TECHNICAL REPORT

ISO/TR 22053

First edition
2021-01

Safety of machinery — Safeguarding supportive system

Sécurité des machines — Système de protection complémentaire

Reference number
ISO/TR 22053:2021(E)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

Foreword

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

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

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

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

For an explanation 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 199, *Safety of machinery*.

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.

Introduction

This document was developed to provide information about systems incorporating measures that can be introduced into machinery, especially in IMS for reducing risks based on human factors.

Due to lack of human attentiveness during any task performed in a hazard zone (for example, inspections, maintenance or set-up), safeguarding supportive systems can be used as a technical measure to minimize the probability of dangerous human errors occurring.

Safety of machinery — Safeguarding supportive system

1 Scope

This document provides guidance for the design and integration of a safeguarding supportive system (SSS) which is intended to include a mode selection as part of an SRP/CS or to add a layer of personnel authentication and authorization to an IMS designed according to ISO 11161.

This document is meant to be used in conjunction with ISO 11161.

This document is applicable to the SSS but does not address personnel qualification and competency.

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 11161:2007, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 11161, ISO 12100 and the following apply.

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

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

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

3.1
safeguarding supportive system
SSS
complementary risk reduction/protective measure to enable mode selection by the use of *authentication* (3.5) means

3.2
identification element
device used in the *safeguarding supportive system* (3.1), referring to all logic units and their peripheral equipment, but excluding the credential database

Note 1 to entry: Examples include readers, key switches, cameras, HMI's, industrial PLCs.

3.3
control zone
identified portion of an IMS coordinated by the control system

[SOURCE: ANSI B11.20-2017, 3.39.1]

3.4
qualified personnel
individual(s) who, as a result of training and experience, understands and demonstrates competence with the design, construction, operation or maintenance of the machine and the associated hazards

[SOURCE: ANSI B11.0-2020, 3.68]

3.5
authentication
verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

[SOURCE: ISO/TR 22100-4:2018, 3.3, modified — In the definition, "verifying" has been changed to "verification of".]

3.6
authorization
right or permission that is granted to a system entity to access a system resource

[SOURCE: ISO/TR 22100-4:2018, 3.4]

3.7
authorized personnel
qualified personnel identified by the user (employer) or supplier to perform a specific task

[SOURCE: ANSI B11.0-2020, 3.7]

4 Symbols and abbreviated terms

HMI	human–machine interface
ID	identification
IMS	integrated manufacturing system
PLC	programmable logic controller
RF	radio frequency
RFID	radio frequency identification
SPE	sensitive protective equipment
SRP/CS	safety-related parts of a control system

5 Safeguarding supportive system

5.1 General

A safeguarding supportive system is used in conjunction with, and not in place of, guards and protective devices.

A safeguarding supportive system enables a requested mode when the authorization matches the requirements for the task to be performed.

The safeguarding supportive system affects all modes of operation requiring tasks in hazard zones including, for example, adjusting, set-up, teaching and troubleshooting. Accordingly, the safeguarding supportive system functions are based on modes of operation of the IMS described in ISO 11161:2007, 5.1.3, 8.2.2, and 8.4, and ISO 12100:2010, 6.2.11.9.

Figure 1 shows a concept of the implementation of an SSS.

NOTE Details on SRP/CS are dealt with in ISO 13849-1. Details on IMS are given in ISO 11161.

