

PGS-004951, Rev.: 00 – 25/11/2021

Issuer Executive Officer: Executive officer of Health, Safety and Operational Risks

Responsible Technician: Rudson Chaves de Souza - Registration: 81013387

Target Audience: 1<sup>st</sup> Defense Line

Training Need: (x) YES () NO

## SUMÁRIO

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>OBJECTIVE</b>                          | <b>4</b>  |
| 1.1      | Introduction                              | 4         |
| 1.2      | Objective                                 | 4         |
| <b>2</b> | <b>APPLICATIONS</b>                       | <b>5</b>  |
| 2.1      | Applicability                             | 5         |
| 2.2      | Legislations                              | 5         |
| 2.3      | Corporate Regulation                      | 5         |
| 2.4      | Standards                                 | 6         |
| 2.5      | Exceptions                                | 7         |
| <b>3</b> | <b>DEFINITION AND REFERENCE DOCUMENTS</b> | <b>8</b>  |
| 3.1      | Internal References                       | 8         |
| 3.2      | Standard and Legislation                  | 8         |
| 3.3      | Complementary Reference                   | 10        |
| 3.4      | Definitions and Terminology               | 10        |
| <b>4</b> | <b>MACHINERY GUIDELINES</b>               | <b>12</b> |
| 4.1      | Inventory                                 | 12        |
| 4.2      | New Machinery                             | 12        |
| 4.3      | Existing Machinery                        | 14        |
| 4.4      | Machinery Modification                    | 15        |
| <b>5</b> | <b>GUIDELINES FOR RISK ASSESSMENT</b>     | <b>16</b> |
| 5.1      | Risk Estimation Method                    | 16        |
| 5.2      | Risk Estimation and Evaluation            | 18        |
| 5.3      | Risk reduction (3 step method)            | 18        |
| <b>6</b> | <b>GENERAL MACHINE SAFETY GUIDELINES</b>  | <b>20</b> |
| <b>7</b> | <b>GUIDELINES FOR SAFETY SYSTEMS</b>      | <b>23</b> |
| 7.1      | Control System                            | 23        |
| 7.2      | Control Device                            | 24        |
| 7.3      | Sound and Visual Signaling                | 25        |
| 7.4      | Start and Stop Devices                    | 26        |

|             |   |           |
|-------------|---|-----------|
| <b>7.5</b>  | <b>Mode Selection</b> .....   | <b>26</b> |
| <b>7.6</b>  | <b>Safeguarding</b> .....   | <b>28</b> |
| 7.6.1       | Safeguards .....  | 28        |
| 7.6.2       | Selection of Guards .....   | 28        |
| 7.6.3       | Fixes Guards .....  | 29        |
| 7.6.4       | Moveable Guards .....   | 30        |
| 7.6.5       | Other Types of Guards .....   | 32        |
| <b>7.7</b>  | <b>Safeguard Devices</b> .....  | <b>32</b> |
| 7.7.1       | Electro Sensitive Protective Equipment (ESPE).....                          | 32        |
| 7.7.2       | Active Optoelectronic Protective Devices (AOPD) .....                       | 33        |
| 7.7.3       | Safety Mats and Safety Floors .....   | 34        |
| <b>7.8</b>  | <b>Safety Distance</b> .....  | <b>34</b> |
| 7.8.1       | Safety Distances to Prevent Access to Upper Limbs .....                     | 34        |
| 7.8.2       | Reaching Over Protective Structures .....                                   | 35        |
| 7.8.3       | Reaching around .....   | 36        |
| 7.8.4       | Reaching Through Openings.....  | 38        |
| 7.8.5       | Minimum Safe Distances Between Moving Parts Which Create a Crushing Risk .. | 38        |
| 7.8.6       | Safety Distance in Relation to Approach Speed.....                          | 39        |
| <b>7.9</b>  | <b>Safety in Fluid System</b> .....   | <b>40</b> |
| <b>7.10</b> | <b>Emergency Stop Devices</b> .....   | <b>41</b> |
| 7.10.1      | Emergency Stop Button.....  | 42        |
| 7.10.2      | Emergency Rope Switch .....   | 43        |
| 7.10.3      | Kick Bars, Plates, Handles and Foot-Pedals .....                            | 44        |
| <b>7.11</b> | <b>Safety Control System</b> .....  | <b>44</b> |
| 7.11.1      | Safety Categories .....   | 46        |
| 7.11.2      | Performance Levels.....   | 47        |
| 7.11.3      | Determination of Required Performance Level (PLr).....                      | 48        |
| 7.11.4      | Safety Related Specification Matrix for Safety Design .....                 | 49        |
| <b>7.12</b> | <b>Energy Sources</b> .....   | <b>50</b> |
| 7.12.1      | Electrical Energy .....   | 50        |
| 7.12.2      | Pneumatic & Hydraulic Energy.....   | 52        |
| <b>7.13</b> | <b>Unexpected Start-up and Control of Hazardous Energy</b> .....            | <b>53</b> |
| 7.13.1      | Exposure Levels to Hazardous Energy .....                                   | 54        |
| 7.13.2      | Control Measures to Prevent Unexpected Start-up .....                       | 57        |
| 7.13.3      | Manual Isolation of Dangerous Energy Sources (LOTO) .....                   | 59        |
| <b>7.14</b> | <b>Means of Access</b> .....  | <b>60</b> |

|           |   |           |
|-----------|---|-----------|
| 7.15      | Signage System .....  | 69        |
| 7.15.1    | Signal dimension .....  | 73        |
| <b>8</b>  | <b>LIST OF PRODUCERS .....</b>                                | <b>74</b> |
| <b>9</b>  | <b>REVISION HISTORY .....</b>                                 | <b>77</b> |
| <b>10</b> | <b>ANNEXS .....</b>   | <b>78</b> |
| 10.1      | Annex A - Differences among Countries/Areas .....             | 78        |
| 10.2      | Annex B – Determination of PLr according to ISO 13849-1 ..... | 81        |
| 10.3      | Annex C – Definition of Safety Category .....                 | 82        |
| 10.4      | Annex D – Warning Pictograms .....                            | 85        |

## 1 OBJECTIVE

### 1.1 Introduction

The intent of this document is to specify minimum safety and health guidelines for machines to prevent work accidents and occupational hazards during all activities related with machinery like un/installation, de/commissioning, operation, and maintenance.

This document seeks to achieve regulatory compliance and a uniform approach to Machinery safeguarding for all machinery in Vale's facilities worldwide. This document is for facilities, original equipment manufacturers (OEMs) and all other machinery, installations, operation, maintenance, engineering and suppliers.

The body of this document describes the general guidelines which shall be met. The information in the document contains guidance, based on current good practices as set out in international safety norms, on Vale's recommended method of achieving these directives.

The guidelines are not limited to the ones specified in this document. Additional guidelines may be required for certain types of machinery, equipment and application.

All facilities should benchmark their management of work equipment safety with the guidance in this document, unless it is not relevant to their situation, or they have alternative local arrangements that deliver at least the same level of safety and health. When local legislation requires or recommends stricter standards, these will need to be applied.

The objective of this document is to protect workers and machinery from the hazards associated with machinery and to prevent accidents and incidents resulting from the use of machinery at work. This will be achieved by providing specifications to:

- Ensure that all machinery for use at work is designed, manufactured, and modified in accordance with the required safety standards;
- Ensure that machinery suppliers take into account the directives explained in this document.

### 1.2 Objective

Establish minimum guidelines for machine protection in acquisition, installation, commissioning, operation and maintenance activities to avoid accidents.

## 2 APPLICATIONS

### 2.1 Applicability

This document applies to all, new and existing, machinery in Vale facilities and third parties at Vale's service:

- Fixed or mobile machinery and installations: New (new project), legacy and modified machines;
- Machinery purchased from supplier catalogues, including those adapted for Vale;
- Machinery specifically manufactured for Vale;
- Modifications carried out in existing machinery and installations.

### 2.2 Legislations

Safety protections, devices and systems must comply with the provisions of all applicable local legislation and national and international technical standards, taking into account aspects of maintenance and operation.

This standard is not intended to replace any local machine regulations or requirements. This shall be met together with the requirements of CAR 7 (PNR-000069), prevailing the most restrictive and safe items. In the event of conflicting requirements, the stricter requirement shall be met.

There is no common regulation about machinery safety worldwide. The most well-known systems are:

- European CE marking of machinery according to the applicable EU directives;
- Brazilian NR12 marking of machinery and equipment according to Norma Regulamentadora 12 (NR-12) – MÁQUINAS E EQUIPAMENTO;
- Russian TR certification;
- Chinese CCC certification;
- UL – Norte Americana certification (EUA e Canada).

More detailed information about specific country/area legislations of machinery safety can be found in Annex A.

### 2.3 Corporate Regulation

The topics mentioned in this corporate standard explains machinery safety aspects in terms of international machinery safety standards. The standards mentioned in item 2.4 are examples of standards issued by standardization organizations, which are not necessarily required to be complied with for the purposes of this document.

All the guidelines and aspects mentioned in this document shall be followed in machines acquisitions, modifications and internal evaluations of Vale's machines.

## 2.4 Standards

Standards are formal documents containing technical specifications or other criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose.

At international level, the most important publishers of engineering standards are the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO). The EN standards are applied at European level by CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) as EU initiatives. National standards are published by national standards institutes. If an ISO standard becomes an EN standard, its title becomes EN ISO. If it then becomes a DIN (German Institute for Standardization - Deutsches Institut für Normung) standard, its full title will be DIN EN ISO, the same occur if a Brazilian standard, if an ISO became a NBR, its title will be NBR ISO.

In the US and Canada, the standardization process is facilitated by ANSI (American National Standards Institute) and SCC (Standards Council of Canada), respectively. Both ANSI and SCC accredit Standards Development Organizations (SDOs) to draft standards that meet the needs of industry, government and consumers. Examples of accredited SDOs and some of their respective standards:

- B11 Standards, Inc. (EUA):
  - ANSI B11.0 - Safety of Machinery;
- American Society of Safety Engineers (ASSE - EUA):
  - ANSI/ASSE Z244.1 - The Control of Hazardous Energy - Lockout, Tagout and Alternative Methods;
- Robotic Industries Association (RIA - EUA):
  - ANSI/RIA 15.06 – Industrial Robots And Robot Systems - Safety Requirements;
- National Fire Protection Association (NFPA - EUA):
  - NFPA 70 - National Electrical Code;
  - NFPA 79 - Electrical Standard for Industrial Machinery;
- Underwriters' Laboratory (UL - EUA e Canada):
  - ANSI/CAN/UL 2808 – Energy Monitoring Equipment;
- Canadian Standards Association (operating as CSA Group - EUA e Canada):
  - CSA Z432 - Safeguarding of machinery;
  - CSA Z460 - Control of hazardous energy - Lockout and other methods;
  - CSA C22.1 - Canadian Electrical Code, Part I, Safety Standard for Electrical Installations;
  - CSA C22.2 No. 301 – Industrial electrical machinery (under Part II of the Canadian Electrical Code).

The Standards can be divided into three main categories as shown in the Figure 1.

A-Type standards are applied for all types of machineries. B-Type standards are applied to almost all machinery containing the aspect/device the standard is mentioning about. C-Type standard are machine type specific standards that contain specific requirements for the mentioned type.

Where Type C standard (Specific Standard) exists for machinery, it shall be used in preference to other standards (A and B types – General Standards). Otherwise A and B type standards should be used accordingly.

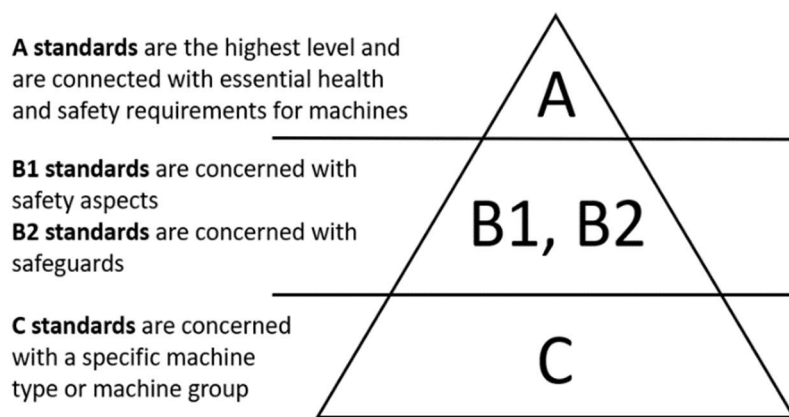


Figure 1 – Standards categorization pyramided

## 2.5 Exceptions

The guidelines of this manual do not apply to:

- a) Parts, components, or interchangeable equipment that by themselves do not constitute a machine;
- b) Lifting Accessories: Chains, Ropes, steel cable;
- c) Machinery and equipment with installation partly completed, for testing at this stage, a preliminary risk assessment of the activity (PRN-000068 ART) and Safe Work Permit (PNR-000031 PTS) shall be established and validated by the safety team and the technician responsible for the assembly / construction of the machine;
- d) Machinery designed for:
  - i. Nuclear and/or windmill power generation purposes;
  - ii. On board for seagoing vessels and mobile offshore units;
  - iii. High voltage electrical equipment (example: generators, transformers, etc.).

## 3 DEFINITION AND REFERENCE DOCUMENTS

### 3.1 Internal References

Vale

- CAR 7 Machine Safeguarding (PNR-000069);
- CAR 4 LOTO (Control of Hazardous Energy) (PNR-000069);
- CAR 1 Work at height (PNR-000069);
- PNR-000081 – Instrumentation and Control - Supervision and Control System - Instrumented Safety System (SIS).

### 3.2 Standard and Legislation

- NR-12 – Segurança de Máquinas e Equipamentos (Machine and Equipment Safety)
- IEC 62046:2018 – Safety of Machinery – Application of Protective Equipment to Detect the Presence of Persons
- EN 619:2002+A1:2010 – Continuous Handling Equipment and Systems – Safety and EMS Requirements for Equipment for Mechanical Handling of Unit Loads
- EN 981:1996+A1:2008 – Safety of Machinery – Systems of auditory and Visual Danger and Information Signals
- IEC 60204-1:2016 – Safety of Machinery – Electrical Equipment of Machines – Part 1: General Requirements
- IEC 60529:1989+A1:1999+A2:2013 – Degrees of Protection Provided by Enclosures (IP Code)
- ISO 4413:2010 – Hydraulic Fluid Power – General Rules and Safety Requirements for Systems and Their Components
- ISO 4414:2010 – Pneumatic Fluid Power – General Rules and Safety Requirements for Systems and Their Components
- ISO 10218-2:2011 – Robots and Robotic Devices – Safety Requirements for Industrial robots – Part 2: Robot Systems and Integration
- ISO 11161:2007+Amd 1:2010 – Safety of Machinery – Integrated Manufacturing Systems – Basic Requirements
- ISO 12100:2010 – Safety of Machinery – General Principles for Design – Risk assessment and Risk Reduction
- ISO 13732-1:2006 – Ergonomics of the Thermal Environment – Methods for Assessment of Human Responses to contact with surfaces – Part 1: Hot surfaces
- ISO 13849-1:2015 – Safety of Machinery – Safety-related parts of control systems – Part 1: General Principles for design
- ISO 13849-2:2012 – Safety of Machinery – Safety-related parts of control systems – Part 2: Validation



- ISO 13850:2015 – Safety of Machinery – Emergency Stop Function – Principles for design
- ISO 13851:2019 – Safety of Machinery – Two-Hand Control Devices – Principles for Design and Selection
- ISO 13854:2017 – Safety of Machinery – Minimum Gaps to Avoid Crushing of Parts of the Human Body
- ISO 13855:2010 – Safety of Machinery – Positioning of Safeguards with Respect to the Approach Speeds of Parts of the Human Body
- ISO 13856-1:2013 – Safety of Machinery – Pressure-Sensitive Protective Devices – Part 1: General Principles for Design and Testing of Pressure-Sensitive Edges and Pressure-Sensitive Floors
- ISO 13856-2:2013 – Safety of Machinery – Pressure-Sensitive Protective Devices – Part 2: General Principles for Design and Testing of Pressure-Sensitive Mats and Pressure-Sensitive Bars
- ISO 13856-3:2013 – Safety of Machinery – Pressure-Sensitive Protective Devices – Part 3: General Principles for Design and Testing of Pressure-Sensitive Bumpers, Plates, Wires and Similar Devices
- ISO 13857:2019 – Safety of Machinery – Safety Distances to Prevent Hazard Zones Being Reached by Upper and Lower Limbs
- ISO 14118:2017 – Safety of Machinery – Prevention of Unexpected Start-up
- ISO 14119:2013 – Safety of Machinery – Interlocking Devices associated with Guards – Principles for Design and Selection
- ISO 14120:2015 – Safety of Machinery – Guards – General Requirements for the design and construction of fixed and moveable guards
- ISO 14122-1:2016 – Safety of Machinery – Permanent Means of Access to Machinery – Part 1: Choice of Fixed Means and General Requirements of Access
- ISO 14122-2:2016 – Safety of Machinery – Permanent Means of Access to Machinery – Part 2: Working Platforms and Walkways
- ISO 14122-3:2016 – Safety of Machinery – Permanent Means of Access to Machinery – Part 3: Stairs, Stepladders and Guard-Rails
- ISO 14122-4:2016 – Safety of Machinery – Permanent Means of Access to Machinery – Part 4: Fixed Ladders
- ISO 7010:2019 – Graphical Symbols – Safety Colours and Safety Signs – Registered Safety Sign
- ISO 3864:2002 – Graphical symbols – Safety Colours and safety signs – Part 1: Design principles for safety signs in workplaces and public areas
- ISO 3864:2004 – Graphical symbols – Safety Colours and safety signs – Part 2: Design principles for product safety labels

## 3.3 Complementary Reference

The Safety Compendium – Pilz

([https://www.pilz.com/mam/pilz/content/editors\\_mm/safety\\_compendium\\_en\\_2017\\_12\\_low.pdf](https://www.pilz.com/mam/pilz/content/editors_mm/safety_compendium_en_2017_12_low.pdf))

## 3.4 Definitions and Terminology

- ALARP: As low as reasonable possible.
- AOPD: Active Opto-electronic Protective Devices (light curtains, area scanners, etc.).
- CCF: Common Cause Failure; failures of different items, resulting from a single event, where these failures are not consequences of each other.
- Control devices: mechanisms used to control a machine function.
- DC: Diagnostic Coverage; measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.
- ESPE: Electro-Sensitive Protective Equipment (e.g., People Presence Sensing Devices (PSDs), light curtains, safety mats).
- FAT Factory Acceptance Test, the tests carried out on the machine in OEM's facility before it is shipped to Vale facility.
- Hazard: potential source of injury or damage
- HRN: Hazard Rating Number used to estimate a risk.
- Interchangeable Equipment: A device which, after the putting into service in the machinery (example: exchanging the excavator shell for a stone crusher) changed by operation/maintenance in order to change its function or attribute a new function, in so far as this equipment is not a tool.
- Machinery: Machinery and equipment has several meanings:
  - an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort (powered by energy sources), consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application;
  - An assembly referred to in the first indent, missing only the components to connect it on site or to sources of energy and motion;
  - An assembly referred to in the first and second indents, ready to be installed and able to function as it stands only if mounted on a means of transport, or installed in a building or a structure;
  - Assemblies of machinery referred to in the first, second and third indents or partly completed machinery (definition available in this chapter) which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole machine;

- an assembly of linked parts or components, at least one of which moves and which are joined together, intended for lifting loads (example: manual hoist) and whose only power source is directly applied human effort.
- Maintenance: All maintenance activities including planned predictive/preventative/corrective maintenance.
- MTTF<sub>D</sub>: Mean Time to Dangerous Failure; expectation of the mean time to dangerous failure.
- OEM: Original Equipment Manufacturer.
- Operation: All activities during normal operation like production, set-up, changeover, and cleaning.
- Partly Completed Machinery: An assembly which is almost machinery, but which cannot in itself perform a specific application. Partly completed machinery is only intended to be incorporated into or assembled with other machinery or other partly completed machinery or equipment.
- P&ID (Pipe & Instruments Diagrams): diagram used in industrial processes to indicate industrial plant piping, equipment and instrumentation.
- PL: Performance Level.
- PLr: Performance Level Required.
- PPE: Personal Protective Equipment.
- Risk: means a combination of the probability and the degree of an injury or damage
- SAT: Site Acceptance test, the tests carried out on the machine in Vale facility during commissioning activities.
- SDOs: Standards Development Organizations (USA and Canada).
- Span of Control: Pre-determined section of the machinery under control of specific emergency stop device(s).
- SRP/CS: Safety-related part of a control system; part of a control system that creates/responds to safety-related input signals and generates/acquires safety-related output signals.
- TM: Time Mission (usage) of a safety component. Represents the reliability of a component with respect to its safety performance.

