Safety Workshop Presentation
MAX IV
2026-06-02

EVIDENTE

Workshop Agenda

10:00 AM → 12:00 PM **1st Session**

10:00 AM	**Introduction** ▪ Are there exemptions for own laboratory use? ▪ How should we handle subsystems and components?	30m
10:30 AM	**CE Fundamentals** ▪ Overview of CE marking process	40m
11:10 AM	**Applicability to Max IV equipment** ▪ System architecture (Max IV presents typical equipment) ▪ Discussion around applicable directives	50m

12:00 PM → 12:45 PM **Lunch: Eatery**

12:45 PM → 3:00 PM **2nd Session**

12:45 PM	**MAX IV guidelines regarding CE marking and motion** B_H_SA_MS_Guid... B_H_SA_MS_MAX... B_H_SA_MS_Proc...	15m
1:00 PM	**Risk assessment (ISO 12100)**	30m
1:30 PM	**Functional safety (ISO 13849)**	30m
2:00 PM	**Testing & technical file**	30m
2:30 PM	**Declaration & CE marking**	30m

EVIDENTE

Are there exemptions for own laboratory use?

Yes

According to Machinery Directive 2006/42/EC in Article 1 is laboratory equipment excluded from the scope:

2. The following are excluded from the scope of this Directive:

(h) machinery specially designed and constructed for research purposes for temporary use in laboratories;

Length of temporary use is stated in compliance documentation a MAX IV according to Hasse Andersson.

At the Same Time

The company or organization still has:

- Employer safety responsibility
- Liability risk

It could be argued that if the machinery is used in the laboratory, it is ‘put into service’.

In practice companies or organizations elect to apply CE as ‘best practice’.

EVIDENTE

How should we handle subsystems and components?

Sourcing

Regulated Component #1
- LVD/EMC
- Technical Documentation
- Declaration of Conformity

Regulated Component #2
- LVD/EMC
- Technical Documentation
- Declaration of Conformity

Regulated Component #3
- LVD/EMC
- Technical Documentation
- Declaration of Conformity

Partly Completed Machine #2 (3PP)
- Risk Assessment
- Supplier Declarations
- Assembly Instruction
- Declaration of Incorporation

Regulated Component #4
- LVD/EMC
- Technical documentation
- Declaration of Conformity

Internal production

Partly Completed Machine #1
- Risk Assessment
- Supplier Declarations
  - Component #1
  - Component #2
  - Component #3
- Assembly Instruction
- Declaration of Incorporation

Internal integration

CE responsibility on system level

Fully Completed Machine
- General Info
- Risk Assessment
- Safety Functions
- Supplier Compliance
  - Component #4
- DoIs
  - PCM #1
  - PCM #2
- Technical Documentation
- Declaration of Conformity
- CE Marking

EVIDENTE

How should we handle subsystems and components?

Sourcing

Regulated Component #1
- LVD/EMC
- Technical Documentation
- Declaration of Conformity

Regulated Component #2
- LVD/EMC
- Technical Documentation
- Declaration of Conformity

Regulated Component #3
- LVD/EMC
- Technical Documentation
- Declaration of Conformity

Partly Completed Machine #2 (3PP)
- Risk Assessment
- Supplier Declarations
- Assembly Instruction
- Declaration of Incorporation

Regulated Component #4
- LVD/EMC
- Technical documentation
- Declaration of Conformity

Internal production

Partly Completed Machine #1
- Risk Assessment
- Supplier Declarations
  - Component #3
- Assembly Instruction
- Declaration of Incorporation

Internal integration

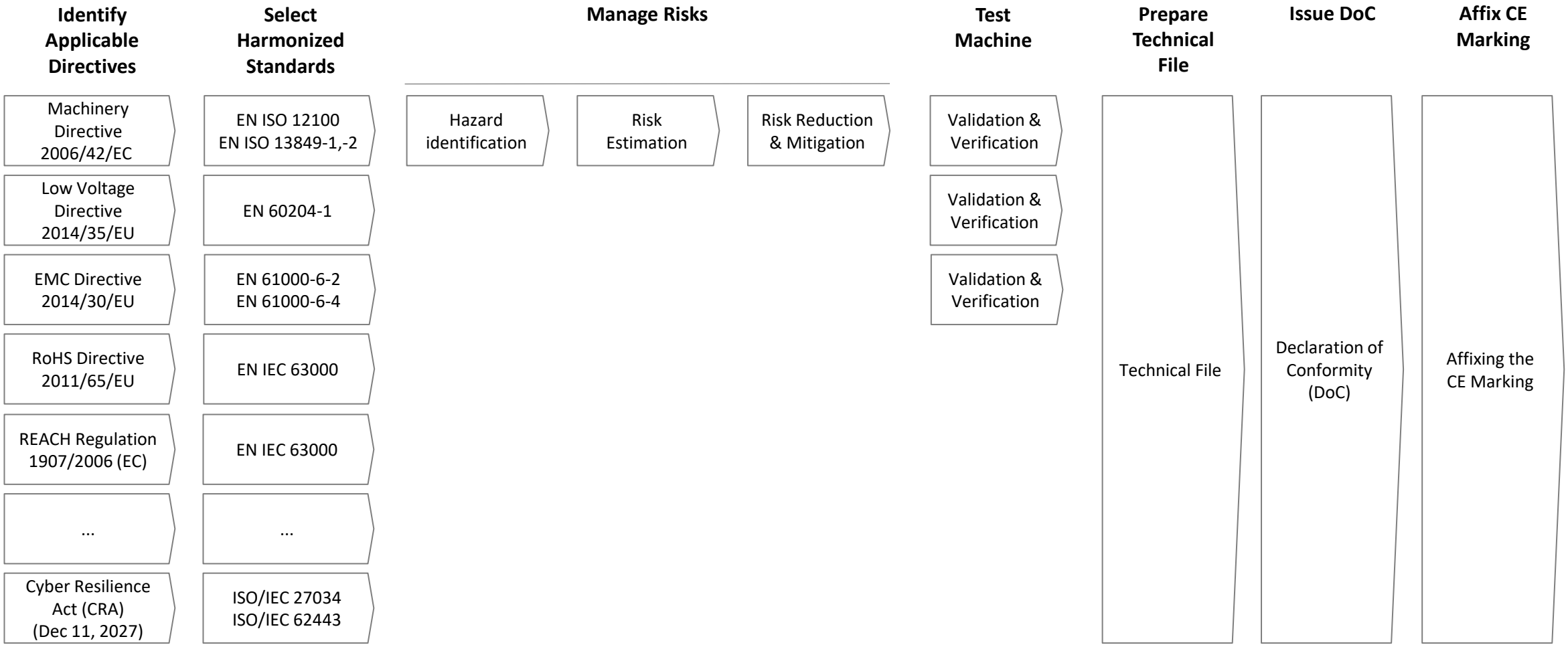
CE responsibility on system level even if all components are CE marked

Fully Completed Machine
- General Info
- Risk Assessment
- Safety Functions
- Supplier Compliance
  - Component #4
  - Component #5
- Dole
  - PCM #1
  - PCM #2
- Technical Documentation
- Declaration of Conformity
- CE Marking

"Can we prove what we declared at the time of delivery?"

EVIDENTE

Overview of CE marking process

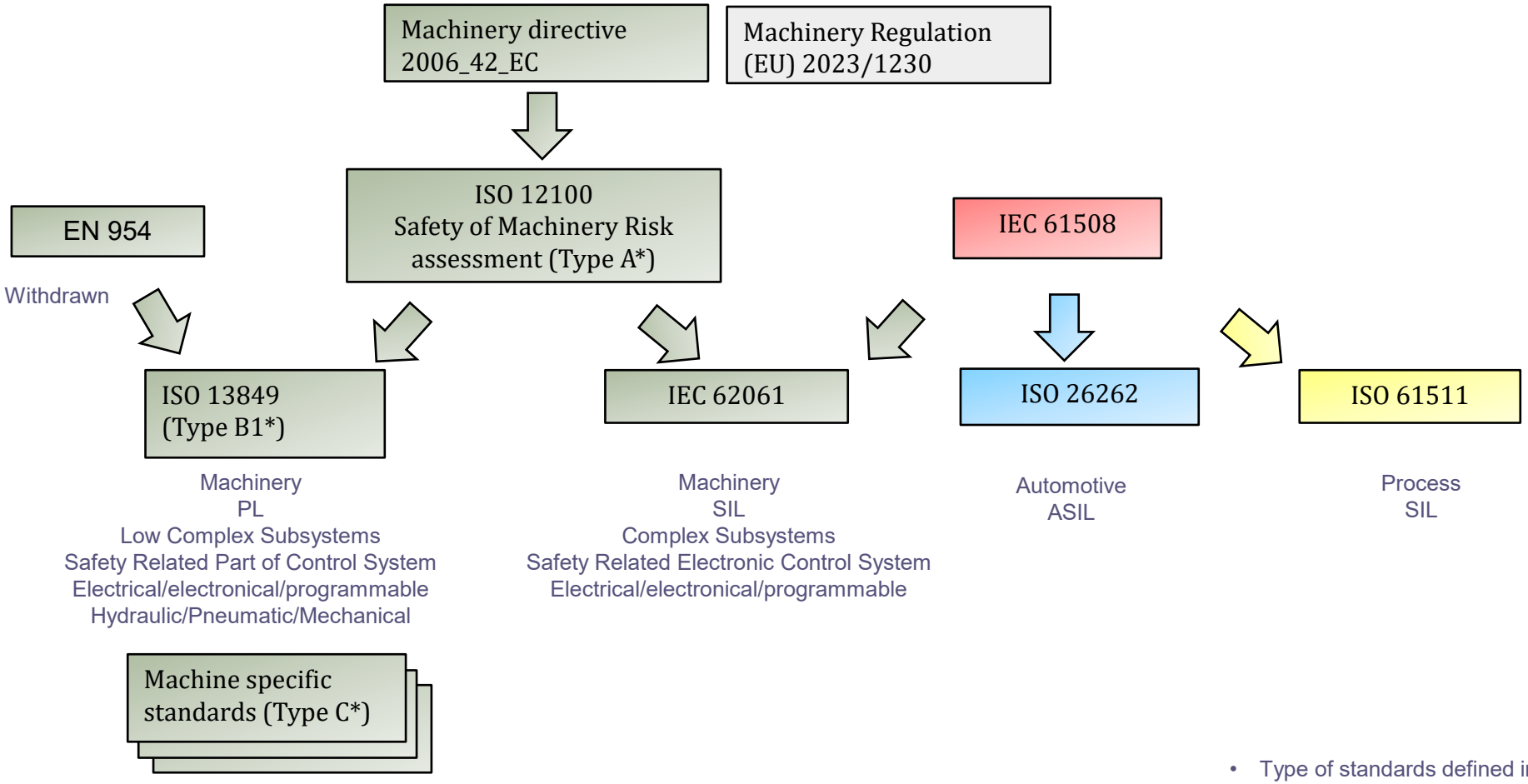


EVIDENTE

Why Safety?

