HANDBOOK

Machine Safety

A practical, easy-to-follow guide for machine builders

- European Directives, Machine Directive
- Designing safe machines in three-steps
- Case studies: protection layouts for a safe, compliant and efficient machines
- Safety Products, ABB Jokab Safety

The design and engineering of machinery differs greatly from machine builder to machine builder; such customized work requires a creative partnership based on decades of experience in safe, production-friendly work environments. No matter how simple or complex the challenge, ABB can offer unique insights in order to develop a solution that best fits your needs. In this way, we work together on safe, smart and sustainable innovations that drive industry forward.

Content

Introduction
Company overview

ABB Jokab Safety has been helping machine builders to create production-friendly and safe work environments for operators since 1988.

We develop products and solutions for machine safety
We make it simple to build safety systems. Developing products and solutions for machine safety has been our business idea since the company Jokab Safety, now a part of ABB, was founded in Sweden in 1988.

Many industries around the world have discovered how much easier it has become to build protection and safety systems with our components and guidance. Our extensive program of products, safety solutions and our long experience in machine safety makes us a safe partner.

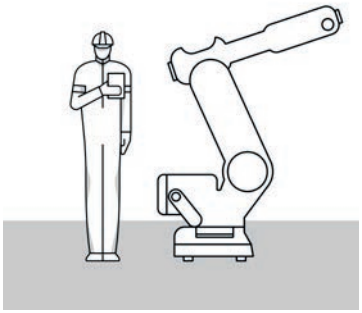
Together we create a safe world!

Introduction
Company overview

Products and systems
We deliver machine safety solutions for single machines or entire production lines. Our long experience of helping customers making solutions for demanding environments has made us experts in combining production demands with safety demands for production-friendly solutions.

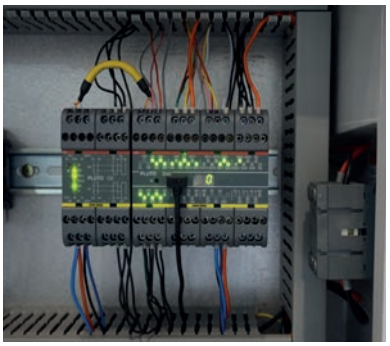
We market a wide range of safety products, which makes it easy to build safety systems. We develop these intelligent products continuously, in cooperation with our customers.

Our experience of safety requirements and standards
Directives and standards are very important to machine builders and safety component manufacturers. We represent Sweden in several international committees that develop standards, for e.g. industrial robots, safety distances and control system safety features. We work daily with the practical application of safety requirements in combination with production requirements. We are happy to share our knowledge of standards with our customers. You can use our experience for training and advice.



Markets and industries
Solutions from ABB Jokab Safety can be found in all types of industries across the globe. But we pride ourselves in having products and solutions that are especially well suited for e.g.:

- Robotics
- Food and beverage
- General machinery (OEM)



Our range of safety products

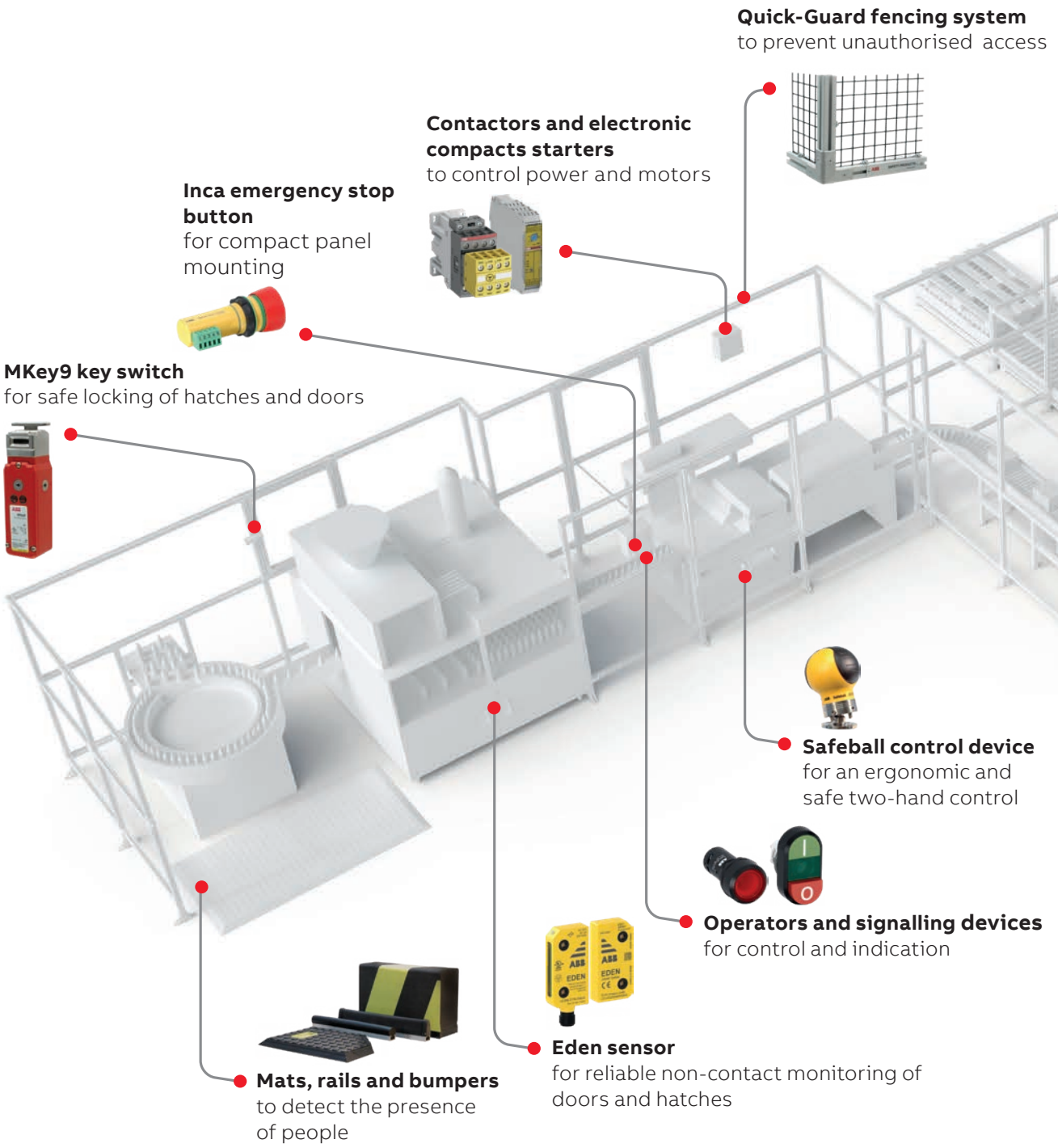


ABB is the only supplier that can deliver complete safety solutions (including output devices such as contactors and frequency converters) together with automation solutions such as robotics, motors, drives and PLCs.

Magne magnetic lock
to keep doors and hatches locked during a process

Pluto programmable safety controller, Vital safety controller, Sentry safety relays and B&R integrated safety technology
for flexible monitoring of safety devices

Smile emergency stop button
to safely stop machinery in hazardous situations

Orion light guards
for a production friendly safety detection

GKey safety lock
for safe locking of doors

JSHD4 three-position device
for safe and ergonomic inspection and troubleshooting

LineStrong pull wire emergency stop switch
for easy access of emergency stop function

European Directives and Standards

Directives and standards are of great importance for manufacturers of machines and safety components. In the European Union, the EU Directives gives requirements for the minimum level of health and safety, and these are mandatory for manufacturers to fulfill. In every member country the Directives are implemented in national legislation.

Machines which have been placed on the market since 2010, must comply with the new Machinery Directive 2006/42/EC. Before that, the old Machinery Directive 98/37/EC was valid.

Although the requirements in the Directives are specific for Europe, they also apply to machines that are imported to Europe. And the Directives are supported by standards, of which many also are valid internationally.

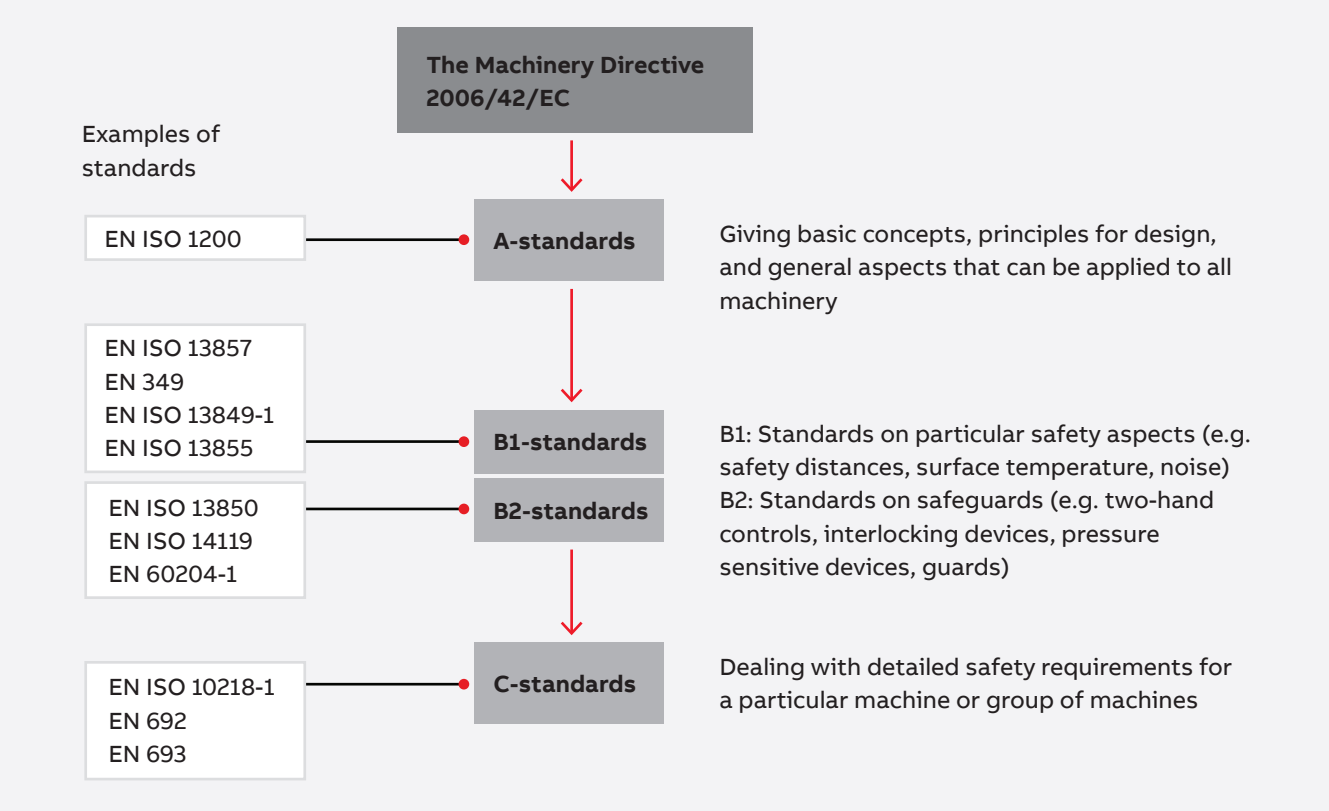
The objectives of the Machinery Directive, 2006/42/EC, are to maintain, increase and equalise the safety level of machines within the members of the European Community. Based on this, the free movement of machines/products between the countries in this market can be achieved. The Machinery Directive is developed according to "The New Approach" which is based on the following principles:

- The directives give the basic health and safety requirements, which are mandatory.
- Detailed solutions and technical specifications are found in harmonised standards.
- Standards are voluntary to apply, but products designed according to the harmonised standards will fulfill the basic safety requirements in the Machinery Directive.