## 4 MACHINERY GUIDELINES

### 4.1 Inventory

Each location shall have an inventory of its own machines and those of contracted companies.

### 4.2 New Machinery

For all new machinery purchased by Vale, the following guidelines shall be met:

- Machinery/equipment shall meet all required local legislation;
- Machinery/equipment shall be provided with an identification plate affixed or marked in local language;
- All certification (e.g. Declaration of Conformity, etc.) and documentation (e.g. Operations manual, maintenance manual, technical drawings, etc.) is provided to Vale in advance in electronic format; <sup>(1)</sup>
- Machines and equipment will only be accepted upon a risk assessment report in accordance with ISO 12100, following the HRN methodology, whose risk levels shall be at most acceptable or tolerable risks and with indication of PL (Performance Level) of the safety systems in accordance with ISO 13849-1;
- For the machines/equipment customized or specifically designed for Vale, in addition to the guidelines above the following procedure shall also be followed:
  - The Original Equipment Manufacturer (OEM) shall carry out a risk assessment and supply the report about all the residual risks present on the machinery, and existing and recommended measures to be implemented for residual risks to Vale:
    - This risk assessment report must be stored in the engineering documentation management system (i.e. GED – Electronic Document Management, SAP, etc.);
    - After the assembly of the machine or equipment, a new risk assessment must be carried out;
    - This risk assessment review must be recorded in the CAR 7 management system;
    - The risk assessment mentioned in the item above must be reviewed by the supplier with the participation of a multidisciplinary team from Vale;
    - The Vale multi-discipline team must assess the equipment and machinery as in accordance with the HRN methodology;
    - The machines will only have a signed and approved “commissioning protocol” if they contain at most tolerable residual risks (according to the HRN methodology);
  - The OEM shall supply a functional testing list for the machinery, with focus on safety-related aspects;
  - Vale shall confirm the functional testing list or specify any additional tests required. Some examples of the tests that may be included are:

- Static/Dynamic mechanical stress analysis;
  - Performance Level Analysis of the Safety Control System;
  - Equipment Electrical Safety Analysis;
  - EMC (Electromagnetic Compatibility) tests, if applicable;
  - Protective Earth Continuity testing;
  - Noise measurement;
  - Safety-related Requirements Specification (SRS) testing, etc.
- An FAT shall be performed (if applicable);
  - All non-conformities and remarks shall be corrected by the OEM before shipment;<sup>(1)</sup>
  - An SAT shall be performed with following the items requirements described below;
  - All non-conformities and remarks shall be corrected by the OEM before commissioning activities.<sup>(1)</sup>

<sup>(1)</sup> In certain cases, some of the non-conformities defined at SAT or FAT activities can be corrected or the documentation submitted to Vale after the stages defined above with the approval of responsible personnel. In any case, all the modifications, certification and documentation shall be provided by the OEM/supplier and controlled before the end of machinery hand-over to Vale.

Vale can appoint third-party organization to conduct the FAT and/or SAT activities. In such cases, Vale will provide the contact details of the third-party organization that will perform the tests to the OEM/supplier.

Specific acceptance tests shall be developed for each machine that will include all the verification and validation activities specified for the machine. However, the general acceptance test items, described briefly below, shall be included as a minimum:

- Hazardous Energies Isolation Check (CAR 4): Testing of energy isolation devices of the machine to determine whether such devices are capable of safely isolated the energy and can be locked-out in “OFF” position;
- Mechanical guards Check: Testing of mechanical guards to ensure they can safely prevent access to hazardous areas and that they are installed respecting safety distances and ergonomic aspects;
- Emergency Stop Devices Check: Testing of emergency stop devices (e.g. pushbuttons, ropes, etc.) to determine whether such devices can safely stop all the hazardous movements of the machinery within its span of control in all operating modes. Reset/restart function controls and de-energization of all relevant actuators shall also be checked;
- Power Control Devices Check: Power control devices (e.g. motor drivers, contactors, etc.) of actuators of hazardous movements can be duplicated, controlled and monitored by the safety control system in accordance with standards on safety-related parts of control system (SRP/CS). Verification and validation of these aspects shall be carried out;

- Safety Interlocks Check: Testing of interlock switches to validate that all hazardous movements within their span of control are stopped and restart is prevented by the safety control system when the interlocks are actuated, in all applicable operating modes, especially automatic mode;
- Enabling Devices (Pushbuttons, foot pedals) Check: Testing of enabling devices (e.g. two-hand controls, hold-to-run, etc.) to confirm that the machine movements are done until controlled by actuation of the enabling device under specified conditions (e.g. reduced speed, jogging, etc.).

The acceptance tests shall be carried out on individual machines first before combining to groups or assemblies of machinery, if applicable. Risks or hazards resulting from the interfaces of two individual machines shall also be considered in such tests.

The list of periodic machine checks and maintenance activities with an emphasis on safety systems and safeguarding's shall be created and followed in accordance with the OEM or a more thorough plan at Vale's discretion.

### 4.3 Existing Machinery

A risk assessment must be carried out for all existing machines in Vale, including Subcontractors, following the HRN methodology.

The risk assessment of the existing machinery shall be revised after any significant operational change that modify the actual safety level or create new hazards, design change or after the occurrence of an accident.

After the occurrence of an accident, a verification shall be carried out to determine whether:

- any change in operation parameters; has occurred;
- new risks have been introduced; or
- any change in remaining risk estimation parameters occurred.

If any safety device is removed or deteriorated and that cannot be solved during the maintenance routine, a new change management process (PNR-0000101) shall be created and safety mitigation measures shall be adopted until the permanent control measure is implemented. The permanent control measure shall be implemented as fast as possible, regardless of the production processes.

If non-existent, a list of periodical inspection and maintenance activities on the machine with emphasis on safety systems and safeguarding shall be created and followed in accordance with the OEM specifications or in accordance with more thorough plan at Vale's discretion.

Measures arising from risk assessments shall be implemented and verified for their effectiveness.

### 4.4 Machinery Modification

Before planning and implementing the machinery modifications the flow chart explained in Figure 2 should be followed.

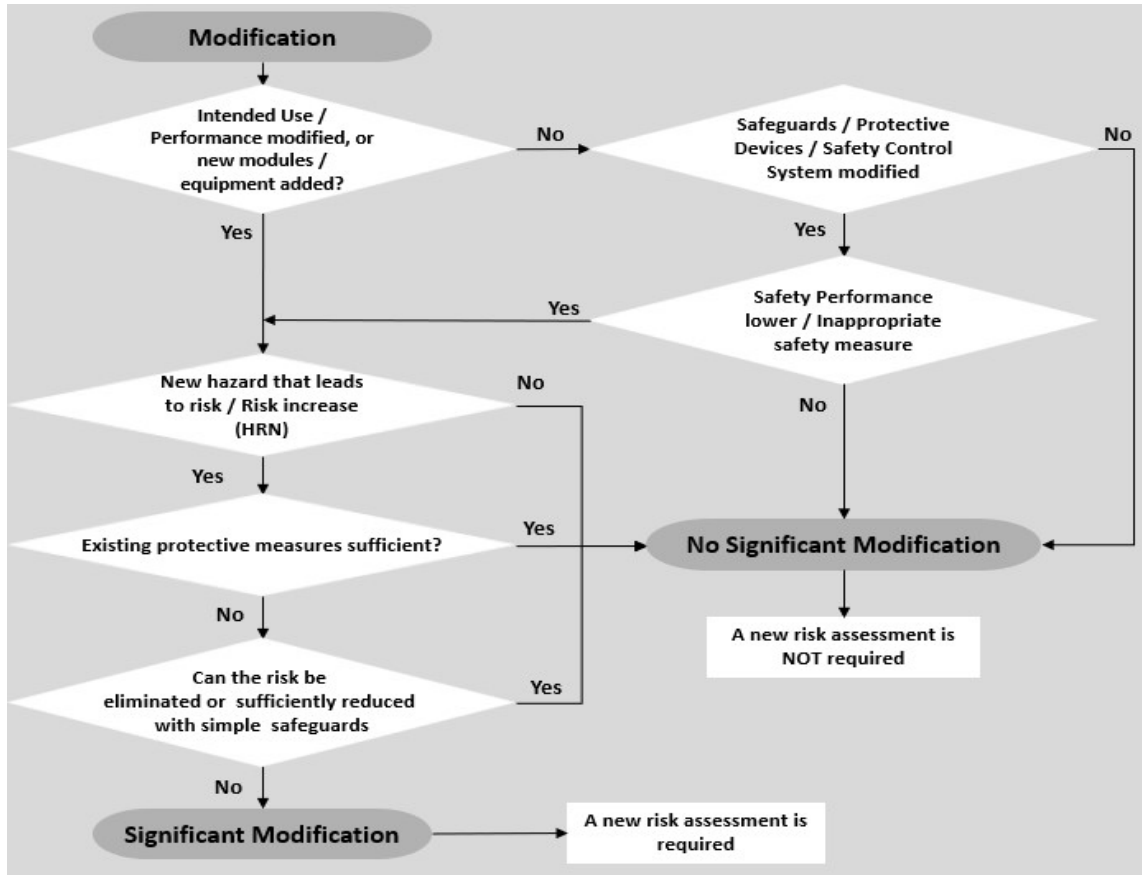


Figure 2 – Significant Modification Determination Flow

If the modification to be made is defined as a significant modification, the process for new machinery shall be applied, i.e., a new risk assessment shall be carried out for the machine. A new change management process (PNR-0000101) shall be created and safety mitigation measures shall be adopted until the permanent control measure is implemented. The permanent control measure shall be implemented as fast as possible, regardless of the production processes.

Before any modification to a machine, suppliers, especially in cases of more than one supplier/OEM/integrator, shall agree with Vale who is responsible for ensuring the machine remains both safe and in compliance with local legislation. In the cases of single OEM/Supplier/integrator, conformance with the legislation is the responsibility of that company.

Measures arising from risk assessments shall be implemented and verified for their effectiveness.



## 5 GUIDELINES FOR RISK ASSESSMENT

The risk assessment process described below applies to new, existing and modified machines.

A risk assessment shall be performed for each individual machine for all life cycle phases of machine (Construction, commissioning, use, maintenance, cleaning, adjustments, decommissioning). The intended and foreseeable misuse of the machinery shall be considered in the risk assessment.

The machine manufacturer (OEM), supplier or Vale engineering/SSMA shall provide a document detailing all of the relevant hazards (e.g. mechanical, control system, ergonomics, etc.) associated with the machine, and details of the methods used to eliminate or reduce the risks of these hazards on the machine.

Furthermore, all the residual risks present on the machinery shall be reported, recommended risk reduction measures to be implemented by Vale and evaluation of risks prior to and after implementation.

The risk assessment should be revised periodically (i.e. after new equipment layout, after the occurrence of an accident, change, etc.) to define if any additional risks or any change in existing risk parameters occurred.

In the cases of significant modifications to existing machinery according to the flowchart in figure 2, a new risk assessment shall be performed by the supplier, OEM, system integrator, a third-party company or Vale depending on the parties involved and their responsibility. The assessment shall consider all the aspects of the modifications and the implications to other machinery, equipment and tasks. The risk assessment including all of the residual risks of the machinery shall be documented.

### 5.1 Risk Estimation Method

The Hazard Rating Number (HRN) method is the method adopted by Vale and shall be used in risk assessments

There are four parameters in HRN methodology:

- Likelihood of Occurrence (LO)
- Degree of Possible Harm (DPH)
- Frequency of Exposure (FE)
- Number of Persons at risk (NP)

These parameters can take different values according to the risk assessed. The different values each parameter can take, and their explanations are shown in Table 1.



| <b>Likelihood of Occurrence (LO)</b> |                   | <b>Degree of Possible Harm (DPH)</b> |  |
|--------------------------------------|-------------------|--------------------------------------|--|
| 0,033                                | Almost impossible | 0,1                                  | Scratch / Bruise   |
| 1                                    | High unlikely     | 0,5                                  | Laceration / cut / mild ill health effect                                |
| 1,5                                  | Unlikely          | 1                                    | Fracture: minor bone – fingers / toes                                    |
| 2                                    | Possible          | 2                                    | Fracture – major bone – hand / arm leg                                   |
| 5                                    | Even chance       | 4                                    | Loss of 1 and 2 fingers / toes   |
| 8                                    | Probable          | 8                                    | Leg / hand amputation, partial loss of hearing or eye                    |
| 10                                   | Likely            | 10                                   | Amputation of legs/hands, total loss of hearing /sight in both ears/eyes |
| 15                                   | Certain           | 12                                   | Critical or permanent illness  |
|                                      |                   | 15                                   | Fatality   |

| <b>Frequency of Exposure (FE)</b> |            | <b>Number of Persons at risk (NP)</b> |                      |
|-----------------------------------|------------|---------------------------------------|----------------------|
| 0,5                               | Annually   | 1                                     | 1-2 persons          |
| 1                                 | Monthly    | 2                                     | 3-7 persons          |
| 1,5                               | Weekly     | 4                                     | 8-15 persons         |
| 2,5                               | Daily      | 8                                     | 16-50 persons        |
| 4                                 | Hourly     | 12                                    | More than 50 persons |
| 5                                 | Constantly |                                       |                      |

**Table 1 – HRN parameter values and definitions**

The risk estimation HRN parameters shall be judged consider the data and evidence analyze in the machine. The following criteria should be taken into account when judging the parameters

- Likelihood of Occurrence (LO):
  - Reliability information;
  - Installed systems;
  - Possibility to avoid;
  - Accident history.
- Degree of Possible Harm (DPH)
  - The nature of what is to be protected (example: people, equipment, environment, etc.)
  - Injury severity or damage size.

- Frequency of Exposure (FE):
  - Need and type of access;
  - Time spent on the activity;
  - Number of accesses.
- Number of Persons at risk (NP)
  - One or more exposed persons;
  - Extent of damage to equipment, facilities, etc.

## 5.2 Risk Estimation and Evaluation

Risk evaluation according to the risk assessment method above will be explained in this section. All risks related with the machinery shall be listed in a document and all of the parameters shall be defined for each individual risk. After defining all parameters, the formula below shall be applied to find the HRN score:

$$HRN = LO \times DPH \times FE \times NP$$

The values of HRN scores for each risk shall be assessed according to the risk level information stated in table below:

| HRN           | MACHINE RISK LEVEL | TOLERANCE                      |
|---------------|--------------------|--------------------------------|
| > 500         | Very high risk     | Mandatory risk level reduction |
| >50 up to 500 | High risk          | Continuous monitoring          |
| >5 up to 50   | Medium risk        | Tolerable                      |
| 0 up to 5     | Low risk           | Acceptable                     |

Table 2 – Risk Level Definition according to HRN score

## 5.3 Risk reduction (3 step method)

Following the risk evaluation, the risk reduction strategy and hierarchy explained below shall be used to reduce the risks to a tolerable (ALARP) level. Generally, risks evaluated as “LOW” or “MEDIUM” are considered tolerable (ALARP). Risks higher than these values shall be considered as intolerable within the approval of responsible Vale team.

### i. Inherently safe design measures (physical characteristics of the machine)

Inherently safe design measures for eliminating or reducing risks shall be the first choice for risk reduction when applicable. Risk reduction or elimination can be achieved by limiting or eliminating the exposure to the existing hazards, respectively, by, for example:

- Increased reliability of machine;
- Use of automation to reduce human intervention;
- Placement of maintenance points outside of hazardous zones;
- Routine operational and maintenance tasks able to be performed without the need for energy.

## ii. Safeguarding and Complementary Protective Measures (safeguarding physical and sensorial)

The second method for risk reduction is implementing engineering solutions for the risks. If strategies explained in Section (i) above are not possible or do not reduce the risk sufficiently, safeguards (e.g. fixed guards, guards and enclosures; moveable guards – interlock doors, etc.) or complementary protective measures (e.g. presence sensing devices – scanners e light curtain, etc.) can be applied to reduce the risks.

## iii. Information for Use

The residual risks remained after implementing the measures in Section items (i) and (ii) above shall be identified in the information for use. The residual risks can be identified through:

- Warnings (pictograms, signs, etc.);
- Audio/visual signals;
- Personal protective equipment;
- Trainings;
- Safe operating procedures, etc.

Implementing either item (i) and or (ii) above or a combination of both is mandatory if any specific risk is evaluated as higher than “low” or “medium”. The risk reduction measures explained on item (iii) can only be adopted in conjunction with risk reduction measures presented on items (i) and (ii).

If it is not possible to adopt the risk reduction measures of items (i) and (ii) and shall be dealt with as an exception criterion to CAR requirements.

If any specific risk is evaluated as “Low” or “Medium” any kind of risk reduction measure can be applied to further reduce the risk.

**NOTE:** the risks classified according to the table above must follow the governance strategy in “Table 5 of the NOR-0003-G (Risk Management) standard”.

After the implementation of risk reduction measures, each risk shall be evaluated again with the measures. If all risks are in “LOW” or “MEDIUM” risk level, risk assessment process finalizes for that instance. If one or more items remained in a higher risk level either additional measures shall be implemented or shall be dealt with as an exception criterion to CAR requirements.

## 6 GENERAL MACHINE SAFETY GUIDELINES

Whether the machines are new, legacy or modified and regardless of the country it is located in, they must comply with the minimum guidelines as followed:

- a) Machinery shall be designed and constructed in such a way that prevents the following people from being exposed to a hazard in any operation mode:
  - i. Operators of the machine;
  - ii. Operators near the machine;
  - iii. People present in the area (Passers-by);
  - iv. Maintenance personnel.
- b) Ensure energy isolation devices are placed such that they are easily accessible and there is sufficient space to stand when switching power on and off;
- c) Ensure all operator panels are located outside the protection zone;
- d) Ensure all components that require regular service are located outside the protection zone;
- e) Ensure all systems, components, and devices used to perform a safety function shall be certified for use as a safety system, device, or component by the manufacturer or by a recognized testing agency;

The supplier of the safety system is responsible for identifying and utilizing all relevant guidelines, standards, and legal requirements. A document must be provided by the supplier with a list of standards used and certifying conformance.

If the list does not exist, a competent person shall provide the required reference documentation.

- f) Machine safety layout;

Machine safety layout shall be created and analyzed including, but not limited to the following:

- i. Mandatory information:
  - Indication of hazard zones where higher residual risk remain;
  - Placement of machine guarding and cell entrances;
  - Location of all energy and fluid supply and actuator devices;
  - Location of relevant safeguarding devices like interlock switches, ESPE, etc.;
  - Locations of complementary protective devices (e.g. emergency stop buttons, etc.).
- ii. Optional information:
  - Parts and material feeding points;
  - Locations of both operation and maintenance tasks.

All machinery safety layout drawings shall be reviewed by the related Vale (Safety, Engineering and Maintenance) personnel prior to final approval.

g) Machine certification;

The machinery shall have received any certification legally required in the country and area where the machinery will be used before being accepted on site.

If necessary for certification or lack of experience/knowledge in the subject, it is recommended that OEM contact an independent and/or notified body experienced in the subject matter, if required for the certification or lack of experience/knowledge, early in the process (preferably from design stage) to prevent any modification required by the independent/notified body in later stages.

In all cases Vale reserves the right to verify the machine compliance by an independent certified company. In such a circumstance the independent certified company assessment will be considered valid and any required modifications will be completed at the expense of the supplier.

h) Machine Documentation;

The OEM / supplier shall indicate a list of the safety standards which are used through the design, construction and manufacturing of the machinery on the commercial proposal.

The non-exhaustive list of documentation that shall be provided with the machinery is as follows:

- i. A risk assessment report, which follows the principles of ISO 12100 explained in Section 5;
- ii. A listing of the standards used to guarantee the safety and details in case those standards were not fully applied;
- iii. A process layout analysis where the machine will be installed including, but not limited to:
  - Actual location of the machine in the site;
  - All facility features and equipment that are intended to be included in the machine;
  - Process and auxiliary equipment (e.g., measurement/gauging systems, transfer systems);
  - Parts and material feeding access points;
  - Locations of both the operator and maintenance tasks;
  - Material stock bins/containers;
- iv. A machine safety layout drawing (as described in Section 6 item f.);
- v. Information relevant for Lockout, Tagout and Zero Energy procedures (In compliance with CAR-04);
  - A Full Lockout, Tagout procedure
  - Partial Lockout, Tagout procedures if applicable
- vi. Operation & Maintenance Manuals

- vii. Technical documentation of the machinery (e.g. electrical drawings, pneumatic drawings, P&ID, etc.)
- viii. Other calculation, simulation and test reports carried out for the machinery (Optional but recommended)
- ix. Ergonomic assessment report for each workstation and activity

The documentation shall be provided in local language of the country the facility is located.

