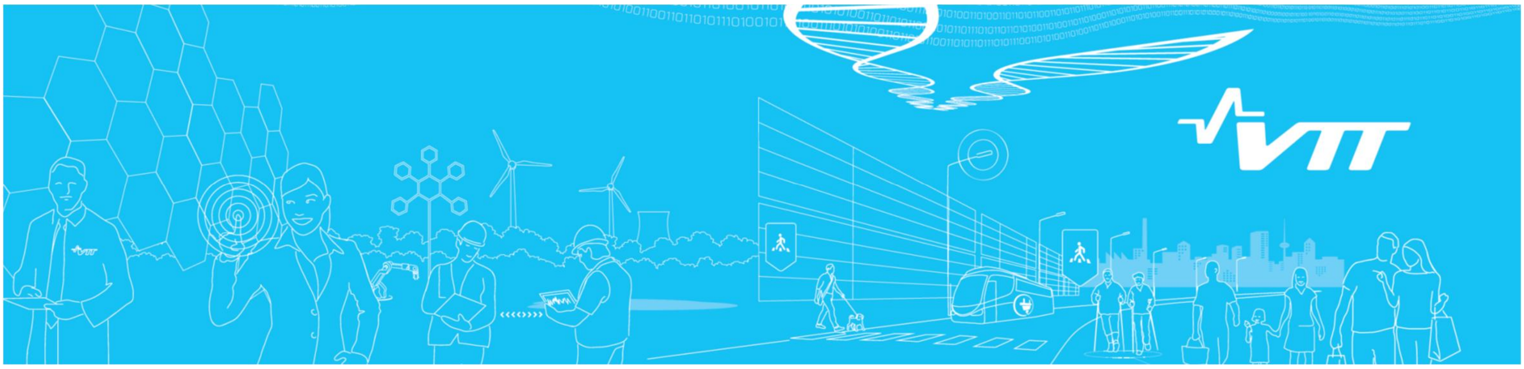
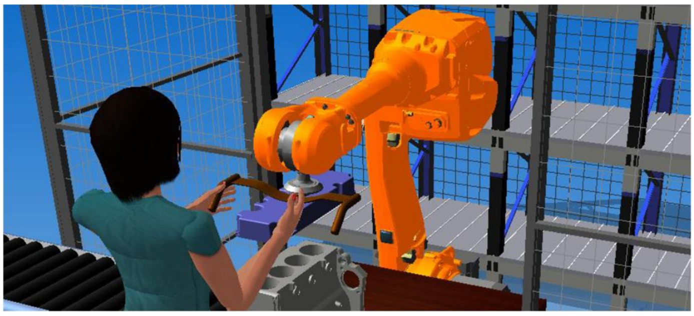


RESEARCH REPORT

VTT-R-01109-17



Guidelines to make safe industrial robot systems

Authors: Timo Malm

Confidentiality: Public

Report's title

Guidelines to make safe industrial robot systems

Customer, contact person, address Tekes – the Finnish Funding Agency for Innovation Matti Evola P.O.Box 69 FI-00101 Helsinki	**Order reference** 1996/31/2014
Project name Tuottavuutta Helppokäytöisellä Ihminen-Robotti –yhteistyöllä - Tuohiro	**Project number/Short name** 101442 / TUOHIRO
Author(s) Timo Malm	**Pages** 30/
Keywords Safety, industrial robot, requirements	**Report identification code** VTT-R-01109-17

Summary

Several requirements are related to the safety of industrial robots. This report points out typical safety challenges and shows sources to find safety requirements. The implementation of a robot cell contains several processes, which are realised concurrently: documentation and requirement process according to Machinery Directive, robot design and risk assessment process according to robot standards (ISO 10218-1 and ISO 10218-2) and design standard (ISO 12100) and functional safety process according to functional safety standard(s) (ISO 13849-1). Depending on the application, also requirements related to, for example, radiation, dust or other machines may be needed.

It is often not safe enough solution to stop a full speed moving industrial robot, because it has long stopping distance and it may have loose objects at its tool. To have practical safety distances in robot cells, the robot speed must be reduced before the robot is stopped. Monitored stop allows quick restart, but to ensure safety, the stand still need to be monitored adequately. Emergency stop is needed in emergency and failure situations. It cuts the servo power and therefore restarting takes some time and it is not feasible in continuous human – robot collaboration.

Confidentiality	Public

Tampere 1.3.2017

Written by	**Reviewed by**	**Accepted by**
Timo Malm, Senior Scientist	Ilari Marstio Senior Scientist	Risto Kuivanen Business Development Manager

VTT's contact address

Teknologian tutkimuskeskus VTT Oy, PL 1000, 02044 VTT

Distribution (customer and VTT)

Tuohiro project participants

The use of the name of VTT Technical Research Centre of Finland Ltd in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.

Preface

This project report is made during 2016 and 2017 in Tuohiro project (Tuottavuutta Helppokäytöisellä Ihminen-Robotti –yhteistyöllä). Tekes (Finnish Funding Agency for Technology and Innovation), VTT and companies have financed the project. The steering group of the project is Janne Leinonen (ABB), Jyrki Anttonen (Cimcorp), Timo Yli-Opas (Konepaja Stamac), Teemu Ritala (MSK Plast), Kari Sivula (Robit Rocktools), Matti Evola (Tekes), Esa Reponen (Työstöhankinta Reponen), Mika Marttila (Valmet Automotive) and Riikka Virkkunen (VTT). The VTT project team is Ilari Marstio, Timo Salmi, Jari Montonen, Iina Aaltonen, Timo Kuula, Pekka Isto, Mervi Hirvonen, Janne Häkli and Timo Malm.

Tampere 1.3.2017

Timo Malm

List of definitions and acronyms

Machine: An assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application. (Machinery Directive 2006/42/EC)

Partly completed machine: Partly completed machinery' means an assembly which is almost machinery but which cannot in itself perform a specific application. A drive system is partly completed machinery. Partly completed machinery is only intended to be incorporated into or assembled with other machinery or other partly completed machinery or equipment, thereby forming machinery to which this Directive applies. (Machinery Directive 2006/42/EC)

Safety component means a component:
− which serves to fulfil a safety function,
− which is independently placed on the market,
− the failure and/or malfunction of which endangers the safety of persons, and
− which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function. [Machinery Directive 2006/42/EC]

Component: There are no specific declarations in machinery directive. The machine manufacturer takes the responsibility of the complete machine, which include all the components. The machine manufacturer must make own judgement in selecting good components.

Industrial robot: automatically controlled, reprogrammable multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications. The industrial robot includes: the manipulator, including actuators (any integrated additional axes), the controller, including teach pendant and any communication interface (hardware and software). The following devices are considered industrial robots for the purpose of the standard: hand guided robots, the manipulating portions of mobile robots and collaborating robots. (ISO 10218-1)

Integrated manufacturing system (IMS): group of machines working together in a coordinated manner, linked by a material-handling system, interconnected by controls (i.e. IMS controls), for the purpose of manufacturing, treatment, movement or packaging of discrete parts or assemblies [ISO 11161].

Collaborative robot: robot designed for direct interaction with a human within a defined collaborative workspace i.e. workspace within the safeguarded space where the robot and a human can perform tasks simultaneously during production operation. (ISO 10218-2)

Collaborative operation: state in which purposely designed robots work in direct cooperation with a human within a defined. [ISO 10218-1]

Operational space: portion of the restricted space (3.13.2) that is actually used while performing all motions commanded by the task programme. (ISO 10218-2)

Restricted space: portion of the maximum space restricted by limiting devices that establish limits which will not be exceeded. It is also within the safeguarded space. It should match the operating space as close as is reasonably practicable. (ISO 10218-2)

Safeguarded space: space defined by the perimeter safeguarding. (ISO 10218-2)

Interlocking device, interlock: mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions (generally as long as a guard is not closed). [ISO 12100]

Enabling device: additional manually operated device used in conjunction with a start control and which, when continuously actuated, allows a machine to function. [ISO 12100]

Hold-to-run control device: control device which initiates and maintains machine functions only as long as the manual control (actuator) is actuated. [ISO 12100]

Two-hand control device: control device which requires at least simultaneous actuation by both hands in order to initiate and to maintain hazardous machine functions, thus providing a protective measure only for the person who actuates it. [ISO 12100]

Emergency stop, emergency stop function: function which is intended to
— avert arising or reduce existing hazards to persons, damage to machinery or to work in progress, and
— be initiated by a single human action. [ISO 12100]

Sensitive protective equipment, SPE: equipment for detecting persons or parts of persons which generates an appropriate signal to the control system to reduce risk to the persons detected. [ISO 12100]

Protective measure: measure intended to achieve risk reduction, implemented
— by the designer (inherently safe design, safeguarding and complementary protective measures, information for use) and/or
— by the user (organization: safe working procedures, supervision, permit-to-work systems; provision and use of additional safeguards; use of personal protective equipment; training) [ISO 12100]

Guard: physical barrier, designed as part of the machine to provide protection. [ISO 12100]

Safety-rated: characterized by having a prescribed safety function with a specified safety-related performance. [ISO 10218-1]

Protective device: safeguard other than a guard. [ISO 12100]

Harm: physical injury or damage to health. [ISO 12100]

Hazard: potential source of harm. [ISO 12100]

Risk: combination of the probability of occurrence of harm and the severity of that harm. [ISO 12100]

Risk estimation: defining likely severity of harm and probability of its occurrence. [ISO 12100]

Risk analysis: combination of the specification of the limits of the machine, hazard identification and risk estimation. [ISO 12100]

Risk evaluation: judgment, on the basis of risk analysis, of whether the risk reduction objectives have been achieved. [ISO 12100]

Risk assessment: overall process comprising a risk analysis and a risk evaluation. [ISO 12100]

Fault: state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. [ISO 12100]

Failure: termination of the ability of an item to perform a required function [ISO 12100]. Note: After failure the item has a fault. A fault is often the result of a failure of the item itself, but may exist without prior failure. “Failure” is an event, as distinguished from “fault”, which is a state. This concept, as defined, does not apply to items consisting of software only. In practice the terms “failure” and “fault” are often used synonymously. [IEC 61496-1]

Inherently safe design measure: protective measure which either eliminates hazards or reduces the risks associated with hazards by changing the design or operating characteristics of the machine without the use of guards or protective devices. [ISO 12100]

Safeguarding: protective measure using safeguards to protect persons from the hazards which cannot reasonably be eliminated or risks which cannot be sufficiently reduced by inherently safe design measures. [ISO 12100]

Information for use: protective measure consisting of communication links (for example, text, words, signs, signals, symbols, diagrams) used separately or in combination, to convey information to the user. [ISO 12100]

Contents

1. Introduction

This report describes the safety requirements of industrial robots, and how to fulfil the requirements. Machinery Directive (2006/42/EC) and the most relevant standards are described. The most common requirements of the robot standards are described using figures together with text. All risks should be considered by applying risk assessment and furthermore for the critical risks by determining the associated requirements and the related safety measures as described in this report.

