supported by the provision of relevant information such as their dependencies and incompatibilities to integrators.

NOTE Relevant information can include source code, documents, computer-aided design (CAD) models, circuit diagrams, design experience, system architectures, software hierarchies, interfacing specifications, etc.

4.2.8 Reusability

Reusability is the ability of modules to be used and re-used in different platforms via appropriately defined interfaces. Interfaces of modules shall be designed in a way, that modules can be re-used. Relevant interfaces allowing re-use can include software interfaces, connectors between modules, and linkages between hardware aspects of modules.

Where appropriate, reusability should be supported by managing builds, configurations and reconfiguration options, upgrading possibilities and overall maintenance requirements of modules.

4.2.9 Safety

Modules should be designed to comply with relevant safety standard in all safety-related applications. They should furthermore be designed to support the overall safety of a modular system. Manufacturers of modules should provide necessary information to support integrators in safety design of system.

4.2.10 Security

Modules with software aspects or communication interfaces should be designed to prevent attempts to access with them by unauthorised methods or persons. They should furthermore be designed to support the overall security of a modular system.

4.3 Abstraction

An abstraction layer should be used to define standard interfaces between hardware and software in order to:

— support interoperability and reusability;

— simplify simulation and modelling;

— foster independence of implementation and platform-independence.

NOTE 1 For example, an infrared sensing software module and an ultrasonic sensing software module may be used together to get the distance from a robot to a nearby object. These two modules can read the distance values from the infrared sensor and the ultrasonic sensor using their device drivers, respectively. In this case, the two modules may not be reusable and interoperable because each module uses its own device driver even though the same data is used. To ensure the reusability of the two modules to read the distance value, one abstracted device driver is necessary, after which a different sensing module can be used because of the abstraction layer even though many manufacturers provide different types of distance measuring sensors.

NOTE 2 Software aspects in software modules use the abstraction layer to access hardware devices such as servo motors and laser sensors.

NOTE 3 The use of a hardware abstraction layer or another form of device driver is optional in this document (see 7.3). If a particular implementation of a modular robot system can be achieved by directly calling software functions of device drivers, then this is allowed. Abstraction can include the use of translation techniques where underlying communication technologies are different.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

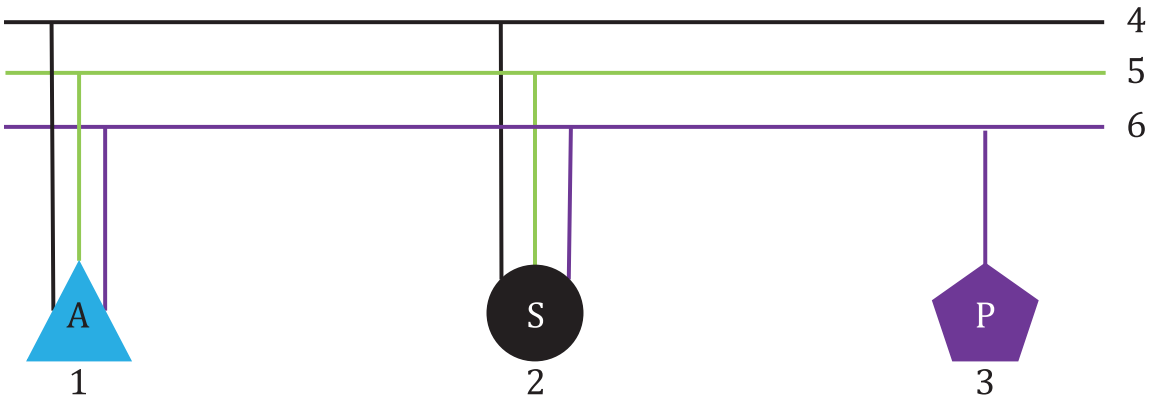
4.4 Electrical interfaces and communication protocols

The electrical interfaces and communication protocols should follow already existing standards.

NOTE 1 Interfaces for data buses and communication networks include hardware and software aspects. A conceptual example of a general interfacing arrangement is shown in Figure 1 covering functionality, powering and the operating environment.

NOTE 2 Table 1 shows some examples of communication protocols. Communications protocols are often implanted in software, but also sometimes in hardware. They represent layer-2 to layer-7 in the OSI reference model as defined in ISO/IEC 7498-1.

The electrical interface hardware should be designed so that the communications do not suffer interference due to close proximity to other electrical wires or devices. Only standardized connectors shall be used.