Harmonised standards
Harmonised standards give support on how to fulfill the requirements of the Machinery Directive. The relationship between the Machinery Directive and the harmonised standards is illustrated by the diagram below.

Within ISO (The International Organization for Standardization) work is also going on in order to harmonise the safety standards globally in parallel with the European standard-isation work.

ABB Jokab Safety takes an active part in the working groups both for the ISO and EN standards.



Machinery Directive

The Machinery Directive, for machines and safety components

From 2006/42/EC

1 § This Directive applies to the following products:

a) machinery;
b) interchangeable equipment;
c) safety components;
d) lifting accessories;
e) chains, ropes and webbing;
f) removable mechanical transmission devices;
g) partly completed machinery.

The Machinery Directive gives a detailed definition of a machine, which can be simplified as something that has linked parts that are moving, where the energy source is not human effort. Two or more machines that are put together into a production line is also regarded as one machine.

CE-marking and Declaration of conformity

Machines manufactured or placed on the market from december 29, 2009, shall be CE-marked and fulfil the requirements according to the European Machinery Directive 2006/42/EC. This is also valid for old machines (manufactured before 1 January 1995) if they are manufactured in a country outside the EEA and imported to be used in a country in the EEA (European Economic Area).

For machines manufactured and/or released to the market between january 1, 1995, and december 28, 2009, the old Machinery Directive (98/37/EC) is valid.

NOTE!

Machines have to be accompanied by a Declaration of Conformity (according to 2006/42/EC, Annex II 1.A) that states which directive and standards the machine fulfills. It also shows if the product has gone through EC Type Examination.

Safety components have to be accompanied with a Declaration of Conformity.

CE

Requirements for the use of machinery

For a machine to be safe it is not enough that the manufacturer has been fulfilling all valid/necessary requirements. The user of the machine also has requirements to fulfill. For the use of machinery there is a Directive 2009/104/EC.

It requires that the work equipment that is provided to workers must comply with relevant Community directives.

This means that when repair/changes are made on the machine it shall still fulfill the requirements of the Machinery Directive. This doesn't have to mean that a new CE-marking is required (unless the changes are extensive).

NOTE!

This means that the buyer of a machine also has to make sure that a new machine fulfills the requirements in the directives. If the machine does not fulfill the requirements the buyer is not allowed to use it.

"Old" machines

For machines delivered or manufactured in the EEA before 1 January 1995 the following is valid.

From 2009/104/EC

b) work equipment which, if already provided to workers in the undertaking or establishment by 31 December 1992, complies with the minimum requirements laid down in Annex I no later than 4 years after that date;

c) without prejudice to point (a) (i), and by way of derogation from point (a) (ii) and point (b), specific work equipment subject to the requirements of point 3 of Annex I, which, if already provided to workers in the undertaking or establishment by 5 December 1998, complies with the minimum requirements laid down in Annex I, no later than 4 years after that date.

Annex I contains minimum requirements for health and safety. There can also be additional national specific requirements for certain machines.

NOTE!

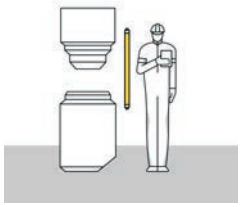
The point in time when the Machinery Directive was implemented in each Member Country varies. Therefore it is necessary to check with the national authorities in ones own country, to find out what is considered as "old" and respectively "new" machines.

Risk assessment

an important tool both when constructing a new machine and when assessing risks on older machines

"Old" machines

Machinery that is placed on the market or put into service before 1995 in the EEA.

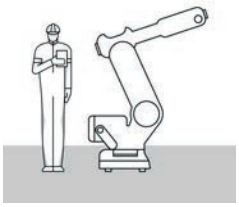


Use of work equipment
2009/104/EC

Possible national legislation on specific machines

"New" machines

1. Machinery that is placed on the market or put into service from 1995 in the EEA.
2. All machinery that are imported to the EEA irrespective of date of origin.



Use of work equipment
2009/104/EC
Note!
Not Annex 1 - instead use applicable directives.

The Machinery Directive
98/37/EC (1995 - 2009)
2006/42/EC (from 2010)

CE-marking + Declaration of conformity

EMC Directive
2014/30/EU

Low Voltage Directive
2014/35/EU

Possible more directives

Risk assessment
A well thought-out risk assessment supports manufacturers/users of machines to develop production friendly safety solutions. One result of this is that the safety components will not be a hindrance. This minimizes the risk of the safety system being defeated.

New machines
The following requirement is given by the Machinery Directive.

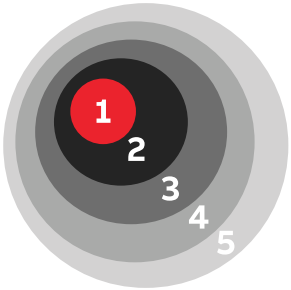
From 2006/42/EC
The manufacturer of machinery or his authorised representative must ensure that a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the risk assessment.

The standard EN ISO 12100 gives guidance on the information required to allow risk assessment to be carried out. The standard does not point out a specific method to be used. It is the responsibility of the manufacturer to select a suitable method.

Machines in use
A risk assessment must have been carried out on all machines that are in use; CE-marked as well as not CE-marked. A risk assessment must also be performed when making changes on a machine, to determine if the safety measures needs to be adapted.

Documentation of risk assessment
The risk assessment shall be documented. The risk assessment should take into consideration the severity of the potential injuries as well as the probability that they occur.

Protection or warning?
How is it possible to choose safety measures that are production friendly and in every way well balanced? The Machinery Directive gives an order of priority for the choice of appropriate methods to remove the risks. Here it is further developed in a five step method.



Prioritize safety measures according to the 5-step-method
1. Eliminate or reduce risks by design and construction
2. Move the work tasks outside the risk area
3. Use guards/safety devices
4. Develop safe working routines/information/education
5. Use warnings as pictograms, light, sound etc.

The further away from the center of the circle, the greater responsibility for the safety is placed onto the user of the machine. If full protection is not effectively achieved in one step, one has to go to the next step and find complementary measures.
What is possible is dependant on the need for accessibility, the severity of the risk, appropiate safety measures etc.

Example on prioritizing according to the 5-step-method

Priority	Example of hazard and safety measure taken	
1. Make machine safe by design and construction	Hazard: Safety measure:	Cuts and wounds from sharp edges and corners on machinery Round off sharp edges and corners
2. Move the work tasks outside the risk area	Hazard: Safety measure:	Crushing of fingers from machine movements during inspection of the production inside the risk area Installation of a camera
3. Use guard/safety devices	Hazard: Safety measure:	Crushing injuries because of unintended start during loading of work pieces in a mechanical press Install a light curtain to detect operator and provide safe stop of the machinery
4. Safe working routines/ information	Hazard: Safety measure:	Crushing injuries because the machine can tip during installation and normal use Make instructions on how the machine is to be installed to avoid the risks. This can include requirements on the type of fastening, ground, screw retention etc.
5. Warning	Hazard: Safety measure:	Burns because of hot surfaces in reach Warning signs

Combine the 5-step-method with production friendly thinking. This can give you e.g.
- fast and easy restart of machines after a safety stop
- enough space to safely program a robot
- places outside the risk area to observe the production
- electrically interlocked doors, instead of guards attached with screws, to be able to take the necessary measures for removing production disturbances
- a safety system that is practical for all types of work tasks, even when removing production disturbances

The likelihood that the safety solution will be well made, well received and suitable for the application increases if each risk is handled according to the 5-step-method.