- i) PPE;

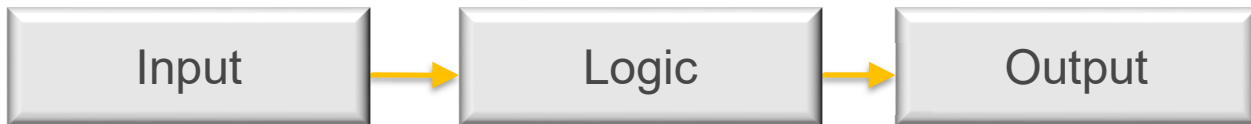
Documentation shall be provided detailing the PPE required and recommended by the OEM/supplier to be used during each work tasks.

Signage and warnings shall be installed on the machine where PPE is required, and which type of PPE is required. Other PPE may be required at Vale's risk assessment

## 7 GUIDELINES FOR SAFETY SYSTEMS

### 7.1 Control System

Safety control systems are parts or subparts of an industrial or process control system that perform specific functions to achieve or maintain a safety state of a machine or process when unacceptable or imminently hazard conditions are detected.



Control systems shall be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they shall be designed and constructed in such a way that:

- I. They can withstand the intended operating conditions and external influences;
- II. A fault in the hardware or the software of the control system does not lead to hazardous situations,
- III. Errors in the control system logic do not lead to hazardous situations;
- IV. Reasonably foreseeable human error during operation does not lead to hazardous situations.

Particular attention shall be given to the following points:

- I. The machinery shall not start unexpectedly;
- II. The parameters of the machinery shall not change in an uncontrolled way, where such change may lead to hazardous situations;
- III. Stop commands of the machinery shall have priority over the start controls;
- IV. No moving part or piece, or component of the machinery or piece held by the machinery shall fall or be ejected;
- V. The protective devices shall remain fully operational or otherwise give a stop command,;
- VI. The safety-related parts of the control system shall apply in a coherent way to the standard to all assembly of machinery and/or partly completed machinery.

From each control position, the operator must be able to ensure that no-one is in the danger zones, or the control system must be designed and constructed in such a way that starting is prevented while someone is in the danger zone.

Where there is more than one control position, the control system must be designed in such a way that the use of one of the control panels precludes the use of the others, except for stop controls and emergency stops. Each position must be provided with all the required control devices without the operators hindering or putting each other into a hazardous situation.

## 7.2 Control Device

Control devices are mechanisms used to control a function of the machinery being operated.

Control devices must be:

- Clearly visible and identifiable, using descriptions or pictograms where appropriate;
- Positioned in such a way as to be safely operated and their operation cannot cause additional risk;
- Designed in such a way that the movement of the control device is consistent with its effect;
- Located outside the hazardous zones, except where necessary for certain control devices such as an emergency stop or a teach pendant;
- Designed or protected in such a way that the desired effect, where a hazard is involved, can only be achieved by a deliberate action;
- Made in such a way as to withstand foreseeable forces; particular attention must be paid to emergency stop devices liable to be subjected to considerable forces;
- The arrangement of controls should be compatible with their associated displays (HIM, Monitor, etc.) or machine functions. Controls should be located close to the associated display and arranged logically in relation to displays (example: Singling, light, etc.).

All pushbuttons, switches, and other devices for the control of the machine shall be labelled by means of a fixed and clearly understandable label.

All components installed inside control and electrical panels shall be identified as per the machine drawings.

Where a control device is designed and constructed to perform several different actions (example: Select with two function), the action to be performed must be clearly displayed and subject to confirmation, where necessary.

Control devices must be so arranged that their layout, displacement, and resistance to operation are compatible with the action to be performed, considering ergonomic principles.



Color coding of pushbutton shall be compliant with the Table 3.

| Color  | Meaning                      | Explanation  | Examples of application                                       |
|--------|------------------------------|--|---|
| Red    | Emergency                    | Actuate in the event of an emergency                   | EMERGENCY STOP<br>Red can be used as normal stop or turn off. |
| Yellow | Abnormal                     | Actuate in the event of an abnormal condition          | Intervention to suppress an abnormal condition,               |
| Green  | Normal                       | Actuate to initiate normal conditions or normal status | START/ON<br>(WHITE should be preferably used)                 |
| White  | NO specific meaning assigned | For general initiation of functions                    | START/ON (preferred), STOP/OFF                                |
| Grey   |                              |  | START/ON, STOP/OFF  |
| Black  |                              |  | START/ON, STOP/OFF (preferred)                                |
| Blue   | Mandatory                    | Actuate for a condition requiring mandatory action     | Reset function  |

Table 3 – Color Coding of the Push Buttons

### 7.3 Sound and Visual Signaling

All machines where it is difficult the visualization of people in hazard zones shall have an audio/visual warning system to alert personnel of machine start and pending movement. The start-up alarm shall only occur if all initial starting conditions are met. No motion shall occur during the alarm period. The alarm period shall be of sufficient length to allow all personnel to clear any hazard area. Continuous activation of the cycle initiation device shall be required during the alarm period.

Color coding for signalization lamps/indicators are given in Table 4

| Color  | Meaning             | Explanation   | Examples of application  |
|--------|---------------------|---|--|
| Red    | Emergency           | Hazardous Condition EMERGENCY   | Pressure outside safe limits, voltage drop                                   |
| Yellow | Abnormal            | Abnormal condition impending critical condition, adjustment, maintenance work | Pressure outside normal operating range limits, tripping a protective device |
| Green  | Normal              | Normal operation  | Pressure within the normal operating ranges                                  |
| White  | Information Neutral | Voltage present<br>Other conditions   | General information  |
| Blue   | Mandatory           | Indication of a condition that requires action by the operator                | Prompt to enter specified values   |

Table 4 – Color Coding of Indicators

All counters, dials, displays and light labels required for normal operation should be readable by the operator from the normal work position under normal lighting conditions.

## 7.4 Start and Stop Devices

Starting/restarting of machinery should only be possible by voluntary actuation of a control device provided for the purpose.

Each workstation must be fitted with a control device to stop some or all of the functions of the machinery, depending on the existing hazards, so that the machinery is rendered safe.

If a stop control that it does not cut-off the energy supply to the actuators is required, the stop condition must be monitored and maintained by the machine control system. Information must be provided in the instruction manual and warning signs fitted to the machinery to ensure workers are aware of that power is still supplied to the actuators.

Where machinery has multiple start control devices and the operators can therefore put each other in danger, additional devices must be fitted to rule out such risks. If safety system requires that starting and/or stopping must be performed in a specific sequence, measures must be taken to ensure these operations are performed in the correct order.

## 7.5 Mode Selection

Change in operating mode of machinery should only be possible by voluntary actuation of a control device provided for the purpose.

Only a single mode selector switch shall be installed for a single machine.

The mode selection should have a means to prevent unauthorized use, i.e. a removable key or password protection.

Where machines are connected to assemblies of machine, and the constituent machines have individual mode selector switches the following shall apply:

- If any mode switch is in manual mode all machines shall be placed in manual mode;
- If any mode switch is operated during a cycle all machines shall complete the present cycle before safeguards are disabled. A deliberate action shall be required to restart the machine.

The emergency stop devices shall be active in all operating modes.

### a) Automatic mode guidelines

In Automatic mode the machine will run continuously until a stop signal is received.

When a machine is switched to automatic mode, or is powered up and is in automatic mode, the machine shall not start until deliberate, reset and start, actions by the operator.

When in Automatic Mode all safety devices shall be operational, i.e. safety gates, light curtains etc.

**NOTE:** Certain machine muting functions can be applied to deactivate safety functions during the non-hazardous phases of the machine movement. (Explained in section 7.7.2.1).

## b) Manual mode guidelines

In manual mode, the machine requires that the operator continuously holds the start button and/or an enabling device to move the machine outside the hazardous zones.

All of the safety measures shall be operational in manual mode.

## c) Special Modes with Suspension of Safeguards

When means/modes to suspend safeguarding devices, or operation with guards displaced is provided for non-operational tasks, e.g. maintenance, set-up, or troubleshooting, the selected operating mode shall be clearly indicated.

The allowed motion of hazardous parts shall be limited as much as possible.

It shall not be possible for the machine to resume its normal operation with the suspension of safeguards.

No safeguard which cannot be clearly seen from the point where the safeguard is suspended ( e.g. from mode selector switch) shall be suspended. The suspension of safeguard circuitry shall be designed and installed to the same performance level as the circuit performance of the device being suspended.

Only authorized personnel can be able to select and change to such modes by a lockable mode selector switch or password protection.

The control or operating mode selected shall override all other control or operating modes, except for the emergency stop devices.

Permit operation of hazardous functions only by control devices requiring sustained action, such as two-hand control devices, or portable control stations (e.g., pendant) with an emergency stop device, an enabling device, and a separate device that initiates motion.

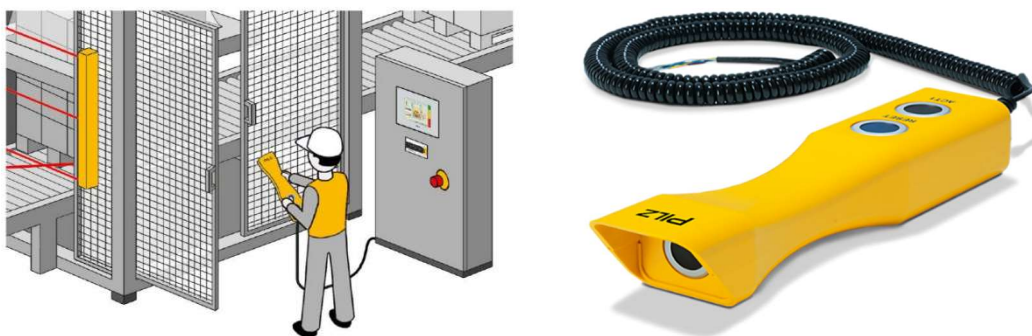


Figure 3 – Application of an enabling device for set-up

Permit the operation of hazardous functions only in reduced risk conditions while preventing hazards from linked sequences, like reduced speed, steps etc.

Prevent any operation of hazardous functions by voluntary or involuntary action on the machine's sensors.

If the conditions described above cannot be fulfilled, the control or operating mode selector must activate other protective measures designed and constructed to ensure a safe intervention zone.

## 7.6 Safeguarding

### 7.6.1 Safeguards

Safeguards are used to prevent access to hazardous parts, movements, and dangerous areas of the machinery. Different kinds of safeguards are explained below.

All guards shall:

- Be robust;
- Be securely held in place;
- Not give rise to any additional hazard;
- Be of size and weight that require a reasonable amount of force to move them out of the way, when necessary;
- Not be easy to bypass or defeat;
- Cause minimum obstruction to the view of the production process;
- Provide minimum possible interference with activities during operation, maintenance, etc.

**IMPORTANT:** It shall not be possible to reach hazardous areas over, under, around or through a guard.

Metals, as materials of guarding is preferred. Where it is required to view the hazardous areas, a suitable sized mesh shall be used to prevent access. If visibility is required or there is a risk of ejected parts, transparent materials such as polycarbonate can be considered.

Where openings are required on the guards, allow the passage of materials, etc., the openings shall be small enough to prevent a person from reaching the hazard. Guidance about opening size limits are explained in detail in section 7.8.4.

Guards shall be installed at a safe distance from the hazardous part. Guidance on safe distances is provided in section 7.8.

Guards shall be located or designed to prevent anyone from being able to reach the danger zone before the machine comes to a complete stop. Otherwise safety devices with guard-locking function can be used. (see also section 7.6.4).

Guards shall protect persons from falling or ejected solid or liquid objects.

### 7.6.2 Selection of Guards

The guarding is appropriate considering the type of hazard, and the access required to the machine.

The method of selecting the type of the guard is explained in Figure 4.

Table 5 can be used for selection the guard type according to the access frequency. This table is provided for guidance only and may not be appropriate for all hazards or machines.

| Frequency of access | Guarding type            | Fixing            | Interlock device required |
|---------------------|--------------------------|-------------------|---------------------------|
| Never               | Fixed guards             | Bolted / welded   | No                        |
| Annual              | Fixed guards             | Bolted            | No                        |
| Weekly              | Fixed or moveable guards | Bolted (if fixed) | Yes (if moveable)         |
| Daily               | Moveable guards          | N/A               | Yes                       |
| Hourly              | Moveable guards          | N/A               | Yes                       |
| More than hourly    | Protective device        | N/A               | No                        |

Table 5 – Selection of Guarding type

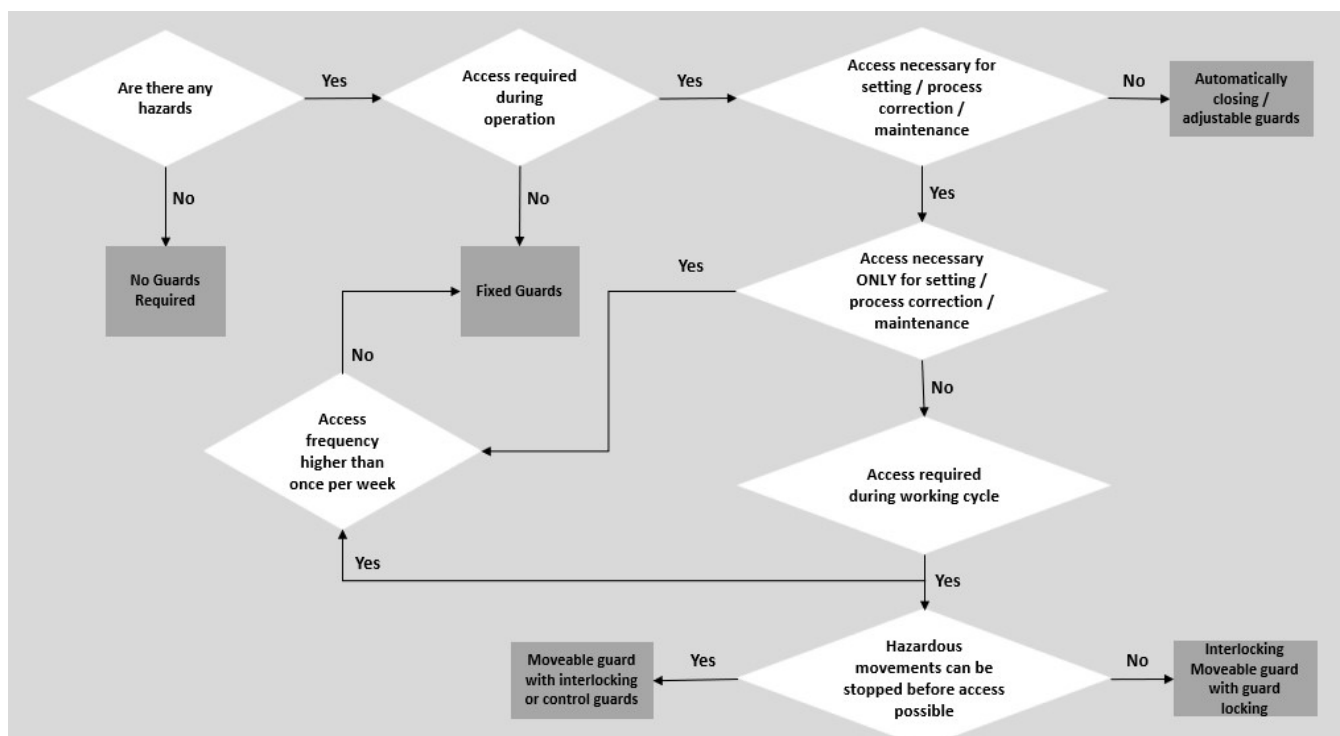


Figure 4 – Selection of Guarding type

### 7.6.3 Fixed Guards

Fixed guards shall be preferred and used whenever practicable (no frequent access needed)

Fixed guards shall only be opened or removed with use of a tool.

Fixing elements (nuts, screws, etc.) should remain attached to the guards or to the machinery when the guards are removed.

Guards shall not remain in place when their fixing elements are removed.

Guards, where possible, should have a weight, dimension and shape allowing easy and safe handing by a single person, for maintenance purposes.

Gaps adjacent to moving parts (nip points) should be less than 4 mm (0.1574 in). Some applications allow bigger gaps (e.g. 5mm (0.1968 in) for conveyor or 6mm (0.2362 in) for certain paper machines). If this opening cannot be met, a full enclosure fixed type guard is required.

Perimeter fixed guarding, in other words safety fences, should be at least 1.6 m (62.9921 in) height from ground level with no footholds. The height, location and openings of the fence shall be defined according to the process and hazard zone, like height of the hazard or vertical distance to the hazard. See also section 7.8.

Gaps under safety fences or barriers should be 180 mm (7.0866 in) or lower to prevent person access.

## 7.6.4 Moveable Guards

All moveable guards shall be interlocked so that opening the guard shall stop the hazardous movements and cut-off all energy supplies. The following should be considered:

- Frequency of access;
- Rundown time;
- Hygienic requirements;
- Self-Testing of Interlock Device.

Interlocked moveable guards shall:

- Remain attached to the machinery when open, if possible;
- Be designed and constructed in such a way that they can be adjusted only by means of an intentional action.

All moveable guards shall be associated with an interlocking device which:

- Is controlled/monitored by the safety control system of the machine;
- Prevents the start of hazardous machinery functions until the guards are closed;
- Gives a stop command whenever the guards are opened;
- Closure of the guard shall not start the machine.

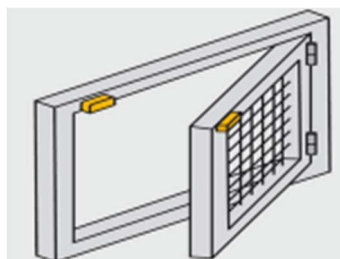


Figure 5 – Interlocked Guard with associated locking device

Interlocking devices shall:

- Be positively installed (not actuated when guard closed);

- Be properly fixed to prevent manual disassembly or easy adjustment (anti tamper fixings);
- Not be used as mechanical stop or holding point, unless specifically designed for;
- Allow their replacement without further adjustments;
- Not be easily bypassed (screws, coins, pins, metallic sheets, manual tools of the machine, etc);

Where it is possible for an operator to reach the danger zone before the hazardous motions have stopped, movable guards shall be installed with a guard locking device to:

- Prevent start of hazardous machinery functions until the guard is closed and locked;
- Keep the guard closed and locked until the risk of injury from the hazardous machinery functions has ceased, including the inertia movement;
- Closure and locking of the guard shall not restart the machine;

Interlocking moveable guards shall be designed in such a way that the absence or failure of one of their components prevents start-up or stops the hazardous machinery functions.

All moveable guards shall be constructed so that they cannot cause a person to be trapped between the guard and the machine.

Preferably access from one machine should not allow access to other machines Where interlocking guards/doors provide access to several machines the following conditions shall be fulfilled:

- Power to all machines shall be removed upon the opening of any guard/door;
- Sufficient physical separation shall be provided between the machines which remain powered and the machine which is being accessed;
- Safeguards and/or barriers must be installed to prevent people accessing the machines from reaching hazards that cannot be controlled by the access guards.

Safety guards or doors shall be designed so that when opened for access and entry to an area, they will be mechanically prevented from inadvertently locking an individual in the machine by closing and locking.

- Emergency exit mechanisms shall be provided with guard locking systems of doors.

## 7.6.4.1 Control Guards

Control guards are interlocking guards with a start function implemented without the necessity of a reset function. This kind of guards can only be used if all requirements stated below are met:

- All requirements of interlocked moveable guards are met;
- Cycle time of the machine is short;
- Maximum opening time of guard is limited to a pre-set value and if this time duration is exceeded resetting is necessary;
- Dimensions and positioning of the guard does not allow anyone to stay between guard and hazardous zone;



- Measures are applied for the failure of functions related with the control guard not to lead unexpected start-up of the machine;
- The guard cannot close automatically, unexpectedly or by its own weight.

## 7.6.5 Other Types of Guards

### 7.6.5.1 Power-operated Guards

This type of guard is not operated manually but with actuators (pneumatic pistons, gears with motors etc.). Closing edge of the guard shall have a safety edge to eliminate crushing hazards.

### 7.6.5.2 Adjustable Guards

This type of guarding should not be selected as a first choice but only if no other option is possible and based on the risk assessment (HRN) or specific safety standards (Type C).

Adjustable guards restricting access to those areas of the moving parts strictly necessary for the work shall be:

- Adjustable manually or automatically, depending on the type of work involved; and
- Readily adjustable without the use of tools.

## 7.7 Safeguard Devices

### 7.7.1 Electro Sensitive Protective Equipment (ESPE)

ESPE devices shall only be used where continuous access is required to a machine, e.g. manual loading and unloading of parts, or in cases where mechanical guarding cannot provide adequate protection.