Key

1 actuator
2 sensor
3 power
4 environment
5 functionality
6 power

Figure 1 — Conceptual example of interface arrangement between modules (elaborated in Clause 6)

Table 1 — Examples of communication protocols able to be used for modules

Reference	Type	Remarks
ISO 11898-1/2 and EN 50325-4/5	CAN and CANopen	The CAN media access unit sub-layer is normally implemented in transceiver ICs, the CAN data link layer protocol and the physical signalling sub-layer are implemented in the CAN protocol controller, and the CANopen application layer is normally implemented in software running on a micro-controller.
ISO/IEC/IEEE 8802-3:2017 IETF 793 or ISO/IEC 14766 (TCP), IETF RFC 768 (UDP), RFC 791 (IPv4), RFC 2460 (IPv6)	Ethernet and TCP/IP	Implemented in PHYs and MAC, which are optionally integrated in technology-specific controllers. (This protocol is widely used worldwide).
IEC 62680 and USB CDC	USB	Many implementations exist and USB communications device class (CDC) is a composite Universal Serial Bus device class.
IEC 61158	Fieldbus	IEC 61158 standardizes commonly used Fieldbus protocols and includes Foundation fieldbus, Profibus, WorldFIP, CC-link, EtherCAT Modbus-RTPS, SERCOS, etc.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

4.5 Interchangeability

Interchangeability and re-composition of modules are strongly related to connectivity of modules and can have different levels; the following are considered in this document:

— Level 1: Exchanging of modules is only possible by the manufacturer or robot system integrator

— Level 2: Exchanging of modules by the user is possible when the robot is switched off

— Level 3: Exchanging of modules by the user is possible while the robot is switched on (hot plugging)

— Level 4: Exchanging of modules by the robot itself is possible (hot plugging with activated drives)

Self-configuration (level 3 and 4) may lead to incorrect operation or to hazardous situations. Relevant safety and security issues are discussed in Clause 5. To avoid ambiguity about the state of modules, self-configuration with ongoing robot functions should be avoided.

Module manufacturers shall provide the interchangeability level for modules. The different levels have different implications on requirements with respect to design of connectors, safety and security, durability, documentation of modules, etc., as shown in Table 2.

Table 2 — Recommendations for different levels of interchangeability

Level	Frequency of changes	Design of connectors	Documentation	Safety	Software
1	Low	Can be simplistic with separate connection of mechanical and electrical parts	For readers with technical knowledge	Issues should be covered by a risk assessment performed after exchanging	Installation and configuration can be complex and include manual adjustment
2	Medium - high	Preferably composite plugs	Also for readers without technical knowledge	Safety limits need to be provided for the user. System can do a consistency check on power-up	Organisation in packages, automated solving of dependencies
3	High	Composite plugs with hot-plug functionality	Also for readers without technical knowledge	Safety limits need to be provided for the user. System needs to perform a consistency check while other functions are executed	Automated loading, unloading and switching of modules during runtime
4	High	Composite plugs with hot-plug functionality and large tolerances for automated connection	Also for readers without technical knowledge	Safety limits need to be provided in machine-readable form. System needs to perform a consistency check while other functions are executed	Automated loading, unloading and switching of modules during runtime

An information model for a modular robot system should provide information about the module properties and capabilities of individual modules regarding interchanging and self-configuration.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

4.6 Module properties

4.6.1 General

Module properties shall be stored in a module property profile. When a module is transferred for use or reuse, the module profile shall go with the module.

NOTE There is no implication here about the nature of this storage.

4.6.2 Module identification

The module should be named or identified using a string or number code that is published by the manufacturer. In addition, the product itself and the vendor should also be identified using a similar name or identification code. This information can be used in designing a service robot based on modules which (semi-)automatically configure the robot system. If the module uses the data bus, it should transfer its own ID on request to other modules and to the supervisor module.

The module may provide automatic configuration of the robot hardware (including structure) and software.

If the feature to automatically configure itself is available in the module, the minimal information made available to identify the module by the manufacturer should be:

— Module type and/or module ID

— Manufacturer name and/or manufacturer ID

— Module version

— Production date

— Serial number

From a system security point of view, module identification should be verified by a properly designed authentication procedure for security related modules.

4.7 Simulation

If simulation is used to verify the design and function of a module, the limitations and constraints of the models used should be recognized. Especially safety and security should be verified in real-world tests for intended use case applications.