EVIDENTE

Functional Safety Standards



- Type of standards defined in ISO 12100

EVIDENTE

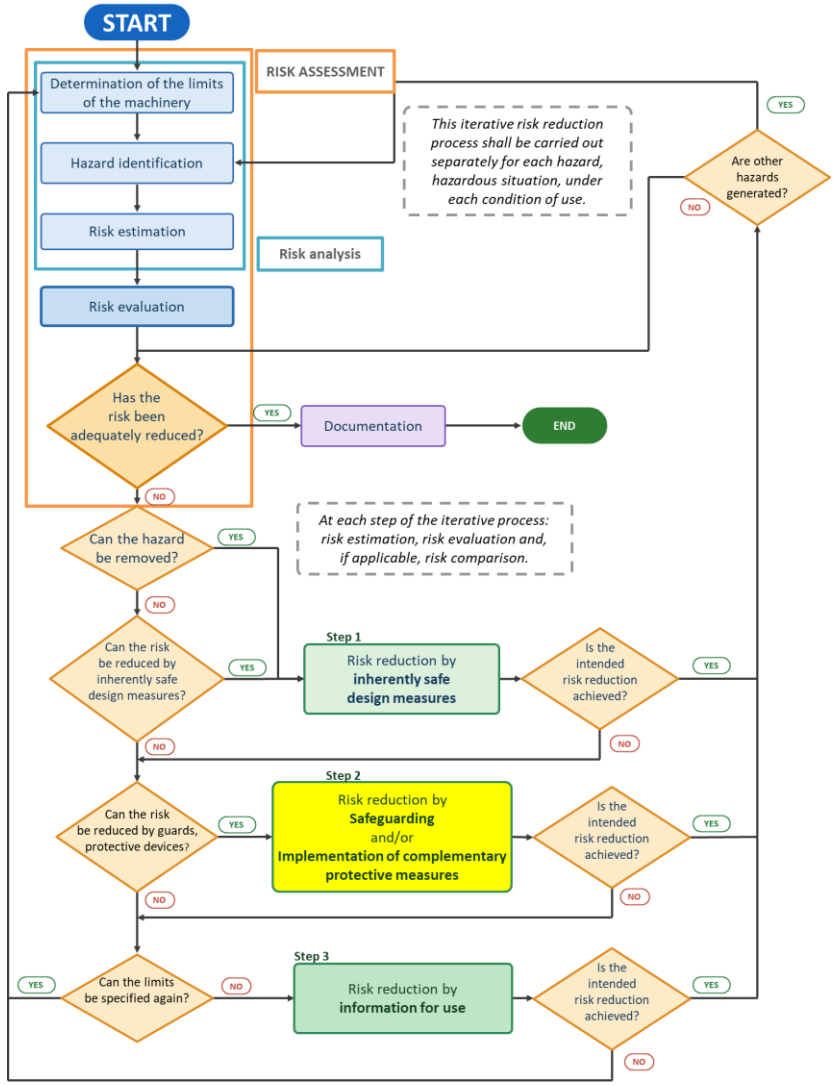
ISO 12100: Safety of machinery - General principles for design – Risk assessment and risk reduction.

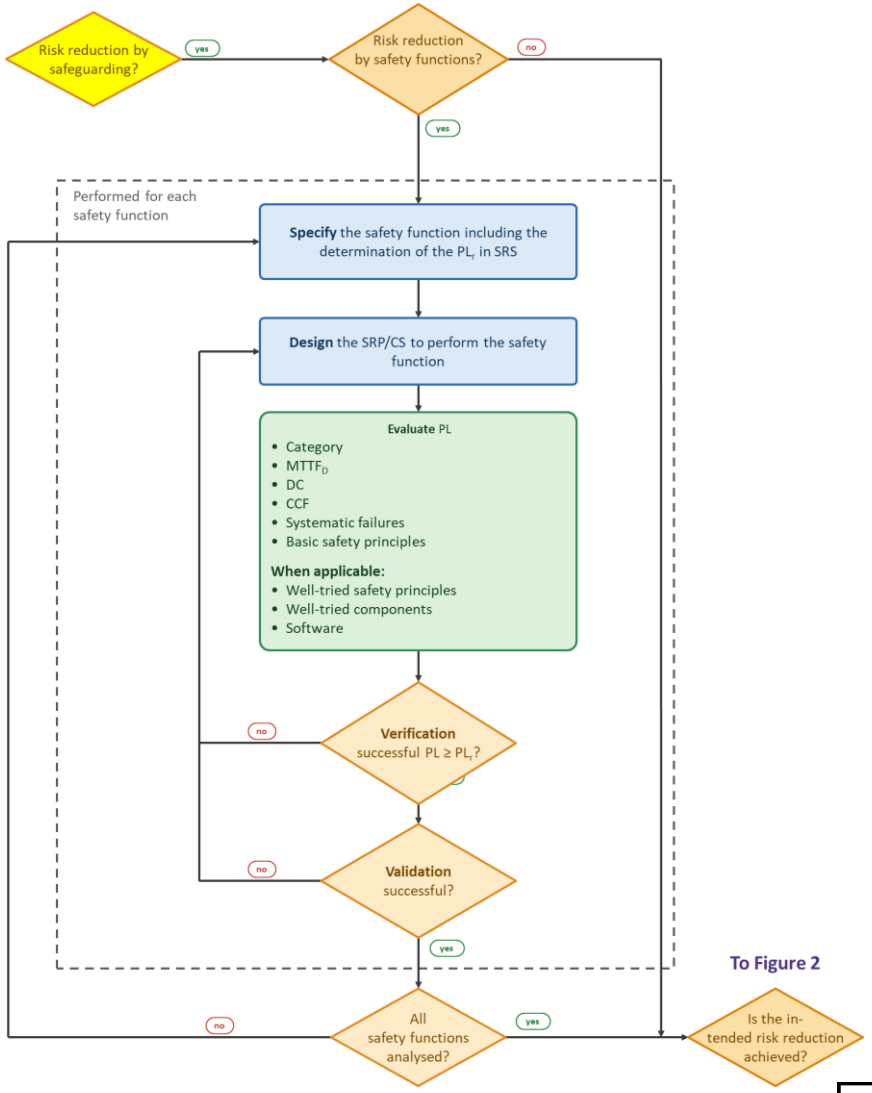
- Specifies basic terminology, principles and a methodology for achieving safety in the design of machinery.

- Specifies principles of risk assessment and risk reduction to help designers in achieving this objective.

- Provide a means of conforming to Essential Requirements of the Directive Machinery, 2006/42/EC