ESPE devices shall be installed in such a way that when the ESPE is triggered:

- Hazardous movements and parts will stop;
- It is not possible for a person to reach the hazardous parts before the moving parts have come to a complete stop;
- It must not be possible to reach hazardous parts of the equipment by reaching over, or around the ESPE.

ESPE devices are safety devices and should comply to IEC 61496 and be connected appropriately to the safety related part of the control system.

Muting of the ESPE devices, or individual beams, shall be permitted only in situations which are detailed in machine specific standards.

If there is a loss of power to the ESPE device, the device shall initiate an immediate stop command to the machinery safety control system.

The effective sensing field shall be of adequate height, width and depth to guard the area and the response time used in the safety distance formula, explained in Chapter 7.8.6. This shall be the maximum (worst case) response time, taking into consideration the impact of sensitivity adjustments and environmental changes (e.g. smoke, dust, haze, vibration or light source decay)



such that an increase in response time or object sensitivity occurs. The device shall not fail to respond to an intrusion due to the presence of a reflective or dull object/workplace.

Where it is possible for a person to stand between an ESPE device and the moving parts of a machine, additional measures, shall be installed to ensure the machine cannot start when a person is in this area.

When the ESPE device is powered up, the work cell's perimeter guard safety circuit shall be automatically operated. Resetting the device or perimeter guard safety circuit shall NOT, by itself, be capable of restarting the machinery, unless it is specifically designed for.

## 7.7.2 Active Optoelectronic Protective Devices (AOPD)

The following AOPD requirements shall apply to light curtains, safety scanners, safety cameras and any other safety devices using beams of light to detect and protect people.

| Tipo AOPD | PL Alcançável |
|-----------|---------------|
| 2         | a, b, c       |
| 3         | a, b, c, d    |
| 4         | a, b, c, d, e |

Table 6 – AOPD Type and achievable PL values

Typically, Light Curtain or Multi Beam system are of Type 4 and Area Scanners are of Type 3. Type 2 AOPD should only be used where there is documented proof that it is deemed suitable based on the risk (HRN) of the application.

### 7.7.2.1 Special Functions of AOPD (Muting / Blanking)

Muting is the temporary, automatically controlled deactivation of the function of a safeguarding device during normal operation (e.g., to allow loading or unloading of materials) by safety-related parts of the control system.

Muting may be used in conjunction with any safeguarding device that electrically signals a stop.

Muting is permitted when:

- During muting, safe conditions are provided by other means so that the hazard cannot be accessed without a stop being initiated and therefore no personnel are exposed to the hazard;
- The muting system is designed and installed consistent with the safety circuit;
- Performance required of the device being muted. In the event of a failure subsequent:
  - Muting shall be prevented until the failure is corrected;
  - Presence in the muted safeguarded space is continually sensed;
  - At the end of muting, all safety functions shall be reinstated;
  - An awareness signal indicating muting is provided.

Blanking is deactivation of a specific segment (predetermined numbers of light beams, etc.), either permanently or temporarily, of a safeguarding device during normal by properties/programming of the related equipment. Permanent blanking is only acceptable if there is a fixed element in the protection area of the device. Both blanking functions can only be used if there is no possibility of accessing to the hazardous area through the blanked segment of the device.

### 7.7.3 Safety Mats and Safety Floors

When the actuating force is applied the output signal switching device(s) shall change from an ON state to an OFF state. It shall remain in the OFF state for at least if the actuating force is applied. In the case of devices with reset, the output signal switching device(s) shall only change to the ON state after the application of a reset signal once the actuation forced is removed.

The circuit through the mat/floor must be monitored by a safety-rated control unit.

Where an effective sensing area is built up from more than one sensor (mat) it shall have no dead zone.

The top surface should be of a material which will withstand the operating duty.

The top surface should not present a risk through becoming slippery due to wear or the effects of liquids.

Safety distance calculation need to be applied for safety mats/floors if they perform a stop reaction or to ensure that no stepping over is possible.

## 7.8 Safety Distance

### 7.8.1 Safety Distances to Prevent Access to Upper Limbs

- Reaching Upwards

When reaching upwards, if there is low risk (injuries normally treated by first aid) from the hazard zone, then the height (h) of the hazard zone shall be 2500mm (98.4251 in) or more. If there is a high risk (injuries beyond first aid) from the hazard zone, then the height of the hazard zone shall be 2700mm (106.2992 in) or more.

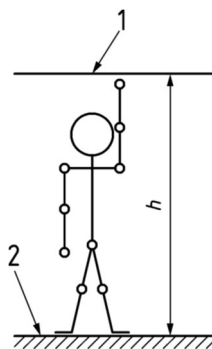


Figure 6 – ISO 13857 Prevent Reaching Upper

Legend:

1 – Danger zone

2 – Reference plane

h – height of the hazard zone

## 7.8.2 Reaching Over Protective Structures

In order to define the distance from the hazard or the height of the protective structure, table below should be used. The information in the table gives the relationship between height of the hazardous zone, height of the protective structure and distance of the protective structure from the hazard zone.

**NOTE:** Note: If a number (between height or distance) not on the table is found, it should be rounded to the closest higher number to be on the safe side.

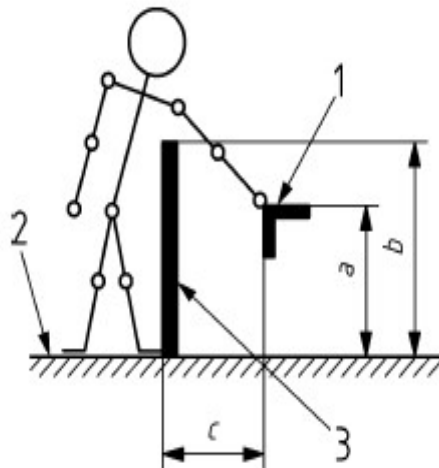


Figure 7 – ISO 13857 Prevent Reach on Protective Structures

Legend:

- |                          |  |
|--------------------------|--|
| 1 – Danger zone          | a – Height of danger zone              |
| 2 – Reference plane      | b – Height of the protective structure |
| 3 – Protective Structure | c – Horizontal Distance to Danger Zone |

Dimension in millimeters

| Height of danger zone<br>a | Height of protective structure b <sup>1)</sup> |      |                    |      |      |      |      |      |      |      |
|----------------------------|--|------|--------------------|------|------|------|------|------|------|------|
|                            | 1000   | 1200 | 1400 <sup>2)</sup> | 1600 | 1800 | 2000 | 2200 | 2400 | 2500 | 2700 |
|                            | Horizontal distance to the danger zone "c"     |      |                    |      |      |      |      |      |      |      |
| 2700 <sup>3)</sup>         | -  | -    | -                  | -    | -    | -    | -    | -    | -    | -    |
| 2600                       | 900  | 800  | 700                | 600  | 600  | 500  | 400  | 300  | 100  | -    |
| 2400                       | 1100   | 1100 | 900                | 800  | 700  | 600  | 400  | 300  | 100  | -    |
| 2200                       | 1300   | 1200 | 1000               | 900  | 800  | 600  | 400  | 300  | -    | -    |
| 2000                       | 1400   | 1300 | 1100               | 900  | 800  | 600  | 400  | -    | -    | -    |
| 1800                       | 1500   | 1400 | 1100               | 900  | 800  | 600  | -    | -    | -    | -    |
| 1600                       | 1500   | 1400 | 1100               | 900  | 800  | 500  | -    | -    | -    | -    |
| 1400                       | 1500   | 1400 | 1100               | 900  | 800  | -    | -    | -    | -    | -    |
| 1200                       | 1500   | 1400 | 1100               | 900  | 700  | ↓    | -    | -    | -    | -    |
| 1000                       | 1500   | 1400 | 1100               | 800  | -    | -    | -    | -    | -    | -    |
| 800                        | 1500   | 1300 | 900                | 600  | -    | -    | -    | -    | -    | -    |
| 600                        | 1400   | 1300 | 800                | -    | -    | -    | -    | -    | -    | -    |
| 400                        | 1400   | 1200 | 400                | -    | -    | -    | -    | -    | -    | -    |
| 200                        | 1200   | 900  | -                  | -    | -    | -    | -    | -    | -    | -    |
| 0                          | 1100   | 500  | -                  | -    | -    | -    | -    | -    | -    | -    |

<sup>1)</sup> Protective structures less than 1000 mm (one thousand millimeters) in height are not included because they do not sufficiently restrict access of the body.

<sup>2)</sup> Protective structures less than 1400 mm (one thousand four hundred millimeters) in height shall not be used without additional safety measures.

<sup>3)</sup> For danger zones greater than 2700 mm (two thousand and seven hundred millimeters) in height, see Figure 2.

Table 7 – (Table 6 from ISO 13857) Definition of height or distance of guards

### 7.8.3 Reaching around

In order to eliminate arm reach to the hazardous motion at least 850 mm (33.4645 in) safety distance shall be provided between the motion and the guard.

If this distance cannot be achieved, special measures shall be taken, and used dimensions indicated below.

Dimension in millimeters

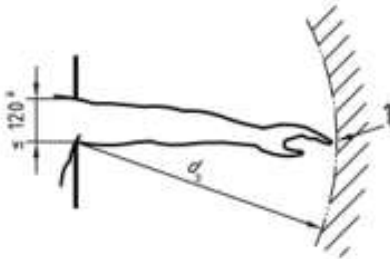
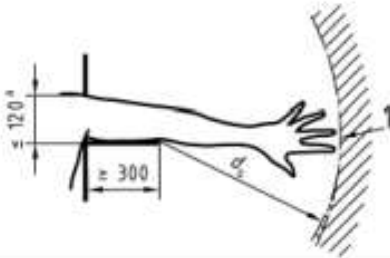
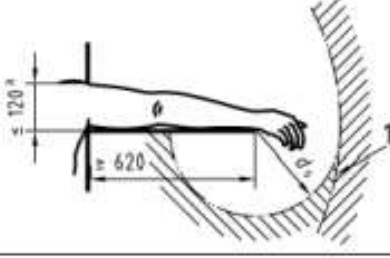
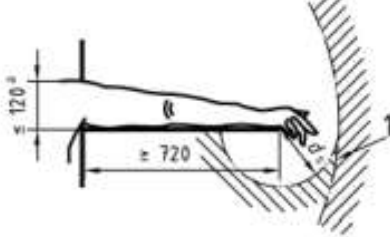
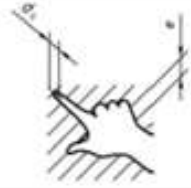
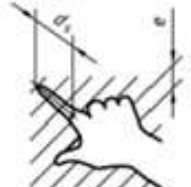
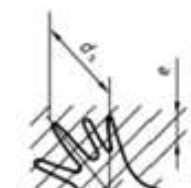
| Limitation of movement   | Safety distance $d^a$ | Illustration  |
|--|-----------------------|---|
| Limitation of movement only at shoulder and armpit   | $\geq 850$            |    |
| Arm supported up to elbow  | $\geq 550$            |    |
| Arm supported up to wrist  | $\geq 230$            |   |
| Arm and hand supported up to knuckle joint   | $\geq 130$            |  |
| <p>1 Range of movement of arm.</p> <p><sup>a</sup> Diameter of a round opening, the side of a square opening or the width of a slot opening.</p> |                       |   |

Table 8 – (Table 7 from ISO 13857) Reach around openings in guards

### 7.8.4 Reaching Through Openings

In order to not reach to hazards from openings in the protective structures, the dimensions in the table below shall be used.

Dimension in millimeters

| Part of body                       | Illustration  | Opening, $e$      | Safety distance, $d_s$ |            |            |
|------------------------------------|---|-------------------|------------------------|------------|------------|
|                                    |   |                   | Slot                   | Square     | Round      |
| Finger tip                         |    | $e \leq 4$        | $\geq 2$               | $\geq 2$   | $\geq 2$   |
|                                    |   | $4 < e \leq 6$    | $\geq 10$              | $\geq 5$   | $\geq 5$   |
| Finger up to knuckle joint or hand |    | $6 < e \leq 8$    | $\geq 20$              | $\geq 15$  | $\geq 5$   |
|                                    |   | $8 < e \leq 10$   | $\geq 80$              | $\geq 25$  | $\geq 20$  |
|                                    |   | $10 < e \leq 12$  | $\geq 100$             | $\geq 80$  | $\geq 80$  |
|                                    |   | $12 < e \leq 20$  | $\geq 120$             | $\geq 120$ | $\geq 120$ |
|                                    |   | $20 < e \leq 30$  | $\geq 850^a$           | $\geq 120$ | $\geq 120$ |
| Arm up to junction with shoulder   |  | $30 < e \leq 40$  | $\geq 850$             | $\geq 200$ | $\geq 120$ |
|                                    |   | $40 < e \leq 120$ | $\geq 850$             | $\geq 850$ | $\geq 850$ |

<sup>a</sup> If the length of the slot opening is  $\leq 65$  mm, the thumb will act as a stop and the safety distance may be reduced to 200 mm.

Table 9 – (Table 4 from ISO 13857) Reach through openings in guards

### 7.8.5 Minimum Safe Distances Between Moving Parts Which Create a Crushing Risk

Minimum gaps to prevent crushing of human body parts between moving parts or between moving and fixed parts shall be considered according to Table 10.

Dimensions in millimetres





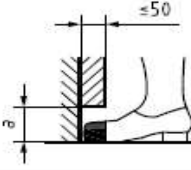


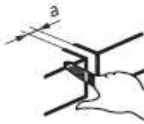
| Part of body                     | Minimum gap $a$ | Illustration  |
|----------------------------------|-----------------|---|
| body                             | 500             |    |
| head (least favourable position) | 300             |    |
| leg                              | 180             |    |
| foot                             | 120             |    |
| toes                             | 50              |   |
| arm                              | 120             |  |
| hand<br>wrist<br>fist            | 100             |  |
| finger                           | 25              |  |

Table 10 – (Table 1 from ISO 13854) Minimum gaps to avoid crushing of parts of the human body

## 7.8.6 Safety Distance in Relation to Approach Speed

Safety functions need to ensure that the hazardous machine task will stop before the person can gain access to the hazard. The safe distance formula is critical in determining that the system will respond properly and the proper installation from the hazard is determined. Typically, the safety distance in relation to the approach speed is relevant for presence sensing devices (e.g. Light curtain, scanners, radars, safety camera etc.), interlocked guards and two hand devices.



The ISO 13855 safe distance formula is as follows:

$$S = K \times T + C$$

Where:

S = the minimum safe distance between the safeguarding device and the closest hazard.

K = Speed constant derived from data on approach speeds of the body or parts of the body (typically 1.6 or 2.0 m/sec). If S is <500 mm (19.6850 in), K = 2.0 m/sec. If S >500 mm (19.6850), K = 1.6 m/sec.

T = t1+t2 = the overall system stopping performance in seconds.

t1 = maximum stopping time of the machine (in seconds)

t2 = response time of the light curtain and related safety interlocking circuits (in seconds)

C = an additional distance. C is dependent on the detection capability (d) of the protective equipment. The detection capability (d) is provided by the manufacturer of the component. Typically, C = 8(d-14 mm) for devices with high resolution, but not less than 0

## 7.9 Safety in Fluid System

Fluid systems that perform safety-related control functions shall have a performance level (PL) in accordance with section 7.11 to ensure the reliability of the systems;

The following safeguards measures must be taken to ensure the proper functioning of fluid systems:

- Ensure the quality of fluids according to ISO 8573-1 standard;
- Regulation of fluid pressure to ensure the limit defined in the project;
- Installation of relief valves to ensure that the system does not exceed the defined maximum limit;
- Installation of a system to prevent excessive fluid heating;
- Elimination of leaks that could cause dangers and reduction of speeds and forces;
- Ensure that the load, stroke and fastening of the actuators are sufficient to prevent buckling and bending of their rod;
- Physical arrangement discourages the use of piping as a ladder and as support for equipment;
- Where hose or piping failures can cause the whiplash effect, contain them by mechanical means (straps, protective mesh, mechanical ducts) or by active means such as “air fuses”;
- To maintain the position of the pistons, active means (piloted retention valves) or passive means (rod brakes) must be used and avoid unexpected startups or falls.



## 7.10 Emergency Stop Devices

Additional protective measures shall stop the machine in an emergency state unless otherwise stated. The purpose of these emergency stop devices is to trigger and start an emergency stop function to avert actual or impending emergency situations.

Machinery must be fitted with one or more emergency stop devices to allow the stopping of the machine in the event of an emergency by removing the power of the machine actuators on the best possible conditions:

- Interrupting the power of actuators immediately (Stop Category 0) or;
- Controlled stop (Stop Category 1): Actuators remain powered until a complete stop. Once the machine stopped, the power is interrupted.

Span of control of an emergency stop device must cover whole machine. If zoning or different span of control areas are needed or stopping all linked machinery creates additional hazards, different (one or more) span of control can be specified for each individual device. In this case, each emergency stop device must have a brief label describing what area the particular stop device is affecting. A zone emergency stop device only affects the components controlled by that zone.

The emergency stop device must:

- Override all other functions and modes of operation;
- Be clearly identifiable, quickly accessible, be easy to activate, and clearly visible control devices;
- Stop the hazardous process within a clearly defined span of control neither creating additional risks nor affecting adjacent equipment that is not posing a hazard;
- Cannot be bypassed or suspended from other locations or by operation modes;
- Once active operation of the emergency stop device has ceased, following a stop command, that command:
  - Must be maintained until manually reset;
  - Keeps any kind of start command non-operational;
- Be actuated with hand and located between 0,6m (23,6220 in) and 1.7m (66,9291 in) above floor level;
  - Foot pedals or kick plates for use of foot shall be located on floor level,
- Electrical emergency stop devices shall apply direct opening action principle with mechanical latching;
- Pneumatic/Hydraulic emergency stop devices shall apply positive (direct) mechanical action principle with mechanical latching;
- Be placed to prevent unintended actuation.

If a line consists of more than one inter-connected item of equipment, the different emergency stops need to be integrated into a single system. The number, type, and location of emergency

stops (as well as selection of global, cell or zone systems) should be determined based on a risk assessment.

Separate operating devices shall be used for Operational Stop control and Emergency-stop control. This requirement applies even in cases where both devices (e.g. button, rope etc.) will have the same effect.

At least one emergency stop device must be provided at each operator station, at locations where intervention/interaction with machinery/process needed or expected. If all emergency stop devices are positioned on detachable or cableless stations (Remote control by cable or wireless), additional measures to detect active devices shall be taken (e.g. safety relay, communication detection, etc.) and at least one device shall be permanently fixed.

Emergency stop devices must be complementary measures to other safeguarding measures. They cannot be used as a substitute for safeguarding measures, other functions (i.e. operational stop, shut-off machine, LOTO applications, etc.) or safety functions.

Emergency stop function must be implemented in a control reliable manner that incorporates dual-channel circuitry and only by wired electromechanical components or safety logic elements (i.e. safety relays, safety PLC's).

An E-stop must function independently from the standard system controller.

The symbol shown in figure below can be used instead of labelling with text.



Figure 8 – Emergency Stop symbol

## 7.10.1 Emergency Stop Button

Emergency stop button is the most common used emergency stop device on the machinery.



Figure 9 – Emergency Stop Button

The emergency stop buttons must:

- Meet all requirements of emergency stop devices;
- Red actuator over yellow background is required;
- Should be of a “maintained contact” type;
- Can be activated easily by the palm of a hand; and
  - If exists, any shrouds or keys shall not prevent triggering by the palm of hand or create additional hazards.

Once active operation of the emergency stop device has ceased, following a stop command, that command:

- Must be sustained by engagement of the emergency stop button until that engagement is specifically overridden (dis-engaged);
- It must not be possible to engage the button without triggering a stop command;
- It must be possible to disengage the button only by a deliberate action;
- Disengaging the button must not restart the machinery but only permit resetting.

## 7.10.2 Emergency Rope Switch

If the design of multi-stations or large machines does not allow placement of emergency stop buttons within easy reach, cord operated, hand reset type switches with non-fraying cords can be used.

Access to red emergency cords/ropes/cables is required from each side of equipment that is accessible for service. The cords shall be located within easy reach and shall be re-settable without opening gates or removing guards.

A single line can be permitted if it can be reached from both sides.

The follow guidelines for Emergency Stop Rope/Cable/Cord shall be applied:

- Shall be clearly marked to ensure visibility. (Red-Yellow marker flags when necessary);
- Pulling or pushing the line in either direction or along its axis shall trigger the device;
- An E-Stop command shall be initiated in the event of breakage, loss of tension or disengagement;
- Tension adjustment must be able to be accomplished using a tool;
- The points of reset should be located such that the entire length of the cable/cord is visible from the reset location. If this is not possible additional measures shall be taken;
- The emergency stop shall be activated from any part of the cable;
- Rope switch systems shall be designed for periodic verification to ensure function as designed.