Functional safety is related to control systems and safety devices. Each safety function should be defined and classified according to the risk and relation to the control system. The classification units are PLs (Performance Levels from “a” to “e”) or SILs (Safety Integrity Levels from “1” to “4”). Each PL and SIL are associated to risks and safety requirements related to the safety functions of the control system or safety device. The higher risk, the more demanding requirements are related to the safety function.

International safety requirements for industrial robots were published already 1992 (EN 775), which means that there is already a long tradition for safety requirements of the robots. Basically, the operator stays outside of the safeguarded area during automatic run, but during teaching, the operator may be beside a slow moving robot (< 250 mm/s) when hold to run control is applied. Many new safety functions and devices have been defined in current robot safety standards ISO 10218-1:2011 and ISO 10218-2:2011. This gives more possibilities for robot system integrators to design safe and productive robot cells. On the other hand, there are more challenges to optimize productivity.

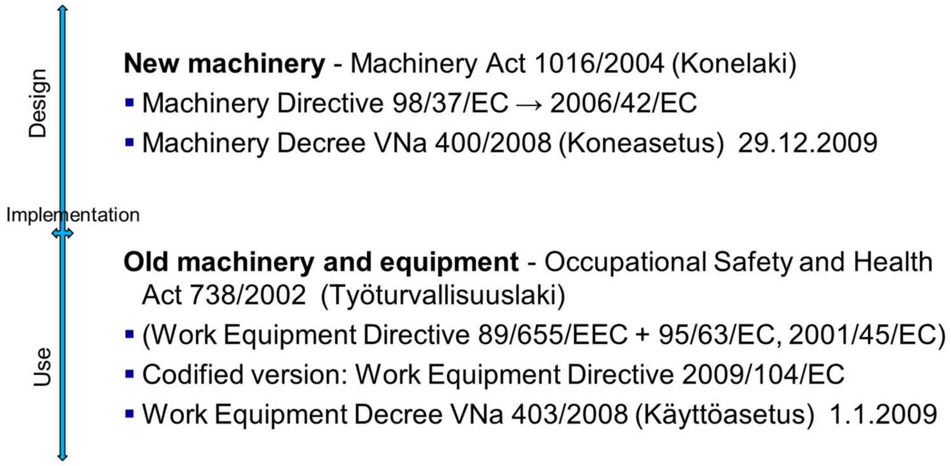
The new topic in robotic safety is “collaborative robots”. The first edition of “ISO/TS 15066 Robots and robotic devices — Collaborative robots” was published at February 2016 [ISO/TS 15066:2016]. Before it the role of collaborative robots was already defined in standard ISO 10218-1. The standards define specific collaborative cases and rules how to work safely together with robots.

Thirty years ago a typical maximum speed for a robot was 3 m/s and stopping distance was 40 cm for emergency stop (Cat 0, servo power off) and 90 cm for production stop (Cat 2, servo power on) [Malm 1986]. Currently typical maximum speed for a robot is 5 m/s and also capacity and outreach are higher and then stopping distance can be 2 m (Cat 2). So, the current development may sound bad from the safety point of view. However, speed is essential, when calculating stopping distances and therefore the development has not been towards unsafe systems, but towards systems that are more versatile. For example, ABB IRB 4600, with 21.8 kg load and speed (TCP) 2500mm/s has stopping distance 65 cm (Cat 2) and when applying emergency stop 38 cm (Cat 0). The stopping distance drops dramatically as the speed is slower. Therefore, speed control is an important feature in robot safety systems.

2. Requirements

2.1 Machinery Directive

In Finland Machinery Act gives the basis to machinery legislation. Similarly, Occupational Safety and Health Act gives the basis for machines and devices at work. All design before implementation is related to Machinery Act and all measures after implementation are related to the Occupational Safety and Health Act. The actual requirements are presented at Machinery Decree (requirements from Machinery Directive 2006/42/EC) and Work Equipment Decree (requirements from Work Equipment Directive). The relation is described at Figure 1.



New machinery - Machinery Act 1016/2004 (Konelaki)

- Machinery Directive 98/37/EC → 2006/42/EC
- Machinery Decree VNa 400/2008 (Koneasetus) 29.12.2009

Old machinery and equipment - Occupational Safety and Health Act 738/2002 (Työturvallisuuslaki)

- (Work Equipment Directive 89/655/EEC + 95/63/EC, 2001/45/EC)
- Codified version: Work Equipment Directive 2009/104/EC
- Work Equipment Decree VNa 403/2008 (Käyttöasetus) 1.1.2009

Figure 1. Legislation of machinery in Finland.

Basically, the regulations related to safety of industrial robots origin from Machinery Directive 2006/42/EC annex I (Essential health and safety requirements relating to the design and construction of machinery). These are binding regulations, which must be obeyed. EU has published guidelines how to follow the Directive in “Guide to application of the Machinery Directive 2006/42/EC 2nd Edition June 2010” [Fraser 2010]. Harmonized standards explain the Machinery Directive more detailed and when harmonized standard is followed in the design, one can suppose that the parts associated to the harmonized standard are designed according to the directive. If a non-harmonized standard refers to harmonized standard, then the referred parts of the text can have similar authority. Other standards or guidelines do not give similar conformity to the Machinery Directive although they can give good information to the subject. The relations between requirements are described at Figure 2.

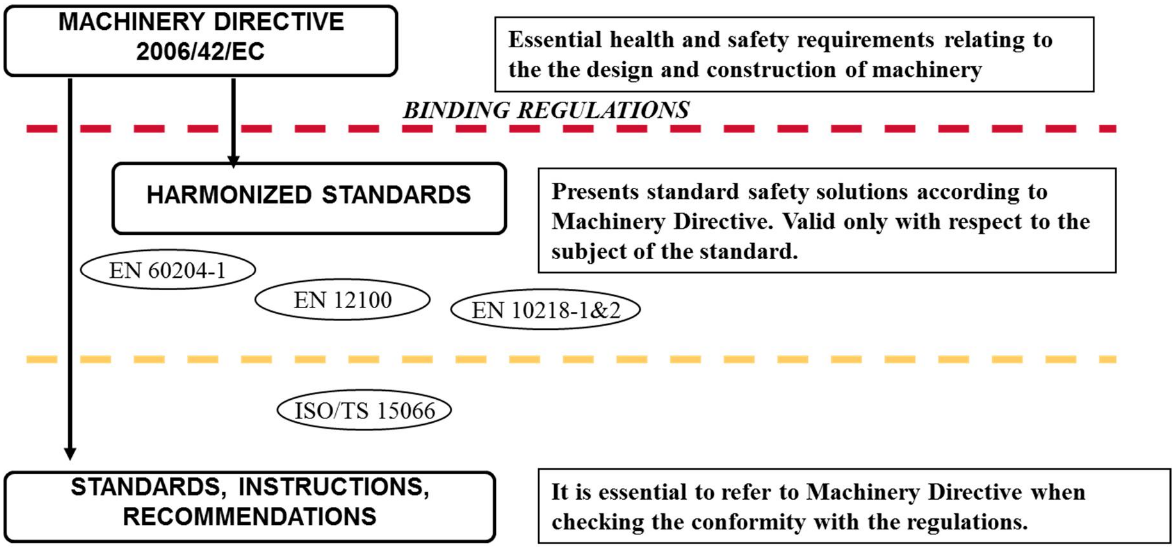

MACHINERY DIRECTIVE 2006/42/EC
Essential health and safety requirements relating to the the design and construction of machinery
BINDING REGULATIONS
HARMONIZED STANDARDS
Presents standard safety solutions according to Machinery Directive. Valid only with respect to the subject of the standard.
EN 60204-1
EN 12100
EN 10218-1&2
ISO/TS 15066
STANDARDS, INSTRUCTIONS, RECOMMENDATIONS
It is essential to refer to Machinery Directive when checking the conformity with the regulations.

Figure 2. Safety requirements for industrial robots.

Machinery Directive describes which requirements must be followed before a machine can be taken into use. One of the first tasks is to define the manufacturer of the robot cell, which takes the main responsibility of the design by signing the Declaration of Conformity. The robot manufacturer is, nowadays, defining the industrial robot as "partly completed machine" and makes the documentation and declaration of incorporation according to Machinery Directive annex II section B. Usually the integrator, who adds all protective devices and other machines and devices, makes the declaration of conformation according to Machinery Directive annex II section A and is therefore the manufacturer of the robot cell. The manufacturer has to make and check that all documentation and required tasks are made. Figure 4 describes the responsibilities related to a machine and to a partly completed machine.

The tasks, which need to be done to make safe machines are described in Machinery Directive:

- Risk assessment (see Figure 10Figure 9, Figure 10 and Figure 14)
- All safety requirements and related directives
- Design the machine according to Machinery Directive annex I (Essential health and safety requirements relating to the design and construction of machinery)
- Write manuals for use and if necessary construction, maintenance, safety
- Compile and maintain technical file (see Annex 2)
- Declaration of Conformation must be drawn up (see Annex 1)
- CE-marking and other markings at the machine (see Figure 3).

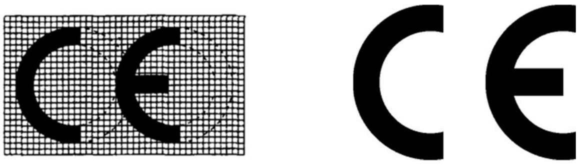


Figure 3. CE-marking. Left figure describes the dimensions of the marking and right figure describes the actual marking [Fraser 2010].

Some of the tasks in the list are made by machine manufacturer and some by the integrator. The complete robot cell or manufacturing system must have CE-marking and Declaration of Conformity.