Examples of regularly used EN/ISO standards

EN ISO 12100	Safety of machinery - General principles for design - Risk assessment and risk reduction	**The primary purpose of this standard is to provide designers with an overall framework and guidance for decisions during the development of machinery to enable them to design machines that are safe for their intended use.**
EN ISO 13857	Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs	**This standard establishes values for safety distances to prevent danger zones being reached by the upper and lower limbs. The distances apply when adequate safety can be achieved by distances alone.**
EN ISO 13854	Safety of machinery – Minimum gaps to avoid crushing of parts of the human body	**The object of this standard is to enable the user (e.g. standard makers, designers of machinery) to avoid hazards from crushing zones. It specifies minimum gaps relative to parts of the human body and is applicable when adequate safety can be achieved by this method.**
EN ISO 13850	Safety of machinery – Emergency stop – Principles for design	**This standard specifies design principles for emergency stop equipment for machinery. No account is taken of the nature of the energy source.**
ISO 13851	Safety of machinery – Two-hand control devices – Principles for design and selection	**This standard specifies the safety requirements of a two-hand control device and its logic unit. The standard describes the main characteristics of two-hand control devices for the achievement of safety and sets out combinations of functional characteristics for three types.**
EN ISO 14120	Safety of machinery – Guards – General requirements for the design and construction of fixed and movable guards	**This standard specifies general requirements for the design and construction of guards provided primarily to protect persons from mechanical hazards.**
EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design	**This standard provides safety requirements and guidance on the principles for the design of safety-related parts of control systems. For these parts it specifies categories and describes the characteristics of their safety functions. This includes programmable systems for all machinery and for related protective devices. It applies to all safety-related parts of control systems, regardless of the type of energy used, e.g. electrical, hydraulic, pneumatic, mechanical. It does not specify which safety functions and which categories shall be used in a particular case.**
EN ISO 13849-2	Safety of machinery - Safety-related parts of control systems - Part 2: Validation	**This standard specifies the procedures and conditions to be followed for the validation by analysis and testing of: • the safety functions provided, and • the category achieved of the safety-related parts of the control system in compliance with EN 954-1 (ISO 13849-1), using the design rationale provided by the designer.**
EN 62061	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	**The standard defines the safety requirements and guiding principles for the design of safety-related electrical/electronic/programmable parts of a control system.**
EN ISO 13855	Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body	**This standard provides parameters based on values for hand/arm and approach speeds and the methodology to determine the minimum distances from specific sensing or actuating devices of protective equipment to a danger zone.**
EN ISO 14119	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection	**This standard specifies principles for the design and selection — independent of the nature of the energy source — of interlocking devices associated with guards. The standard provides measures to minimize defeat of interlocking devices in a reasonably foreseeable manner.**
EN 60204-1	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	**This part of IEC 60204 provides requirements and recommendations relating to the electrical equipment of machines so as to promote: – safety of persons and property; – consistency of control response; – ease of maintenance.**

Standards for safety in control systems

Building a protection system that works in practice and provides sufficient safety requires expertise in several areas. The design of the safety functions in the protection system in order to ensure they provide sufficient reliability is a key ingredient. As help for this there is, for example, the EN ISO 13849-1 standard. The purpose of this text is to provide an introduction to the standard and its application in conjunction with our products. Please note that outside of the European Union there are often other standards that are used in place of EN ISO 13849.

Introducing the standard
The generation change for standards on safety in control systems introduced new concepts and calculations for machine builders and machine users. The EN 954-1 standard has been phased out and is replaced by EN ISO 13849-1 (PL, Performance Level) and EN 62061 (SIL, Safety Integrity Level).

PL or SIL? What should I use?
The standard you should use depends on the choice of technology, experience and customer requirements.

Choice of technology
– PL (Performance Level) is a technology-neutral concept that can be used for electrical, mechanical, pneumatic and hydraulic safety solutions.
– SIL (Safety Integrity Level) can, however, only be used for electrical, electronic or programmable safety solutions.

Experience
EN ISO 13849-1 uses categories from EN 954-1 for defining the system structure, and therefore the step to the new calculations is not so big if you have previous experience of the categories. EN 62061 defines the structures slightly differently.

Customer requirements
If you or your end customer comes from an industry that is accustomed to using SIL (e.g. the process industry), requirements can also include safety functions for machine safety being SIL rated.

We notice that most of our customers prefer PL as it is technology-neutral and that they can use their previous knowledge in the categories. In this text we show some examples of how to build safety solutions in accordance with EN ISO 13849-1 and calculate the reliability of the safety functions to be used for a particular machine. The examples in this text are simplified in order to provide an understanding of the principles. The values used in the examples can change.

What is PL (Performance Level)?
PL is a measure of the reliability of a safety function. PL is divided into five levels (a-e). PL e gives the best reliability and is equivalent to that required at the highest level of risk.

To calculate which PL level the system achieves you need to know the following:
– The system's structure (categories B, 1-4)
– The Mean Time To dangerous Failure of the component ($MTTF_d$)
– The system's Diagnostic Coverage (DC)

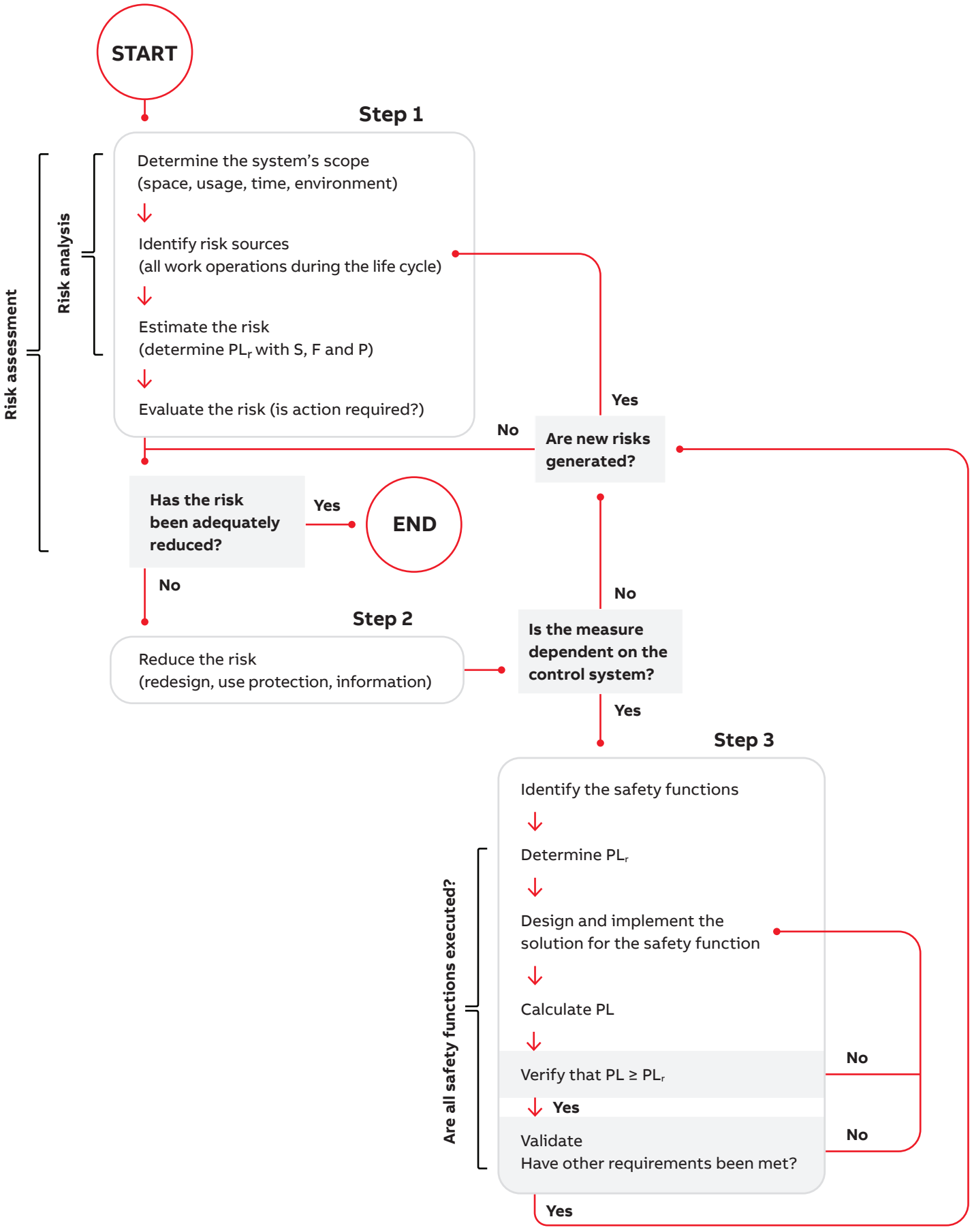
You will also need to:
– protect the system against simultaneous failure of both channels (CCF)
– protect the system from systematic errors built into the design
– follow certain rules to ensure software can be developed and validated in the right way

The five PL-levels (a-e) correspond to certain ranges of PFH_D-values (probability of dangerous failure per hour). These indicate how likely it is that a dangerous failure could occur over a period of one hour. In the calculation, it is beneficial to use PFH_D-values directly as the PL is a simplification that does not provide equally accurate results.

What is the easiest way of complying with the standard?
1. Use pre-calculated components.
As far as it is possible, use components with pre-calculated PL and PFH_D-values. You then minimise the number of calculations to be performed. All ABB Jokab Safety products have pre-calculated PFH_D-values.

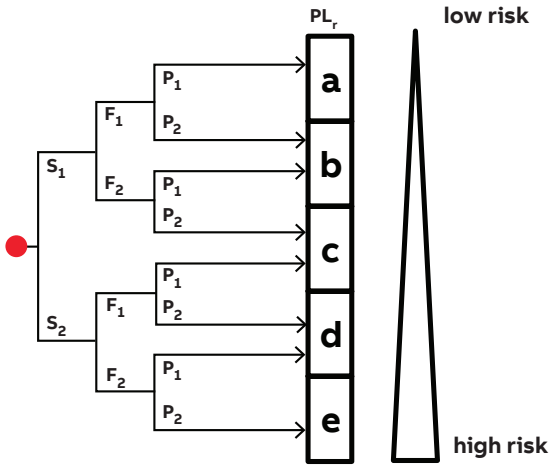
2. Use a calculation tool.
With the calculation softwares FSDT or SISTEMA you avoid making calculations by hand. You also get help to structure your safety solutions and provide the necessary documentation.

3. Use Pluto or Vital
Use the Pluto programmable safety controller or Vital safety controller. Not only is it easier to make calculations and changes in the future, but above all it is easier to ensure a higher level of safety.


START
Step 1
Determine the system's scope
(space, usage, time, environment)
Identify risk sources
(all work operations during the life cycle)
Estimate the risk
(determine PLr with S, F and P)
Evaluate the risk (is action required?)
Risk analysis
Risk assessment
Yes
No
Are new risks generated?
Has the risk been adequately reduced?
Yes
END
No
Step 2
Reduce the risk
(redesign, use protection, information)
No
Is the measure dependent on the control system?
Yes
Step 3
Identify the safety functions
Determine PLr
Design and implement the solution for the safety function
Calculate PL
Verify that PL ≥ PLr
No
Yes
Validate
Have other requirements been met?
No
Yes
Are all safety functions executed?

Risk estimation
To calculate the performance level required (PL_r).

S	**Severity of injury**
S1	slight (normally reversible injury)
S2	serious (normally irreversible 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	possible under specific conditions
P2	scarcely possible



Risk assessment and risk minimisation
According to the Machinery Directive, the machine builder (anyone who builds or modifies a machine) is required to perform a risk assessment for the machine design and also include an assessment of all the work operations that need to be performed. EN ISO 12100 stipulates the requirements for a risk assessment. It is this that EN ISO 13849-1 is based on, and a completed risk assessment is a prerequisite for being able to work with the standard.