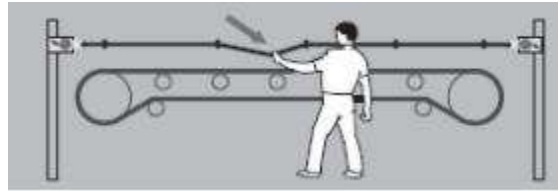


Figure 10 – Example of an Emergency Pull Cord

The whole machine shall be inspected to find the reason of triggering the device before disengaging and restarting the machine. The task shall be explained and detailed in the documentation

### 7.10.3 Kick Bars, Plates, Handles and Foot-Pedals

Other devices or mechanisms for triggering emergency stop functions can be implemented in machines, like bars, plates or handles to be kicked by hand or foot or foot pedals for the purpose of emergency stop.

These mechanisms shall not be used instead of the standard emergency stop devices explained above but only complementary to them. Some of these devices are mandatory for specific machinery types as stated in their related C-Type standards.

Triggering shall be possible among the whole length of the triggering part (i.e. bar, plate, etc.)

These devices are not designed as latching type but instead return to its original position after release. That is why these devices can never be used for auto-initiation of the machines.

Foot pedals for emergency stop devices shall not have any protective covers on or around them. They shall only be used if not other solutions as an emergency stop device is applicable

## 7.11 Safety Control System

Safety-Related Parts of Control Systems (SRP/CS) are the parts of an industrial or process control system that performs specified functions to achieve or maintain a safe state of the machine/ process when unacceptable or dangerous process conditions are detected.

The design of a safety command system is part of a cycle that must start with risk assessment, which is the basis for defining the required performance level (PLr) and ends with the validation of the system, where it is verified that it meets the reliability and availability requirements needed for safety functions.

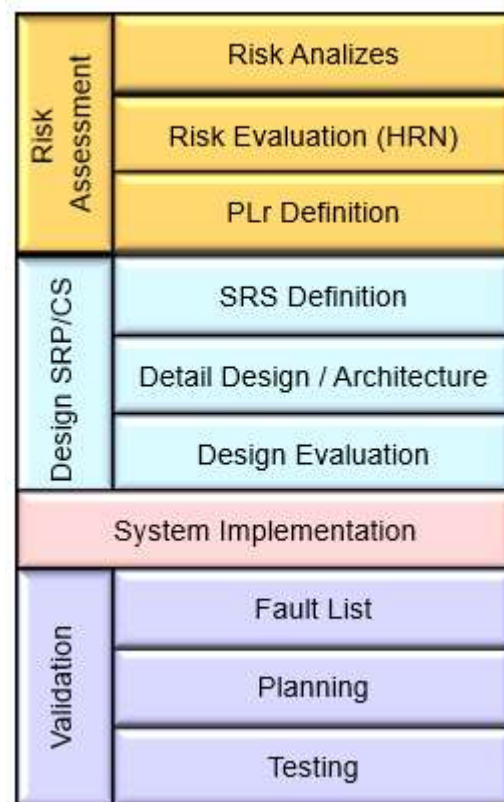


Figure 11 – Cycle a safety control system

Structure of a safe control system:

- Two separate channels (recommended);
- Diverse structure using different hardware;
- Inputs and outputs are constantly tested;
- User data is constantly compared;
- Voltage and time monitoring functions;
- Safe shutdown in the event of error/hazard.

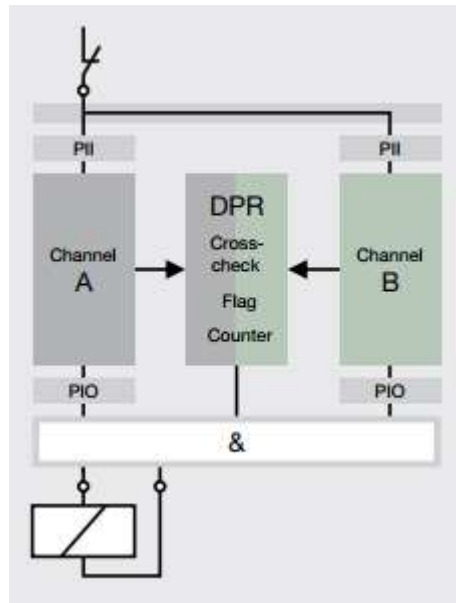


Figure 12 – Structure of a Safe Control System

Safety control systems shall be implemented whenever a failure in the control system could cause an injury or increase the likelihood of injury.

Safety control systems shall have an increased reliability in comparison to standard control functions. The increase in reliability can be achieved by:

- Increasing the reliability of the components;
- Changing the structure of the control system ( i.e. redundancy and monitoring);
- Both of the above.

All safety control system components should be safety-rated, i.e. tested, and certified for use in safety control systems. The performance of systems and components should be validated in accordance with relevant international or national standards (ISO 13849 or IEC 62061).

Process safety control systems must comply with the requirements of PNR-000081 - Instrumentation and Control - Supervision and Control System - Instrumented Safety System (SIS).

### 7.11.1 Safety Categories

A more detailed information is given in Annex C.

#### I. Category B

SRP/CSs and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards and using basic safety principles so that they can withstand the expected influence.

Lowest level of safety categories in a single channel architecture. Components do not need to be special safety equipment.

## II. Category 1

Requirements of Category B shall apply. Additionally, well-tried components and well-tried safety principles shall be used. Still uses a single channel architecture, but by using specific components suitable to the safety task the reliability is higher than Cat B

## III. Category 2

Requirements of Category B and well-tried safety principles shall be applied. Safety function shall be checked at suitable intervals by machine control system.

A second channel need to be provided in this category but not to the extent of the further categories

## IV. Category 3

Requirements of Category B and well-tried safety principles shall be applied. Safety function shall be designed so that:

- A single fault in any of these parts does not lead to the loss of the safety function, and
- Whenever reasonably practicable the single fault is detected

Redundant architecture is in use with some monitoring of the safety function.

## V. Category 4

Requirements of Category B and well-tried safety principles shall be applied. Safety function shall be designed so that:

- A single fault in any of these parts does not lead to the loss of the safety function, and
- The single fault is detected at or before the next demand upon the safety function; an accumulation of faults shall not lead to the loss of the safety function.

Redundant architecture and monitoring to full extent of the safety function.

### 7.11.2 Performance Levels

Safety components' ability to perform a safety function is shown by the determination of the performance level. Both estimation and validation of performance levels (PL) of safety function shall be done.

The performance level (PL) of safety related part of control system (SRP/CS) is determined by the following:

- I. MTTFD value for each single component;
- II. DC;
- III. CCF;
- IV. The connection architecture;
- V. Safety-related software;
- VI. Systematic failures;

VII. The ability to perform a safety function under expected environmental conditions.

There are 5 levels of PL stated with letters. PLa is the lowest level and PLe is the highest.

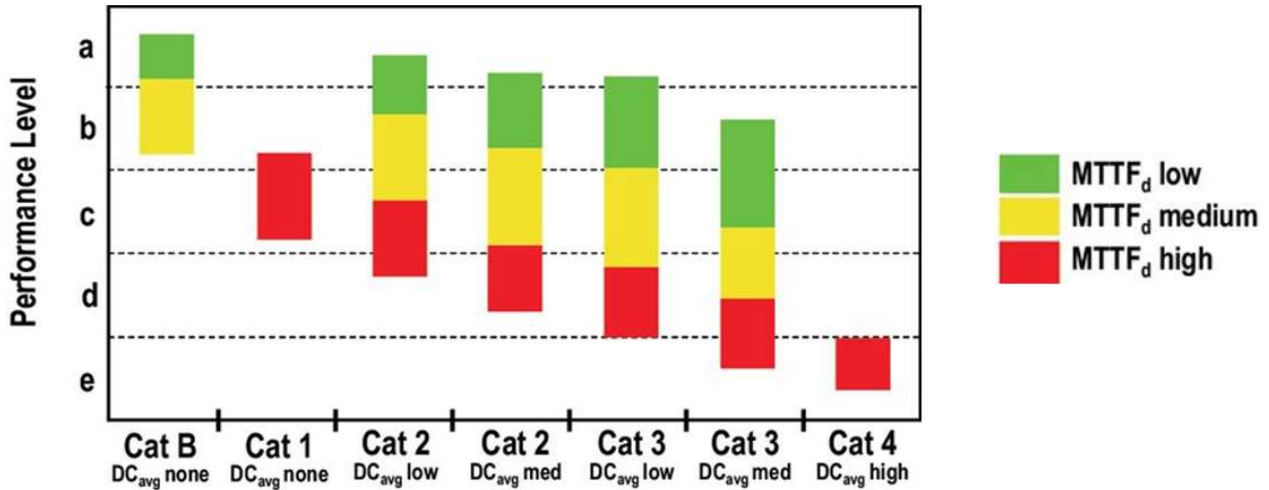


Figure 13 – Relationship of PL with Category, DC, MTTFD

### 7.11.3 Determination of Required Performance Level (PLr)

Required performance level of the safety functions are defined according the highest risk level it is related with.

The results acquired from risk evaluation gives the PLr and safety category that should be used in the related safety function. (See Table below).

| Inherent risk level of the Hazard, unguarded | PL <sub>r</sub> | Min. Safety Category |
|--|-----------------|----------------------|
| Low  | c               | 1                    |
| Medium                                       | d               | 3                    |
| High   | d               | 3                    |
| Very High                                    | e               | 4                    |

Table 11 – Relation of risk level with PLr and Safety Category

As an alternative method to determine PLr according to the standard ISO 13849-1 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.



## 7.11.4 Safety Related Specification Matrix for Safety Design

The safety related specifications (SRS) matrix shall be created in order to determine:

- What are the safety control system inputs (Both equipment code and equipment Type);
- What is the initiating event of these inputs;
- Which area of the machine are the input devices located;
- Either they are already present on the machine or recommended/required by the risk assessment;
- What are the safety control system outputs (Both equipment code and equipment Type);
- What is the resulting action of these outputs;
- Which area of the machine are the actuators controlled by output devices located;
- The relationship among these input elements and output elements, if the power of the related output element is cut-off or not if any specific input element is triggered.

|   |                       |                         |             |                         |                  |                        |
|---|-----------------------|-------------------------|-------------|-------------------------|------------------|------------------------|
| <b>Machine / Line Name</b>                  |                       |                         |             | <b>Output Type</b>      | Electrical Panel | Dual Channel Contactor |
| <b>Safety Related Specifications Matrix</b> |                       |                         |             | <b>Output Code</b>      |                  | GHI789                 |
| <b>Prepared By:</b><br><b>Date:</b>         |                       |                         |             | <b>Resulting Action</b> | Shut-off         | Shut-off               |
|   |                       |                         |             | <b>Area</b>             | Loading          | Loading                |
| <b>Component Code</b>                       | <b>Component Name</b> | <b>Initiating Event</b> | <b>Area</b> | <b>Exist / Planned</b>  |                  |                        |
| ABC123                                      | Emergency Stop Button | Triggering              | Loading     | Exist                   | OFF              | OFF                    |
| CDE456                                      | Interlock Switch      | Triggering              | Safety Door | Planned                 | OFF              | ON                     |

Table 12 – Sample of SRS matrix

This matrix is important to determine if all safety functions are correctly designed and all inputs (Interlocks, emergency buttons, scanners etc.) correctly cut-off all related outputs (contactors, drives, valves etc.) as specified during risk assessment. It also assists designing the non-existing but required safety functions.

The next step after creating the SRS matrix is validating it. This step is also one of the machines required documentation for CE marking process. In this process all inputs are triggered manually on the machine and cut-off of the output signal and stop of the physical actuator are both confirmed.

## 7.12 Energy Sources

All energy systems shall be designed and installed in a way that will not endanger the safety or health of person working on or near the machine.

All energy systems shall be clearly identified, showing the type of energy and the level (i.e. pressure, voltage, current, etc.).

A safe isolation device and, if necessary, a dissipation device shall be supplied for each energy source.

Safety aspects of the operation in the event of any relevant energy source failure shall be considered. The machine shall be able to return to a safe state in such cases.

The restoration of energy source shall not restart the machinery automatically. A deliberate action from the operator (reset and start) shall initiate the automatic operation of the machine.

### 7.12.1 Electrical Energy

Where machinery has an electricity supply, it shall be designed, constructed, and equipped in such a way that all hazards of an electrical nature are or can be prevented.

All electrical measures must have sufficient safety measures to prevent persons coming in contact with live voltages either by direct or indirect means.

For electrical energy, implementation of the following isolators are required:

- Circuit breaker;
- Circuit interrupter;
- Switch disconnecter;
- If current < 32 A, an electrical plug is acceptable.

Electrical equipment shall be installed in an electrical cabinet which:

- Includes a means of interrupting the electrical supply;
- A “Voltage Indication Lamp” which will light if there is a voltage in the panel;
- The degree of protection level (IP) shall be suited to machine’s usage and to the working environment in which it is installed. A minimum IP2X is required;
- Cabinet doors shall only be operable by the use of a tool and by the authorized personnel;
- Components installed in the electrical panel should be “touch proof”, i.e. exposed live parts are protected by IP2X openings;
- The panel shall provide suitable cooling for the components and the environment installed in;
- Equipment required to control, or adjustment processes characteristics must be accessible without opening the panel;

- Lighting has been provided to ensure maintenance work can be carried out safely.

All circuits shall be protected by a suitable overcurrent protection device, i.e. Fuses, circuit breakers, Moulded Case Circuit Breaker (MCCB), Miniature Circuit Breaker (MCB).

Overcurrent protection shall be installed to protect the entire electrical installation. The preferred location for the main overcurrent protection device is immediately after the main isolator. Additional dedicated overcurrent protection shall be installed to protect;

- Components which may be damaged by the current allowed to flow through by the main overcurrent protection;
- Internal power supplies;
- Motors;
- Lighting;
- General purpose socket outlets.

Circuits for socket-outlets should be provided with residual current protective devices (RCDs) with a maximum rating of 30mA with a break time of <30ms. It is recommended that instantaneous RCD's without a time delay are used.

Measures must be taken to prevent malfunction of the machinery due to electromagnetic interference, such as the presence of arc welding at the machine. These measures shall include:

- Use of components certified as compliant with the EMC directive;
- Use of shielded cables;
- Grounding of all shields and enclosures;
- Installation of all components in accordance with the information for use;
- Use of filters as per drive manufacturers instructions.

Low Voltages such as 24VDC and 48VDC are recommended for control circuits.

DC control circuit must be feed from a separate power supply installed inside the control panel. This power supply must be protected against overcurrent

AC control circuits, if exists, must be powered through isolated transformers, except for machines less than 3 kW with only one motor and maximum two external control devices. Nominal voltage of AC control circuits through transformers must be lower than 250 VAC.

All conductive parts shall be insulated. The insulation must be sufficient to withstand any foreseen overvoltage but at least twice the nominal voltage.

All exposed metallic parts and conductive surfaces shall be connected directly to an earth conductor. Protective bonding points shall be marked with the pictogram in Figure 15



Figure 14 – Protective bonding pictogram

Only a single earth conductor shall be connected to each earth terminal.

The overcurrent protection shall be sized to operate when any exposed conductive parts become live. Otherwise a separate earth current protection device is required.

The marking of the equipment in cabinets and covers chutes shall be made with permanent labels on the equipment.

The color coding of the wires should be compliant with the colors in table 6 below.

|                                |              |
|--------------------------------|--------------|
| AC and DC Power Circuits       | BLACK        |
| Neutral                        | BLUE         |
| AC Control circuits            | RED          |
| DC Control Circuits            | DARK BLUE    |
| Protective Conductor / Bonding | GREEN YELLOW |
| Excepted Circuits*             | ORANGE       |

Table 13 – Color Coding of Cables

\*Excepted circuits are the circuits that does not need to be disconnected by the supply disconnecting device, i.e. panel lightning.

Where local regulations differ from the table above, the regulations shall be followed.

### 7.12.2 Pneumatic & Hydraulic Energy

Hydraulic and pneumatic systems shall have pressure gauges to indicate the current pressure value.

Intended or unintended loss of pressure shall not cause a hazard like dropping of the held part or unintentional move with the effect of gravity.

Pneumatic systems shall have a “soft start” system which prevents rapid increases in the pressure of the system, especially in repressurizing after a dissipation, following the reconnection of the main supply shall be fitted on all machines.

All elements of the system shall have a unique code attached on or near the equipment in relation with the technical drawings.

## I. Over-pressure

Over pressure protection, such as a pressure relief valve, must be provided on the discharge side of each source of pressure.

The set pressure of the relief valve shall not exceed 10% higher value of the maximum permissible pressure of the system or the lowest pressure-rated component in the circuit; whichever is lowest. The set value shall be permanent, or it shall be possible to change the value only by authorized personnel.

In case of over-pressure, relief valves shall be vented to a safe location.

## II. Pressure vessels

All equipment and vessels intended to contain substances at a pressure of greater than normal atmospheric pressure shall be designed and constructed in such a way that shall not create any additional hazards.

Before being put into service all equipment shall be tested at least at normal working pressure.

Vessels with a volume of greater than 2 liters shall be tested at 1.5 times the intended normal working pressure.

A name plate shall be present on the vessel indicating the minimum and maximum working temperature, and the maximum working pressure and regulatory marking.

All pressurized vessels shall be fitted with at least one pressure relief device, rated for 85% of the maximum working pressure.

It shall be possible to safely drain pressure vessels.

## 7.13 Unexpected Start-up and Control of Hazardous Energy

Nowadays most accidents happen as a result of unexpected start-up of machinery or unexpected exposure to hazardous energies. Machinery must provide various measures which either can be applied via the control system or manually to control hazardous energies. See Figure below.

### 7.13.1 Exposure Levels to Hazardous Energy

The levels which relate to the risk of hazardous energy and unexpected start-up shall be categorized and link them to specific safety measures. The exposure levels can be divided according to their characteristics and nature of the task into 5 categories (See Table 14). The “3” and “4” exposure level require specific actions and caution

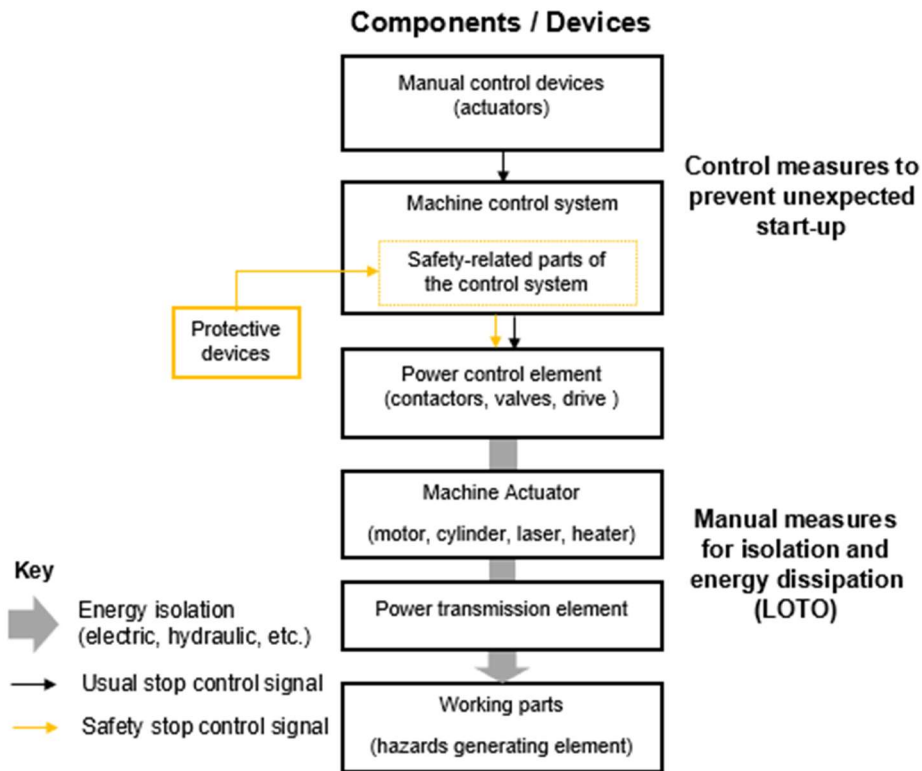


Figure 15 – Levels of Prevention for Unexpected Start-up

| Exposure Level to Hazard | 1                                 | 2                       | 3  | 4   | 5                                |
|--------------------------|-----------------------------------|-------------------------|--|---|----------------------------------|
| Task Characteristics     | Work outside safeguards           | Work through safeguards | Work inside the machine, behind safeguards   | Work near hazardous energy/ movements         | No safeguards, everything is off |
| Task                     | Normal Operation                  |                         | Clearing Jams / Tool change, etc.  | Set-Up, Adjustment, Process monitoring, etc.  | Maintenance                      |
| Safety Measures          | Fixed guards or Perimeter Fencing | Protective Devices      | Key exchange / Trapped-key interlock, Multiple Reset, Tag System, partial Lockout/Tagout, etc. | Partial Lockout/Tagout / Alternative Measures | Lockout, Tagout and Zero Energy  |

Table 14 – Levels of Exposure

**NOTE:** The designer must interact with the engineering, maintenance, and safety areas to define the machine devices and protections according to the type of exposure that allow accessibility for operation and maintenance.