Risk Assessment and Risk Reduction ISO 12100 and ISO 13849

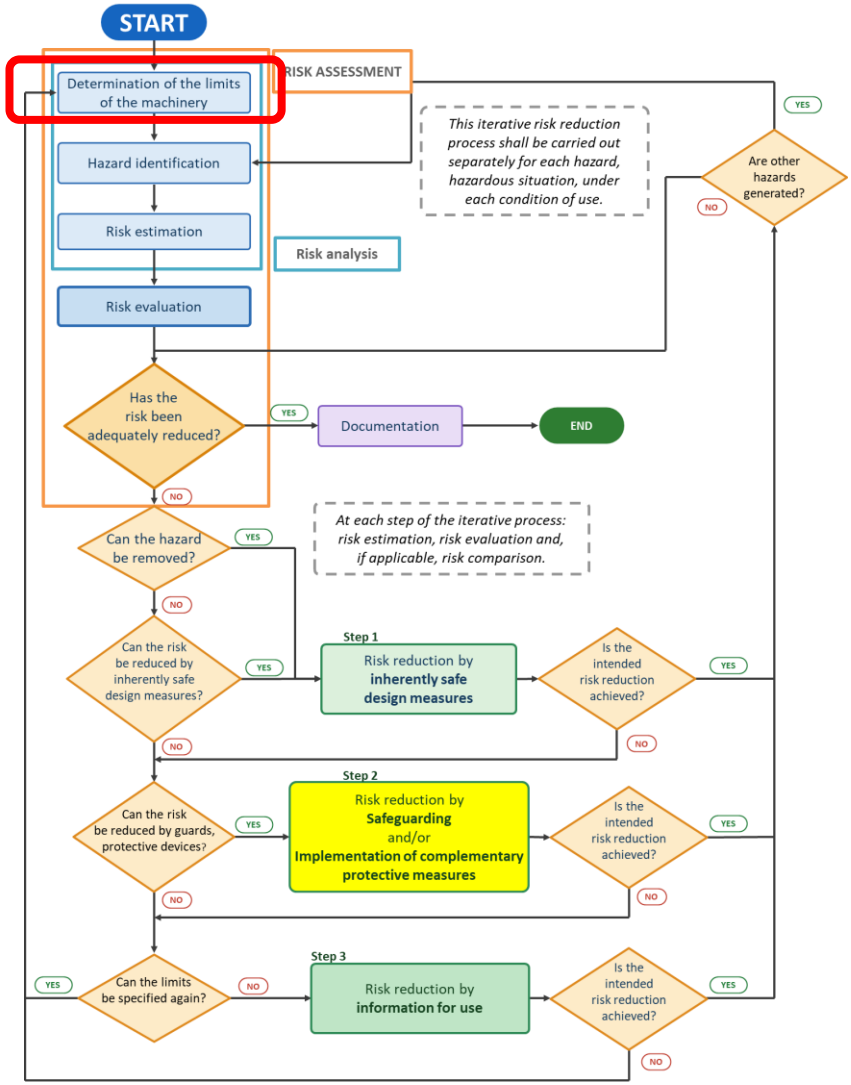




EVIDENTE

Risk Analysis: Determination of the limits of the machinery

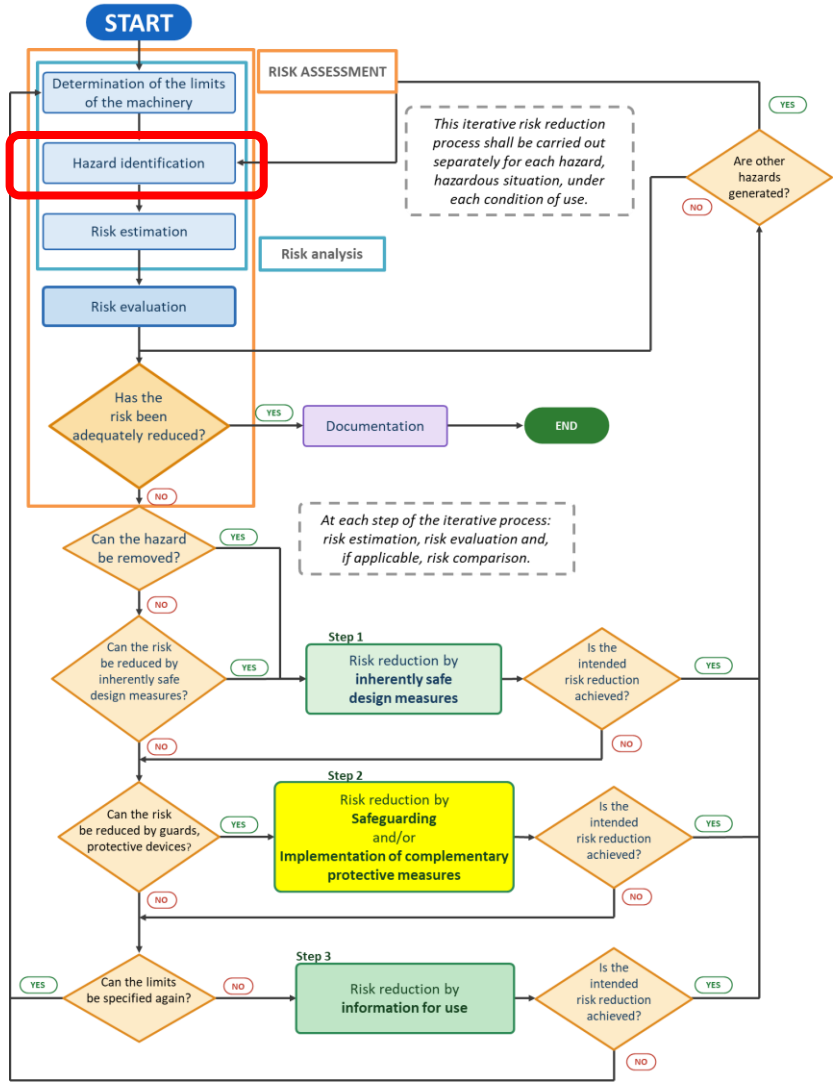
- Use Limits
  - Operation modes
  - Who is the user? (training, experience, ability)
  - Other exposed persons. (Hazard awareness)
- Space Limits
  - the range of movement,
  - space requirements for persons interacting with the machine
  - human interaction such as the operator–machine interface
  - the machine power supply interface
- Time Limits
  - the life limit of the machinery,
    - consider intended use and reasonably foreseeable misuse
  - recommended service intervals.
- Other Limits
  - Properties of the materials)to be processed
  - Housekeeping — the level of cleanliness required
  - Environmental — Temp range, In/Outdoor, Dry/Wet …



EVIDENTE

Risk Analysis: Hazard identification

- Machine Lifecycle
  - Transport, assembly and installation
  - Commissioning
  - Use;
  - Dismantling, disabling and scrapping
- Human interaction
  - Testing, setting, Programming
  - Tool change
  - Emergency stop, Restart
  - Maintenance, Trouble-shooting
- Possible states of the machine
  - Intended function
  - Malfunction
- Unintended behaviour of the operator or foreseeable misuse
  - Reflex behaviour by operator
  - Lack of concentration
  - External pressure – keep the machine running



EVIDENTE

Risk Analysis: Risk estimation

RISK

related to the considered hazard

is a function of

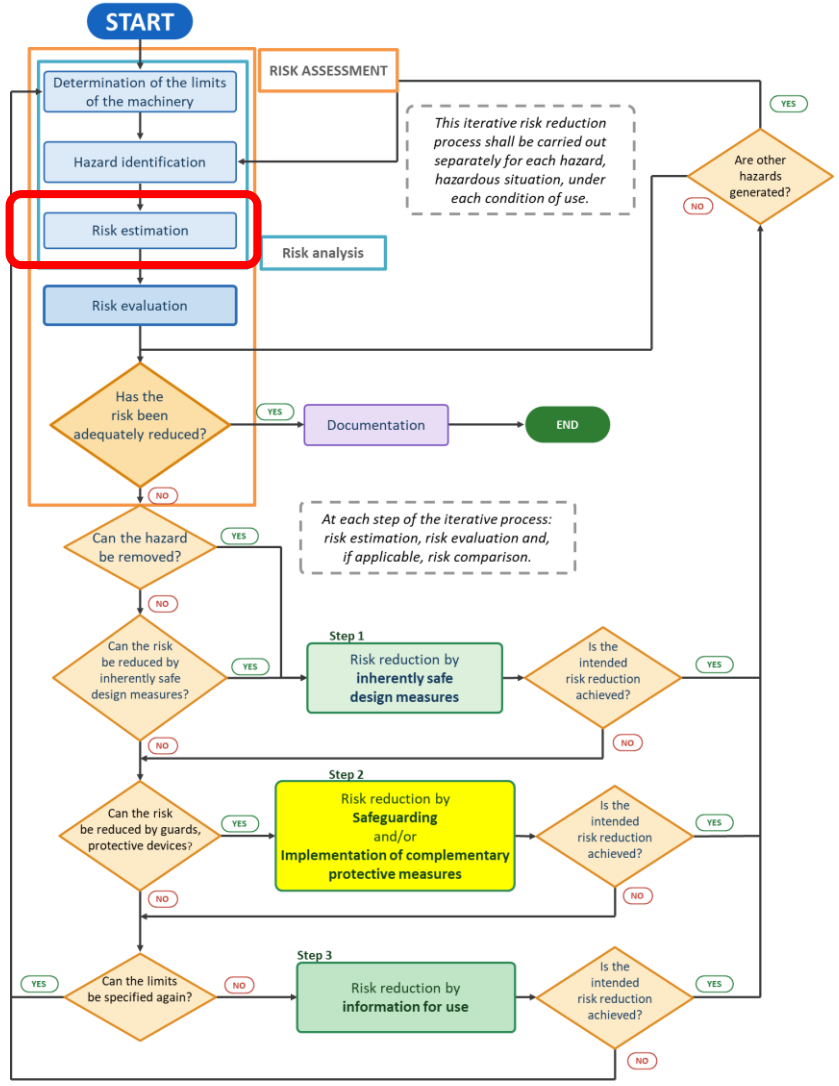
SEVERITY OF HARM

that can result from the considered hazard

and

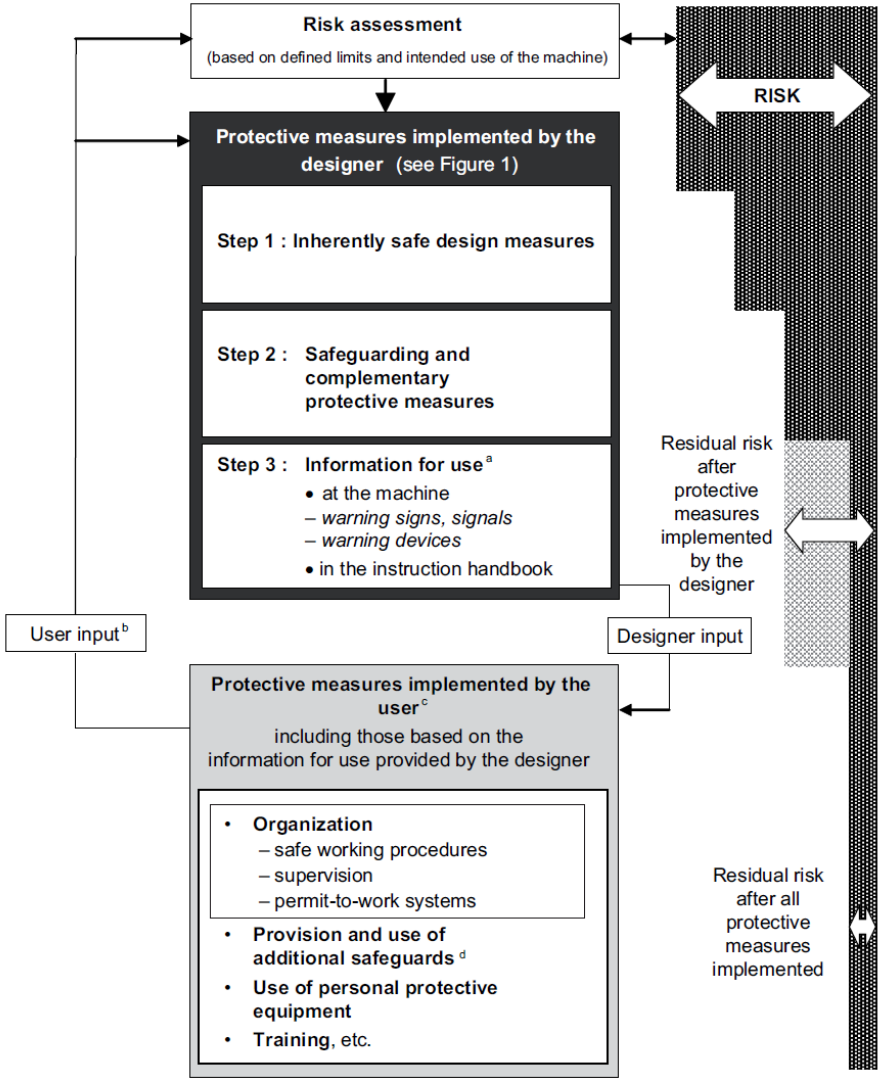
PROBABILITY OF OCCURRENCE of that harm

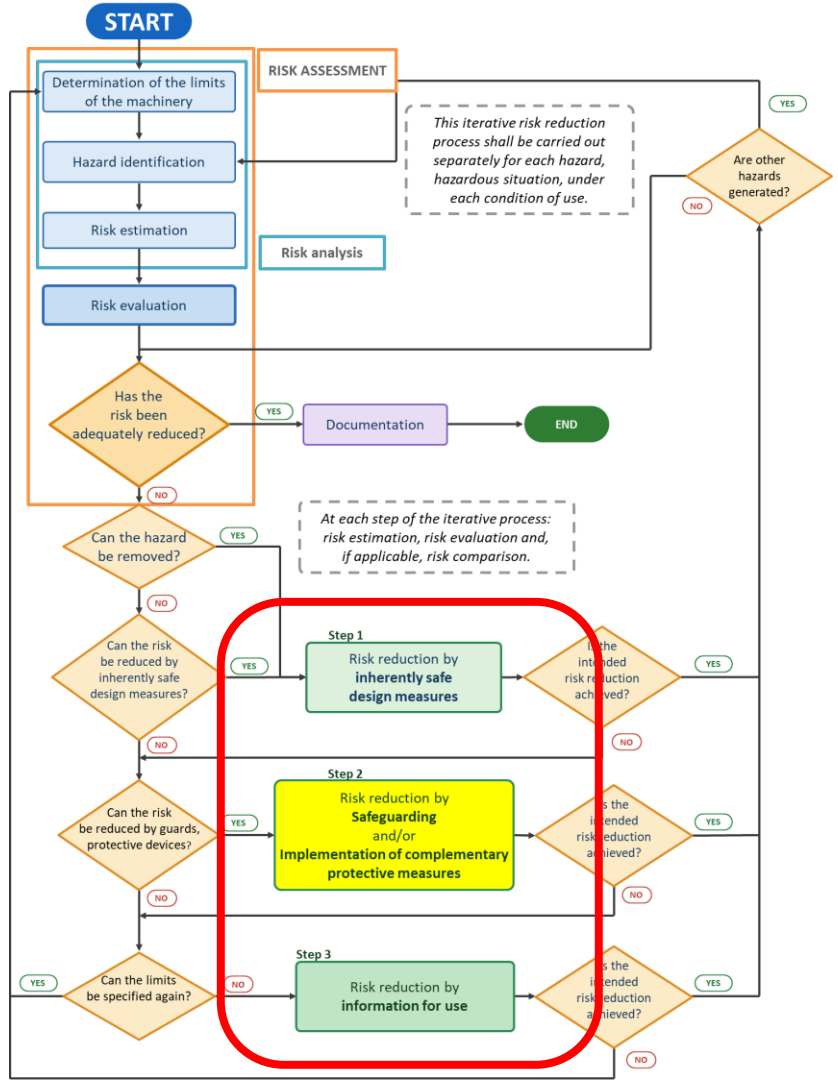
- Exposure of person(s) to the hazard
- the occurrence of a hazardous event
- the possibility to avoid or limit the harm