Step 1 – Risk assessment
A risk assessment begins with determining the scope of the machine. This includes the space that the machine and its operators need for all of its intended applications, and all operational stages throughout the machine's life cycle.
All risk sources must then be identified for all work operations throughout the machine's life cycle.
A risk estimation is made for each risk source, i.e. indication of the degree of risk. According to EN ISO 13849-1 the risk is estimated using three factors: injury severity (S), frequency of exposure to the hazard (F) and the possibility you have of avoiding or limiting the injury (P). For each factor two options are given. Where the boundary between the two options lies is not specified in the standard, but the following are common interpretations and our recommendations:

S1	**bruises, abrasions, puncture wounds and minor crushing injuries**
S2	**skeletal injuries, amputations and death**
F1	**less frequent than once a week**
F2	**once a week or more often**
P1	**slow machine movements, plenty of space, low power**
P2	**quick machine movements, crowded, high power**

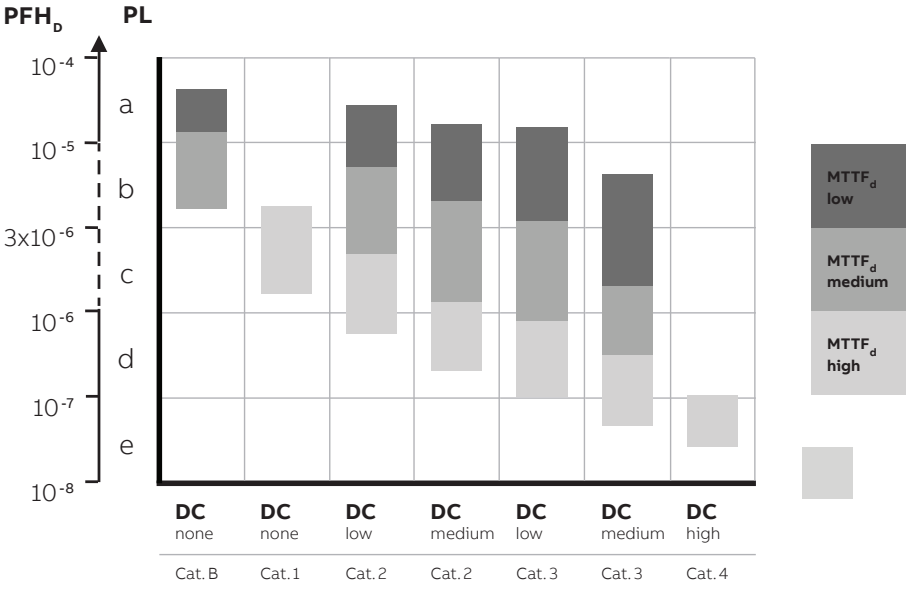
By selecting S, F and P for the risk, you will get the PL_r that is necessary for the risk source.
Finally, the risk assessment includes a risk evaluation where you determine if the risk needs to be reduced or if sufficient safety is ensured.

Step 2 – Reduce the risk
If you determine that risk reduction is required, you must comply with the priority in the Machinery Directive in the selection of measures:
1. Avoid the risk already at the design stage. (E.g. reduce power, avoid interference in the danger zone.)
2. Use protection and/or safety devices. (E.g. fences, light grids or control devices.)
3. Provide information about how the machine can be used safely. (E.g. in manuals and on signs.)

If risk reduction is performed using safety devices, the control system that monitors these needs to be designed as specified in EN ISO 13849-1.

Step 3 – Design and calculate the safety functions
To begin with you need to identify the safety functions on the machine. (Examples of safety functions are emergency stop and monitoring of gate.)

For each safety function, a PL_r should be established (which has often already been made in the risk assessment). The solution for the safety function is then designed and implemented. Once the design is complete, you can calculate the PL the safety function achieves. Check that the calculated PL is at least as high as PL_r and then validate the system as per the validation plan. The validation checks that the specification of the system is carried out correctly and that the design complies with the specification. You will also need to verify that the requirements that are not included in the calculation of the PL are satisfied, that is, ensure that the software is properly developed and validated, and that you have taken adequate steps to protect the technical solution from systematic errors.



The relationship between categories, the DC$_{avg}$, MTTF$_d$ for each channel and PL. The table also shows the PFH$_D$-range that corresponds to each PL.

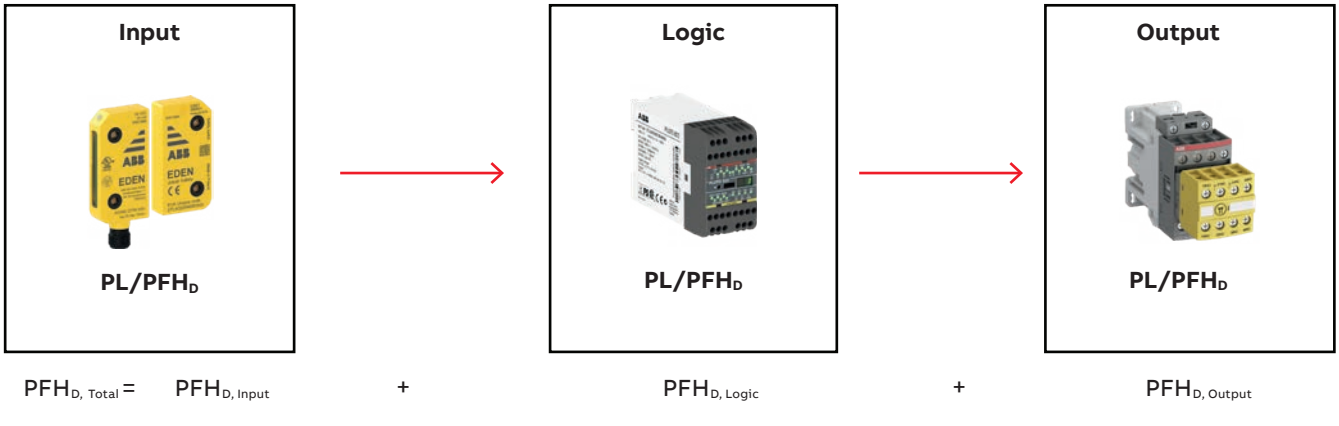
PL calculation in Step 3

When you calculate the PL for a safety function, it is easiest to split it into separate, well defined blocks (also called subsystems). It is often logical to make the breakdown according to input, logic and output (e.g. switch - safety relay - contactors), but there may be more or fewer than three blocks depending on the connection and the number of components used (an expansion relay could for example create an additional logic block).

For each block, you calculate a PL or PFH$_D$-value. It is easiest if you obtain these values from the component manufacturer, so you do not have to calculate yourself. The manufacturer of switches, sensors and logic devices often have PL and PFH$_D$-values for their components, but for mechanical devices (such as key switches or contactors) a PL-value cannot be supplied since it depends on how often the component will be used. You then need to calculate yourself according to EN ISO 13849-1 or use default values from the standard, if provided.

To calculate PL or PFH$_D$ for a block, you need to know its category, DC and MTTF$_d$. In addition, you need to protect the system against systematic errors and ensure that an error does not knock out both channels, and generate and validate any software used correctly. The following text gives a brief explanation of what to do.

Safety function (SF)



Category
The structure for the component(s) in the block is assessed to determine the category (B, 1-4) it corresponds to. For category 4, for example, individual failures do not result in any loss of the safety function.
In order to achieve category 4 with contactors, you need to have two channels - i.e., two contactors - that can cut the power to the machine individually. The contactors need to be monitored by connecting opening contacts to a test input on, for example a safety relay. For monitoring of this type to work, the contactors need to have positive-guided contacts.

Diagnostic Coverage (DC)
A simple method to determine DC is explained in Appendix E in EN ISO 13849-1. It lists various measures and what they correspond to in terms of DC. For example, DC=99 % (which corresponds to DC high) is achieved for a pair of contactors by monitoring the contactors with the logic device.

Mean Time To dangerous Failure ($MTTF_d$)
The $MTTF_d$-value should primarily come from the manufacturer. If the manufacturer cannot provide values, they are given from tables in EN ISO 13849-1 or you have to calculate $MTTF_d$ using the B_{10d}-value, (average number of cycles until 10% of the components have a dangerous failure). To calculate the $MTTF_d$, you also need to know the average number of cycles per year that the component will execute.

Calculation of the average number of cycles is as follows:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

where

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cycle}}$$

n_{op}	=	Number of cycles per year
d_{op}	=	Operation days per year
h_{op}	=	Operation hours per day
t_{cycle}	=	Cycle time (seconds)

Example: d_{op}= 365 days, h_{op}= 24 hours and t_{cycle}= 1,800 seconds (2 times/hour) which gives n_{op}= 17,520 cycles. With a B_{10d}=2·106 this gives a $MTTF_d$=1,141 year which corresponds to $MTTF_d$=high.
Note that when you calculate $MTTF_d$ you have to calculate according to the total number of cycles the component will be working. A typical example of this is the contactors that frequently work for several safety functions simultaneously. This means that you must add the number of estimated cycles per year from all the safety functions that use the contactors.

When $MTTF_d$ is calculated from a B_{10d}-value, also consider that if the $MTTF_d$-value is less than 200 years, the component needs to be replaced after 10% of the $MTTF_d$-value (due to the T_{10d}-value). That is, a component with $MTTF_d$ = 160 years needs to be replaced after 16 years in order for the conditions for achieving PL to continue to be valid. This is because EN ISO 13849-1 is based on a “mission time” of 20 years.

Common Cause Failure (CCF)
In Appendix F of EN ISO 13849-1 there is a table of actions to be taken to protect against CCF, to ensure a failure does not knock out both channels.

Systematic errors
Appendix G of EN ISO 13849-1 describes a range of actions that need to be taken to protect against incorporating faults into your design.