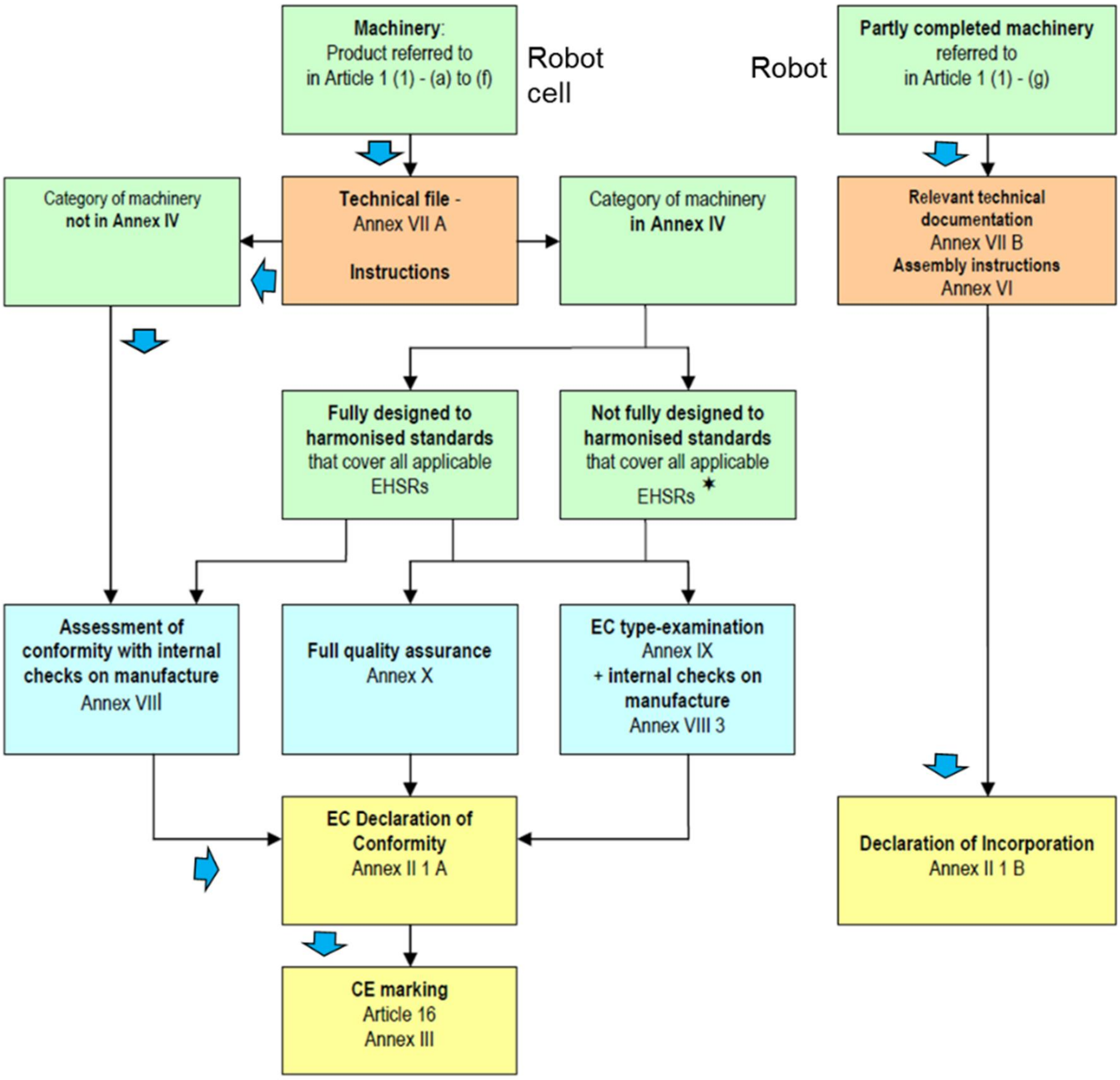

Machinery: Product referred to in Article 1 (1) - (a) to (f)
Robot cell
Robot
Partly completed machinery referred to in Article 1 (1) - (g)
Category of machinery not in Annex IV
Technical file - Annex VII A
Instructions
Category of machinery in Annex IV
Relevant technical documentation Annex VII B
Assembly instructions Annex VI
Fully designed to harmonised standards that cover all applicable EHSRs
Not fully designed to harmonised standards that cover all applicable EHSRs *
Assessment of conformity with internal checks on manufacture Annex VIII
Full quality assurance Annex X
EC type-examination Annex IX + internal checks on manufacture Annex VIII 3
EC Declaration of Conformity Annex II 1 A
Declaration of Incorporation Annex II 1 B
CE marking Article 16 Annex III

Figure 4. Procedure to fulfil requirements of the Machinery Directive [Fraser 2010].

2.2 Safety standards for robots

Design and risk assessment process is described in ISO 12100 standard. It is almost obligatory, since it describes the basic safety principles and risk assessment, which both should be followed. It does not give detailed guidelines for selecting detailed measures for risk reduction. Guidelines selection of safety measures are described in robot standards ISO 10218-1, ISO 10218-2 and IEC/TS 62046. Information how to apply a specific safety device can be found from specific standards. The design process related to control systems and their safety functions is described at section “2.3 Functional safety” and general safety conscious design process at section 3. Figure 5 describes the most common standards, which need to be applied in designing safety features of an industrial robot cell.

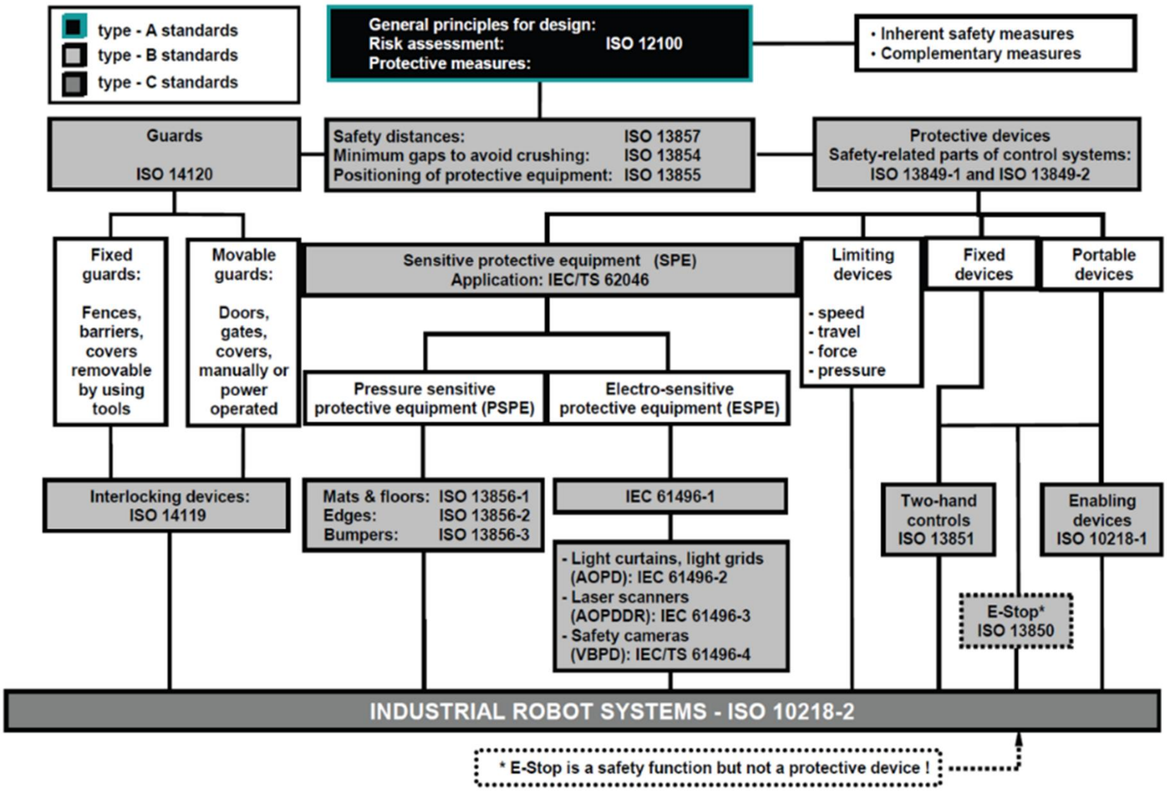

type - A standards
type - B standards
type - C standards
General principles for design:
Risk assessment: ISO 12100
Protective measures:
• Inherent safety measures
• Complementary measures
Guards
ISO 14120
Safety distances: ISO 13857
Minimum gaps to avoid crushing: ISO 13854
Positioning of protective equipment: ISO 13855
Protective devices
Safety-related parts of control systems:
ISO 13849-1 and ISO 13849-2
Fixed guards:
Fences, barriers, covers removable by using tools
Movable guards:
Doors, gates, covers, manually or power operated
Sensitive protective equipment (SPE)
Application: IEC/TS 62046
Limiting devices
- speed
- travel
- force
- pressure
Fixed devices
Portable devices
Pressure sensitive protective equipment (PSPE)
Electro-sensitive protective equipment (ESPE)
Interlocking devices:
ISO 14119
Mats & floors: ISO 13856-1
Edges: ISO 13856-2
Bumpers: ISO 13856-3
IEC 61496-1
- Light curtains, light grids (AOPD): IEC 61496-2
- Laser scanners (AOPDDR): IEC 61496-3
- Safety cameras (VBPD): IEC/TS 61496-4
Two-hand controls
ISO 13851
Enabling devices
ISO 10218-1
E-Stop*
ISO 13850
INDUSTRIAL ROBOT SYSTEMS - ISO 10218-2
* E-Stop is a safety function but not a protective device !

Figure 5. Typical safety devices and standards related to industrial robots. [ISO 10218-2]

2.2.1 ISO 10218-1 and ISO 10218-2

The standards: “Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots (ISO 10218-1:2011)” and “Part 2: Robot systems and integration (ISO 10218-2:2011)” set the basis for industrial robot safety. Part 1 is dedicated to robot manufacturers and part 2 to robot system integrators, but some requirements are mentioned only in one standard and therefore often both standards are needed. All the safety measures, features and requirements should be first searched from the standards and after that from ISO 12100 and then from relevant safety device or feature standards (B-type standards) (cmp. Figure 5).

Table 1. Typical safety topics, when a person is entering the robot safeguarded area. [ISO 10218-2], [ISO 12100]

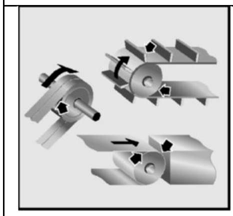
Figure	Situation	Safety measures
	All unnecessary risks at the robot safeguarded area should be minimized.	All rotating parts and nibs must be protected.