EVIDENTE

General Risk reduction ISO EN ISO 12100

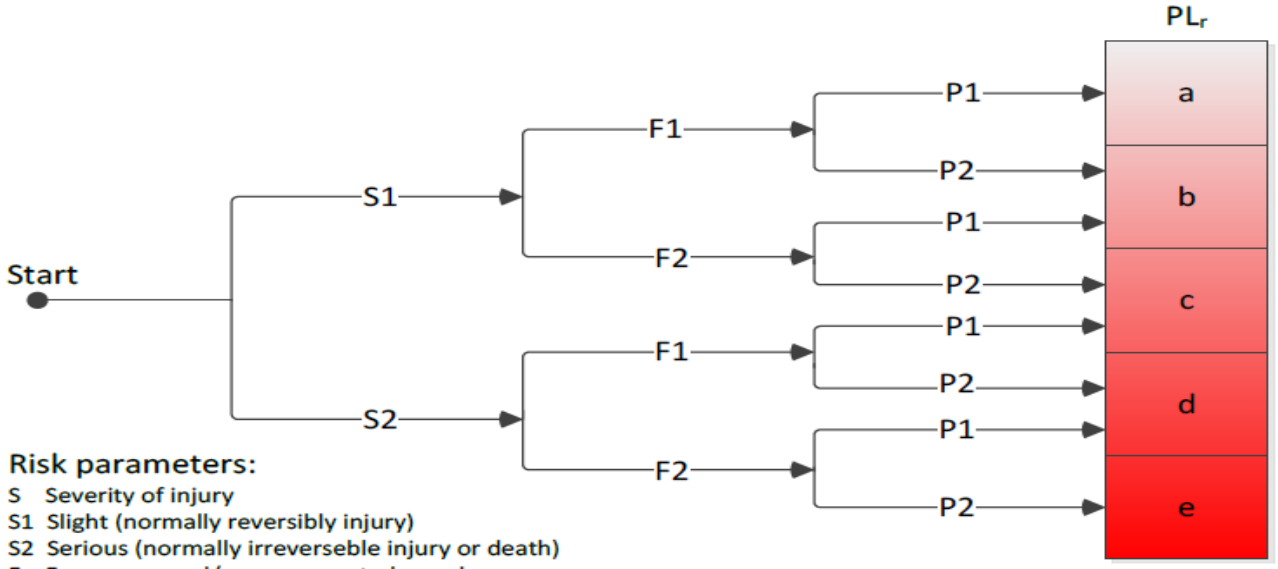




EVIDENTE

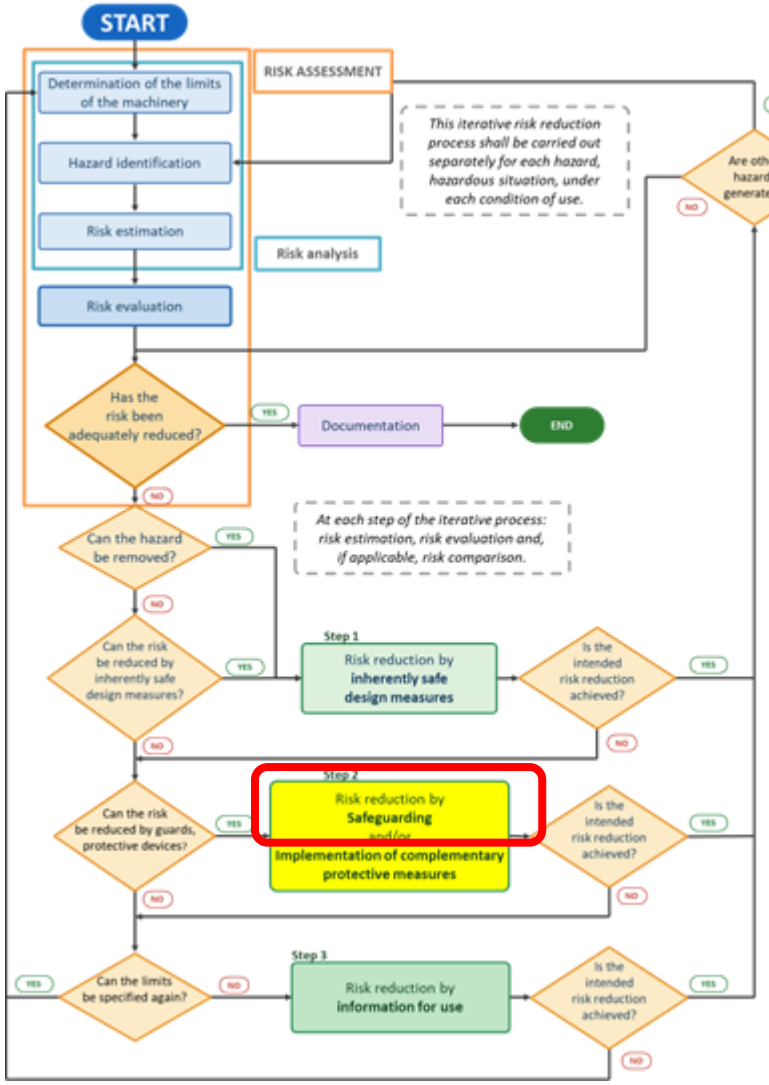
Risk reduction EN13849

- The graph below is based on the situation prior to the provision of the intended safety function.
- Risk reduction by technical measures independent of the control system (e.g. mechanical guards), or additional safety functions, are to be taken into account in determining the PLr of the intended safety function; in which case, the starting point is selected after the implementation of these measures



Risk parameters:

S Severity of injury
S1 Slight (normally reversibly injury)
S2 Serious (normally irreverseble injury or death)
F Frequency and/or exposure to hazard
F1 Seldom-to-less-often and/or exposure time is short
F2 Frequent-to-continuous and/or exposure time is long
P Possibility of avoiding hazard or limiting harm
P1 Possibility under specific condition
P2 Scarcely possible



EVIDENTE

Basic EN13849 Terms and definitions

- PL performance level
- PL_r required performance level
- MTTFd mean time to dangerous failure
- CCF common cause failure
- DC diagnostic coverage
- SRP/CS safety–related part of a control system