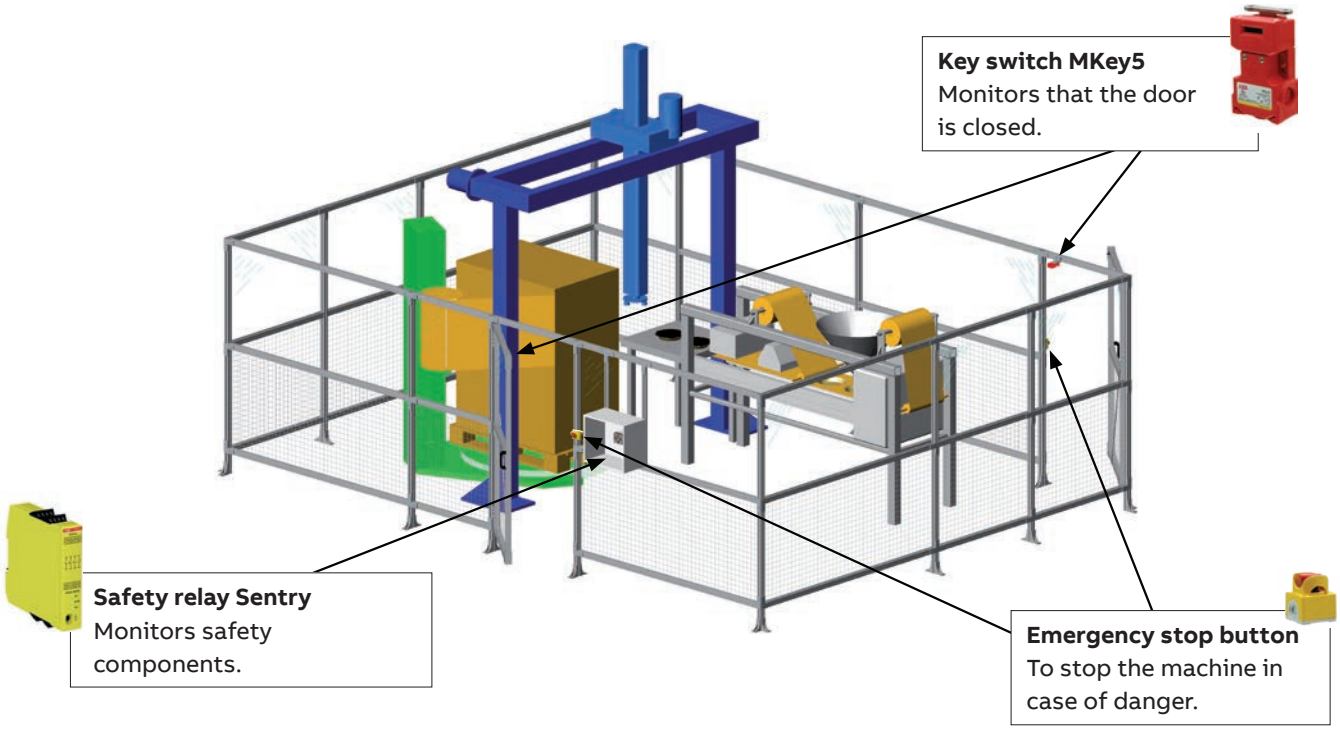
PL for safety functions
PL is given in the table on the previous page. If you want to use an exact PFH_D-value instead, this can be produced using a table in Appendix K in EN ISO 13849-1.
Once you have produced the PL for each block, you can generate a total PL for the safety function in Table 11 of EN ISO 13849-1. This gives a rough estimate of the PL. If you have calculated PFH_D for each block instead, you can get a total of PFH_D for the safety function by adding together all the values of the blocks. The safety function’s total PFH_D corresponds to a particular PL in Table 3 of EN ISO 13849-1.

Requirements for safety-related software
If you use a safety PLC for implementing safety functions, this places requirements on how the software is developed and validated. To avoid error conditions, the software should be readable, understandable and be possible to test and maintain.
A software specification must be prepared to ensure that you can check the functionality of the program. It is also important to divide the program into modules that can be tested individually. Paragraph 4.6 and Appendix J of EN ISO 13849-1 specify requirements for safety related software.
The following are examples of requirements for software from EN ISO 13849-1:

- A development life cycle must be produced with validation measures that indicate how and when the program should be validated, for example, following a change.
- The specification and design must be documented.
- Function tests must be performed.
- Validated functional blocks must be used whenever possible.
- Data and control flow are to be described using, for example, a condition diagram or software flow chart.

Case study 1 - Safety relay Sentry

Protection layout for a packaging machine with low risks

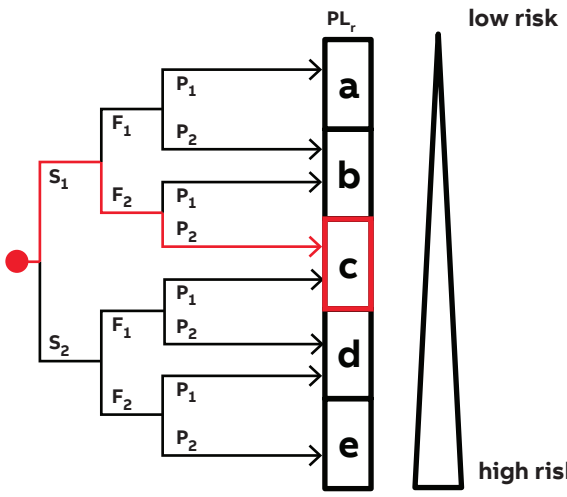


Step 1 – Risk assessment
Food to be packaged is loaded into the cell manually through the rear door. A batch is prepared for the packing conveyor in the infeed hopper. The cell is reset and restarted. The packaging machine with conveyor belt only operates when both doors are closed and when the protection system has been reset.

In the risk assessment it was established that the machine is to be operated in three shifts (8 hours per shift) 365 days a year. The total access to the danger zone is estimated to be two times per hour (F2), including manual packaging and tending operational disturbances. Unexpected start-ups are not considered to cause serious injury but rather minor healable injuries (S1). The operator is considered not to have the possibility of avoiding injury as the machine moves quickly (P2).

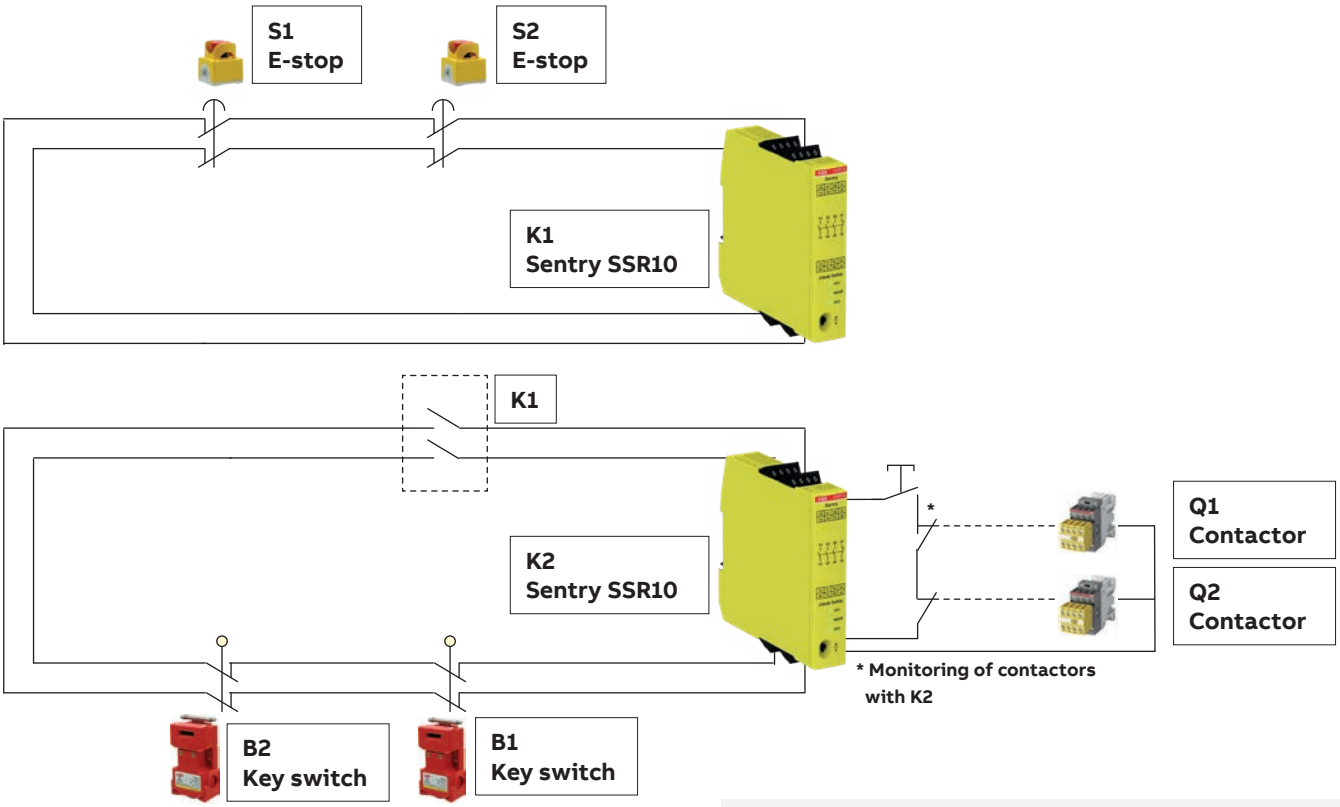
The number of cycles for the safety function = 365 days/year x (3x8) hours/day x 2 cycles/hour = 17,520 cycles/year
The assessment for the safety function required for access to the machine is PL_r= c (S1, F2, P2). In addition to this safety function, an emergency stop function is needed. This is also assessed as PL_r=c.

Step 2 – Reduce the risk
As protection, an interlocked door is selected with the key switch MKey5. Stopping time is short enough for the dangerous movement to have ceased before the operator can access it. The emergency stop is placed within easy reach, on both sides of the cell near the doors.



Determination of the PL_r necessary for the safety function with interlocked door for this example.

NOTE!
The assessment needs to be made for each safety function.



Step 3 – Calculate the safety functions

The output subsystem that is composed of double monitored contactors has been calculated at $2.47x10^{-8}$. The safety functions are represented by block diagrams.

Safety functions 1 and 2 are identical. Therefore, only safety function 1 is shown.

Safety functions 3 and 4 are identical. Therefore, only safety function 3 is shown.

How safe is a mechanical switch?