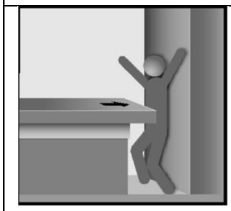
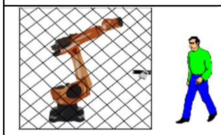
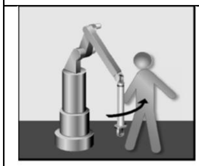
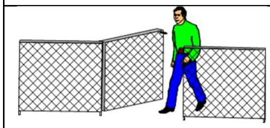
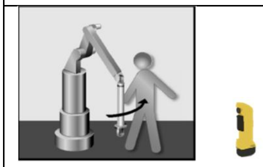
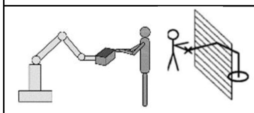
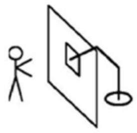
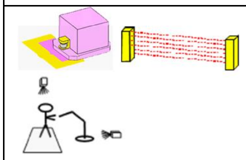
Figure	Situation	Safety measures
	Crushing hazard between moving parts and rigid objects	Adequate clearance between moving parts and rigid objects should be arranged (for human body 500 mm). It is measured from the robot operating space to rigid structures.
	Person is outside robot safeguarded area. Robot is in automated mode.	Robot safeguarded area is protected with adequate means against e.g. radiation, heat, debris or other flying objects.
	Before a person enters the robot safeguarded area a suitable mode of the robot must be selected.	Manual mode, teach mode, collaborative mode, reduced speed mode etc.
 	Manual mode, teach mode, hand-guiding mode.	Reduced speed < 250 mm/s User is applying teach pendant, which has hold-to-run functions and emergency stop.
	Manual high speed mode	This mode is intended to be restricted to program verification only. Manual mode is selected. Hold-to-run functions, high speed selector and enabling device required. Clearance 500 mm between moving and rigid objects (or safety-rated space limiting).
	Person enters the robot safeguarded area. Robot is in automated mode.	Person is detected when he enters the robot safeguarded area. Robot stops (protective stop).
	Robot is in automated mode.	Robot speed is reduced to below 250 mm/s. No specific risks related to e.g. sharp tools. Enabling device is applied.
	Robot is in collaborative mode.	Hand-guiding device, which has emergency stop and enabling device (if not inherently safe solution; limited force). Robot moves only when hand-guiding is applied. When hand-guiding is not applied, the safety-rated monitored stop is on.

Figure	Situation	Safety measures
	Robot is in collaborative mode.	Safety-rated monitored stop. The servo power on and any movement causes emergency stop. Restarting after safety-rated monitored can be automatic if there are no persons at the vicinity of the robot.
	Robot is in collaborative mode.	Power and force limiting by inherent design or control. At the collaborative workspace the robot applies on speeds and forces, which are not harmful to persons (see ISO/TS 15066).
	Robot is in collaborative mode.	Speed and separation monitoring. Sensors detect that robot can stop before human can touch a moving robot and safety system realizes the performance.

Ref: Black and white drawings at the table are from [ISO 10218-2:2011] and [SFS-EN ISO 12100:2010].

The performance of safety-related parts of the control system must be according to PL d of ISO 13849-1. One of the main requirements related to PL d is: when the single fault occurs, the safety function is always performed and a safe state shall be maintained until the detected fault is corrected. Section 2.3 Functional safety describes more detailed about performance levels.

Figure 6 shows safety measures as a person enters the robot workspace. In automated mode the robot should stop. When collaborative mode is selected, the options are safety-rated monitored stop (enables quick restart), speed and separation monitoring (enables safe working beside a slow moving robot), power and force limitation (enables close collaboration with a small robot) or hand-guiding (enables hand-guiding of the robot). The robot can have also manual modes, which enable moving the robot with a pendant.

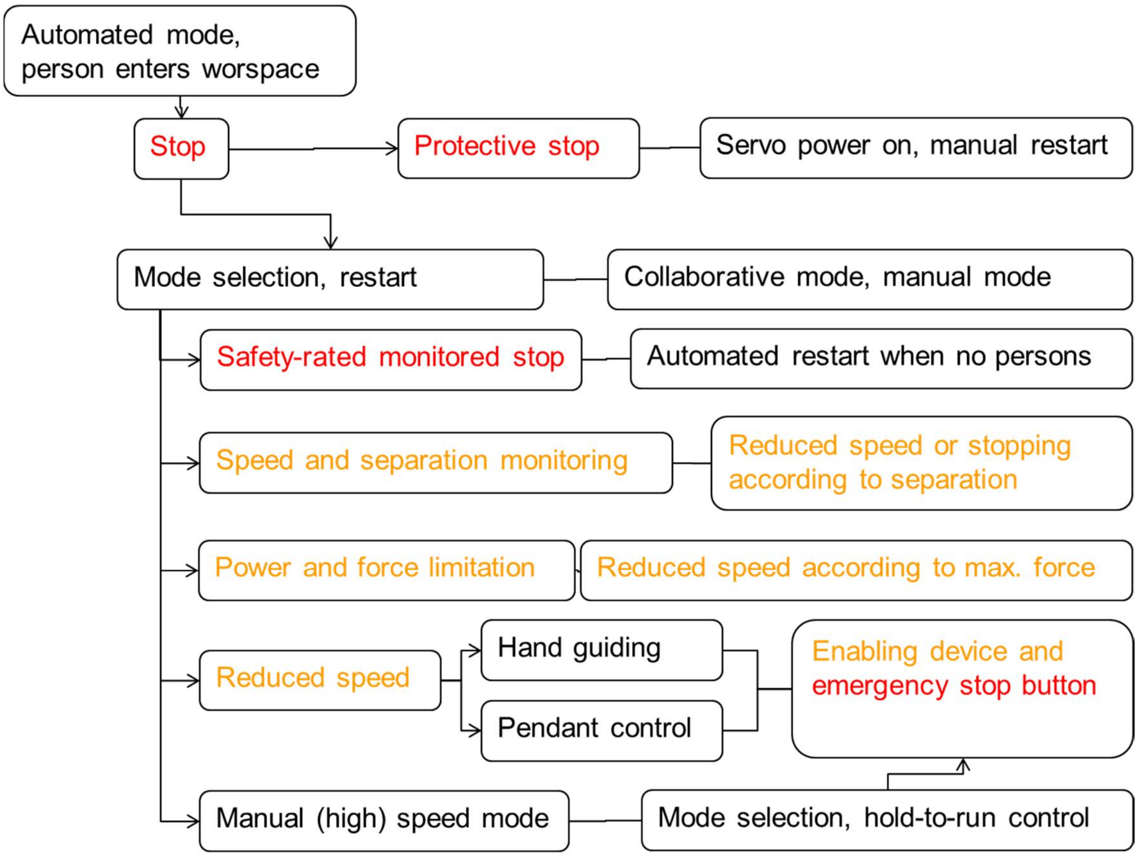

Automated mode, person enters worspace
Stop
Protective stop
Servo power on, manual restart
Mode selection, restart
Collaborative mode, manual mode
Safety-rated monitored stop
Automated restart when no persons
Speed and separation monitoring
Reduced speed or stopping according to separation
Power and force limitation
Reduced speed according to max. force
Reduced speed
Hand guiding
Pendant control
Enabling device and emergency stop button
Manual (high) speed mode
Mode selection, hold-to-run control

Figure 6. Safety measures as a person enters the robot workspace.

2.2.2 Collaborative robots

The modes of human robot collaboration are defined in ISO 10218-1 and ISO/TS 15066 standards. Basically, the idea is that robot does not hurt a person and the means to protect a person are controlled range, force and speed, separation monitoring and safety-rated monitored stopping. In emergency stop servo power is cut off, whereas in collaborative modes the servo power is on. This means that restarting is easier and can be automated if risk assessment allows it. Collaborative modes cannot be realised with any robot with simple safety system, but it requires a specific robot and/or a safety system for separation and robot control. In Table 1 the collaborative modes of a robot system are mentioned at “Situation” column and described in “Safety measures” column.

The standard specification ISO/TS 15066 defines the maxim forces and pressures (biomechanical limits) that may occur in collaborative mode. For example, maximum force against face in 65 N (pressure 110 N/cm^2) and kneecap 220 N. The maximum forces against other body parts are between those two values. This means that the risk assessor must estimate, which parts of the human body can be exposed to the force. The specification gives both maximum force and pressure limits and neither limits may be exceeded. Pressure value exceeds easily when the part touching a person is sharp or small. It is difficult say exactly, which force would be harmful to a person and therefore it is possible that values presented at the standard specification may change in the future. [ISO/TS 15066:2016]

2.3 Functional safety

Functional safety is related to safe performance of actuators when a specified safety function is initiated by safety-related control system. In machinery branch, the harmonized functional safety standards are ISO 13849-1 and IEC 62061. The ISO 13849-1 is related a little bit more to machine builders and IEC 62061 is related more to control system builders, but basically the difference is not big. Both standards refer to IEC 61508 standard family “Functional safety of electrical/electronic/programmable electronic safety-related systems”, which set the basis for functional safety of programmable electronic systems.

Although the functional safety standards have many similar principles, there are also differences. ISO 13849 standards give only basic information about safe software, but there are requirements and examples related to many kind of technologies. IEC 61508 and IEC 62061 are concentrating on programmable systems and electronics. For distributed systems only specific standards (IEC 61784-3) give adequate information how to treat message errors, which are not usually hardware or software specific. Figure 7 shows the basic properties functional safety standards to ease the selection of the standard.

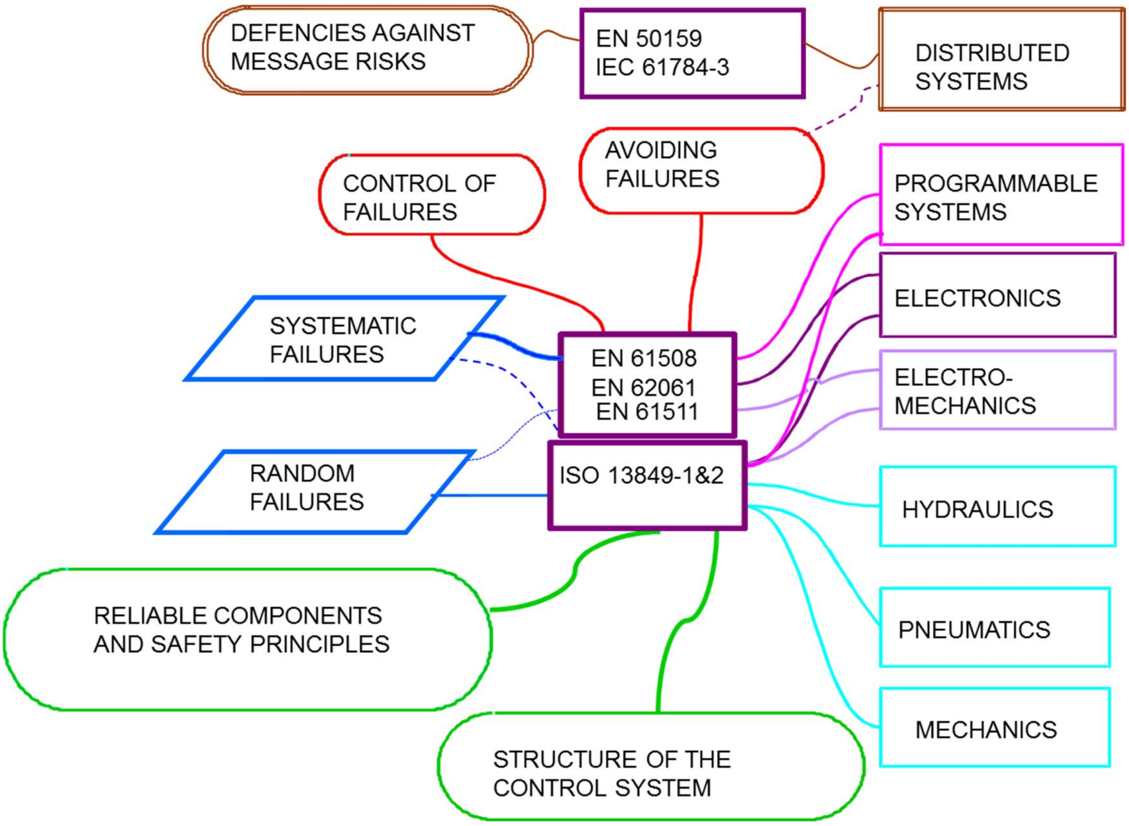


Figure 7. Functional safety standards can be associated to specific safety properties and technologies.