- LEVEL 1**

Level “1” means that no exposure is needed or possible. The most common example is observing the operation without any intervention. The related personnel do the task outside safeguards and type of tasks are normal operational tasks generally. Nobody is inside the hazardous zone which is covered by safety fences or other safeguarding measures.

- **LEVEL 2**

Level “2” includes regular operational tasks through the safeguarding (example: Violating light curtain with some part of the body, standing on a safety mat, open the safety gate with safety sensor, etc.). In this case, the protective device will act, and the machine will stop, the most common example is manual feeding or assembly tasks related with the process. In general, only one person is in the hazardous zone, but is completely sensed and protected by protective measures. No exposure to hazardous movement or energies is possible while personnel is in or near the hazard zone. There is limited risk of un-expected start-up, because it is essential that the protective device is fully capable of detecting personnel breaching the safeguard.

- **LEVEL 3**

Level “3” level include irregular operational tasks or minor maintenance activities inside the machine which is behind the safeguarding. The most common example is clearing of jams or tool change operations. While the machine will switch off as a result of a safety function (example: opening a door or stepping through a light beam system) a person can be near or inside the hazardous zone without being discoverable by protective devices. The risk of unexpected start-up is high, especially where multiple persons are needed to perform a specific task. Ideally presence sensing devices like area scanners, safety mats, etc. are used and properly configured to cover the inside area and prevent start-up (which would turn this exposure into a level “2”).

**NOTE:** The activities to be carried out with level 3 exposure shall have procedures and ART.

Level “3” exposures require approved specific actions (Because thy this exposure level cannot be technically changed to “Level 2”) which can include:

- Where lockable doors are used as safeguards, a key transfer system allows authorized personnel to hold their “key to safety”;
- Multiple Reset sequence, e.g. a “Pre-Reset” needs to be activated inside the cell and within a time frame followed by the “normal Reset” outside of a cell (hazardous area), ensure inspection and assurance of the absence of people within the danger area;
- Lockout and tagout system for dangerous energy or locks for cell entry identification.

- **LEVEL 4**

The level “4” include tasks where the work needs to be performed near hazardous energies and/or movements. These can be adjustment or process monitoring activities or some maintenance or set-up activities (e.g. teaching, balance calibration). The risk of un-expected start-up or exposure to hazardous energies is extremely high, especially where multiple persons are involved. Ideally only one person should be in the hazardous zone to perform related tasks.

Wherever possible (partial) Lockout Tagout procedure should be applied to energy sources. For remaining energy sources, alternative safety measures need to include one or more of the following:

- “Special” modes only accessible to authorized personnel (e.g. special key, password, etc.);
- Hold-to-run (example: Dead man, Enable device) devices to enable slower motions;



Rev.: 00 – 25/11/2021

- Additional warning devices;
- Nearby access to emergency stop/motion-off devices;
- Mode Limitation in terms of time or functionality to force the return to “normal” modes;
- Need for administrative measures like PPE, training, etc.

**NOTE:** The activities to be carried out with level 4 exposure are pre-established and shall have procedures and ART.

- **LEVEL 5**

The level 5 include task which relate to (full) maintenance activities, either preventative or corrective. Presence of more than one person in the hazardous area may be necessary during such tasks. There may be a need to remove safeguards as part of the task. **The risk of unexpected start-up or exposure to hazardous energies is high.** The risks can be handled with proper application of a full Lockout and Tagout methodology (which includes all the energy sources) to “black-out” the machine fully.

### 7.13.2 Control Measures to Prevent Unexpected Start-up

One way of preventing unexpected start-up is a properly designed and applied full CAR 4 Lockout Tagout procedure, In accordance with Lockout matrix, In the cases where RAC4 cannot be applied, shall be complied with the "exception criteria" as PNR-000069

Special attention must be paid to prevent unintended start-up resulting from:

- Closure of interlocked guards;
- Releasing of an emergency stop device;
- Changing the machine operating mode;
- Power on after any outage of energy of any type.

There shall be no hazardous movements in the machine/equipment in the cases of:

- Energy loss or drop of energy/pressure;
- Restoration of energy;
- Release of energy.

Machine/equipment shall not restart automatically after restoration of energy without the necessity of resetting and restarting by a deliberate and dedicated action.

Measures in the control systems shall be taken to prevent intended start-up command resulting from actuation of material (i.e. triggering of sensors, limit switch, load, etc.), failures or from external factors (i.e. vibrations, etc.).

Start control devices shall be properly designed, located, marked and protected. If several start control buttons exist in a specific panel controlling different machines and/or equipment and/or tasks, each should be clearly identified about their action.

Requirements of STOP devices explained in section 7.4 shall be applied.

For safety related stops, once the machinery or its hazardous functions have stopped, the energy supply to the actuators concerned must be cut off or controlled safely.

If a mode selection switch exists in a machine, it shall be lockable type (i.e. key-locked, password, etc.) in order to prevent unauthorized change of the operation mode.

Reset function can be used as part of the SRP/CS to avoid an unexpected start-up, before manually restarting the machinery. Reset devices are the devices triggering this function.

After a stop command initiated by a safeguard or protective measure or a switch-off application, the command shall be maintained until all safety conditions are met and a deliberate sequence of activating reset function is activated.

The reset function shall:

- Be activated by a separate (or multiple) reset device;
- Be operated manually and deliberately;
- Be a part of SRP/CS (especially where working behind safeguards is possible);
- Only be activated successfully if all safety measures are operational (without error or warnings);
- Not initiate any hazardous motion or situation by activation;
- Enable the control system of the machine for accepting a separate start command;
- Only be triggered by disengaging the reset device actuator from its energized (on) position;
- Be identifiable through BLUE color of the button.

The reset actuator shall be situated outside the hazardous zone and in a safe position. The location of the button shall be selected to clearly view all hazardous area, in order to confirm no person is in the hazardous area. If this requirement cannot be met, additional measures shall be taken like:

- Implementation of presence detection measures to cover all hazardous area;
- Implementation of a pre-defined activation sequence of multiple reset devices;
  - Multiple reset button devices shall be present, some of which can be located inside the hazardous zone;
    - Sufficient number of devices needs to be used to cover all hazardous area;
  - Activation sequence of the reset devices shall be pre-defined;
  - Activation sequence shall be completed in a pre-determined time;
- Implementation of visualization systems (i.e. CCTV, etc.) to the button location in order to see all hazardous zones to be reset.

Mechanical elements can move unintendedly because of:

- Their mass and position (i.e. unbalanced elements, etc.);
- Mechanical energy storage via springs, etc.;
- Parts continuing to move with their inertia;
- Unintended movement because of gravity.

Measures shall be applied to prevent these kinds of movements. When applicable, brakes, mechanical locking via pins, etc. or mechanical restraint devices can be used to bring them to a safe controlled state.

### 7.13.3 Manual Isolation of Dangerous Energy Sources (LOTO)

Machine and all installation devices shall be provided with isolation devices capable of:

- Securely isolating the machine from all external sources of hazardous energy;
- Safely releasing any internal stored residual hazardous energy;
- Blocking and visually identifying any residual hazardous energy that cannot be released.

Energy isolation and blocking devices shall be:

- Easily identifiable and accessible;
- Labelled with its function or code as it is stated in the blocked local procedure (RAC4);
- Clearly indicate its status (ON/OFF);
- Capable of being locked or secured in isolated (OFF) position;
- Installed outside the safeguards of the machinery;
- Be activated only by direct mechanical action;
- Designed to enable easy and fast a lockout procedure;
- Be preferably centralized, located in close proximity to their associated machinery to facilitate use;
- Be fitted with devices that allow the dissipation of potential residual energies, where applicable;
- Grouped together, if possible.

Lockable machine control or protective devices (e.g. E-Stop, etc.) should not be used as energy lockout devices.

If the locking of isolating devices or the dissipation of residual energies requires dedicated equipment, these accessories or equipment shall be supplied with the machinery.

If energy accumulators are present, they shall also be identified and include an easily accessible device to release the energy provided.

For the tasks (i.e. maintenance) related with energy storage devices, proper instructions and warnings shall be prepared. Necessary procedures should be implemented to machinery documentation.

Wherever dropping/drifted of equipment/parts presents a hazard, devices shall be installed to eliminate, or measures shall be applied control the hazard.

Mechanical limitation devices shall be monitored in both their locking position and stored position to prevent starting the equipment unless the pin or block is removed and returned to its stored position.

Tension pressure devices that can cause a hazard shall be capable of being released, locked, or otherwise controlled.

## 7.14 Means of Access

Machinery and the installation devices must be designed and constructed in accordance with the standard ISO 14122 - Safety of machinery - Permanent means of access to machinery (Parts 1,2,3,4), in such a way as to allow access safely to all areas where intervention is necessary during operation, adjustment, maintenance, and other activities related with the machinery.

Access to machinery should be either from ground level or from platforms to reduce the use of ramps, stairs and ladders.

The means access to machines shall be defined according to the angle of the measure:

- 0° - 10° Ramps;
- 10° - 20° Ramps with enhanced slip resistance;
- 20° - 45° Stairs (The recommended slope angle is between 30° and 38°);
- 45° - 75° Stepladder (The recommended slope angle is between 45° and 60°);
- 75° - 90° Fixed ladder.

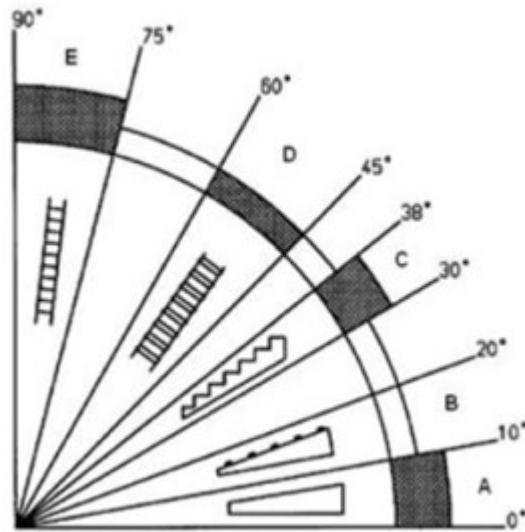


Figure 16 – Angle for select means of access

Legenda:

■ Preferred means of access

A – Ramp

B – Ramps with enhanced slip resistance

C – Stairs

D – Stepladder

E – Fixed ladder

## a) Working Platforms and Walkways

Walkways and platforms shall be designed and placed to prevent hazards from people falling, falling objects or, exposure to harmful materials from them.

There shall be no obstacle or tripping point, floor height difference higher than 4 mm (0.1574 in) and gap more than 20 mm (0.7874 in), on the walkways or platform floors. The maximum diameter of an opening in the platform or walkway floor shall be lower than 35mm (1.3780 in). If there are persons passing below, this diameter shall be lower than 20 mm (0.7874 in).

The surfaces shall have slip resistant properties and designed to prevent accumulation of, liquids, dirt, snow, ice etc.

Where access to the machine is required at heights greater than 1.8 m (70.8661 in) (or more restrictive local legislation) a working platform shall be provided.

Minimum height clearance (h) shall be 1900 mm (74.8031 in) and minimum width clearance (w) shall be 800 mm (31.4961 in).

Handrails or other supports shall be designed and placed to be used instinctively. Guard rails shall be installed for walkways and platforms that has a falling risk higher than 500 mm (19.6850 in).

All activities shall be done without the removal of guard rails, flooring, or other permanent barriers, if possible.

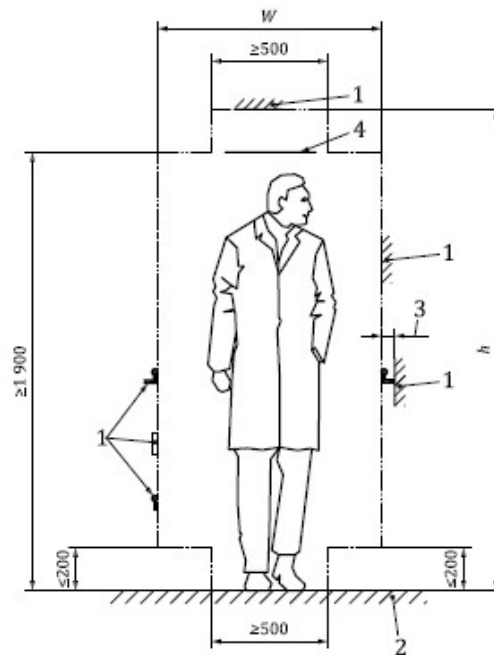


Figure 17 – ISO 14122-2 for safe access in walkways and platforms

Legend:

 Limitation of the access gauge

1 – Permanent obstruction

2 – Walkway/platform

3 – Minimum gap between handrail and obstacle

4 – Crossing obstacle

w – Clear width

h – Head-height

## b) Guard-rails:

A guard rail shall be used for the following situations

- A risk of a fall higher than 500 mm (19.6850 in);
- A gap in the floor larger than 180 mm (7.0866 in);
- A gap between a platform and structure of machine is larger than 180 mm (7.0866 in);
- A climb in a stairs or stepladder higher than 500 mm (19.6850 in).

## Dimensions of the guardrail:

- A The minimum height of the guard rail shall be 1100 mm (43.3070 in);
- The height of the hand shall be lower than 1100 mm (43.3070 in);
- The handrail shall be parallel to the walking line;
- If there are additional steps near guard rails, the total height of the guard rail shall be designed accordingly;
- A toe-plate with a minimum upstand of 100 mm (3.9370 in) shall be placed. It can be start 12 mm maximum from the walking level;
- The clear space between the handrail and the knee rail, as well as between the knee rail and the toe-plate, shall not exceed 500 mm (19.6850 in);
- When guardrails are made in modules, the clear space between the two stanchions shall not be greater than 120 mm (4.7244 in).

NOTE 1: Whenever the local legislation / standards are more restrictive shall be adopted the local legislation / standards values.

NOTE 2: Guardrails on escape routes must comply with the guidelines of PNR-000127 – Facility Layout – Escape Routes.

NOTE 3: If indicated by the risk assessment, the clear space between knee rail and the toe-plate and handrail must be mechanically closed (examples: mesh, steel plate, etc.).

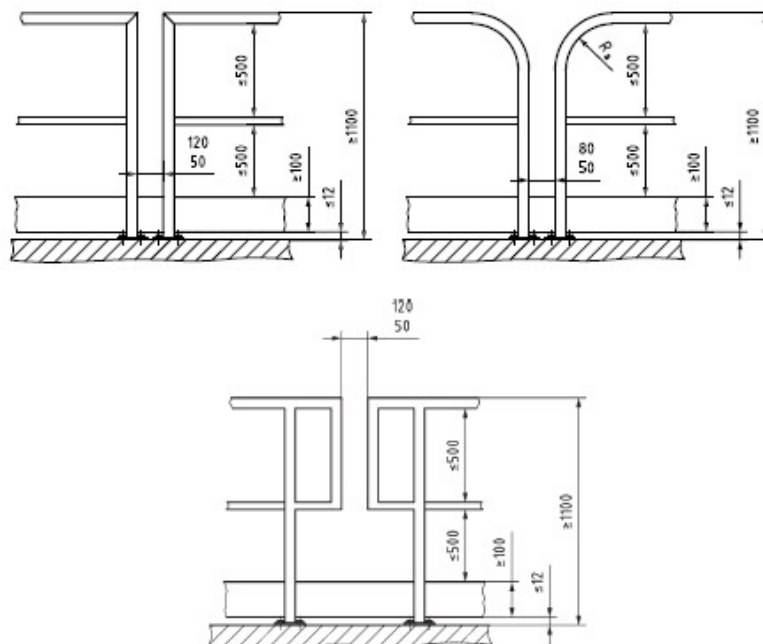


Figure 18 – ISO 14122-2 Fall protection system for access means

The guard rails on stairs and stepladders shall be continuous and be on both sides.

If access through the guard-rail is necessary, a gate shall be used which shall be:

- Self-closing;
- Held in closed position;
- Open easily to platform or floor;
- A device to prevent to open in falling through side.

The shape of the handrail should have a diameter between 25 mm (0.9843 in) to 50 mm (1.9685 in).

## c) Stairs

Stairs can be used to access platforms if the slope is between  $20^{\circ}$  -  $45^{\circ}$  but the recommended slope angle is between  $30^{\circ}$  and  $38^{\circ}$ .

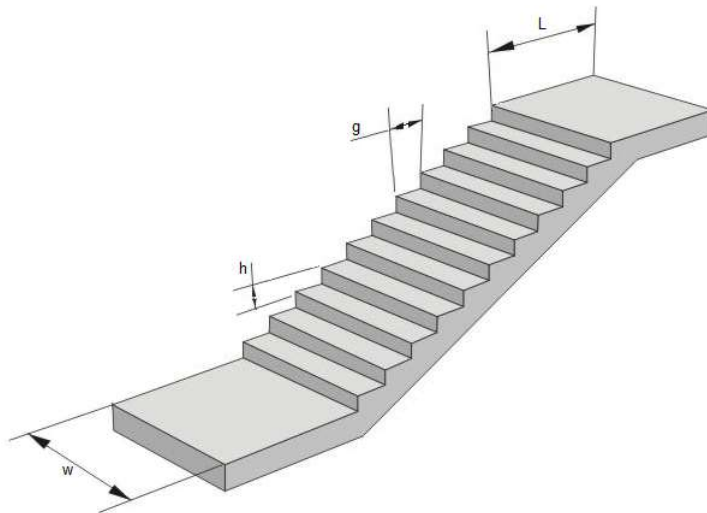


Figure 19 – Detailed image of a stair

Legend:

h – Height between treads

g – Step width

w – Stair width

L – Rest platform length

Rise values of the steps in the same stair shall be equal.

The uppermost step shall be level with the platform/walkway surface.



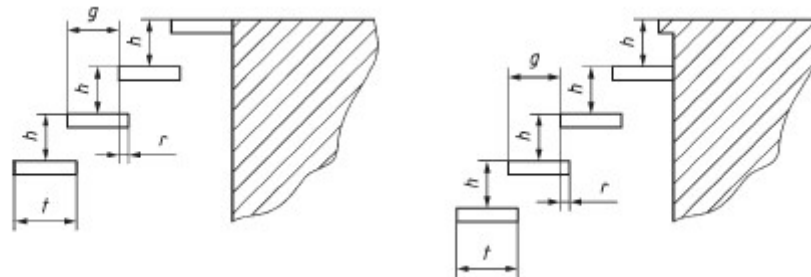


Figure 20 – ISO 14122-3 Positioning of the uppermost step

The minimum vertical, head-height, clearance shall be 2.300 mm (90.5512 in). The minimum perpendicular height clearance to the aim of the stair shall be 1.900 mm (74.8031 in). The minimum width clearance of the stairs shall be 800 mm (31.4960 in).

**d) Stepladders**

Stepladders should be used to access platforms if the slope is between 45° - 75°.

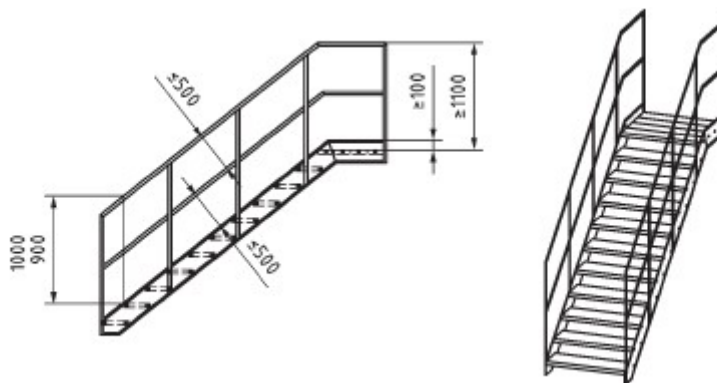
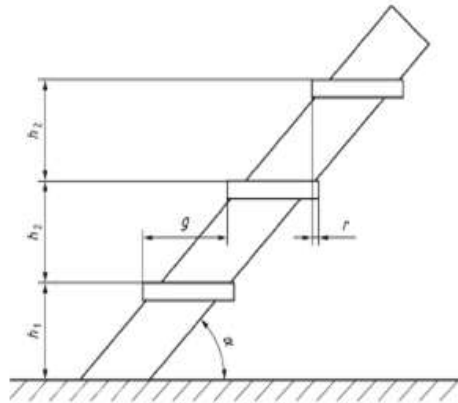


Figure 21 – ISO 14122-3 of implementation of guard-rails to stairs

Rise values of the steps in the same stepladder shall be equal.