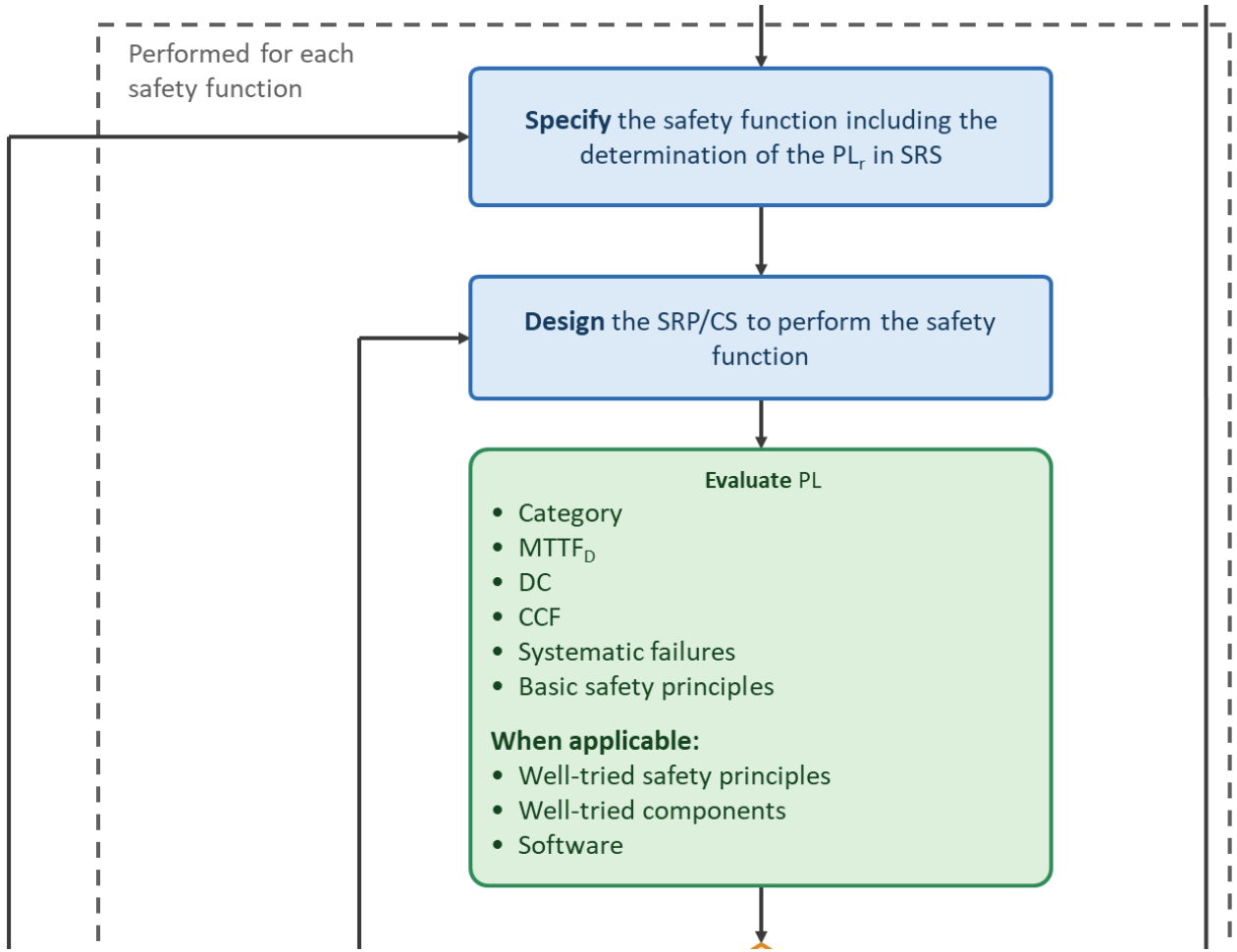
EVIDENTE

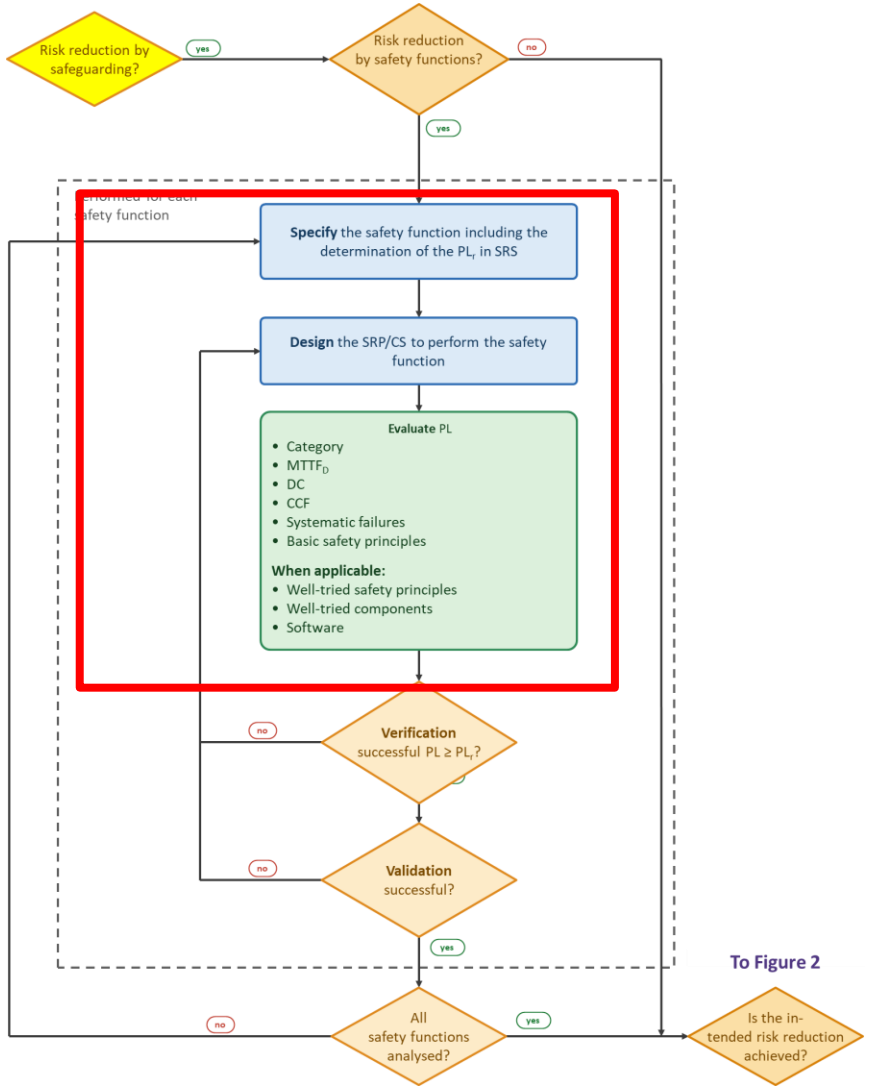
Safety Functions

- Safety function
  - Function of a machine whose failure can result in an immediate increase of the risk(s) (ISO 12100).
  - Part of the risk reduction process is to determine the safety functions of the machine. This will include the safety functions of the control system, e.g. prevention of unexpected start-up.
  - Machinery control systems provide operational and/or safety functions. Operational functions (e.g. starting, normal stopping) can also be safety functions, but this can be ascertained only after a complete risk assessment on the machinery has been carried out.

EVIDENTE

Risk Reduction by Safeguarding





EVIDENTE

ISO 13849 Performance levels PL

- Performance Level
  - Discrete level used to specify the ability of safety-related parts of control systems (SRP/CS) to perform a safety function.

PL	Average probability of dangerous failure per hour (PFH_D) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

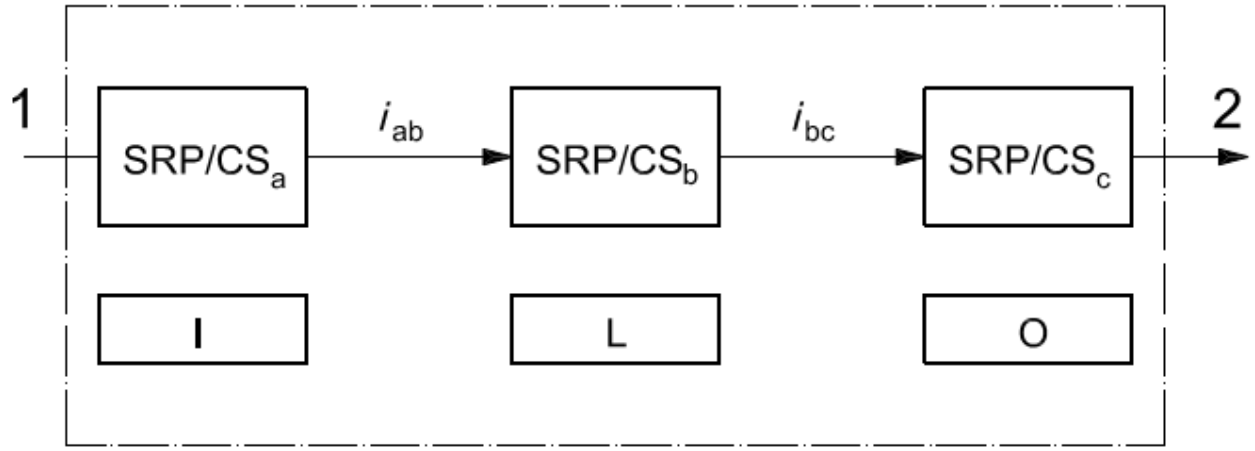
EVIDENTE

Evaluation of the achieved performance level PL

- The PL of the SRP/CS shall be determined by the estimation of the following aspects:
  - Quantifiable aspects
    - Mean time to dangerous failure (MTTFD) value for single components
    - Diagnostic coverage (DC)
    - Designated architectures Categories
    - Common cause failure (CCF)
  - Non-quantifiable, qualitative aspects
    - Behaviour of the safety function under fault condition(s)
    - Safety-related software
    - Systematic failure
    - Ability to perform a safety function under expected environmental conditions.

EVIDENTE

ISO 13849 Typical Safety Function Diagrammatic Presentation



Key

I input (e.g. limit switch, sensor, AOPD)

L logic

O output (e.g. valve, contactor, current converter)

1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)

2 machine actuator (e.g. motor, cylinder)

EVIDENTE

Mean time to dangerous failure (MTTFD)

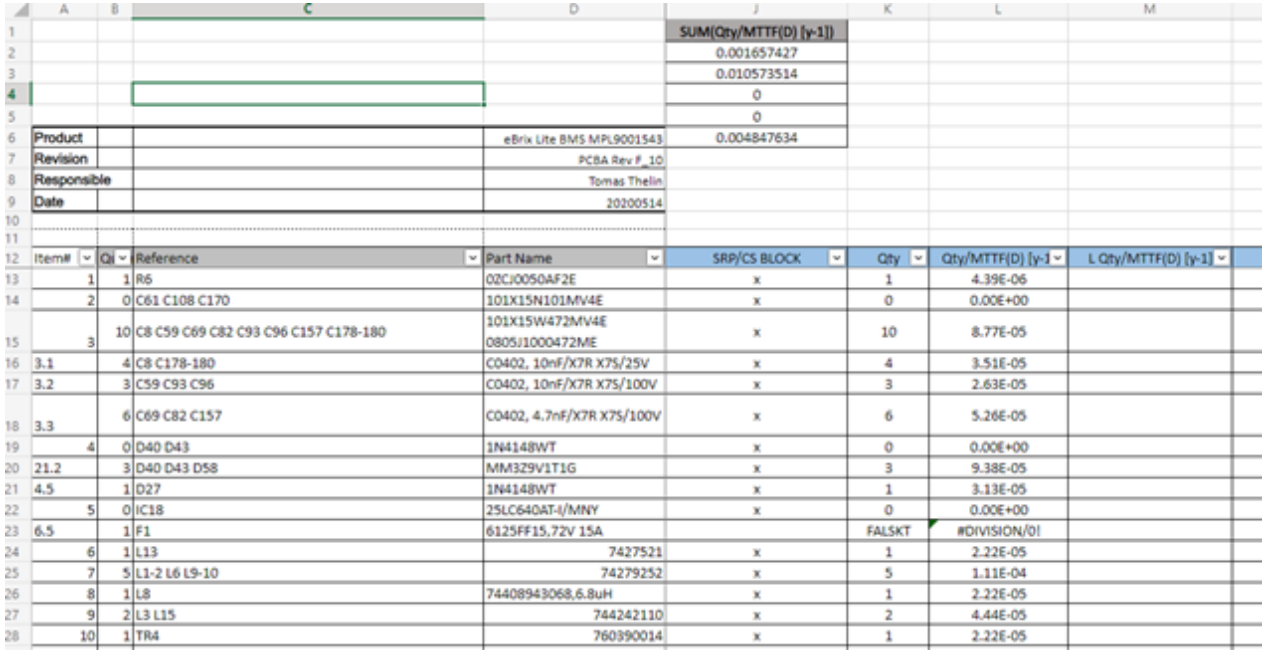
- The value of the MTTFD of each channel is given in three levels and shall be taken into account for each channel (e.g. single channel, each channel of a redundant system) individually.

$MTTF_D$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years

EVIDENTE

FMEDA

- The probability of failure of the SRP/CS can be calculated by considering all components and the probability of their fault modes. The analysis method is called Failure Modes, Effects and Diagnostics Analysis (FMEDA). This is similar to the FMEA used to determine the behaviour at fault, with the important difference that numeric values are included for the probability of failure of the components.
- FMEDA example for BMS MTTF_data_BMS.xlsx



	A	B	C	D	J	K	L	M
1					SUM(Qty/MTTF(D) [y-1])			
2					0.001657427			
3					0.010573514			
4					0			
5					0			
6	Product			eBrix Lite BMS MPL9001543	0.004847634			
7	Revision			PCBA Rev F_10				
8	Responsible			Tomas Thelin				
9	Date			20200514				
10								
11								
12	Item#	Qt	Reference	Part Name	SRP/CS BLOCK	Qty	Qty/MTTF(D) [y-1	L Qty/MTTF(D) [y-1]
13	1	1	R6	0ZCJ0050AF2E	x	1	4.39E-06	
14	2	0	C61 C108 C170	101X15N101MV4E	x	0	0.00E+00	
15	3	10	C8 C59 C69 C82 C93 C96 C157 C178-180	101X15W472MV4E 0805J1000472ME	x	10	8.77E-05	
16	3.1	4	C8 C178-180	C0402, 10nF/X7R X7S/25V	x	4	3.51E-05	
17	3.2	3	C59 C93 C96	C0402, 10nF/X7R X7S/100V	x	3	2.63E-05	
18	3.3	6	C69 C82 C157	C0402, 4.7nF/X7R X7S/100V	x	6	5.26E-05	
19	4	0	D40 D43	1N4148WT	x	0	0.00E+00	
20	21.2	3	D40 D43 D58	MM3Z9V1T1G	x	3	9.38E-05	
21	4.5	1	D27	1N4148WT	x	1	3.13E-05	
22	5	0	IC18	25LC640AT-I/MNY	x	0	0.00E+00	
23	6.5	1	F1	6125FF15.72V 15A		FALSKT	#DIVISION/0!	
24	6	1	L13	7427521	x	1	2.22E-05	
25	7	5	L1-2 L6 L9-10	74279252	x	5	1.11E-04	
26	8	1	L8	74408943068,6.8uH	x	1	2.22E-05	
27	9	2	L3 L15	744242110	x	2	4.44E-05	
28	10	1	TR4	760390014	x	1	2.22E-05	

EVIDENTE

Diagnostic coverage (DC)

- 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.