Table 2 shows the equivalence between PL and SIL. PL a is below the described SILs and there is no equivalence. SIL 1 is divided to PL b and PL c, apparently, because in machinery many systems (actually safety functions) are associated to SIL 1 and the cost difference between PL b and PL c systems can be considerable.

Table 2. The relation between PL and SIL.

Performance level (PL)	Probability of dangerous failure per hour [1/h]	Safety integrity level (SIL)
a	$10^{-5} \leq PFH_d < 10^{-4}$	-
b	$3{\cdot}10^{-6} \leq PFH_d < 10^{-5}$	1
c	$10^{-6} \leq PFH_d < 3{\cdot}10^{-6}$	1
d	$10^{-7} \leq PFH_d < 10^{-6}$	2
e	$10^{-8} \leq PFH_d < 10^{-7}$	3

The safe performance design of control systems begins with risk assessment. When the risk is considerable and the control system (including electrical safety/protective devices) is required to maintain safety, then the PL estimation is required. The performance level (PL) of the safety function is associated to the safe operation of machine functions. The PL is defined in standard ISO 13849-1. The required PL can be determined by using machinery standards, risk graphs or comparing the risks to similar systems. High risks related to the safety function mean more specific requirements. Figure 8 shows the process how PL is first defined and then realized and validated. The following list shows the phases of the Figure 8:

1. The risk is found in the risk assessment.
2. Each remarkable risk is considered in safety requirement specification. In safety requirement specification phase the requirements are specified and a risk graph can be used if standards do not give suggestions to PL requirements.
3. The required PL (PL_r) is defined for each safety function
4. The control system is designed according to the safety requirements.
5. The control system and each safety function is validated in order check are the PL requirements fulfilled.

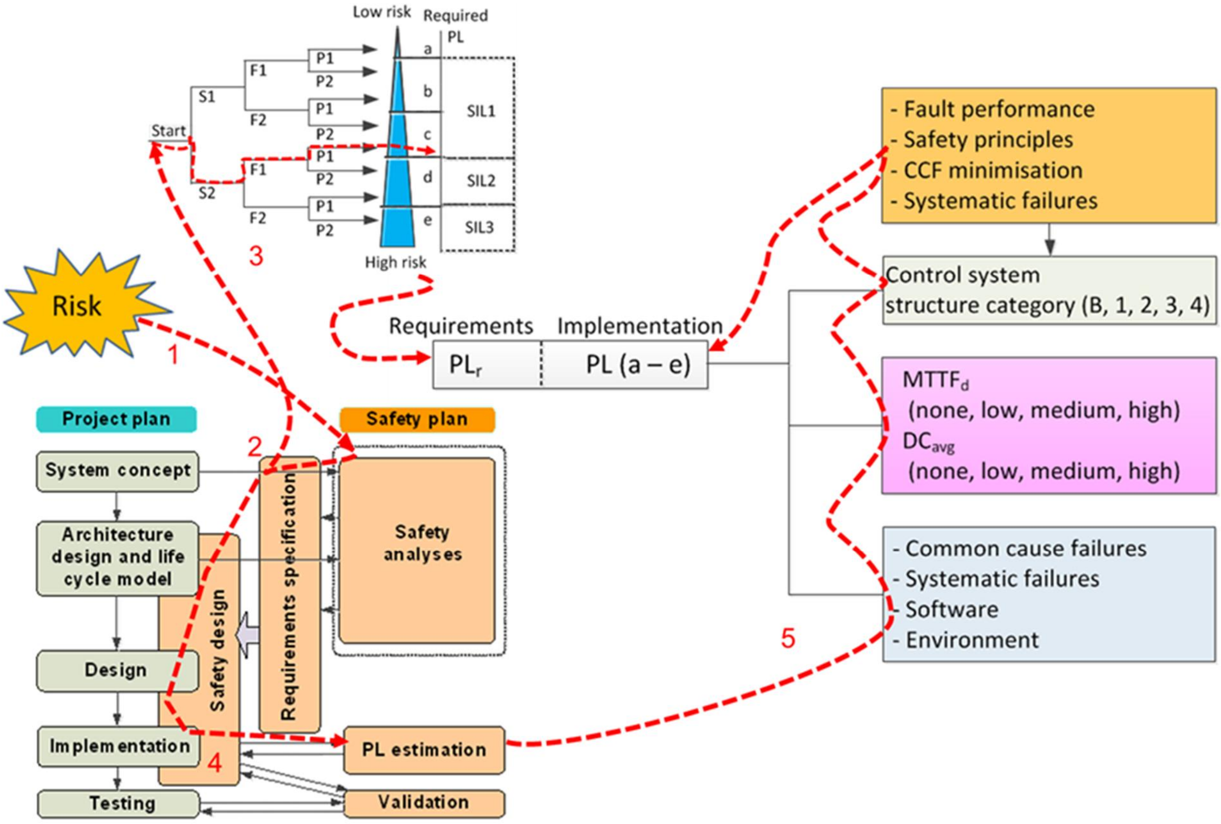
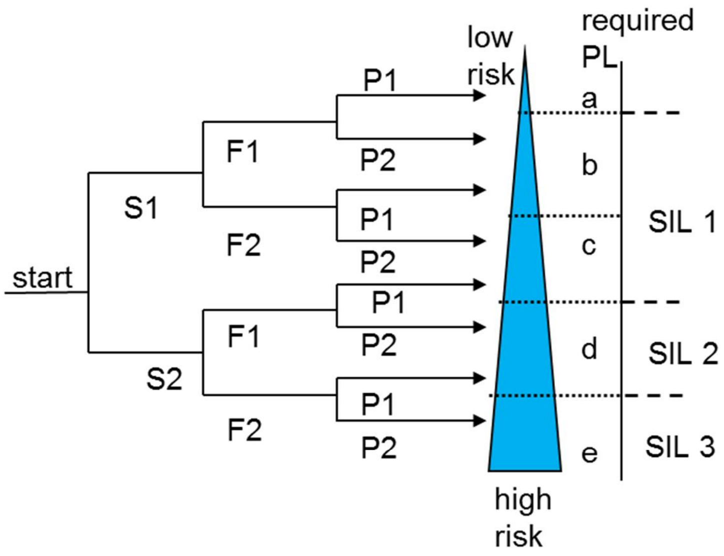


Figure 8. Basic procedure to follow functional safety requirements of the standard ISO 13849-1.

2.3.1 Definition of required PL for a safety function

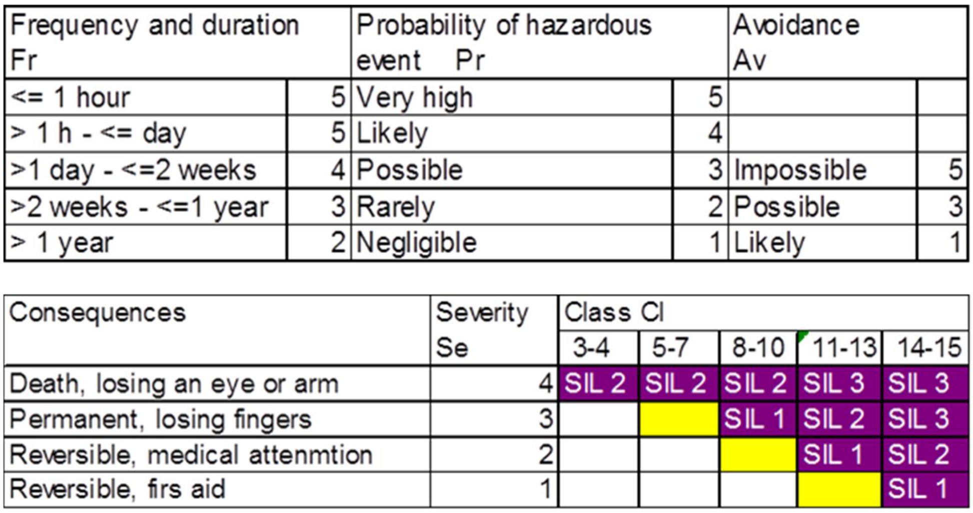
The first phase in estimating PLs is to identify the safety functions and specify required characteristics for each safety function. For each selected safety function, it is necessary to define the required performance level (PL_r). If the PL_r is expressed in C type machinery safety standard, it can be used as a basis for the design. If PL_r is not expressed in C type standard or this standard is not available or PL_r for a safety function is not known, it can be estimated using a risk analysis. If the application has more or less risks in comparison with the application standard, the PL_r can be changed according to the risk analysis. Risk graph method (see Figure 8) is one technique for defining PL_r for a safety function. In the risk graph method, the PL_r is defined by estimating the following parameters: the severity of possible injury, frequency and/or exposure to hazard and the possibility of avoiding hazard or limiting harm. The estimation of these parameters may be challenging. Thus this method can be considered subjective i.e. the result depends on the analyst. To confirm the results it is possible to apply risk matrix method, which is presented in IEC 62061 (see Figure 10). The method has one more parameter, more levels in parameters and the result is expressed as SILs. SIL 1 is not as accurate as PL b and PL c partly because SIL 1 is divided into two PLs and partly because the method does not result as often SIL 1 as the risk graph results PL b or PL c.