Mechanical switches have a tendency to break if misused. Manufacturer instructions must be followed, e.g. no excessive force or dirty environment. For interlocking switches in general EN ISO 14119 must be considered. It handles e.g. the possibility to defeat a switch and requirements on key switches. Connecting key switches in series gives a significant risk of masking errors, as stated in the technical report ISO/TR 24119, which limits the maximum achievable DC depending on the number of frequently used doors connected in series.

Safety function 1	Input	Logic	Output	Result
PL_r=c →	**B1** MKey5 (PL c) →	**K2** Sentry (PL e) →	**Q1/Q2** Contactors (PL e) →	**PL c**

$PFH_{D,\ MKey5} + PFH_{D,\ Sentry} + PFH_{D,\ Contactors} = 1.14x10^{-6} + 4.9x10^{-9} + 2.47x10^{-8} = 1.17x10^{-6}$ → PL c

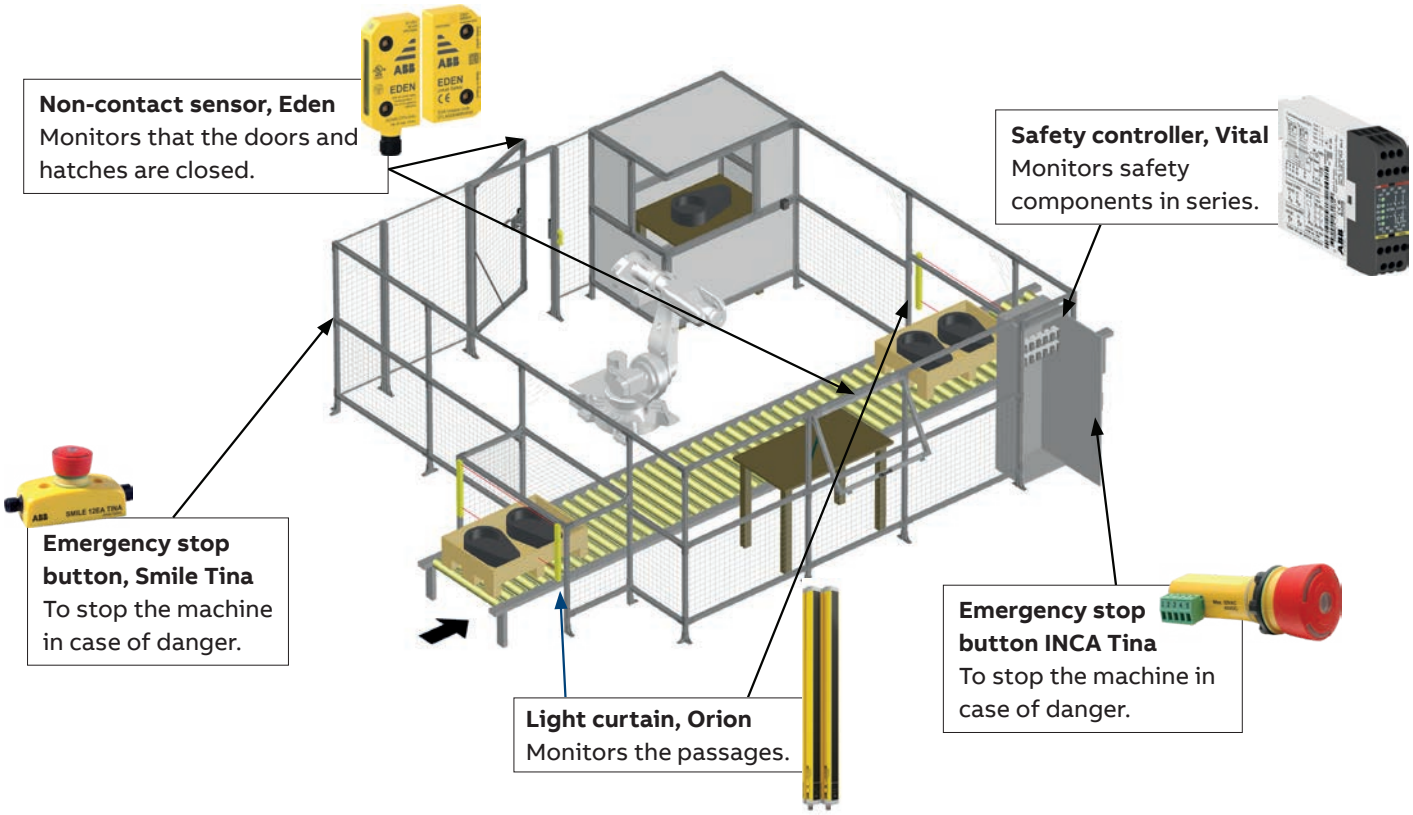
Safety function 3	Input	Logic	Logic	Output	Result
PL_r=c →	**S1** E-stop (PL e) →	**K1** Sentry (PL e) →	**K2** Sentry (PL e) →	**Q1/Q2** Contactors (PL e) →	**PL e**

$PFH_{D,\ E\text{-}stop} + PFH_{D,\ Sentry} + PFH_{D,\ Contactors} = 4.3x10^{-8} + 4.9x10^{-9} + 4.9x10^{-9} + 2.47x10^{-8} = 7.75x10^{-8}$ → PL e

The reason for not achieving more than PL c with Safety function 1 is that only one key switch is used per door, and a key switch is mechanically a Category 1 device. For e-stop devices though, a fault exclusion for the mechanical parts is allowed according to EN ISO 13849-2 if a maximum number of operations is considered. For this solution to reach a higher PL, EN ISO 14119 and ISO/TR 24119 need to be consulted.

Case study 2 - Safety controller Vital

Protection layout for a robot cell with high risks



Step 1 – Risk assessment

The workpieces are transported into the robot cell where the robot places them in a test cabinet. Approved work-pieces leave the cell on the conveyor belt, while workpieces that fail the tests are placed on the table for manual adjust-ments. The work that needs to be done in the robot cell is to correct operational disturbances for the test equipment and the conveyor belt (about once an hour), unloading from the manual station (about once an hour), program adjustments (once/week) and cleaning (once/week) (F2). Unexpected start-ups of the robot are considered to cause potentially serious injury (S2). The operator is considered not to have the possibility of avoiding injury as the robot moves quickly (P2). The risk estimation gives PLr=e (S2, F2, P2) for the safety functions required for access to the machine.

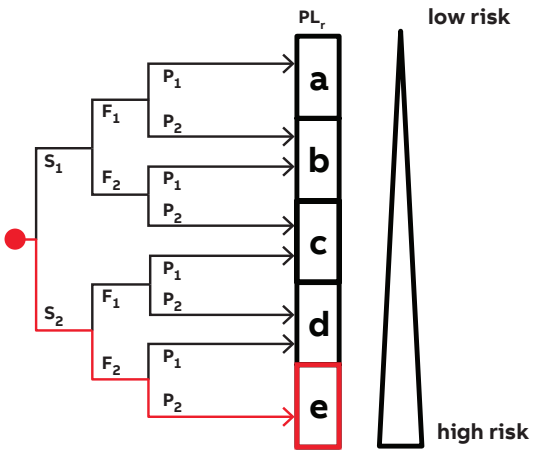
The standard for robot systems/cells (EN ISO 10218-2) speci-fies that safety functions shall comply with at least PL d, unless the risk assessment determines otherwise. In this case the risk assessment gives us PL_r= e.

Step 2 – Reduce the risk

As protection, the door and hatch are interlocked with Eden non-contact sensors. To protect against entering the cell the wrong way, transport of materials in and out is protected with light curtains and provided with muting to distinguish between material and people. The emergency stop function is also a safety function that is required.

The energy to all hazardous machine functions shall be removed by all safety functions.

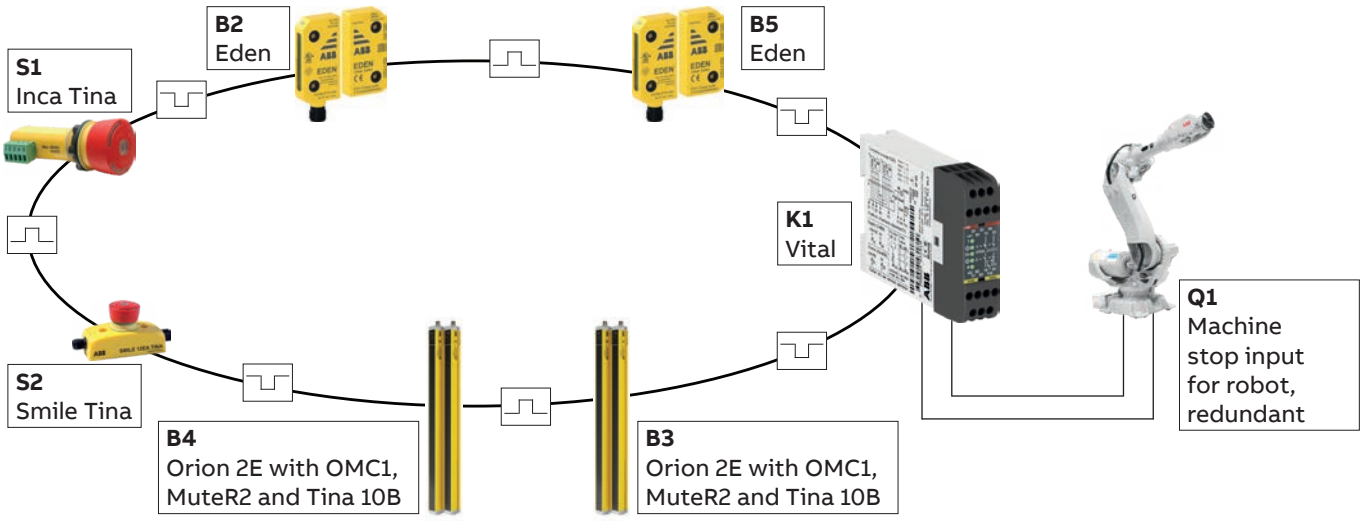
The solution with Vital makes it possible to implement a robot application with only one safety controller, which does not need to be configured or programmed. Vital makes it possible to connect up to 30 safety functions in a single DYNlink loop, with PL e in accordance with EN ISO 13849-1.



Determination of PLr for the safety function with interlocked door.

NOTE!

The assessment needs to be made for each safety function.



Step 3 – Calculate the safety functions
The PFH_D-value of the robot's safety stop input is $5.79x10^{-8}$ (the value applies to ABB industrial robots with IRC5 controller). The safety functions are represented by block diagrams.