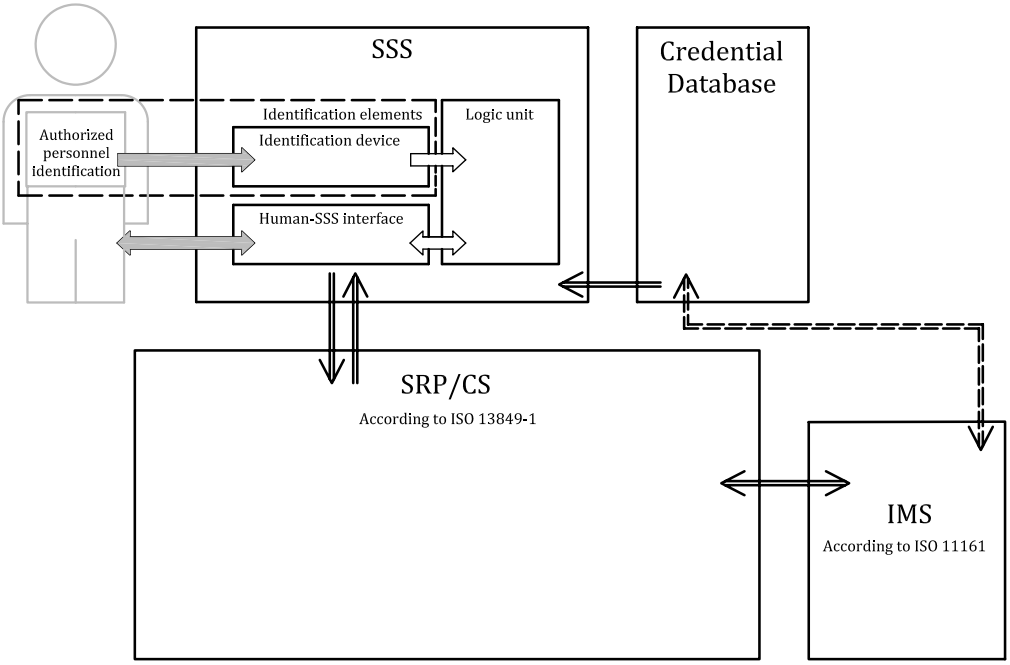

Figure 1 — Concept of the implementation of a SSS

5.2 Description of safeguarding supportive system

Safeguarding supportive systems (SSS) provide the following functions:

a) identification of authorized personnel;

b) check that the authorization for the selected task matches with the personnel identified;

c) information of the user about the task(s) authorized;

d) enabling of the operating mode corresponding to the selected task(s);

e) indication of the zones to be accessed by the authorized personnel.

The SSS is an additional layer which provides input(s) to the logic unit of the SRP/CS in order to enable the appropriate operating mode for the required task based on authentication. The mode selection itself is a safety function that requires SRP/CS with a performance level according to ISO 13849-1.

See also Figure A.1.

5.3 Interface between SSS and SRP/CS

The interface allows information exchange between SSS and the logic unit(s) of the SRP/CS. The safety functions enabled/disabled by the SSS can include but are not limited to:

a) restart;

b) reset;

c) release of guard locking device which locks the guard in the closed position (see ISO 14119).

6 Design of safeguarding supportive system

6.1 General

The integrator reviews the risk assessment of machinery/IMS considering the task zoning and the relevant spans-of-control. As shown in Figure 2, the system components of the SSS are identification elements (see 6.2.2), human–SSS interface (see 6.2.3) and logic unit (see 6.2.4). The SSS can be part of the SRP/CS or separated.

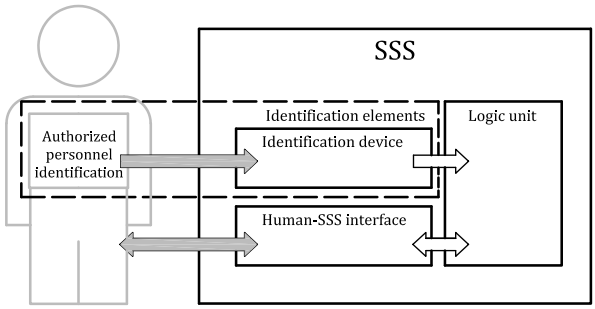

Figure 2 — Overview of safeguarding supportive system

The SSS design should consider as a minimum:

a) identification elements suitable for the application;

b) location of the identification device in relation to access zones/paths;

c) interface to credential database;

d) task(s) which require local operations;

e) relevant protective devices for local operations (for example, enabling device, SPE);

f) information to be displayed (for example, applied task, access/exit path).

6.2 System components

6.2.1 General

The system components consist of identification elements (see 6.2.2), human–SSS interface (see 6.2.3) and logic unit (see 6.2.4).

6.2.2 Identification elements

6.2.2.1 General

The identification elements comprise any technology by which authentication can be achieved. The authentication can be related to personnel skills and/or authorization and can be used to register entry and exit to a control zone, or subsequent control zones.

The identification elements comprise of an identification device (see 6.2.2.2) and an authorized personnel identification (see 6.2.2.3).

6.2.2.2 Identification device

The identification device reads the authorized personnel identification and transmits the information to the logic unit of the system components (see Annex A).

The identification device should be located to easily perform the required tasks.

NOTE Examples of identification devices include biometric devices (e.g. camera), RF tag readers, barcode readers, mechanical/electromechanical key cylinders, key pads for password(s).

6.2.2.3 Authorized personnel identification

Authorized personnel identification can include biometric properties (e.g. retina scan, fingerprints) and/or identifiers assigned to the user (e.g. RF tag, authorized personnel identification card, key).

6.2.3 Human–SSS interface

The human–SSS interface is where the request is made. The human–SSS interface exchanges information with the logic unit. The human–SSS interface indicates visibly and/or audibly the IMS status information including the results of the request.