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

- Estimation of the average DC for whole SRP/CS

$$DC_{avg} = \frac{\sum_{n=1}^{k} \frac{DC_n}{MTTF_{d,n}}}{\sum_{n=1}^{k} \frac{1}{MTTF_{d,n}}}$$

EVIDENTE

Estimates for diagnostic coverage (DC) for functions and modules Input

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

EVIDENTE

Estimates for diagnostic coverage (DC) for functions and modules Logic

Measure	DC
Logic	
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508–2:2010, Tables A.2 to A.15.	
NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.	
NOTE 3 For measures where a DC range is given (e.g. fault detection by the process) the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt a FMEA should be the basis for the estimation of the DC.	

Measure	DC
Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic	90 %
Start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	90 % (depending on the testing technique)
Checking the monitoring device reaction capability (e.g. watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility	90 %
Dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99 %
Invariable memory: signature of one word (8 bit)	90 %
Invariable memory: signature of double word (16 bit)	99 %
Variable memory: RAM-test by use of redundant data e.g. flags, markers, constants, timers and cross comparison of these data	60 %
Variable memory: check for readability and write ability of used data memory cells	60 %
Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. “galpat” or “Abraham”)	99 %
Processing unit: self-test by software	60 % to 90 %
Processing unit: coded processing	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!

EVIDENTE

Estimates for diagnostic coverage (DC) for functions and modules Output

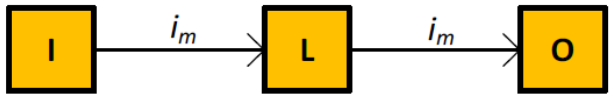
Measure	DC
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!

EVIDENTE

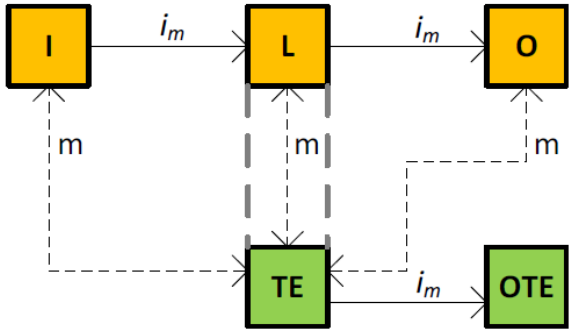
Designated Architectures and Categories

- The structure of a SRP/CS is a key characteristic having great influence on the PL.
- Even if the variety of possible structures is high, the basic concepts are often similar.
- Thus, most structures which are present in the machinery field can be mapped to one of the categories. For each category, a typical representation as a safety-related block diagram can be made.

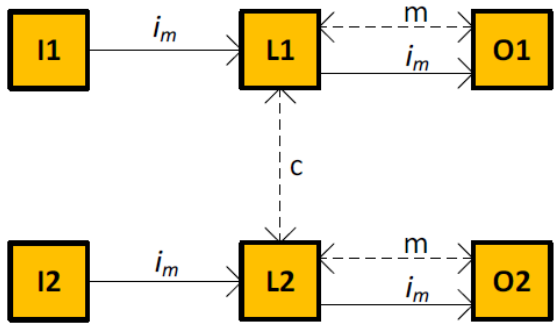
Category B and 1



Category 2

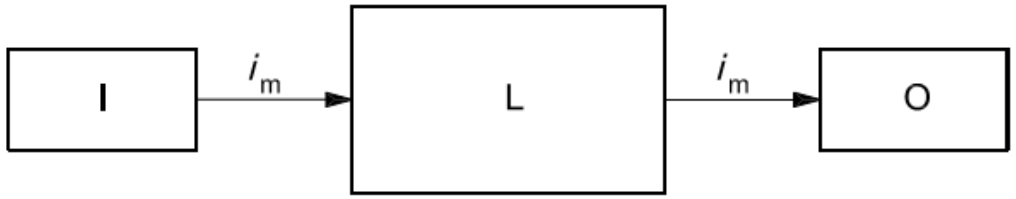


Category 3 and 4



EVIDENTE

ISO 13849 Category B



Key

i_m	interconnecting means
I	input device, e.g. sensor
L	logic
O	output device, e.g. main contactor

The $MTTF_D$ of the channel shall be at least low.

The maximum PL achievable with category B is PL b.

NOTE 1 There is no average diagnostic coverage (DCavg = none) within category B architectures. In such structures, the consideration of CCF is not relevant.

NOTE 2 When a fault occurs it can lead to the loss of the sub-function.

EVIDENTE

ISO 13849 Category 1

Only "well-tried components" are allowed

Key

i_m	interconnecting means
I	input device, e.g. sensor
L	logic
O	output device, e.g. main contactor

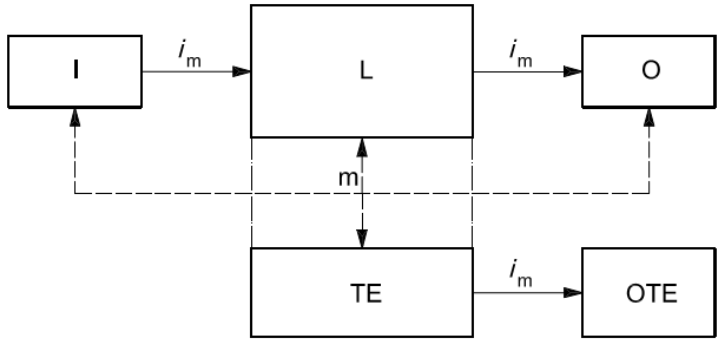
Subsystems of category 1 shall be designed and constructed using "well-tried components" and "well-tried safety principles".
The MTTFD of the channel shall be high.
The maximum PL achievable with category 1 is PL c.

NOTE 1: There is no average diagnostic coverage (DCavg = none) within category 1 architectures. In such structures (single-channel architectures) the consideration of CCF is not relevant.

NOTE 2: When a fault occurs it can lead to the loss of the safety function. However, the MTTFD of the single channel in category 1 is higher than in category B. Consequently, the loss of the safety function is less likely.

EVIDENTE

ISO 13849 Category 2



Key

i_m	interconnecting means
I	input device, e.g. sensor
L	logic
m	monitoring
O	output device, e.g. main contactor
TE	test equipment
OTE	output of TE

Dashed lines represent reasonably practicable fault detection.

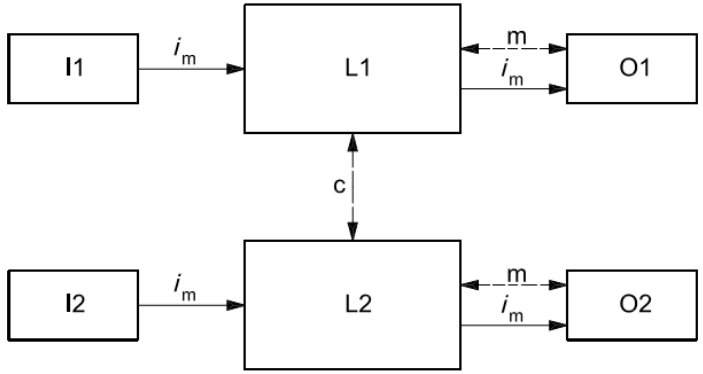
Subsystems of category 2 shall be designed so that their functional channel (I, L, O) is tested at suitable intervals. The test of the sub-function(s) shall be performed before or at least at the demand of the safety function prior to any hazardous situation. The test itself shall not lead to a hazardous situation (e.g. due to an increase in response time). The test equipment may be integral with, or separate from, the safety-related part(s) providing the safety function.

The DC of all parts of the functional channel (I, L, O) shall be at least low. The MTTFD of the functional channel shall be low-to-high, depending on the required performance level (PLr). Measures against CCF of the functional channel and the testing channel shall be applied.

The maximum PL achievable with category 2 is PL d.

EVIDENTE

ISO 13849 Category 3



Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O_2	output device, e.g. main contactor

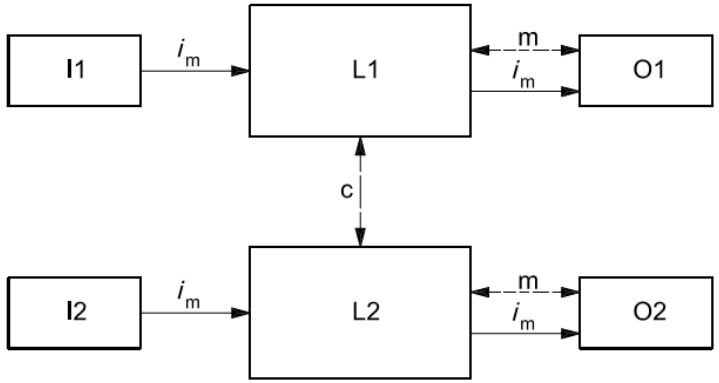
Dashed lines represent reasonably practicable fault detection.

Subsystems of category 3 shall be designed so that a single fault does not lead to the loss of the subfunction. Whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function.

The DC of the total subsystem shall be at least low. The MTTFD of each of the redundant channels shall be low-to-high, depending on the PLr. Measures against CCF shall be applied

EVIDENTE

ISO 13849 Category 4



Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O_2	output device, e.g. main contactor

Dashed lines represent reasonably practicable fault detection.