Safety function 3 – muting of light guards
If the logic of the muting function is included in the light guard, the PFH_D-value of the light guard should include the PFH_D-values for the muting components. If the logic is external (i.e. safety PLC) the muting sensors should be added as separate blocks in the safety function.

Safety function 1

	Input	Logic	Output	Result
PL_r=e →	B1 Eden (PL e) →	K1 Vital (PL e) →	Q1 Robot (PL e) →	PL e

$PFH_{D, Eden} + PFH_{D, Vital} + PFH_{D, Robot} = 4.5x10^{-9} + 2.74x10^{-8} + 5.79x10^{-8} = 8.98x10^{-8}$ → PL e

Safety function 2

	Input	Logic	Output	Result
PL_r=e →	S2 Smile Tina (PL e) →	K1 Vital (PL e) →	Q1 Robot (PL e) →	PL e

$PFH_{D, Smile\ Tina} + PFH_{D, Vital} + PFH_{D, Robot} = 4.66x10^{-9} + 2.74x10^{-8} + 5.79x10^{-8} = 9.0x10^{-8}$ → PL e

Safety function 3

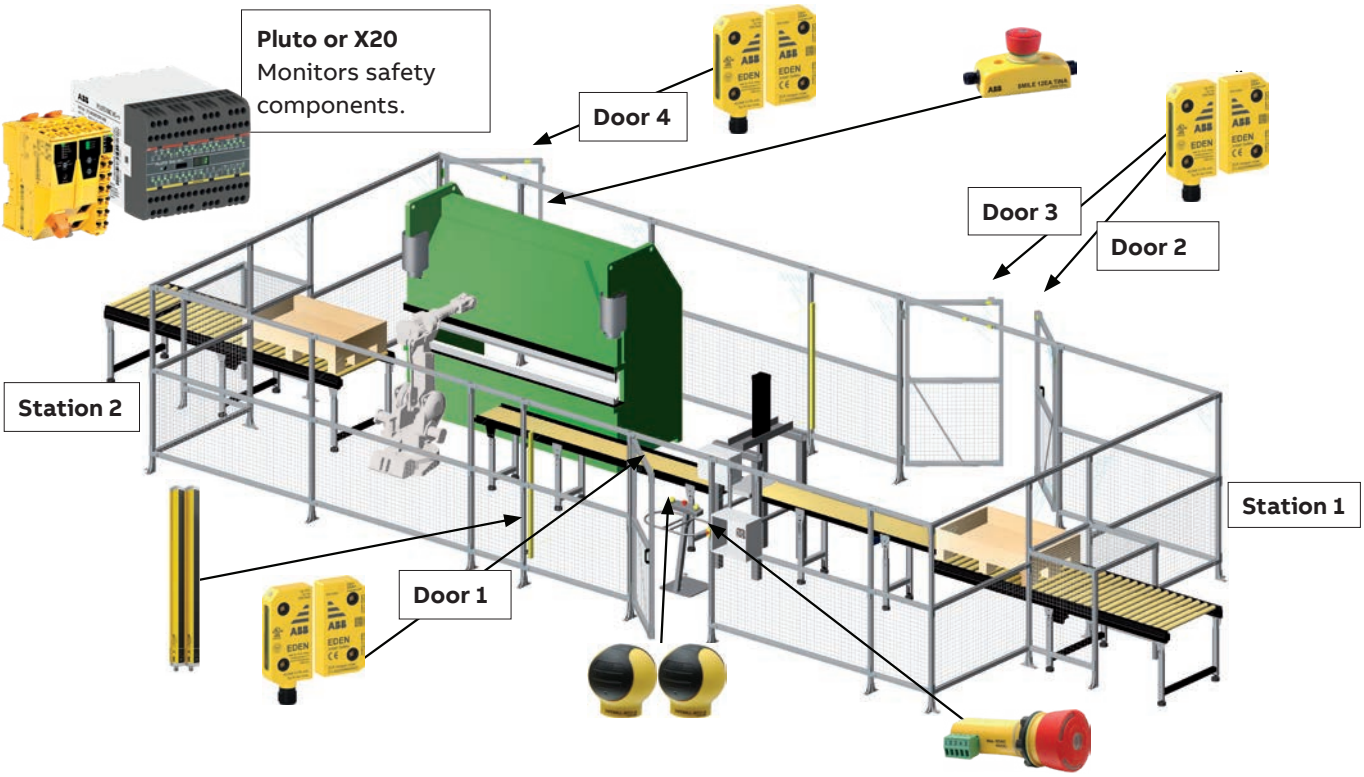
	Input		Logic	Output	Result
PL_r=e →	B3 Orion with muting (PL e) →	Tina 10B (PL e) →	K1 Vital (PL e) →	Q1 Robot (PL e) →	PL e

$PFH_{D, Orion} + PFH_{D, Tina\ 10} + PFH_{D, Vital} + PFH_{D, Robot} = 2.64x10^{-9} + 4.5x10^{-9} + 2.74x10^{-8} + 5.79x10^{-8} = 9.24x10^{-8}$ → PL e

These safety functions with Vital meet PL e in accordance with EN ISO 13849-1. Note that the above functions are only selected examples of the safety functions in the robot cell.

Case study 3 - Programmable safety controller Pluto or B&R X20 integrated safety technology

Protection layout for a production cell with high risks



Step 1 – Risk assessment

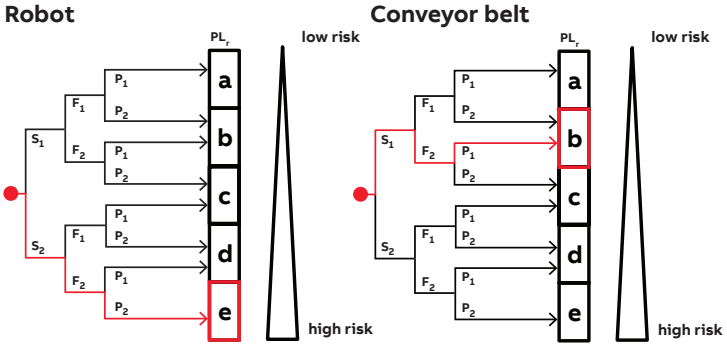
The workpieces are fed into the cell through a conveyor belt and positioned by the operator in the pneumatic machining tool in station 1. The operator starts station 1 manually. The operator then places the workpiece on the conveyor belt for transfer to station 2. A light curtain prevents the operator from entering station 2 unnoticed. The robot in station 2 places the workpiece in the hydraulic press. The workpiece leaves the cell by transport out onto the conveyor.

The work that needs to be done in station 2 is, e.g. to address operational disturbances in the press and the robot a few times a week (F2). Unexpected start-ups of the robot are considered to cause serious injury (S2). The operator is considered not to have the possibility of avoiding injury as the robot moves quickly (P2). The risk estimation for the safety function required for access to station 2 is PL_r=e (S2, F2, P2). This estimation would still be the same for the press. For the safety function for the risks associated with the conveyor belt, the estimation S1, F2, P1 is made giving PL_r= b.

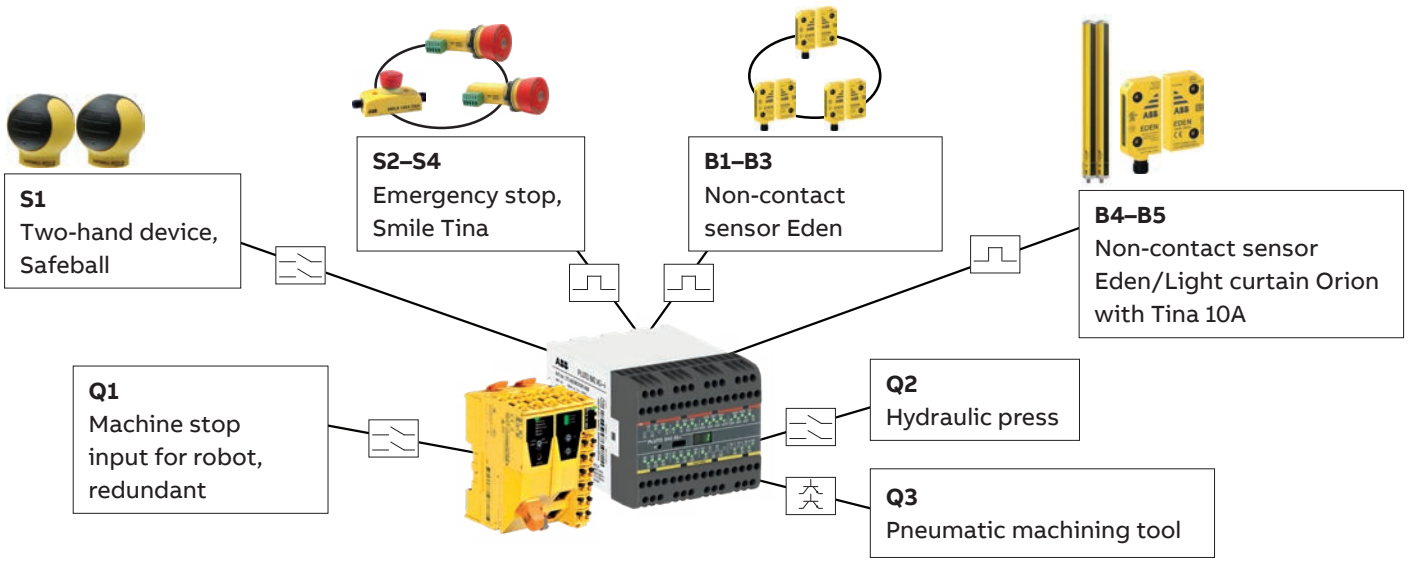
Step 2 – Reduce the risk

As protection, interlocked doors are selected with the Eden non-contact sensor. Station 1 with the pneumatic machining tool is operated by a two-hand device. When the two-hand device is released, the dangerous movement will be stopped safely. Station 2 can be in automatic mode, when a light curtain (Orion) and a non-contact sensor at door 4 (Eden) protects the entry. If the door is opened or the light curtain is interrupted, energy to the hazardous functions in station 2 is removed. By opening doors 2 and 3 (also monitored by Eden sensors) the conveyor belt and the pneumatic machining tool will stop safely. Manual reset must always be done after actuation of any safety device.