After determining PL_r for a safety function component and architecture selections can be designed so that the defined PL_r is fulfilled. Thus it is important to get the right PL_r for a certain safety function applied in a machine control system.



S= severity:
S1slight ;
S2 is serious (normally irreversible injury or death).
F= frequency and/or exposure to hazard:
F1 seldom, exposure time is short;
F2 frequent-to-continuous .
P= possibility of avoiding hazard or limiting harm:
P1 possible under specific conditions;
P2 scarcely possible.

Figure 9. Determination of performance level according to SFS-EN ISO 13849-1.



Frequency and duration Fr		Probability of hazardous event Pr		Avoidance Av	
<= 1 hour	5	Very high	5		
> 1 h - <= day	5	Likely	4		
>1 day - <=2 weeks	4	Possible	3	Impossible	5
>2 weeks - <=1 year	3	Rarely	2	Possible	3
> 1 year	2	Negligible	1	Likely	1

Consequences	Severity Se	Class Cl				
		3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		🟨	SIL 1	SIL 2	SIL 3
Reversible, medical attenmtion	2			🟨	SIL 1	SIL 2
Reversible, firs aid	1				🟨	SIL 1

Figure 10. Determination of safety integrity level applying risk matrix [SFS EN 62061].

2.3.2 Safety block diagrams

After identifying and specifying safety functions and safety-related part of a control system (SRP/CS) a technical realisation for each safety function in a machine control system is designed. A safety block diagram for each safety function to be estimated is created based on the characteristics of safety functions. Five designated architectures are presented in ISO 13849-1, which fulfil specific design criteria and behaviour under fault conditions. These designated architectures can be utilized in creating safety block diagrams for the safety functions of a machine control system. The safety block diagram consists of only those components that participate in the execution of a safety function. Usually safety block diagram consists of input (e.g. sensors, limit switches etc.), logic (e.g. programmable logic controller, i.e. PLC) and output (e.g. actuators, contactors etc.) components (into which also cables and connectors are included). The safety function can be either single channel solution or duplicated one. The category of safety functions can be estimated based on safety block diagrams.

2.3.3 Categories and architectures of control systems

The references to categories and safety integrity levels mean also that the requirement become more specific and later, hopefully, the level of safety becomes more similar in different machines. Then the operator can be more confident with the safety of a machine.

The categories can be associated to architecture and performance in a case of a failure. Figure 11 shows the designated architectures for which the standard provides precalculated solutions to be applied in performance level calculations. Failure, mode and effect analysis (FMEA) can be applied to confirm the selected category. The failure modes to be analyzed are described in ISO 13849-2. Category B is basic category (“state-of-the-art”) and it is the basis for all other categories. Table 3 shows some typical properties related to the categories. The examples of structure describe a typical architecture used in the category. Of course, in each category several more complex architectures are possible.

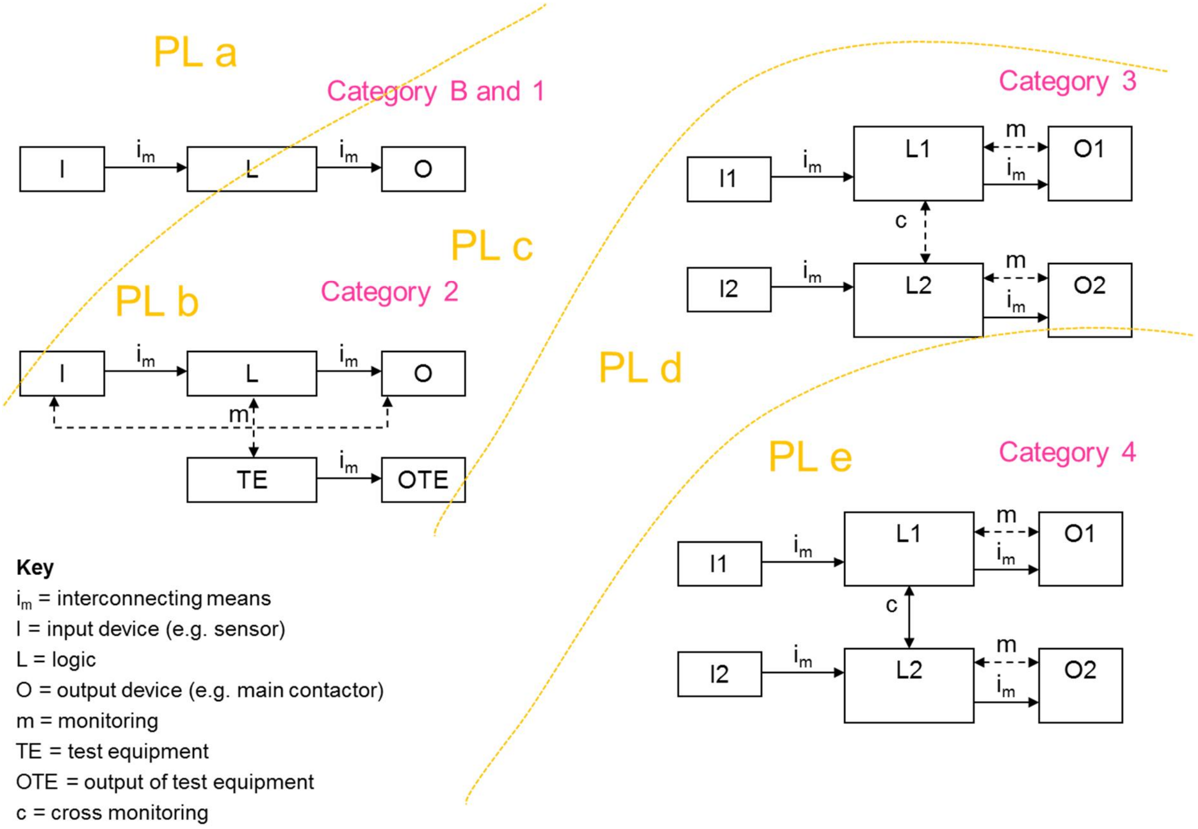
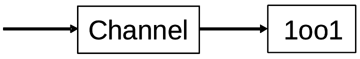
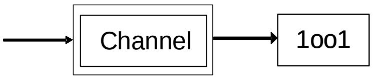
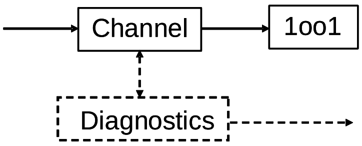
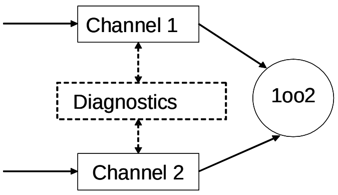
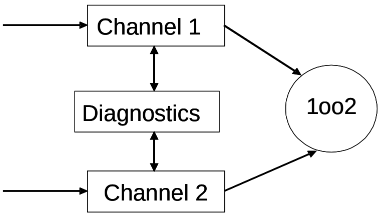


Figure 11. Designated architectures and related PLs according to ISO 13849-1 [SFS-EN ISO 13849-1:2008].

Table 3 Typical properties of control systems suitable for specific categories.

Cat.	Operation at fault	Typical	Example of structure
B	Fault may lead to a hazard.	Standard "state of the art" technology.	
1	Fault is unlikely, but it may lead to a hazard.	Reliable technology and over dimensioning.	
2	Most faults are detected sooner or later, but a fault may lead to a hazard.	The system tries to detect faults before hazard.	
3	Single fault does not lead to a hazard.	Architecture or components are often duplicated or performance at a fault is under control.	

Cat.	Operation at fault	Typical	Example of structure
4	Single fault does not lead to a hazard. Single faults are detected or they have no effect on safety.	Architecture or components are usually duplicated and monitored by the system.	
Note: 1oo1 means "one out of one"; 1oo2 means "one out of two". Basically, 1oo2 means that one safety signal (or channel) is enough to trigger safety function.			

2.3.4 Mean time to dangerous failure of each channel

When the safety block diagrams have been created for safety functions, the mean time to failure (MTTF) or mean time to dangerous failure ($MTTF_d$) values of components are collected. These values are necessary to be collected only for those components that participate in the execution of safety functions. Usually MTTF or $MTTF_d$ values are asked from the component manufacturers' representatives or gathered from component data sheets. If there is not any component manufacturers' data about MTTF or $MTTF_d$ values available, the values mentioned in ISO 13849-1 can be used. Fault exclusions presented in ISO 13849-2 for different component types can be taken into account. Reasons for fault exclusions should be presented to show that the probability of failure is sufficiently low.

The $MTTF_d$ for each channel can be estimated using "parts count method", which serves to estimate the $MTTF_d$ for each channel separately. The $MTTF_d$ values of all single components that are parts of the channel are used in this calculation. The general formula for this is:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{1}{MTTF_{dj}} \qquad (1)$$

$MTTF_d$ is for the complete channel and $MTTF_{d\,i}$, $MTTF_{d\,j}$ is the $MTTF_d$ of each component which has a contribution to the safety function.

The $MTTF_d$ for each channel is expressed in three levels: low, medium and high. The denotation is "low", for the range 3 years ≤ $MTTF_d$ < 10 years, "medium" for the range 10 years ≤ $MTTF_d$ < 30 years and "high" for the range 30 years ≤ $MTTF_d$ ≤ 100 years. The $MTTF_d$ values are associated to each channel of the subsystems and not to complete two channel systems.

2.3.5 Diagnostic coverage

Diagnostic coverage (DC) is a measure for the effectiveness of diagnostics. It can be determined as a ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures. The value of the DC is provided in four levels: none, low, medium and high. DC is "none" for DC < 60 %, "low" for the range 60 % ≤ DC < 90 %, "medium" for the range 90 % ≤ DC < 99 % and "high" for DC ≥ 99 %. The common methods for estimating DC are FMEA and Annex E of ISO 13849-1.

A safety function typically includes several parts and thus the average DC (DC_{avg}) is necessary to be calculated for category 2, 3 and 4 safety functions:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}} \qquad (2)$$

2.3.6 PL estimation

When the levels for $MTTF_d$ and DC have been defined for all the parts a safety function, the attainable PL for this safety function can be defined based on the graph of Figure 12. For category 2, 3 and 4 safety functions, common cause failures (CCF) are necessary to be estimated. Basic method is presented at ISO 13849-1. Common cause failure is defined as failures of different items that result from a single event, but these failures are not consequences of each other. In addition to CCF, requirements presented for software and measures against systematic failures need to be considered to complete PL estimation.