The minimum vertical, head-height, clearance shall be 2300 mm (90.5512 in) and minimum width clearance of the steps shall be 850 mm (33.4646 in).



|             | $45^\circ < \alpha \leq 60^\circ$ |       | $60^\circ \leq \alpha \leq 75^\circ$ |       |
|-------------|-----------------------------------|-------|--------------------------------------|-------|
|             | $h_1$                             | $h_2$ | $h_1$                                | $h_2$ |
| <b>Min.</b> | $0,5 \times h_2$                  | 150   | $0,5 \times h_2$                     | 230   |
| <b>Max.</b> | $h_2 + 15$                        | 200   | $h_2 + 40$                           | 300   |

Figure 22 – ISO 14122-3 figure to define climb heights for stepladders

Legend:

g – Tread free length

h – Step height

r – Overlap

$\alpha$  – Angle of the Stepladder

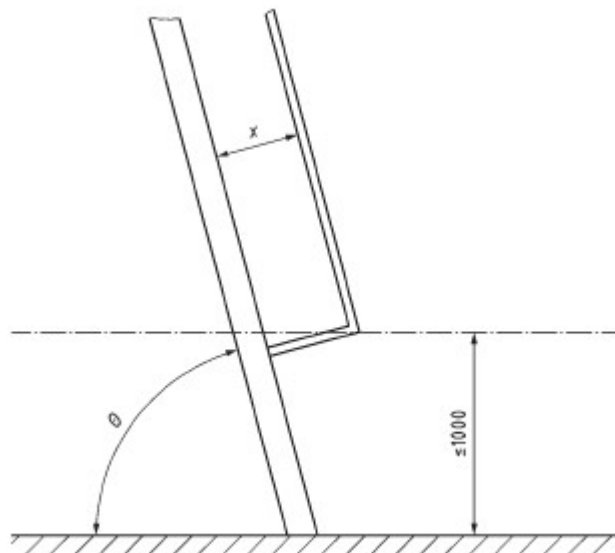


Figure 23 – ISO 14122-3 positioning of a handrail on a step ladder

| $\theta$<br>degrees | X<br>mm |
|---------------------|---------|
| 45                  | 625     |
| 50                  | 500     |
| 55                  | 375     |
| 60                  | 250     |
| 65                  | 200     |
| 70                  | 150     |
| 75                  | 100     |

Table 15 – Table ISO 14122-3 to define the clear width between the pitch line on a stepladder and the handrail

## e) Fixed Ladders

Fixed ladders should be used to access platforms if the slope higher than 75°. The requirements in RAC 1 must be followed.

Dimensions:

- Distance between Ladders must be 700mm (27.5591 in);
- Ladder width should be from 400mm (15.7480 in) to 600mm (23.6220 in);
- Height between steps must be 250mm (9.8425 in) to 300mm (11.8110 in);
- It is mandatory to have a device to prevent a fall as from 1.80m (70.8661 in);
- Ladder with a single flight, maximum of 10m (393.7008 in);
- Ladder with more than 10 meters, each flight must be a maximum of 6m (236.2205 in).
- The ladder must have a spacing between the fixing structure of at least 200mm (7.8740 in);
- The opening between the ladder and a passageway must be at least 650mm (25.5906 in).

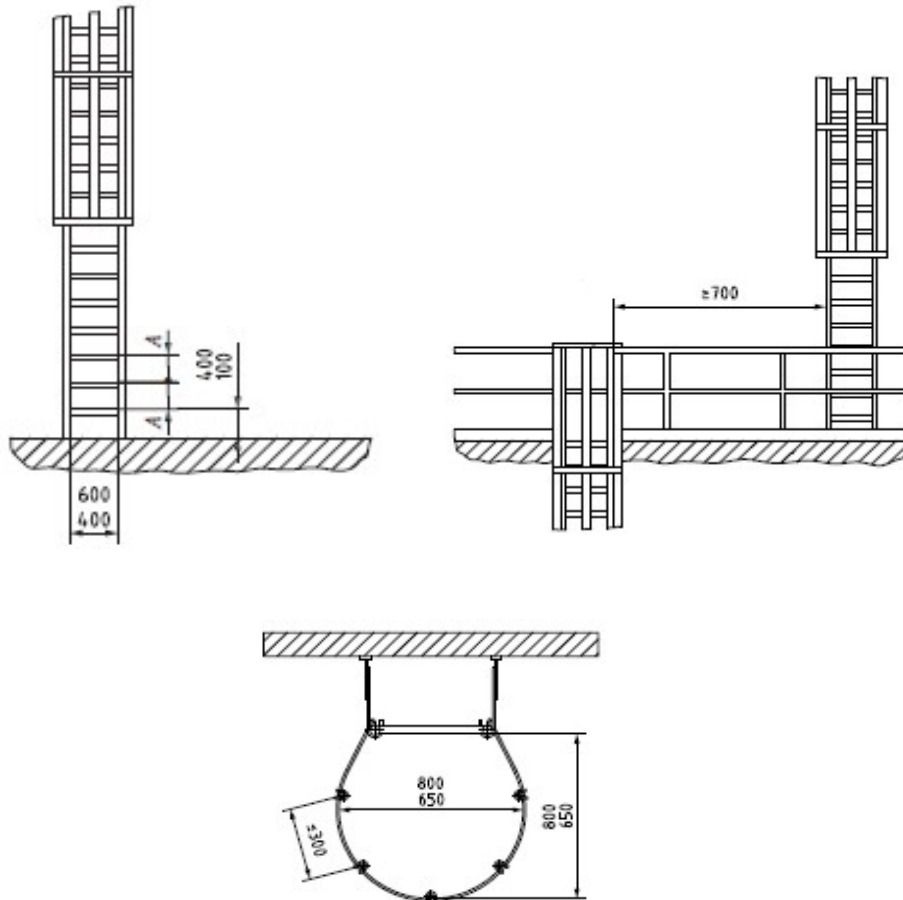


Figure 24 – ISO 14122-4 dimensions of a fixed ladder and safety cage

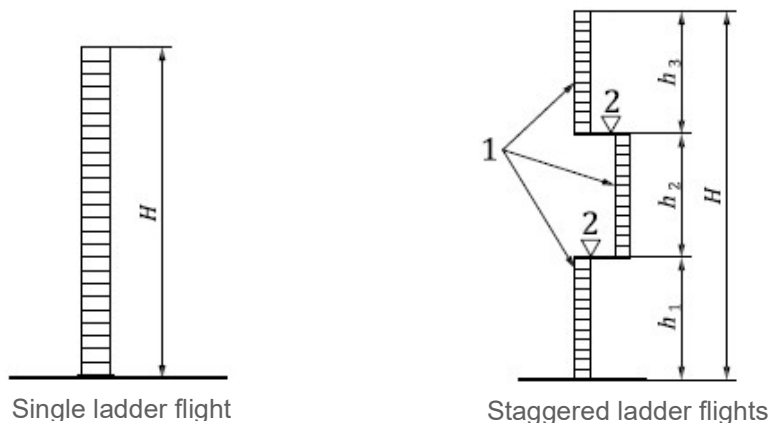


Figure 25 – ISO 14122-4 dimensions of different types fixed ladders

Legend:

1 – Ladder flight

2 – Arrival area

H – Climbing height of ladder

h – Height of ladder flight

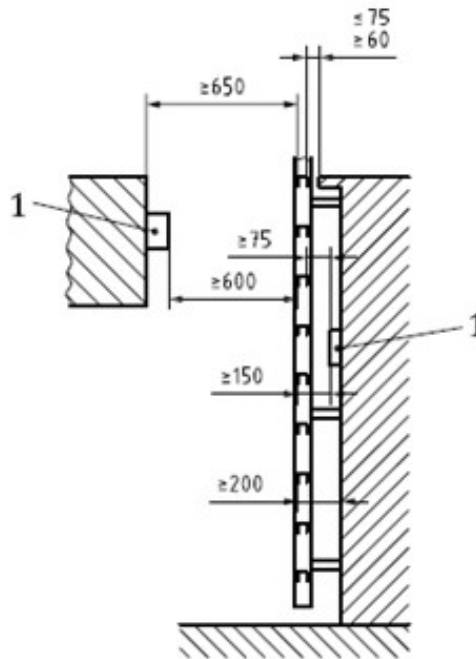


Figure 26 – ISO 14122-4 Space dimensions with permanent obstacles

Legend:

1 – obstacles such as pipes or trays

### 7.15 Signage System

Where a residual risk remains in the machinery, warning signs should use standard pictograms as per local legislation or standards, together with simple text in the local language. Signs should typically indicate the nature of the hazard and the precautions required.

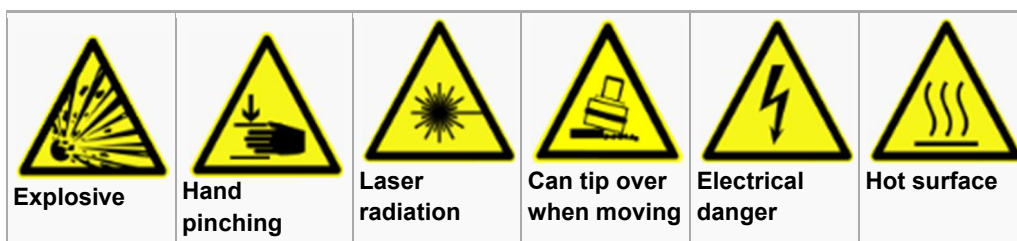


Figure 27 – Examples of Pictograms

A more comprehensive list of warning pictograms can be found in Annex D.

The ISO 3864 standard, parts 1, 2 and 3 defines the safety identification colors and the design principles for safety signs and markings to be used in the workplace, with the purpose of preventing accidents and information about the risks that the worker is exposed.

Graphical safety signage provides a general safety message through a combination of color and geometric shape and which, by adding a graphical symbol, conveys a specific safety message.

The material used to make the graphic signage must be durable and suitable for the environment. International safety symbols are described in the ISO 7010 standard and should preferably be used to indicate hazards where there is a risk to people.

| Geometric shape   | Meaning          | Safety color | Contrast color | Graphical symbol color | Example of use  |
|---|------------------|--------------|----------------|------------------------|---|
|    | Prohibition      | Red          | White          | Black                  | <ul style="list-style-type: none"> <li>- No smoking</li> <li>- No unauthorized vehicles</li> <li>- Do not drink</li> </ul>  |
|    | Mandatory action | Azul         | White          | White                  | <ul style="list-style-type: none"> <li>- Wear eye protection</li> <li>- Wear personal protective equipment</li> <li>- Switch off before beginning work</li> </ul> |
|  | Warning          | Yellow       | Black          | Black                  | <ul style="list-style-type: none"> <li>- Danger hot surface</li> <li>- Danger acid</li> <li>- Danger high voltage</li> </ul>                                      |
|  | Safe condition   | Green        | White          | White                  | <ul style="list-style-type: none"> <li>- First aid room</li> <li>- Fire exit</li> <li>- Fire assembly point</li> </ul>  |
|  | Fire safety      | Red          | White          | White                  | <ul style="list-style-type: none"> <li>- Fire alarm call point</li> <li>- Firefighting equipment</li> <li>- Fire extinguisher</li> </ul>                          |

Table 16 –Safety graphic symbols definition table

Supplemental safety information, such as text and/or in the layout of a graphic symbol, may be used to describe, supplement or clarify the meaning of a safety sign.

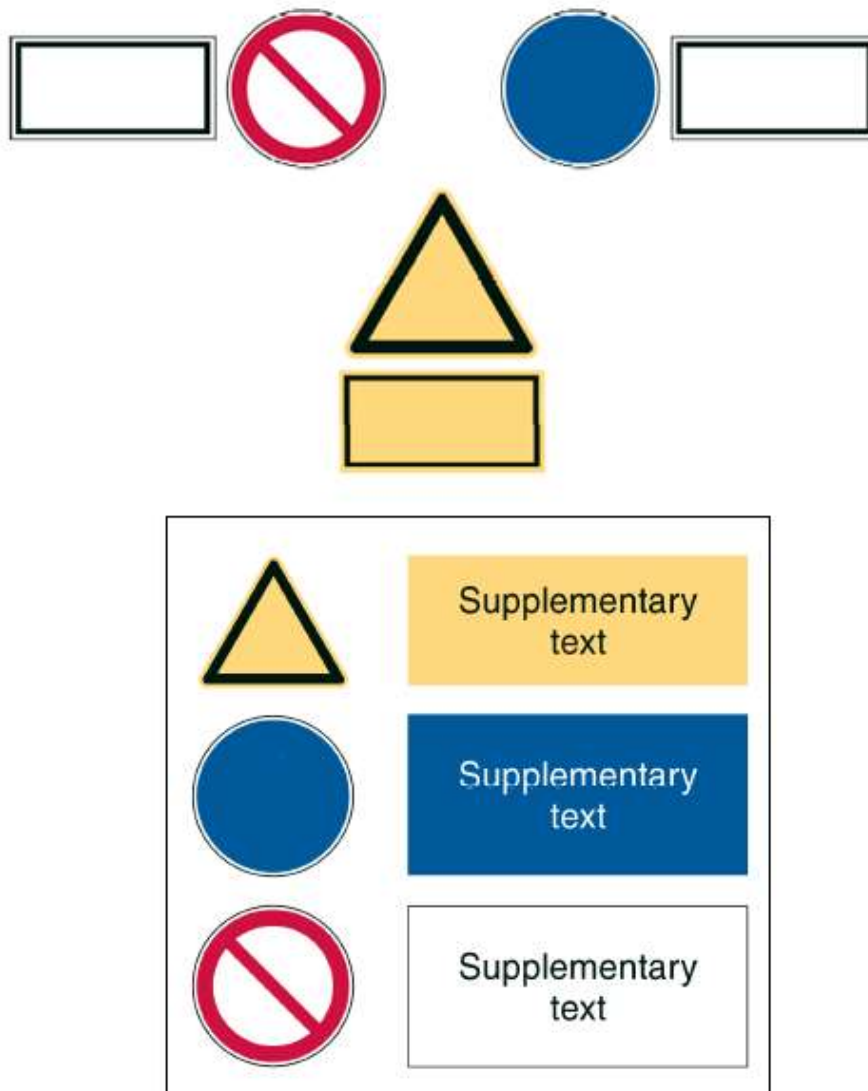


Figure 28 – Graphic signage with supplementary information

Use of colors and hazard severity:




| Background color of panel | Text color | Meaning/Use  | Hazard severity panel illustration   |
|---------------------------|------------|--|--|
| Red                       | White      | DANGER hazard severity panel to identify a high level of risk    |  |
| Orange                    | Black      | WARNING hazard severity panel to identify a medium level of risk |  |
| Yellow                    | Black      | CAUTION hazard severity panel to identify a low level of risk    |  |

Table 17 – Hazard severity panel color definition table

Examples:



Figure 29 – Example of graphic signage

The purpose of the sign is to inform, so it is essential that it be identifiable.

The identification of signaling elements depends on several factors:

- Size;
- Type of confection material;
- Illuminance and contrast;
- Lighting conditions;
- Observation angle;
- Familiarity with shapes and elements.



## 7.15.1 Signal dimension

The relationship between the greatest distance from which the safety sign is readable and conspicuous in shape and color and the height of the safety sign together with the distance factor Z is given by the following equation:

$$h = l / Z$$

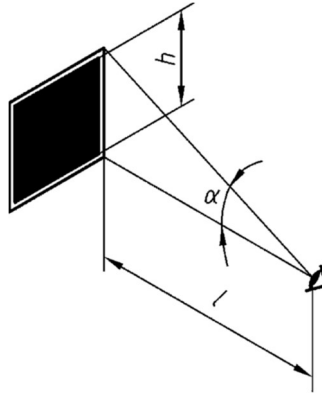


Figure 30 – Example for the angular extension of a safety sign

Legend:

l - distance of observation

h - height of the sign

Z - factor of distance =  $1 / \tan \alpha$

$\alpha$  - angular extension of the sign

## 8 LIST OF PRODUCERS

| Full name                       | E-mail                                 |
|---------------------------------|--|
| Aender Vaz                      | aender.vaz@vale.com                    |
| Ahmed Kalbani                   | ahmed.kalbani@vale.com                 |
| Alcemir Alves                   | alcemir.alves@vale.com                 |
| Alcimar Silva                   | alcimar.silva@vale.com                 |
| Alexandre Simoes                | Alexandre.simoese@vale.com             |
| Alice Sousa                     | alice.sousa@vale.com                   |
| Aline Ribeiro Da Silva          | Aline.Ribeiro1@vale.com                |
| Anderson Fontes                 | anderson.fontes@vale.com               |
| Anderson Lomasso                | anderson.lomasso@vale.com              |
| Anderson Souza Pereira Cruz     | anderson.s.cruz@vale.com               |
| Andre Barreto                   | andre.barreto@vale.com                 |
| Angela Grubber                  | Angela.Grubber@vale.com                |
| Asri Djaya                      | Asri.Djaya@vale.com                    |
| Maurício Barile                 | M.Barile@pilz.com.br                   |
| Breno Rossi                     | Breno.Rossi@vale.com                   |
| Bruno Reda                      | bruno.reda@vale.com                    |
| Camila Nunes                    | camila.nunes@vale.com                  |
| Cara Seiler                     | Cara.Seiler@vale.com                   |
| Carlos Dias                     | carlos.dias@nacalalogistics.com        |
| Chris Lepera                    | Chris.Lepera@vale.com                  |
| Clauder Wagner Mangelo Da Silva | clauder.silva@vale.com                 |
| Claudio Ataide                  | claudio.ataide@vale.com                |
| CONSTÂNCIO ROBERTO              | constancio.roberto@nacalalogistics.com |
| Donizetti Silva                 | Donizetti.silva@vale.com               |
| Edmilson Pires                  | edmilson.pires@vale.com                |
| Eric Rodrigues Santos           | eric.rodrigues.santos@vale.com         |
| Erick Araujo                    | erick.araujo@vale.com                  |
| Ernane Costa                    | ernane.costa@vale.com                  |
| Evandro Diceri                  | Evandro.Diceri@vale.com                |
| Evandro Lopes                   | evandro.lopes@vale.com                 |
| Everton Gianlorenco             | everton.gianlorenco@vale.com           |
| Felipe Motta Teixeira           | felipe.teixeira@vale.com               |
| Francisco Ricarte               | francisco.ricarte@nacalalogistics.com  |
| Gencil, Can                     | c.gencil@pilz.com.tr                   |
| Gerle Ferraco                   | Gerle.Ferraco@vale.com                 |
| Gisela de Camargo               | giselabc@gmail.com                     |
| Grack Rodrigues Gama            | grack.gama@vale.com                    |
| Hamyar Alriyami                 | hamyar.alriyami@vale.com               |
| Hayes, David                    | D.Hayes@pilz.ie                        |
| Iderson Fabiano                 | iderson.fabiano@vale.com               |
| Igor Hosken                     | igor.hosken@vale.com                   |

|   |                                     |
|---|-------------------------------------|
| Irismar Mesquita                        | Irismar.Mesquita@vale.com           |
| Jeff Wilkinson                          | Jeff.Wilkinson@vale.com             |
| Jim Mathiasen                           | Jim.Mathiasen@vale.com              |
| Joao Claudio Dos Santos Loureiro Junior | joao.loureiro@vale.com              |
| Joao David                              | joao.david@nacalalogistics.com      |
| Joao Samuel De Carvalho Neto            | Joao.Neto@vale.com                  |
| Junio Marins                            | junio.marins@vale.com               |
| Keijiro Shibata                         | keijiro.shibata@vale.com            |
| Laiz Fonseca                            | Laiz.Fonseca@vale.com               |
| LEONARDO RODRIGUES PAES                 | leonardo.paes@vale.com              |
| Leonardo Silva Dias                     | dias.leonardo@vale.com              |
| Lucas Arigoni Guimaraes                 | lucas.arigoni.guimaraes@vale.com    |
| Lucas Evangelista De Carvalho           | lucas.evangelista.carvalho@vale.com |
| Lucas Veiga Chetto Coutinho             | Lucas.Veiga.Coutinho@vale.com       |
| Luciano Ruy                             | luciano.ruy@vale.com                |
| Luis Renato                             | luis.renato@vale.com                |
| Marco Mendes                            | marco.mendes@vale.com               |
| Marcus Batista Bandeira Dos Santos      | Marcus.Batista.Santos@vale.com      |
| Marina Veronese Resston                 | Marina.Resston@vale.com             |
| Mayk Ferreira                           | mayk.ferreira@vale.com              |
| Moacir Santiago                         | moacir.santiago@vale.com            |
| Nicholas Pankiw                         | Nicholas.Pankiw@vale.com            |
| NURFATIHA AISHAH AMIRUDIN               | nurfatiha.aishah@vale.com           |
| Olavo Caetano                           | olavo.caetano@vale.com              |
| OMAYMA AL FARSI                         | omayma.farsi@vale.com               |
| Paulo Cueller                           | paulo.cueller@vale.com              |
| Paulo Lacerda                           | paulo.lacerda@vale.com              |
| Priscila Jardim Mariano Cabral          | Priscila.Cabral@vale.com            |
| Rafael Costa De Oliveira                | Rafael.Oliveira5@vale.com           |
| Raphael Zerrenner                       | raphael.zerrenner@vale.com          |
| Regina Penna                            | regina.penna@vale.com               |
| Reginaldo Mendes                        | reginaldo.mendes@vale.com           |
| Renato Nogueira Oliveira                | renato.nogueira.oliveira@vale.com   |
| Reynaldo Junior                         | reynaldo.junior@vale.com            |
| Rhomer Mello                            | rhomer.mello@vale.com               |
| Rodrigo Pantoja                         | Rodrigo.Pantoja@vale.com            |
| Rogeria Colen                           | rogeria.colen@vale.com              |
| Ronan Santos                            | Ronan.Santos5@vale.com              |
| Rudson Chaves de Souza                  | rudson.souza@vale.com               |
| Saud Alhabsi                            | saud.alhabsi@vale.com               |
| Srebovt, Ana Maria                      | A.Srebovt@pilz.ie                   |
| Stephen Lawson                          | Stephen.Lawson@vale.com             |
| Suryanto Slamet                         | Suryanto.Slamet@vale.com            |

|                                   |                             |
|-----------------------------------|-----------------------------|
| Talal Rushdi                      | talal.rushdi@vale.com       |
| Tejvinderjit Singh Gill Git Singh | tejvinderjit.singh@vale.com |
| THAIS ARYADNE NASCIMENTO ALVES    | thais.alves@vale.com        |
| Thomas Fontes                     | Thomas.Fontes@vale.com      |
| Tinelli, Denise                   | D.Tinelli@pilz.com.br       |
| Vaz, Joao                         | J.Vaz@pilz.ca               |
| Vinicios Marcelino                | Vinicios.Marcelino@vale.com |
| Vinycios Barbosa                  | vinycios.barbosa@vale.com   |
| Wagner Martins                    | wagner.martins@vale.com     |
| Waldemir Sousa                    | waldemir.sousa@vale.com     |
| Wellington Santana                | wellington.santana@vale.com |
| Zelica Alves                      | zelica.alves@vale.com       |