In order to allow proper simulation of a modular system, module manufacturers shall provide relevant information needed for simulation with their modules. It should be specified by the framework designer as to which information is necessary and in which form they should be provided (e.g. on paper or as a parameter file which can be imported into the simulation tool). Information about the module used in the simulation can include:

— its physical characteristics, including its physical properties (e.g. dimensions, mass, density, static and dynamic characteristics, structural strength, etc.), and appearance;

— its electrical characteristics, such as peak and average power requirements for operation;

— the general control algorithms that it can execute;

— the interfaces for input (sensors) or output (actuators) modules, that determine the format and style of the information to be exchanged;

— the method by which a sensor module acquires information from the simulated world; and

— the method by which an actuator module acts upon the simulated world.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

NOTE 1 Detailed specifications for the various models are outside the scope of this document.

NOTE 2 It is also possible to provide simulation data within the module template.

4.8 Data types for interoperability

A modular framework shall define data types that can be used within the modular framework and the middleware. This includes the precision of common integer- and real-valued numerical data types as found in IEC/TR 62390.

A modular framework shall also define conventions for commonly used composite data types. Defining the following conventions is recommended. There are also a small number of common composite data-types built upon these [see also OMG RLS (Robotic Localisation Service)], namely:

a) A position in space is defined with respect to some coordinate system that is defined in a fixed position and orientation according to the implementation. A coordinate can be given in Cartesian form with respect to the orthogonal fixed coordinate system using a triple (x, y, z) of real numbers. A pair (x, y) of numbers can also be given, but is interpreted as a triple with z=0.

b) Orientations may be specified in one of two ways. A general orientation in three-dimensional space is to be given as a quaternion, which is transferred as a four-tuple of numbers $<c, su, sv, sw>$ where (u, v, w) is the axis of rotation and c and s are the cosine and sine of the half-angle of rotation respectively. Alternatively, a rotation about the z-axis only can be given as a rotation angle about that axis, with the angle measured in radians.

c) The position and orientation of a mobile robot is given by its standard coordinate system as specified in ISO 19649 and ISO 9787.

d) 2D and 3D object geometry data — to be chosen from existing standards.

A modular framework may in addition define guidelines or limitations, how input/output data to/from modules should be structured.

A module manufacturer should pick suitable data types and data structures from the range allowed in the modular framework definition for his module. Information on the data types and data structure shall be stated in the module description (see Annex B for example modules).

5 Provisions for safety and security

5.1 General

This Clause provides guidelines of how requirements from published safety and security standards can be applied to design modules and module-based systems. Its contents shall not be used as a justification to deviate from applicable safety and security standards.

NOTE 1 Safety can be assessed on the level of a single module (normally done by the module manufacturer) and on the level of the service robot system (normally addressed by the integrator).

Safety and security are different design aspects that can influence each other in robot design and in robot module design. A security breach in a robot system and/or robot module can result in safety-related hazards. Therefore, a robot module manufacturer should evaluate, through risk assessment, the potential for security related properties to cause hazards within the intended use cases, which the designer should mitigate through the module design.

A security vulnerability in one module of a service robot system can lead to a security breach for the whole service robot system which can result in hazard(s). A module manufacturer should be aware of security vulnerabilities of a module that can propagate through the robot system. For this reason, safety and security aspects should be addressed to ensure that robot designers take them into account in their modular design.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

Existing safety standards apply for robots and robot systems including

— ISO 12100 for risk assessment and risk reduction of machinery,

— ISO 10218-1, ISO 10218-2, and ISO/TS 15066 for industrial robots,

— ISO 13482 for personal care robots,

— IEC/TR 60601-4-1, IEC 80601-2-77 and IEC 80601-2-78 for various aspects of medical robots, and

— ISO 13849-1, IEC 61508 series, and IEC 62061 for functional safety.

In a modular robot system software can be involved in various modules of the robot. ISO/IEC/IEEE 12207:2017 and ISO/IEC/IEEE 15288:2015 have defined the life cycle processes for the development of software to ensure required quality is achieved. IEC 61508-3 specifies safety requirements for software that is part of the safety-related part of the control system. The safety requirements for software apply only to the safety-related parts of the software and are presented in 7.2 and 7.4.