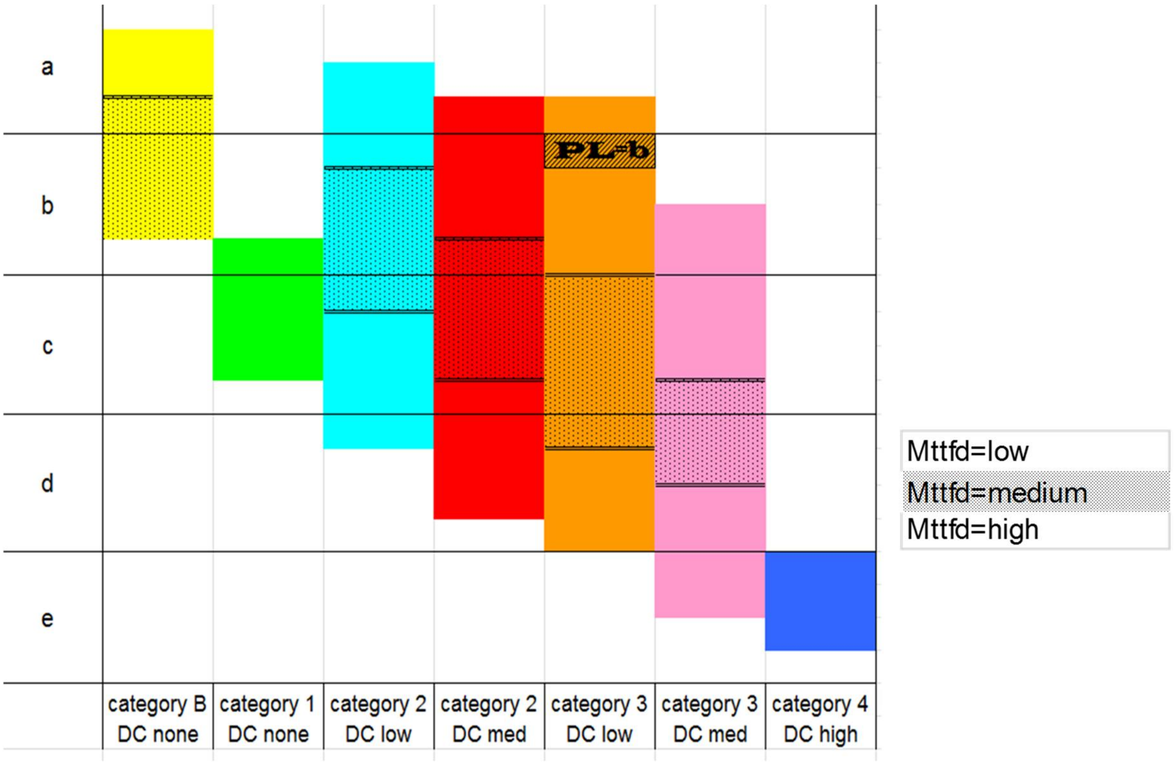


Figure 12 Relationship between categories, DC_{avg}, $MTTF_d$ of each channel and PL.

3. Design process

3.1 Safety conscious design process according to SFS EN 12100

Figure 13 describes the basic risk reduction process, which is applicable for robots also. After risk assessment the risk reduction starts by considering inherently safe design principles. This means that, for example, all crushing points of the system are so narrow (< 5 mm) that a finger cannot be crushed or so wide that human body parts do not crush. Of course, in a robot system there are a lot of places where safeguarding is needed. The third means to minimize risk is giving information to the user. Information may not replace inherently safe design means or safeguarding. The information can be e.g. user manuals, training, warning signs, sound or lights. The phases of risk reduction are described more detailed in robot standards (see ISO 10218-2).

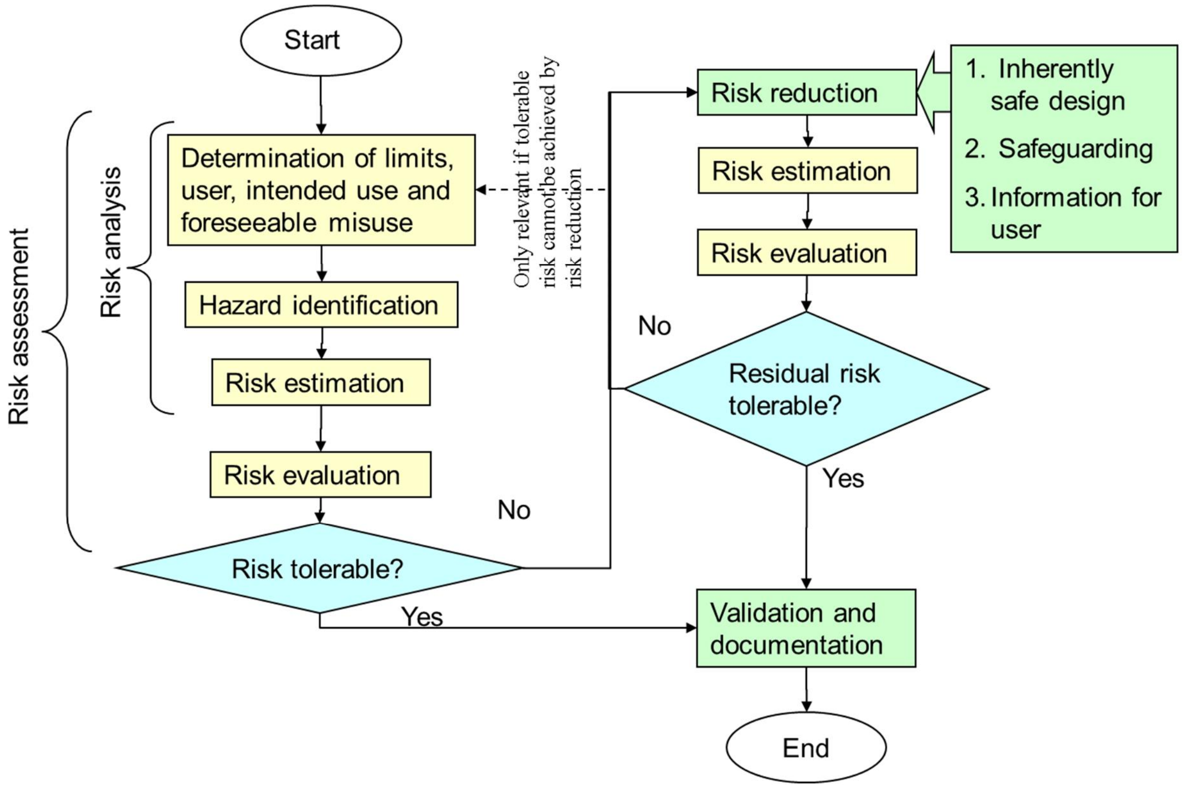


Figure 13. Safety-conscious design process for machinery.

3.2 Risk assessment

Risk assessment is applied in robotic systems to check and confirm that adequate means are applied to maintain safety. The Hazards and related risks must be identified first to determine the nature and quality of safety measures. At the end of the design process risks and related safety measures are validated in order to see are the risks minimized adequately and are the residual risks at acceptable level.

Hazard identification phase is the most critical phase of the risk assessment since if the risk is not found it is not under control. At the risk estimation phase the risk is typically divided into two parts: severity and probability. Severity describes how severe the consequences of the hazards can be and the probability factor describes the probability of a hazardous or initiating event. The risk evaluation is, typically, made by a person, who has the power to decide about the risk reduction measures.

3.2.1 Risk Assessment process

The risk assessment process is described in ISO 12100. Figure 14 shows the phases of risk assessment and the following list describes more about the tasks:

- **Determination of limits**. The limits of the machinery include the intended use, operation modes, required level of training, exposure to hazards, space limits, time limits (e.g. service intervals) and other limits (e.g. environmental limits, housekeeping, material properties).
- **Hazard identification**. Identify the hazards that can be generated by the machinery and the associated hazardous situations. Apply checklists presented in standards ISO 10218-1&2 and if necessary for general risks checklist from standard ISO 12100.
- **Risk estimation**. Estimate the risks, taking into account the severity of the possible injury or damage to health and the probability of its occurrence.
- **Risk evaluation**. Evaluate the risks, with a view to determining whether risk reduction is required, in accordance with the objective of the Machinery Directive.
- **Risk reduction**. Eliminate the hazards or reduce the risks associated with these hazards by application of protective measures. Priority for measures is: inherent 1) safe measures, 2) safeguarding and 3) warnings and guidelines.

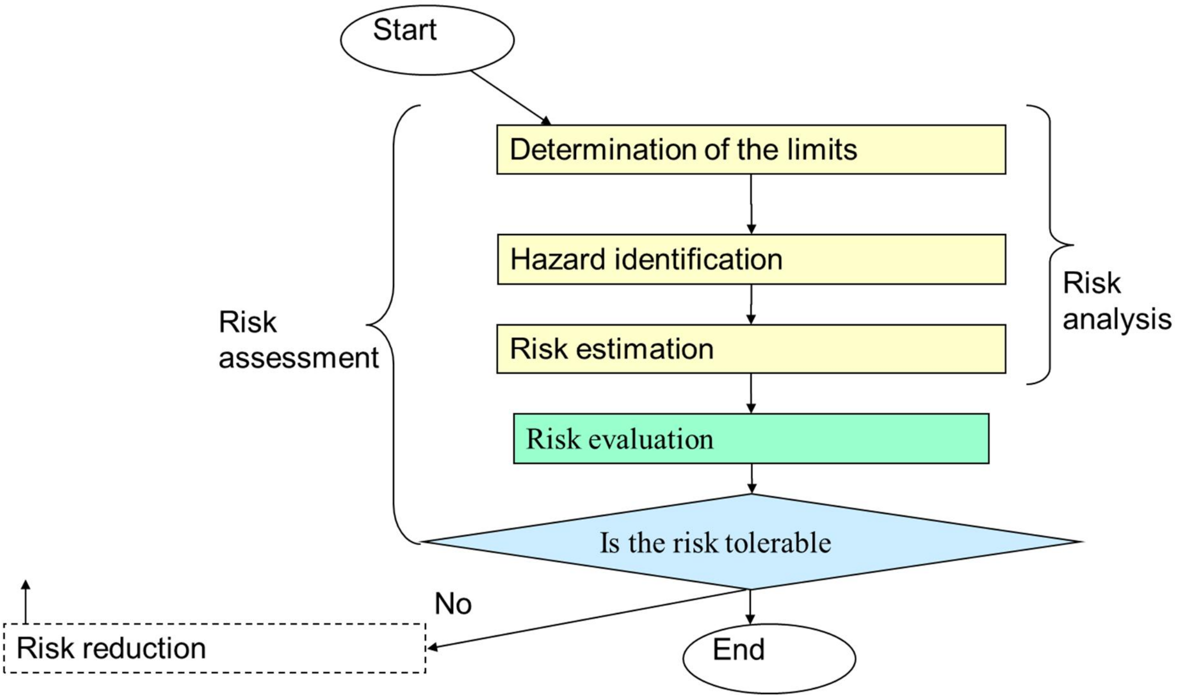


Figure 14. Risk assessment procedure.