## 9 REVISION HISTORY

| Revision Number | Date       | Reviewed by   | Description |
|-----------------|------------|---------------|-------------|
| 00              | 19/11/2021 | Rudson Chaves | Emission    |
|                 |            |               |             |

## 10 ANNEXS

### 10.1 Annex A - Differences among Countries/Areas

#### a) Brazil – NR12

There is a national law in Brazil that stipulates minimum safety requirements for machines and (machine) equipment:

- Norma Regulamentadora 12 (NR-12) – SEGURANÇA DE MÁQUINAS E EQUIPAMENTO

The European declaration of conformity or other international certifications as north America as confirmation of the implemented safety requirements in accordance with NR-12, is currently not required from the operator or the manufacturer. Machinery built in accordance with current European directives and harmonized standards with CE conformity e North America standards generally have excellent preconditions for problem-free commissioning in Brazil.

NR12 is applied to all types of machines, new or used, with some specific exceptions: machines for export, machines moved by human or animal force, machines without productive purposes exposed as antiques, household appliances, portable tools and machines certified by INMETRO.

Compliance must take into account all other NRs, official national technical standards in force or applicable international standards and in the absence of these European standards type “C”.

Except for Brazil, there are currently no product-specific safety requirements for plant and machinery that are concrete and applicable for South American countries

#### b) North America (United States and Canada)

In the USA and Canada, CE mark and CE declaration of conformity have no legal acceptance. An export solely based on CE conformity is illegal and to be categorized as very critical regarding product liability. In general, plant and machinery cannot be commissioned in the USA or Canada without approval by special officials from the states, counties or municipalities, the so-called Authorities Having Jurisdiction (AHJ) in USA or Safety Authority Officers (SAO) in Canada.

The Occupational Safety and Health Administration (OSHA), a sub-agency of the US Department of Labor, is responsible for defining and monitoring basic health and safety measures in the USA. They specify minimum requirements in the OSHA standards; these can be found in the Code of Federal Regulations (CFR) under 29 CFR 1910.

The Canadian Center for Occupational Health and Safety (CCOHS) is responsible for defining and monitoring basic health and safety measures in Canada just like OSHA in USA.

With regard to machine safety in the USA and Canada, the general position can be taken that a consistent implementation of safety requirements based on international standards provides a significant basis for satisfying the safety requirements that apply in the USA and Canada but that difference of national standards (e.g NFPA, ANSI) still need to be applied.

## c) Europe – CE marking

The common regulation among Europe about machinery safety is CE marking of machinery. The CE mark stands for “Communauté Européenne”. A manufacturer uses this mark to document compliance to all the European internal market directives that are relevant to the product. Products that carry the CE mark may be imported and sold without considering national regulations. EU formulates general safety objectives via the directives which deal with specific issues. Where a product falls under the scope of several directives which provide for CE marking, the marking indicates that the product is assumed to conform with the provisions of all these directives. The directives only come into effect through the agreements of individual countries within the EU, who incorporate these directives into their domestic law. In each EU country, a law or regulation refers to the relevant EU directive and thus elevates it to the status of domestic law.

The safety objectives that are needed to be specified more precisely; the actual provision is made via standards. The standards have no direct legal relevance on their own until they are published in the Official Journal of the EU or are referenced in domestic laws and regulations. These are the publications by which a standard can acquire “presumption of conformity”. Presumption of conformity means that a manufacturer can assume meeting the requirements of the corresponding directive that are covered by the standard provided he/she has complied with the specifications in the standard.

Where the manufacturer applies a harmonized, published in Official EU Journal, standard, if there is any doubt, misconduct will need to be proven. Where the manufacturer has not applied a harmonized standard, he will need to prove that he has acted in compliance with the directives. Such a route is usually more complex but, in an innovative industry in particular, it is often unavoidable.

The highly comprehensive system for the EU directives established in Europe with the corresponding harmonized standards in combination with the CE conformity assessment procedure and CE marking procedure for safety components and machinery, is typically providing a very good base of safety but is not automatically accepted around the world but other legally binding laws, directives and standards apply.

## d) Russia - TR

In Russian Federation a decree stipulates basic minimum requirements for safety for machines and equipment as well as a mandatory conformity assessment procedure combined with a certification procedure:

- N 753 Decree of the Government of the Russian Federation – Technical Regulation (TR) on safety of machines and equipment

The basis is a contractual harmonization process between the EU and the Russian Federation to align the different safety-related regulation and conformity assessment procedures for machinery in the Russian Federation. The decree includes two annexes, one a list of the machines requiring certification and one with machines for which a Russian declaration of conformity is sufficient. With an obligation for certification, the machine must be checked by a locally accredited test laboratory and a TR certificate must be issued. The procedure is comparable to a type examination in accordance with the Machinery Directive. If a declaration

of conformity is sufficient, this must still be additionally checked, approved, and registered by a nationally accredited certification body.

The TR for machinery is valid in all countries in the customs union and the relevant Russian GOST standards are recognized as the basis for conformity. The EAC (EurAsian Conformity) is an independent Eurasian conformity mark that exists as an externally visible mark:

## **e) Japan**

The Japanese Industrial Safety and Health Law places demands on design issues relating to certain machinery (cranes, lifts etc.). The law also states that the machine operator is responsible for carrying out risk analyses and ensure safety in the workplace. The law also contains requirements for pressure vessels, packaging machines for the food industry and mobile machines. There are currently no concrete obligations for acceptance or approval for plant and machinery.

## **f) China - CCC**

In China the State Administration of Work Safety is responsible for defining and monitoring health and safety measures. Monitoring is guaranteed by local health and safety inspectors. Chinese machine safety standards are used for plant and machinery. China has its own Chinese certification system – Chinese Compulsory Certificate (CCC). The CCC mark is used to mark certified products is defined products categories. Plant and machinery are not subject to this.

## **g) South Korea - KCs**

In South Korea, the Korea Occupational Safety & Health Agency (KOSHA) is the governmental agency responsible for developing, implementing, and monitoring health and safety measures. The Korean Occupational Safety & Health Act forms the basis for KOSHA's work. An important element of the monitoring performed by KOSHA is the approval procedure for various safety components, machines, and plants. On plant and machinery, the KCs mark (Korean Certification Safety Mark) and documented by means of a certificate is mandatory. The nationally accredited testing institutes are responsible for the certification. There are two different certification or approval procedures that are to be requested by the machine and plant manufacturer as the importer before export; these must be performed with a positive test result, mandatory certification for hazardous machinery and self-certification by the machine manufacturer.

## **h) Australia and New Zealand**

In Australia, the national office Safe Work Australia is responsible for developing and defining the legal framework conditions and for monitoring. The national law Work Health and Safety Act (WHS) forms the basis for health and safety. Only the states Victoria and West Australia have developed and implemented their own health and safety requirements as Occupational Health and Safety Acts. The defined health and safety measures are generally legally binding and must therefore be observed. The monitoring is performed by inspectors in the respective states and territories.

The Health and Safety Work Act (HSW) has applied in New Zealand for necessary health and safety measures to be implemented. The national office WorkSafe New Zealand is responsible for developing and defining the legal framework conditions and for monitoring. The defined



health and safety measures are generally legally binding and must therefore be observed. The monitoring is also performed by local inspectors in New Zealand.

The manufacturer/supplier shall ensure that machinery meets the specifications in this standard and all local regulations of the country where the machinery will be used.

## 10.2 Annex B – Determination of PLr according to ISO 13849-1

For each safety function a required performance level (PLr) shall be determined. This determination shall be based on the risk assessment or can be given to applicable machine standards. The method below is taken from EN ISO 13849-1 standard.

There are 3 parameters for determining PLr value:

- Severity of injury (S);
- Frequency and/or exposure times to hazard (F);
- Possibility of avoiding the hazardous event (P).

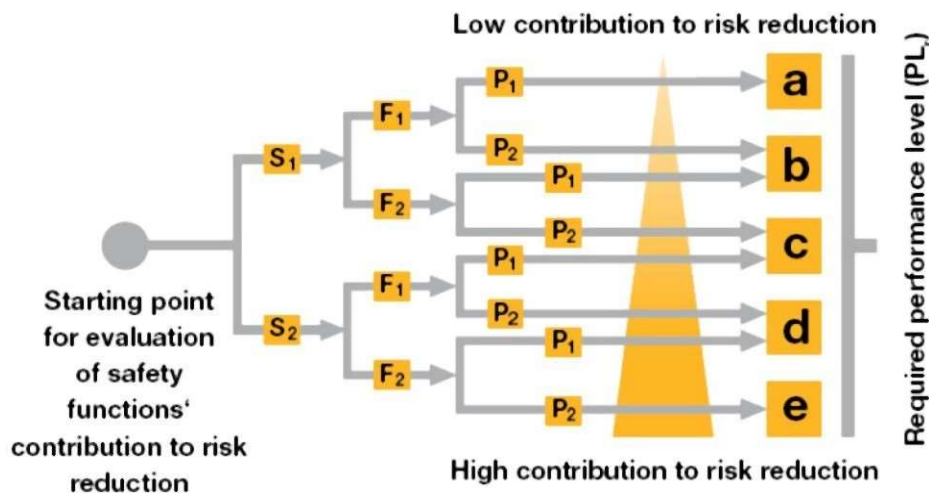


Figure 31 – Determination of PLr process

- S1: Low Severity – Slight/Reversible injury;
- S2: High Severity – Serious/Irreversible injury or death;
- F1: Low frequency – Seldom to less often and/or exposure time is short (Lower than once per 15 minutes or lower than 1/20 of overall operating time);
- F2: High frequency – Frequent to continuous and/or exposure time is long (Higher than once per 15 minutes or higher than 1/20 of overall operating time);
- P1: Possible under specific conditions (visibility is high, and movement is slow, etc.);
- P2: Scarcely possible (High speed movements, etc.).

According to the answers, specified above, given for the hazardous event, the path from Figure 31 should be followed to determine the PLr value of the specific safety function.

## 10.3 Annex C – Definition of Safety Category

### a) Category B

SRP/CSs and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards and using basic safety principles so that they can withstand the expected influence.

Lowest level of safety categories. There is no DC and MTTFD is low to medium. CCF is not relevant.

The maximum achievable PL with Category B is  $PL = b$ .

The occurrence of a fault can lead to the loss of the safety function.

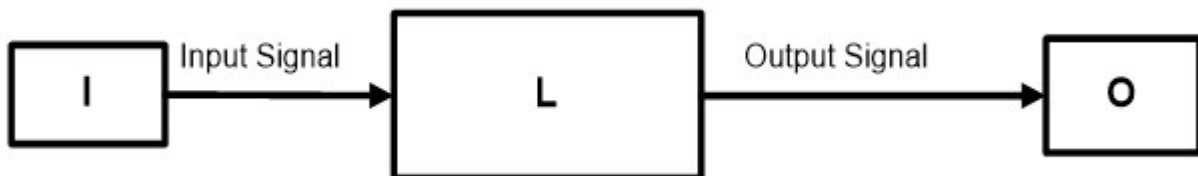


Figure 32 – Category B and Category 1 Architecture

I = Input (Sensor or input Signal)

L = Logic or Safety Circuit

O = Output or actuator

### b) Category 1

Requirements of Category B shall apply. Additionally, well-tried components and well-tried safety principles shall be used.

There is no DC and MTTFD is high. CCF is not relevant.

The maximum achievable PL with Category B is  $PL = c$ .

The occurrence of a fault can lead to the loss of the safety function, but the probability of occurrence is lower than Category B

### c) Category 2

Requirements of Category B and well-tried safety principles shall be applied. Safety function shall be checked at suitable intervals by machine control system.

The DC of the functional channel shall be at least low. MTTFD of each channel can be low to high. Measures against CCF shall be applied.

If test equipment output (OTE) can initiate a safe state until fault is cleared PL = d can be achieved. Otherwise (warning only) maximum achievable PL is PL=c.

The occurrence of a fault can lead to the loss of safety function between the checks. The loss of safety function is detected by the check.

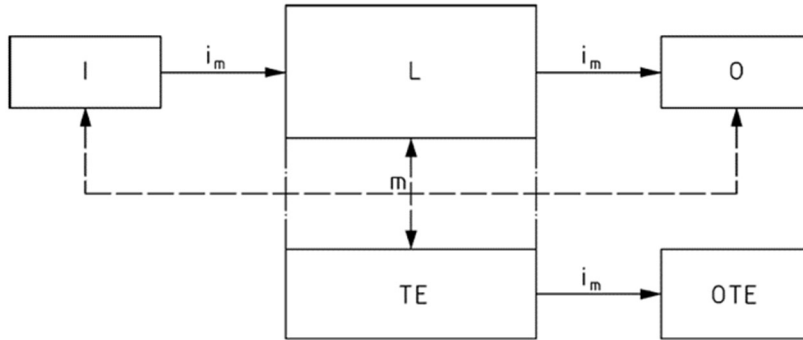


Figure 33 – Category 2 Architecture

|                                    |  |                  |
|------------------------------------|--|------------------|
| I = Input (Sensor or input Signal) | TE: Test Equipment                     | im = Connections |
| L= Logic or Safety Circuit         | OTE: Output of TE (output or actuator) | m = Monitoring   |
| O = Output or actuator             |  |                  |

### d) Category 3

Requirements of Category B and well-tried safety principles shall be applied. Safety function shall be designed so that:

- A single fault in any of these parts does not lead to the loss of the safety function; and
- Whenever reasonably practicable the single fault is detected.

The DC of the functional channels shall be at least low. MTTFD of each channel can be low to high. Measures against CCF shall be applied.

For the presence of a single fault, the safety function can be preserved. Detection of some but not all faults is possible. Accumulation of undetected faults can lead to the loss of safety function.

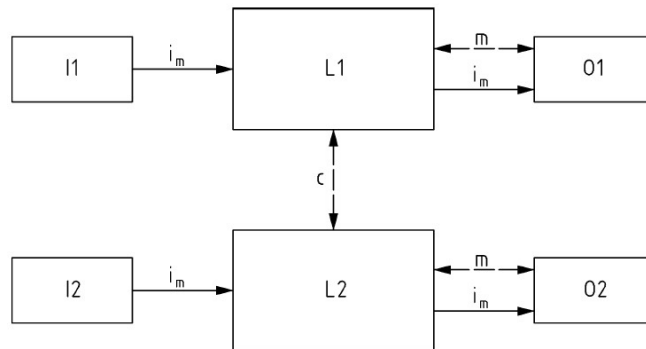


Figure 34 – Category 3 Architecture

I = Input

$i_m$  = Connections

L = Logic or Safety Circuit

m = Monitoring

O = Output or actuator

c = Cross monitoring

## e) Category 4

Requirements of Category B and well-tried safety principles shall be applied. Safety function shall be designed so that:

- A single fault in any of these parts does not lead to the loss of the safety function; and
- The single fault is detected at or before the next demand upon the safety function; an accumulation of faults shall not lead to the loss of the safety function.

The DC of the functional channel and MTTFD of each channel shall be high. Measures against CCF shall be applied.

For the presence of a single fault, the safety function is preserved. Detection of faults in time to prevent the loss of the safety function is present. Accumulation of undetected faults is taken into account.

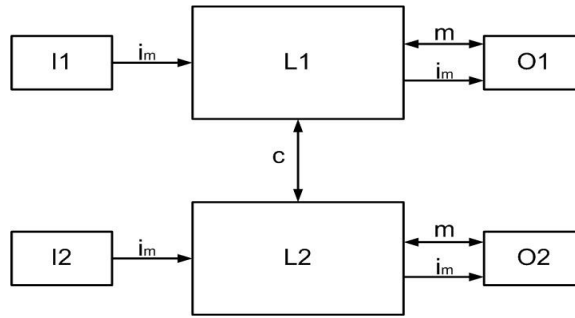


Figure 35 – - Category 4 Architecture

I = Input

L= Logic or Safety Circuit

O = Output or actuator

im = Connections

m = Monitoring

c = Cross monitoring

### 10.4 Annex D – Warning Pictograms

A selected list of warning pictograms can be found in this section:



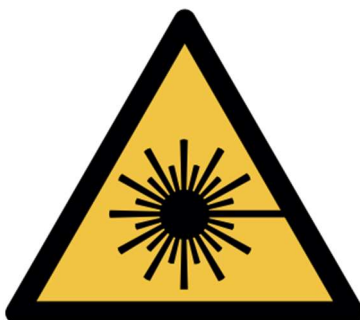
General Warning Sign



Explosive Material



Radioactive material or ionizing radiation



Laser Beam



Non-ionizing radiation



Magnetic Material



*Floor-level Obstacle*



*Drop (Fall)*



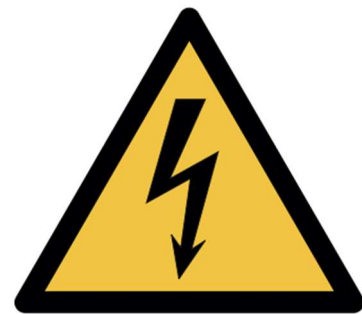
*Biological Hazard*



*Low temperature / Freezing Conditions*



*Slippery Surface*



*Electricity*



*Forklift and other industrial vehicles*



*Overhead Load*



*Toxic Material*



*Hot Surface*



*Automatic Start-up*



*Crushing*



*Overhead obstacle*



*Flammable Material*



*Sharp Element*



*Corrosive substance*



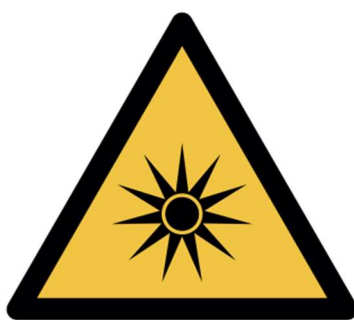
*Crushing of Hands*



*Counterrotating rollers*



*Battery Charging*



*Optical Radiation*



*Oxidizing Element*



*Pressurized Cylinder*



*Hand Crushing between press  
brake tool*



*Hand Crushing between press  
brake and material*



*Rapid movement on workpiece  
in press brake*



*Falling Object*



*Run over by remote operator-  
controlled machine*



*Sudden Loud Noise*



*Asphyxiating atmosphere*



*Arc-flash*

Figure 36 – Pictogram Examples