When a modular design approach is adopted, the increased ability to reconfigure a service robot system for multiple applications shall be accounted for in the risk assessment and risk reduction process described in ISO 12100 to ensure that the safety requirements are satisfied even after adding/removing/reconfiguring modules, e.g. by reviewing risk assessment again after a reconfiguration. These requirements can apply on the system level as well as on the module level. In addition to the normal safety-based risk assessment, the designer and/or the service robot integrator shall incorporate a security risk assessment to assess the consequences for safety. For example, a hazardous situation can be mitigated by adding a module. However, after any change in the modular structure of the robot system, the risks after performing a modular reconfiguration should to be assessed again for both safety and security.

The following standards shall be used when evaluating robot system and module security:

— ISO/TR 22100-4 dealing with IT-security aspects for machinery

— ISO/IEC 27032 for general guidelines on cybersecurity

— IEC/TS 62443-1-1 for terminology, concepts and models

— IEC 62443-2-1 dealing with security programs for industrial automation

— IEC 62443-3-3 for security levels in control systems

— NIST SP 800-154 for data-centric system threat modelling

— NIST SP 800-160 volumes 1 and 2 for system security engineering

Figure 2 shows how safety and security risks are related and how they can be addressed. Module manufacturers and integrators (and where applicable module framework designers) shall follow the rules, and requirements established in existing, applicable safety standards. This is indicated in the horizontal line of Figure 2. Security risks for a module shall be assessed with reference to the same intended use, foreseeable misuse, and “limits of the machine” (as per ISO 12100:2010, 5.3) as used in the safety analysis for the module. The process of assessing and mitigating security risks (vertical line of Figure 2) should be performed in an iterative process: either parallel to steps 1 and 2 of Figure 1 in ISO 12100:2010, Clause 4, or at the end of the respective process. The integrated process of assessing and mitigating both security risks and safety risks (diagonal line of Figure 2) should be performed in an iterative process. In cases where implementing security measures conflict with implementing an intended safety function (to meet a safety requirement), mitigating the safety risk shall take precedence, while still mitigating the security risk as far as reasonably possible.

NOTE 2 A module manufacturer can either try a different implementation of the respective safety function, which still meets the safety requirement. Or it can approximate the security measure to extend possibly without hampering the safety function.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