3.2.2 Risk assessment methods

There are a lot of different risk analysis methods and Machinery Directive does not obey the analyst to apply a specific method, but the analyst can choose. Each method has its pros and cons and therefore it is often useful to apply different methods.

Preliminary Hazard Analysis (PHA) is good in finding hazards by applying checklists of robot standards or more general ISO 12100. Because the checklists of harmonized standards suit well to the PHA analysis, it is almost obligatory.

Operation Hazard Analysis (OHA) is good for finding hazards related to operator tasks. OHA is good when the user has many complex tasks at the robot cell.

HAZOP (Hazard and Operability study) or FMEA (Failure mode and effects analysis) are good in finding results of failures or exceptional situations. FMEA is often related to design and validation of control systems.

Fault tree analysis (FTA) is good in combining, describing and calculating results of many inputs.

4. Discussion

To have practical safety distances in robot cells, the robot speed must be reduced before the robot is stopped. Monitored stop allows quick restart, but to ensure safety, the stand still need to be monitored adequately. Emergency stop is needed in emergency and failure situations. It cuts the servo power and therefore restarting takes some time and it is not feasible in continuous human – robot collaboration.

The designer has to follow several processes during the design of a robot cell (see Figure 15). The obligatory process, which can also be associated to documentation, is described in Machinery Directive:

- Risk assessment (see Figure 9, Figure 10 and Figure 14)
- All safety requirements and related directives
- Design the machine according to Machinery Directive annex I (Essential health and safety requirements relating to the design and construction of machinery)
- Write manuals for use and if necessary construction, maintenance, safety
- Compile and maintain technical file (see Annex 2)
- Declaration of Conformation must be drawn up (see Annex 1)
- CE-marking and other markings at the machine (see Figure 3).

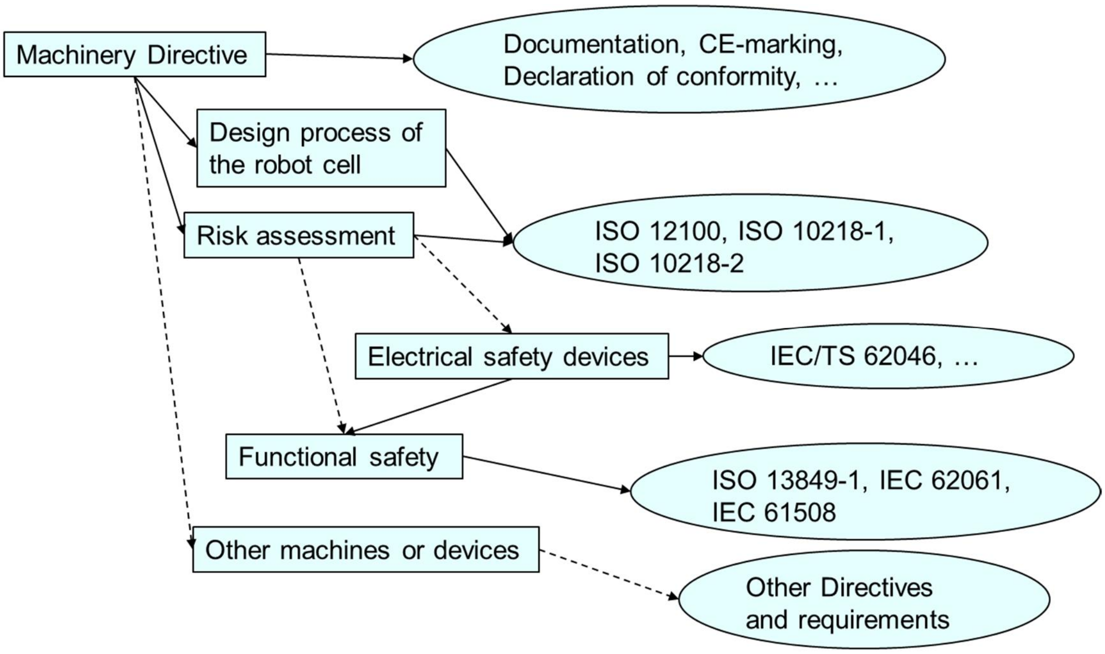

Machinery Directive
Documentation, CE-marking, Declaration of conformity, …
Design process of the robot cell
Risk assessment
ISO 12100, ISO 10218-1, ISO 10218-2
Electrical safety devices
IEC/TS 62046, …
Functional safety
ISO 13849-1, IEC 62061, IEC 61508
Other machines or devices
Other Directives and requirements

Figure 15. Safety procedures related to robot cell design. Machinery Directive gives the obligatory tasks for the designer. The dotted lines show the tasks, which are realised if the previous phase requires it.

The risk assessment is the first mentioned task at the list and it starts a new procedure, which is described in section 3.2.1 Risk assessment process. At the requirements, the risk assessment method is not mentioned explicitly, but the analyst may choose from large variety of analyses. In practice, preliminary hazard analysis (PHA) is very common and it enables the use of hazard checklists described in many standards (ISO 12100, ISO 10218-1 and ISO 10218-2).

When safety devices and safety functions are applied then also functional safety must be considered. The PL or SIL assignment is made applying risk graph (Figure 9) or matrix (Figure 10), but all typical safety functions and associated PLs are described at robot standards. Usually the standard estimation is correct, but it can be changed if the risk assessment gives another result. Furthermore, the functional safety is related to safety requirements of control system and safety devices. In practice, the control system and safety devices are selected according to the functional safety requirements. The control system refers often to safety-rated I/O, which fulfils the requirements.

The verification of a robot cell should be done by applying the table of Annex G of ISO 10218-2, since it covers well the requirements of the standard. Since it presents the requirements as a list, it is probably not the best tool for design process, but for verification it is good. Each row of the table refers to the original text, which presents the requirements in details.

References

Fraser I. (ed). Guide to application of the Machinery Directive 2006/42/EC 2nd Edition June 2010. 406 p.

IEC 61496-1:2012. Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests. 50 p.

ISO 10218-1. 2011. Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robot systems and integration. 43 p.

ISO 10218-2. 2011. Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robots. 72 p.

ISO 13855:2010. Safety of machinery. Positioning of safeguards with respect to the approach speeds of parts of the human body. 40 p.

ISO/TS 15066. 2016. Robots and robotic devices — Safety requirements for Industrial robots — Collaborative operation. 33 p.

Machinery Directive 2006/42/EC. DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.

Malm T. 2016. Älykäs anturi teollisuusrobotin vaara-alueen valvonnassa (Intelligent sensor controlling the danger zone of an industrial robot). Diplomityö. 64 p. app. 8

Malm T., Venho-Ahonen O., Hietikko M., Stålhane T., de Bésche C. & Hedberg J. 2015. From risks to requirements - Comparing the assignment of functional safety requirements. Espoo. VTT Technology 241. 58 p. + app. 9 p.

SFS-EN 62061. 2005. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.

SFS-EN ISO 11161:2007. Safety of machinery — Integrated manufacturing systems — Basic requirements. 80 p.

SFS-EN ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. Finnish Standards Association SFS. 172 p.

SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.

Annex 1: Declaration of conformity

Declaration of conformity (Annex II A)

1. business name and full address of the manufacturer and, where appropriate, his authorised representative;

2. name and address of the person authorised to compile the technical file, who must be established in the Community;

3. description and identification of the machinery, including generic denomination, function, model, type, serial number and commercial name;

4. a sentence expressly declaring that the machinery fulfils all the relevant provisions of this Directive and where appropriate, a similar sentence declaring the conformity with other Directives and/or relevant provisions with which the machinery complies. These references must be those of the texts published in the Official Journal of the European Union;

5. where appropriate, the name, address and identification number of the notified body which carried out the EC type-examination referred to in Annex IX and the number of the EC type-examination certificate;

6. where appropriate, the name, address and identification number of the notified body which approved the full quality assurance system referred to in Annex X;

7. where appropriate, a reference to the harmonised standards used, as referred to in Article 7(2);

8. where appropriate, the reference to other technical standards and specifications used;

9. the place and date of the declaration;

10. the identity and signature of the person empowered to draw up the declaration on behalf of the manufacturer or his authorised representative.

Example of Declaration of Conformity following the previous numbering

1. Oy Robot business AB

Robotie 1, 33720 Tampere, Finland

2. Tuomo Tietäväinen, Oy Robot business AB

Robotie 1, 33720 Tampere, Finland

3. Product model: Super-robotti 1. Serial number 1.

4. The object of described above is in conformity with relevant EU harmonization legislation:

Machinery Directive 2005/42/EC

(5.-6. No notified body required)

7. Reference to relevant harmonized standards:

SFS-EN ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction.

ISO 10218-1. 2011. Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robot systems and integration.

ISO 10218-2. 2011. Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robots.

(8. Reference to other technical standards and specifications

No other specifications.)

9. -10. Signed for and behalf of

At Tampere 19th January 2017

Manufacturer:

Oy Robot business AB

Tapio Tekoäly

Tapio Tekoäly, CEO

Annex 2: Technical file

The technical file is described in Machinery Directive as follows:

(a) a construction file including:

— a general description of the machinery,

— the overall drawing of the machinery and drawings of the control circuits, as well as the pertinent descriptions and explanations necessary for understanding the operation of the machinery,

— full detailed drawings, accompanied by any calculation notes, test results, certificates, etc., required to check the conformity of the machinery with the essential health and safety requirements,

— the documentation on risk assessment demonstrating the procedure followed, including:

(i) a list of the essential health and safety requirements which apply to the machinery,

(ii) the description of the protective measures implemented to eliminate identified hazards or to reduce risks and, when appropriate, the indication of the residual risks associated with the machinery,

— the standards and other technical specifications used, indicating the essential health and safety requirements covered by these standards,

— any technical report giving the results of the tests carried out either by the manufacturer or by a body chosen by the manufacturer or his authorised representative,

— a copy of the instructions for the machinery,

— where appropriate, the declaration of incorporation for included partly completed machinery and the relevant assembly instructions for such machinery,

— where appropriate, copies of the EC declaration of conformity of machinery or other products incorporated into the machinery,

— a copy of the EC declaration of conformity;

(b) For series manufacture, the internal measures that will be implemented to ensure that the machinery remains in conformity with the provisions of this Directive. The manufacturer must carry out necessary research and tests on components, fittings or the completed machinery to determine whether by its design or construction it is capable of being assembled and put into service safely. The relevant reports and results shall be included in the technical file.