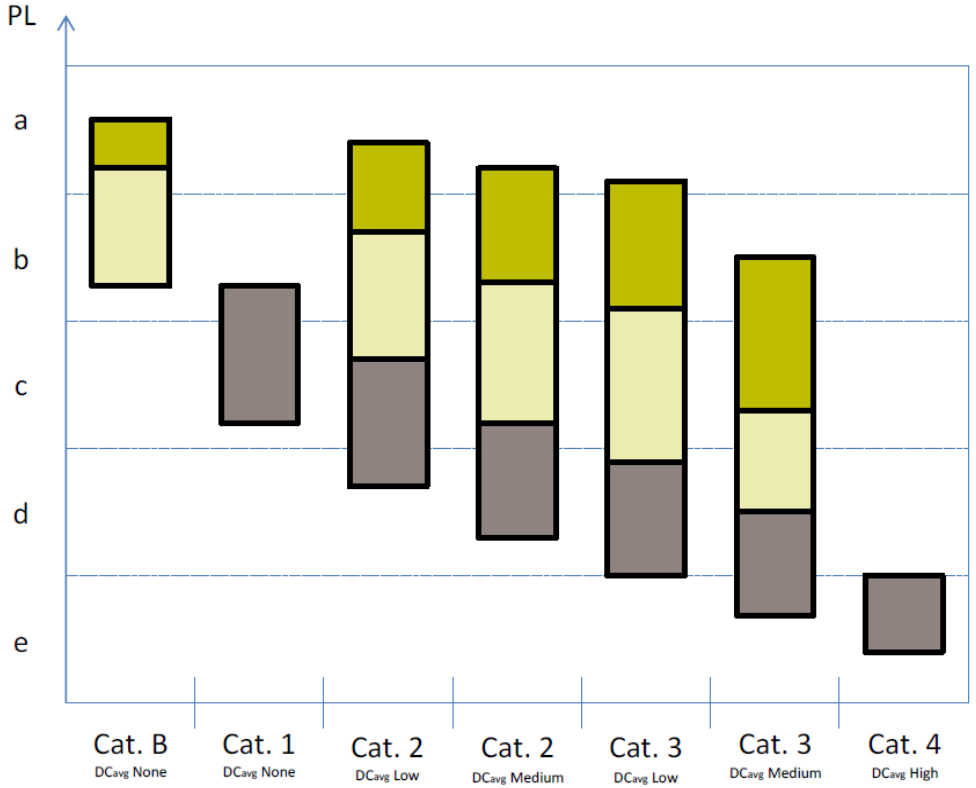
Subsystem of category 4 shall be designed such that

- a single fault does not lead to a loss of the safety function, and
- the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, or at the end of a machine operating cycle but if this detection is not possible, then an accumulation of undetected faults shall not lead to the loss of the safety function.

The average diagnostic coverage (DCavg) of the total subsystem shall be high. The MTTFD of each of the redundant channels shall be high. Measures against CCF shall be applied

EVIDENTE

Relationship between categories, DCavg, MTTFD of each channel and PL



Denotation	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

MTTF$_D$ = Low

MTTF$_D$ = Medium

MTTF$_D$ = High

Denotation of each channel	Range of each channel
Low	3 years ≤ MTTF$_D$ < 10 years
Medium	10 years ≤ MTTF$_D$ < 30 years
High	30 years ≤ MTTF$_D$ < 100 years

EVIDENTE

Common Cause Failure (CCF)

- ISO 13849 lists the measures and contains associated values, based on engineering judgement, which represent the contribution each measure makes in the reduction of common cause failures.
- A scoring process and quantification of measures against CCF are defined.
- Example:

No	Measure against CCF	Max score	Achieved score
1	Separation / segregation	15	15
2	Diversity	20	20
3.1	Design: Protection against overvoltage, current, etc.	15	15
3.2	Design: Components are well tried	5	0
4	Assessment / analysis	5	5
5	Competence / training	5	0
6.1	Environmental: EMC	25	25
6.2	Environmental: Other influences	10	10
	Total	100	90

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

EVIDENTE

Systematic Failures

The following measures should be applied:

- Use of de-energization
- Measures for controlling the effects of voltage breakdown, voltage variations, overvoltage, undervoltage
- Measures for controlling or avoiding the effects of the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference and its effects)
- Program sequence monitoring shall be used with SRP/CS containing software in order detect defective program sequences
- Measures for controlling the effects of errors and other effects arising from any data communication process
- Functional safety management: structured project management, documentation, configuration/change control and review

EVIDENTE

ISO 13849 Software safety lifecycle (FVL)

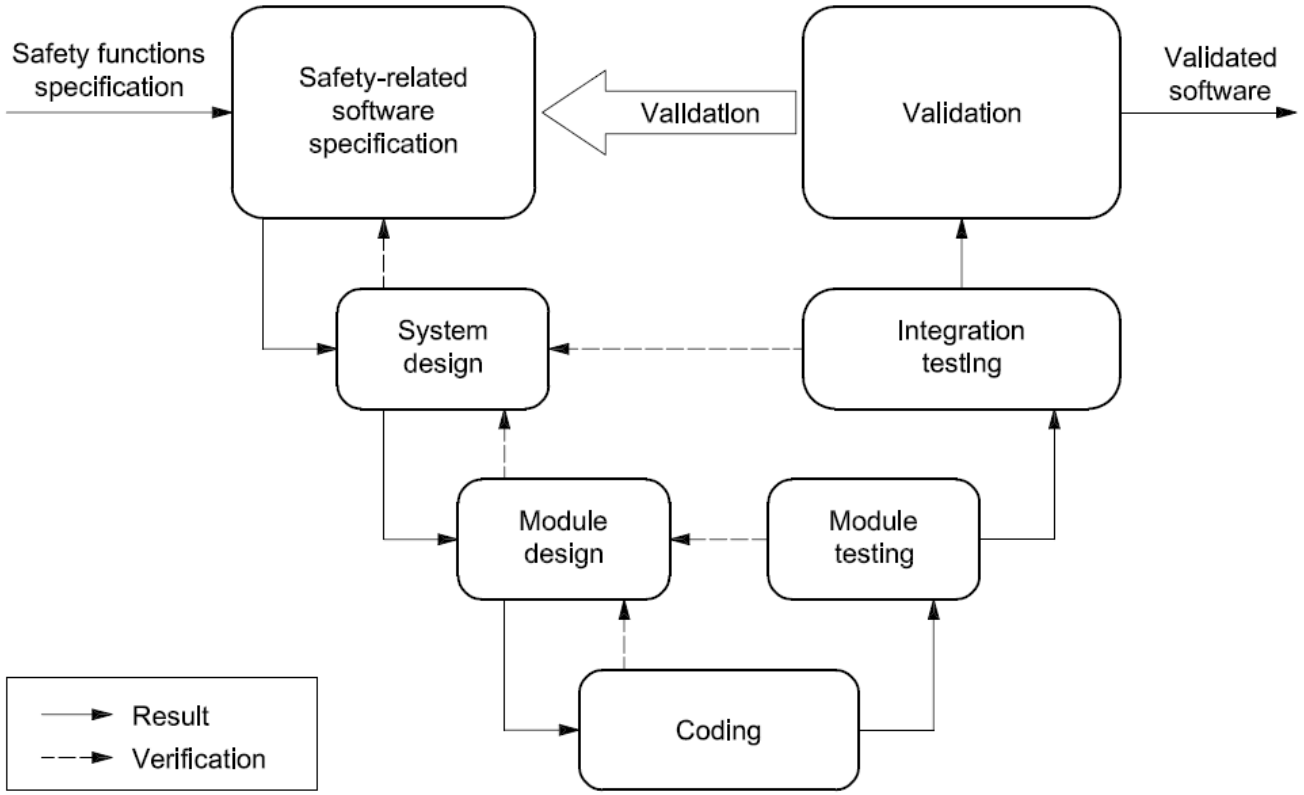
Different lifecycle requirements depending on

- Safety-related Application SW (SRASW)
- Safety-related Embedded SW (SRESW)

And the type of programming language

- Limited Variability Language (LVL)
- Full Variability Language (FVL)

Example of FVL SW development V-model



EVIDENTE

ISO 13849-1 Requirements on SW to reach PL_d

- Requirements for Safety-related embedded software (SRESW)
  - PL a-d
    - software safety lifecycle with verification and validation activities, see Figure 6;
    - documentation of specification and design;
    - modular and structured design and coding;
    - control of systematic failures (see G.2);
    - where using software-based measures for control of random hardware failures, verification of correct implementation;
    - functional testing, e.g. black box testing;
    - appropriate software safety lifecycle activities after modifications.
  - Additional requirements for PL c-d
    - project management and quality management system comparable to, e.g. IEC 61508 or ISO 9001;
    - documentation of all relevant activities during software safety lifecycle;
    - configuration management to identify all configuration items and documents related to a SRESW release;
    - structured specification with safety requirements and design;
    - use of suitable programming languages and computer-based tools with confidence from use;
    - modular and structured programming, separation from non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards;
    - coding verification by walk-through/review with control flow analysis;
    - extended functional testing, e.g. grey box testing, performance testing or simulation;
    - impact analysis and appropriate software safety lifecycle activities after modifications.

Parameterization (6.3.3)

- Parameterization shall be carried out using a dedicated software tool provided by the supplier of the SRP/CS. This tool shall have its own identification (name, version, etc.) and shall prevent unauthorized modification, for example, by use of a password.
  - The integrity of all data used for parameterization shall be maintained. This shall be achieved by applying measures to
    - control the range of valid inputs,
    - control data corruption before transmission,
    - control the effects of errors from the parameter transmission process,
    - control the effects of incomplete parameter transmission, and
    - control the effects of faults and failures of hardware and software of the tool used for parameterization.
    - control the effect of the interruption of the power supply
- Alternatively, a special procedure shall be used for setting the safety-related parameters. This procedure shall include confirmation of input parameters to the SRP/CS by either
  - retransmission of the modified parameters to the parameterization tool,
    or
  - other suitable means of confirming the integrity of the parameters.
  - as well as subsequent confirmation, e.g. by a suitably skilled person and by means of an automatic check by a parameterization tool.
- All parameterization must be documented in a traceable way regarding date, data-set version, name of the person who downloaded etc.