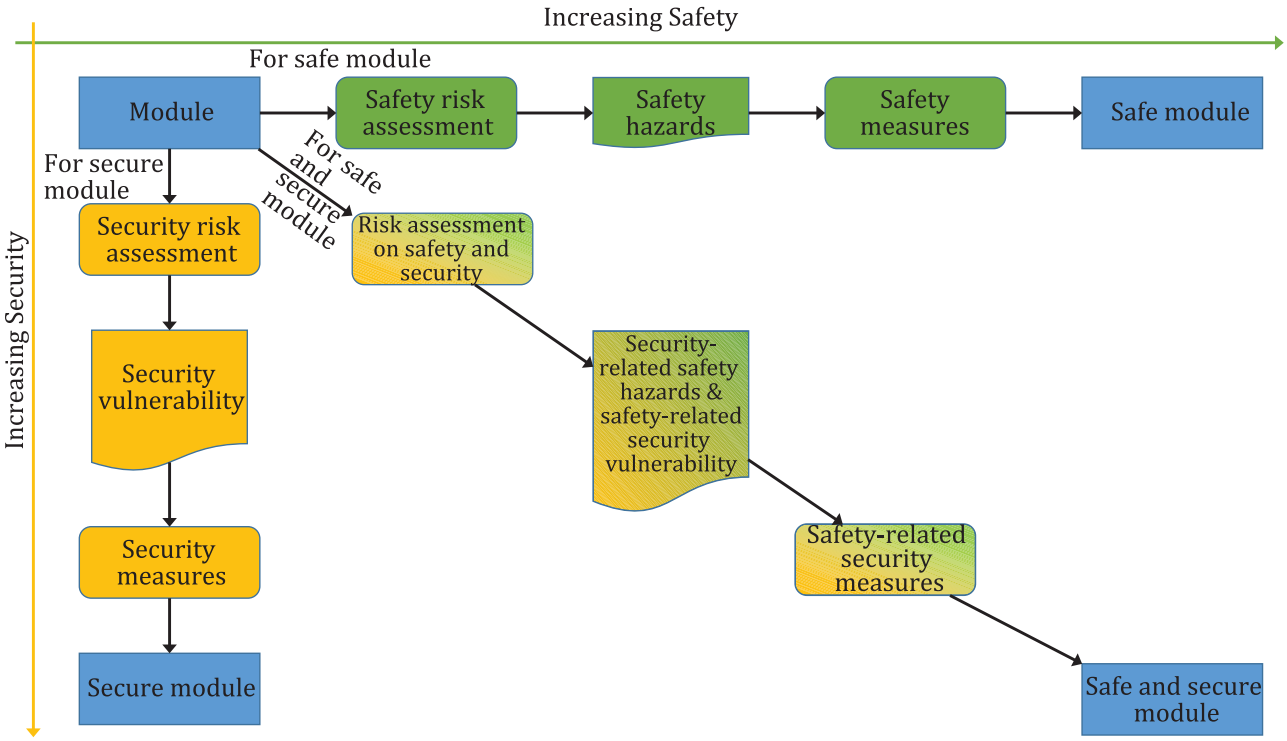


Figure 2 — Safety and security risk considerations for robot modules

A module manufacturer should consider the module's intended use cases and the technology it uses to identify the needed requirements for various application domains (e.g. mechanics, electromagnetics, software, security, environments, biology, chemistry, usability, etc.). In addition, the module manufacturer shall identify and list the considered use cases with concrete limitations and exclusions. While modularity may not be explicitly within the scope of existing standards in the intended application domains, the principles presented in existing standards can be useful to derive appropriate module requirements and testing methods. See Annex D for more detailed information on testing robot modules.

A module integrator should consider the following information:

— Relationship with external system (physical layout, interface, etc.);

— Maintenance guidelines for module and system levels.

5.2 Robot system level safety

The methods used to evaluate the safety of a robot system comprised of robot modules are not different from the methods used to evaluate robot systems without modules, and they are published in existing standards.

The modular service robot framework developers are responsible for:

— Designing the architecture and the composition of the various service robot modules,

— Ensuring proper connection and processing of the safety signals between modules, and

— Evaluating the required safety of the robot for the typical use case applications.

NOTE 1 Typical use case applications can cover different levels of safety; security; combined safety and security; and quality.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021

NOTE 2 Signals refer both to hardwired signals like emergency stop signals in to or out of a module and also data exchanged over a wired or wireless network, in which case the network should satisfy the functional safety requirements.

The module manufacturers shall be responsible for specifying the intended use case applications for the modules.

The module integrators shall be responsible for:

— Complying with the applicable robot safety standards mentioned in 5.1,

— Accounting for the systems' planned use cases, which is compared for relevance and closeness to the intended use cases presented by the module manufacturer, and

— Complying with safety guidelines specified by the module manufacturer, including the required conditions for use.

If the robot system or its use case applications change, then the risk assessment process shall take in account the changes. Examples are presented in Annex C. If parts of a modular robot system are intended to be changed by the end user, the risk assessment shall cover hazards from possible configurations.

NOTE 3 Applicable limits of use and required safety precautions or follow-up steps are part of the user manual of the robot system.

The modular service robot framework developers shall carry out to design measures to support risk reduction to ensuring the following:

— global safety signals and error states and rules for their use and propagation;

— safety features or a minimum safety performance that all modules should maintain;

— core items to be included in the documentation of safety performance.

5.3 Module level safety

The design of the module shall take into account the applicable published standards for electrical and mechanical safety (see Annex D for testing robot modules). Safety-requirements for software are discussed in 5.4.

If motors are designed to have a stop function, the module should provide a respective safety function in compliance with IEC 61800-5-2.

To prevent failure due to module-to-module communication, the system should use black channel communication (see IEC 62280 and IEC 61784-3). In this case the reliability block of the module should be designed as safety-related and a route should be constructed that guarantees the reliability of the safety function.

Performance levels (PL) or safety integrity levels (SIL) shall be assigned to safety functions implemented. These PL/SIL can be used to evaluate the overall performance of a safety function with respect to the complete robot system. A module manufacturer should publish PL or SIL for all safety functionality shared by the module with other modules. Signals in a module that are not safety-related in that module, may still be useful and reported to other modules for safety-related functions.

The process followed in designing robot modules can be different from normal system design because the module designer/manufacturer does not have the final specific application available at the time of design (only typical use case scenarios are known).

The robot module manufacturer can use the following steps to ensure appropriate and adequate safety design requirements are included:

1. Define intended use cases, and for each use case, describe as many relevant details as possible.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22166-1:2021