NOTE The human–SSS interface can be a keyboard, a switch, a touch panel, etc.

The following information can be considered for display:

a) task zones that the authorized personnel can access, access paths to those zones and exit routes when necessary;

b) selected task;

c) tasks for which the authorized personnel is permitted;

d) authorization results in response to a request to perform a safety-related operation.

e) significant information of accessible adjacent task zones, for example, operating modes, if automatic/unexpected restart can occur (see ISO 12100:2010, 6.3.3.2.5).

6.2.4 Logic unit

The logic unit authenticates the authorized personnel identification and the request to the human-SSS interface with the credential database. Upon authentication, the logic unit presents authorized actions and enables the selection of the authorized personnel, e.g. selection of a mode.

6.3 Output from the credential database

The following information can be used as output from the credential database as defined by the user (see Figure 1):

a) tasks based on the authorized personnel permissions;

b) modes based on the authorized personnel permissions;

c) combination of authorized personnel and tasks associated with each mode of operation.

The credential database can be part of the SSS or a remote network resource or some combination thereof.

6.4 Verification and validation

The SSS integrator should verify and validate the design and structure of the SSS according to ISO 12100:2010, 6.2.11.7.

The SSS integrator should verify and validate the mode selection meets or exceeds the requirements for the safety function according to ISO 13849-1 and ISO 13849-2.

7 Information for use

The information for use should include guidance necessary for the authorization to be granted.

Advice should be given in the information for use of the machine or IMS concerning the risks associated with the handling of authorized personnel identification (ID cards, RFID tags, keys, etc.) and also about the availability of spare authorized personnel identifications.

See also ISO 11161:2007, Clause 9, and ISO 20607.

Annex A
(informative)

Visualization of integration of SSS within IMS

See Figure A.1.

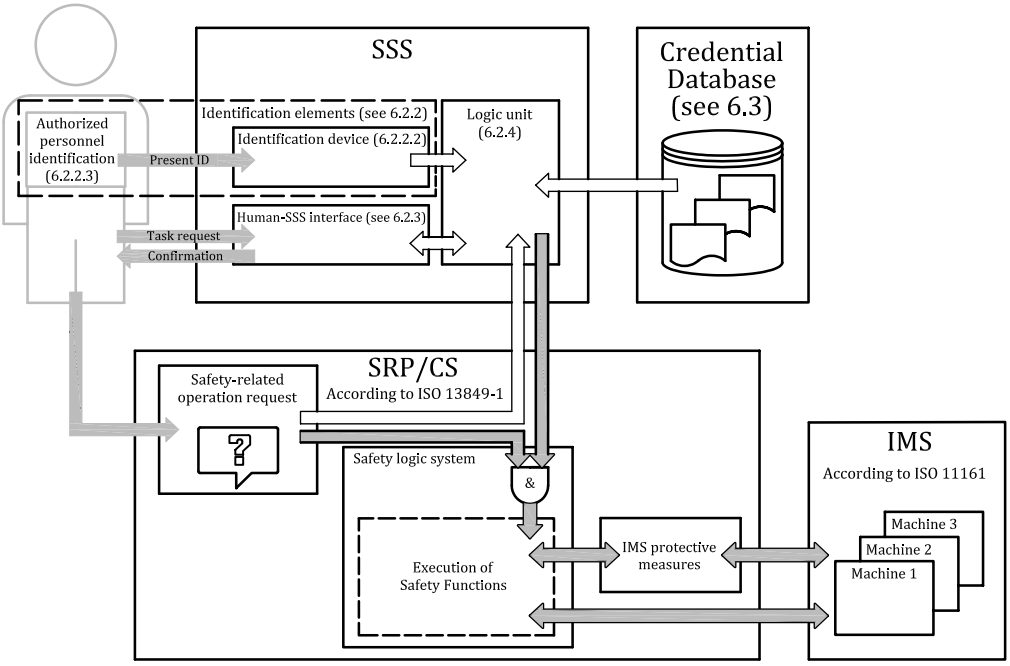

Figure A.1 — Elements relating to an SSS with all details regarding the SRP/CS and the IMS

Bibliography

[1] ISO 13849-1:2015, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

[2] ISO 13850, *Safety of machinery — Emergency stop function — Principles for design*

[3] ISO 14119:2013, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[4] ISO 20607, *Safety of machinery — Instruction handbook — General drafting principles*

[5] 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*

[6] ANSI B11.0-2020, *Safety of Machinery*

[7] ANSI B11.20-2017, *Safety Requirements for Integrated Manufacturing Systems*

ICS 13.110
Price based on 8 pages