EVIDENTE

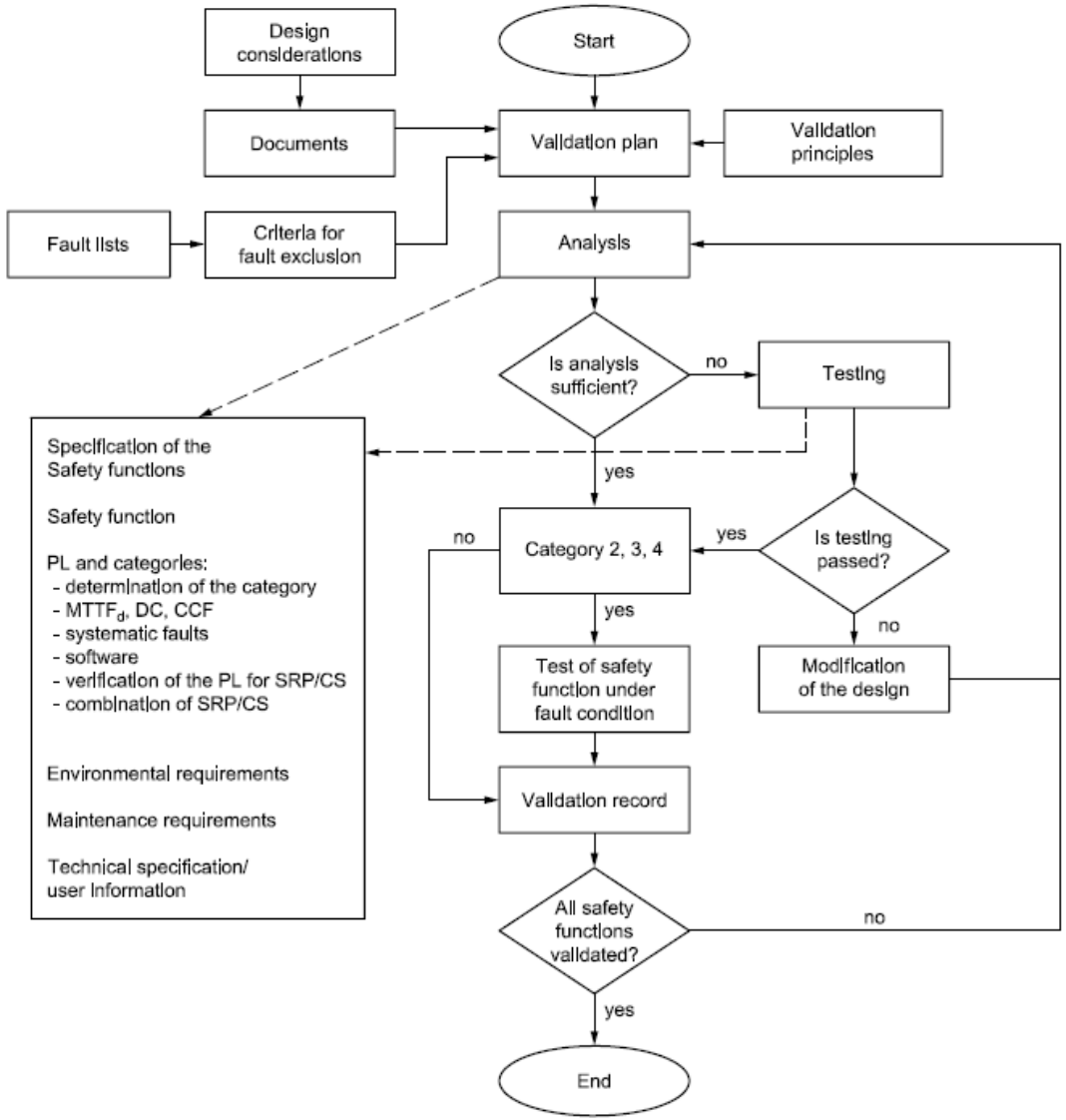
Technical Documentation ISO13849

When designing a SRP/CS, its designer shall document at least the following information relevant to the safety-related part:

- safety function(s) provided by the SRP/CS;
- the characteristics of each safety function;
- the exact points at which the safety-related part(s) start and end;
- environmental conditions;
- the performance level (PL);
- the category or categories selected;
- the parameters relevant to the reliability (MTTFD, DC, CCF and mission time);
- measures against systematic failure;
- the technology or technologies used;
- all safety-relevant faults considered;
- justification for fault exclusions (see ISO 13849-2);
- the design rationale (e.g. faults considered, faults excluded);
- software documentation;
- measures against reasonably foreseeable misuse.

EVIDENTE

Validation Process



EVIDENTE

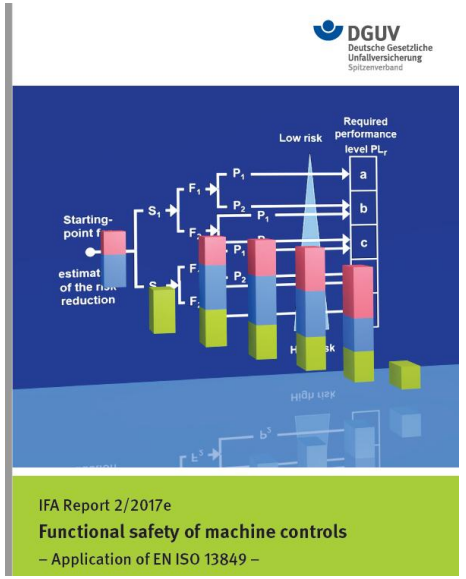
Information for use

- Information for all product lifcycles where SRP/CS is involved shall be provided to Integrator and User:
  - Intended use and limitations of the SRP/CS
  - Description of provided Safety Functions.
    - Operating limits
    - Response time
    - …
  - Interfaces
  - Maintenance information
  - Mission time
  - Test intervals
  - Parameterization, Programming, Setting

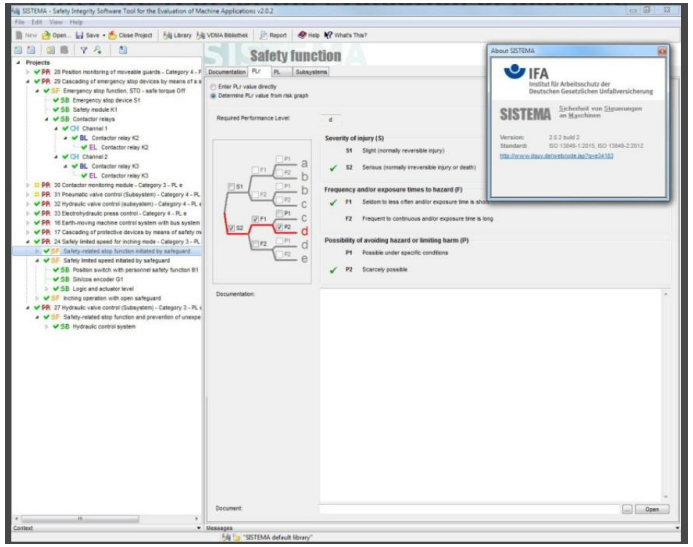
EVIDENTE

Guidelines and Tools

- IFA Report 2/2017e, "Functional safety of machine controls – Application of EN ISO 13849
  - Practical application of the standard
  - Explains the standard with examples.
  - Free to download



- SISTEMA
  - Safety Integrity Software Tool for the Evaluation of Machine Applications
  - A Tool for the Easy Application of the Control Standard EN ISO 13849-1
  - Free to download from IFA
  - A SISTEMA Cookbooks are also free to download



EVIDENTE

Testing

Area	Main Verification Activities	Evidence for Technical File
Machinery Directive	Risk assessment, interlock validation, emergency stop test, unexpected start-up test, guard inspection, PLr/PL validation	Risk register, SISTEMA/PL report, functional safety validation, guard/interlock test reports
Low Voltage Directive	Dielectric strength, leakage current, protective bonding, temperature rise, abnormal operation, X-ray shielding/leakage and interlock tests	Electrical safety report, radiation leakage report, markings/labels review, user manual safety review
EMC Directive	Conducted/radiated emissions, ESD, RF immunity, EFT/burst, surge, voltage dips/interruptions	Accredited EMC test report, test setup photos, configuration record, deviation/mitigation log

EVIDENTE

Technical File 1 (2)

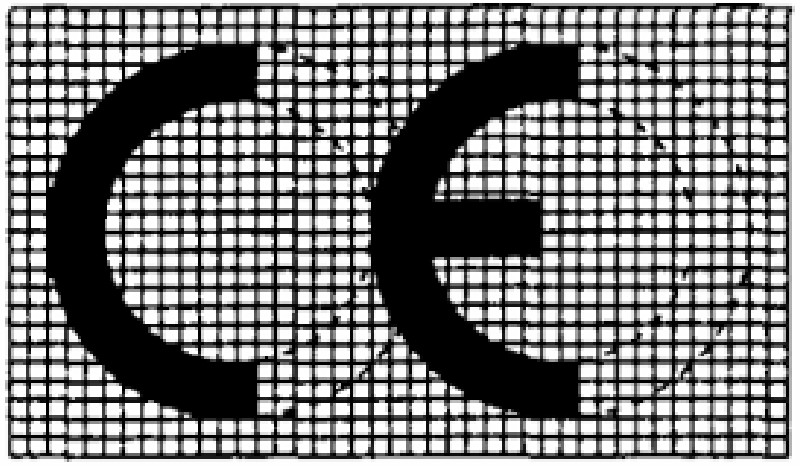
Area	Descriptions, Declarations, and Test Results
Product Description	• Describes the machinery, product variants, main functions, configuration, photos, nameplate information, and overall system architecture.
Intended Use and Operating Limits	• Defines intended users, use environment, sample types, operating limits, foreseeable misuse, installation constraints, and lifecycle assumptions.
Manufacturer Information	• Provides manufacturer name, address, responsible legal entity, contact details, and if applicable EU authorized representative or importer information.
Applicable Directives and Regulations	• Lists all EU legislation considered and applied, for example Machinery Directive, LVD, EMC, RoHS, WEEE, REACH, and RED if applicable.
Harmonized Standards Applied	• Lists the harmonized standards used to demonstrate conformity, including edition/version and whether applied fully or partially.
Risk Assessment and Risk Register	• Contains the EN ISO 12100 hazard identification, risk estimation, risk reduction measures, residual risk evaluation, and final risk register.
Functional Safety Documentation	• Documents safety functions requiring EN ISO 13849-1/-2 treatment, including PLr, achieved PL, SISTEMA calculations, validation results, and safety circuit design.
Design Drawings and Schematics	• Includes mechanical drawings, assembly drawings, enclosure drawings, shielding design, layout diagrams, and system block diagrams.
Electrical Design Documentation	• Contains electrical schematics, wiring diagrams, grounding/bonding concept, power distribution, insulation approach, circuit protection, and safety-related electrical design.
Bill of Materials (BoM)	• Lists key parts, components, assemblies, materials, suppliers, part numbers, revision levels, and safety/compliance relevance.

Technical File 2 (2)

Area	Descriptions, Declarations, and Test Results
Safety Components Documentation	• Collects documentation for safety-relevant components such as interlocks, emergency stops, safety relays, guard locks, key switches, and shielding-related parts.
Supplier Compliance Documentation	• Contains supplier Declarations of Conformity, Declarations of Incorporation, material declarations, RoHS/REACH declarations, certificates, and supplier test reports.
Test Plan and Test Reports	• Includes verification plan and evidence from electrical safety, EMC, radiation leakage, interlock validation, functional safety, guarding, and other compliance tests.
Software and Control System Documentation	• Describes operating software, safety-related control logic, software versions, access control, diagnostics, fault handling, and update/change control.
Instruction Manual / User Guide	• Provides the user-facing instructions for installation, operation, cleaning, maintenance, warnings, residual risks, emergency procedures, and disposal.
EU Declaration of Conformity	• Contains the signed legal declaration that the product complies with applicable CE directives and applied harmonized standards.
RoHS Compliance File	• Provides EN IEC 63000 documentation, supplier material declarations, BoM assessment, restricted substance evidence, exemptions if used, and RoHS DoC support.
WEEE Marking and Registration	• Documents the crossed-out wheeled bin marking, producer responsibility information, user disposal instructions, and national WEEE registration evidence if applicable.
REACH Statement / SCIP Documentation	• Contains REACH supplier declarations, SVHC assessment, Article 33 communication status, Annex XVII restriction check, and SCIP records if required.

Declaration of Conformity and CE marking

Area	What to Prepare	Key Points
EU Declaration of Conformity	Signed declaration covering all applicable CE directives	Include Machinery Directive, LVD, EMC, RoHS, and RED if applicable. WEEE and REACH are normally handled through separate compliance documentation rather than CE DoC.
CE Marking	Place the CE mark on the product or nameplate so it is easy to see, easy to read, and cannot easily be removed	CE mark may only be applied after conformity assessment is complete and DoC is signed.



EVIDENTE

Thanks for your attention!

EVIDENTE