When the protection system requires a number of safety devices and that multiple machines must be stopped, Pluto programmable safety controller is the most effective solution. If the protection system also has to work by zones and in different modes of operation, this is another good reason to use Pluto. With Pluto, PL e can be achieved regardless of the number of connected safety devices. Or choose for an integrated safety solution from B&R.



PL_r= e for the robot and hydraulic press. PL_r=b for the conveyor belt.



Step 3 – Calculate the safety functions for the robot cell
The PFH_D-value for the robot's safety stop input is $5.79x10^{-8}$ (the value applies to ABB industrial robots with IRC5 controller).

Only safety functions to help remove energy to the industrial robot are shown below. This is only a subset of the safety functions. When energy is removed to multiple machines in a cell, the safety functions can be defined in different ways depending on the risk assessment. The safety functions are represented by block diagrams.

Safety function 1

	Input	Logic	Output	Result
PL_r=e →	**B1** Eden (PL e) →	**K1** Pluto, relay outputs (PL e) →	**Q1** Robot (PL e) →	**PL e**

$PFH_{D, Eden} + PFH_{D, Pluto} + PFH_{D, Robot} = 4.5x10^{-9} + 2x10^{-9} + 5.79x10^{-8} = 6.44x10^{-8}$ → PL e

Safety function 2

	Input	Logic	Output	Result
PL_r=e →	**S2** Smile Tina (PL e) →	**K1** Pluto, relay outputs (PL e) →	**Q1** Robot (PL e) →	**PL e**

$PFH_{D, Smile\ Tina} + PFH_{D, Pluto} + PFH_{D, Robot} = 4.66x10^{-9} + 2x10^{-9} + 5.79x10^{-8} = 6.46x10^{-8}$ → PL e

Safety function 3

	Input		Logic	Output	Result
PL_r=e →	**B5** Orion (PL e) →	Tina 10A (PL e) →	**K1** Pluto, relay outputs (PL e) →	**Q1** Robot (PL e) →	**PL e**

$PFH_{D, Orion} + PFH_{D, Tina\ 10} + PFH_{D, Pluto} + PFH_{D, Robot} = 2.5x10^{-9} + 4.5x10^{-9} + 2x10^{-9} + 5.79x10^{-8} = 6.69x10^{-8}$ → PL e

These safety functions with Pluto meet PL e in accordance with EN ISO 13849-1. Note that the above functions are only selected examples of the safety functions in the robot cell.

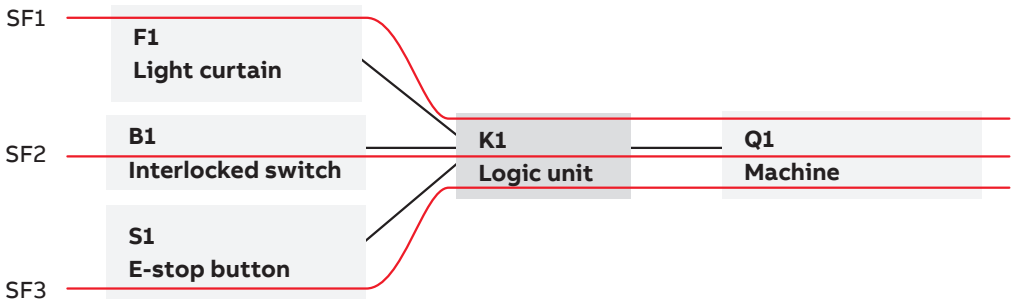
What defines a safety function?

Calculating that you have achieved the PL_r that is required is not difficult, especially if you use "pre-calculated" safety devices and logic units. But which parts should be included in each safety function?
This must be resolved before you start the calculations. To summarise in simple terms you can say that each safety device should be a part of the safety function for each machine that is affected by the safety device in question. Three safety devices that all remove the energy to three machines in a cell is therefore equal to nine safety functions. In the section that follows, we explain the background.

Multiple safety functions for a machine

Multiple safety devices are often used on a machine in order to provide satisfactory and practical protection for the operators. In the following example, a machine is protected by three safety devices connected to a logic device. The following figure illustrates this interconnection schematically.

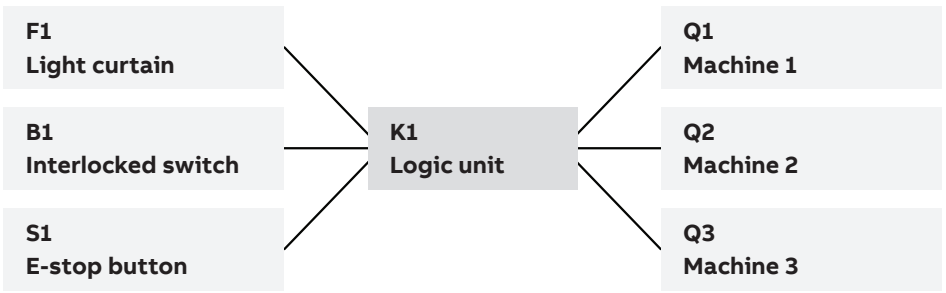
Three safety functions (SF) are defined for the machine and are calculated as:
SF1: $PFH_{D,\,F1} + PFH_{D,\,K1} + PFH_{D,\,Q1} = PFH_{D,\,SF1}$
SF2: $PFH_{D,\,B1} + PFH_{D,\,K1} + PFH_{D,\,Q1} = PFH_{D,\,SF2}$
SF3: $PFH_{D,\,S1} + PFH_{D,\,K1} + PFH_{D,\,Q1} = PFH_{D,\,SF3}$



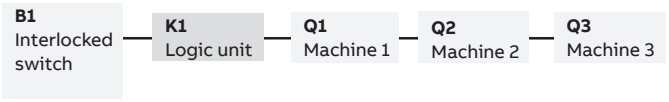
Multiple safety functions for multiple machines in a cell

It is quite common for several machines in a single cell/zone to be protected by multiple safety devices. The following figure illustrates the interconnection schematically for an example. Each of the machines Q1 – Q3 is shut down separately and independently by K1.

If the operator enters the cell, he is exposed in this case to the same type of risk from all three machines. The power to all three machines must be cut e.g. when the operator enters the cell through the door interlocked by B1.



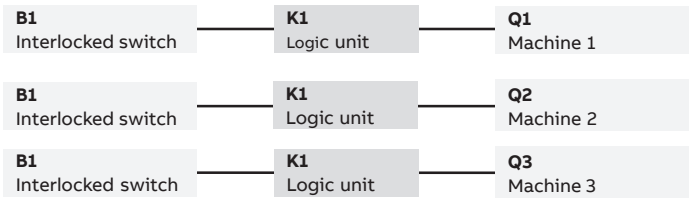
Theoretical approach for multiple machines
The theoretical approach to calculate the safety function is as follows:



For the full safety function to be performed you require all the components to be working. Note that if B1 or K1 has a dangerous malfunction, the entire safety function is disabled. However, if for example machine Q1 has a dangerous malfunction, and is not shut down, machines Q2 and Q3 will still be shut down. One disadvantage in considering the safety function in this way is that you may have trouble achieving the PL_r required. But if you achieve the PL_r required, you can use the theoretical approach.

Sources:
http://www.dguv.de/medien/ifa/en/pra/en13849/safety_functions.pdf

Practical approach for multiple machines
A more practical approach is to divide the safety function into three parts, one for each of the three machines.



This is an approach that can provide a more accurate way of looking at the safety functions, especially where a different PL_r is required for the safety functions above. If machine Q1 is a robot and machine Q2 is a conveyor which is designed to have negligible risks, the different PL_r required to protect against risks from Q1 and Q2 will also be different. This practical approach is therefore the one recommended. The interpretation is based on information provided by IFA (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung). For more information on this and other issues, see Sources.

Example of safety functions for multiple machines in a cell
For a cell with three machines (one robot, one hydraulic press and one pneumatic machining tool) a risk assessment is made resulting in different PL_r for the individual machines. The robot and the hydraulic press requires PL_r = e, while the pneumatic machining tool requires PL_r = d.
One of the safety functions is that a non-contact sensor. (Eden) supervised by a safety PLC (Pluto) shall disconnect the energy to all three machines in the hazard zone:

- Eden B1 ($PFH_{D, B1} = 4.5x10^{-9}$)
- Pluto K1 ($PFH_{D, K1} = 2x10^{-9}$)
- Robot Q1 ($PFH_{D, Q1} = 5.79x10^{-8}$)
- Hydraulic press Q2 ($PFH_{D, Q2} = 8x10^{-8}$)
- Pneumatic machining tool Q3 ($PFH_{D, Q3} = 2x10^{-7}$).

Practical approach
If you use the practical approach the safety functions are as follows:
Robot:
$PFH_{D, B1} + PFH_{D, K1} + PFH_{D, Q1} = 4.5x10^{-9} + 2•10^{-9} + 5.79x10^{-8} = 6.44x10^{-8} \longrightarrow$ PL e
Hydraulic press:
$PFH_{D, B1} + PFH_{D, K1} + PFH_{D, Q2} = 4.5x10^{-9} + 2•10^{-9} + 8x10^{-8} = 8.65x10^{-8} \longrightarrow$ PL e
Pneumatic machining tool:
$PFH_{D, B1} + PFH_{D, K1} + PFH_{D, Q3} = 4.5x10^{-9} + 2x10^{-9} + 2x10^{-7} = 2.07x10^{-7} \longrightarrow$ PL d
This is to be done in a similar way with other safety functions for the cell. For each safety device, you define the machines it affects, and establish the various safety functions according to this.

Theoretical approach
What would the result be using the theoretical approach? Would the safety function achieve PL e?
All machines:
$PFH_{D, B1} + PFH_{D, K1} + PFH_{D, Q1} + PFH_{D, Q2} + PFH_{D, Q3}$
$= 4.5x10^{-9} + 2x10^{-9} + 5.79x10\text{-}8 + 8x10^{-8} + 2x10^{-7} = 3.44x10^{-7} \longrightarrow$ PL d
In this case, the safety function would not achieve a total PL e, which was required for the risks associated with the robot and hydraulic press.

Conclusions

- Use the practical approach for multiple machines.
- Use safety devices/logic units with high reliability (low PFH_D) to make it easy to achieve the PL_r required.
- With Vital or Pluto, it is easier to achieve the PL_r required.

Please note that the examples on these pages are simplified in order to explain the principles. Values of products can also change.

FSDT and SISTEMA

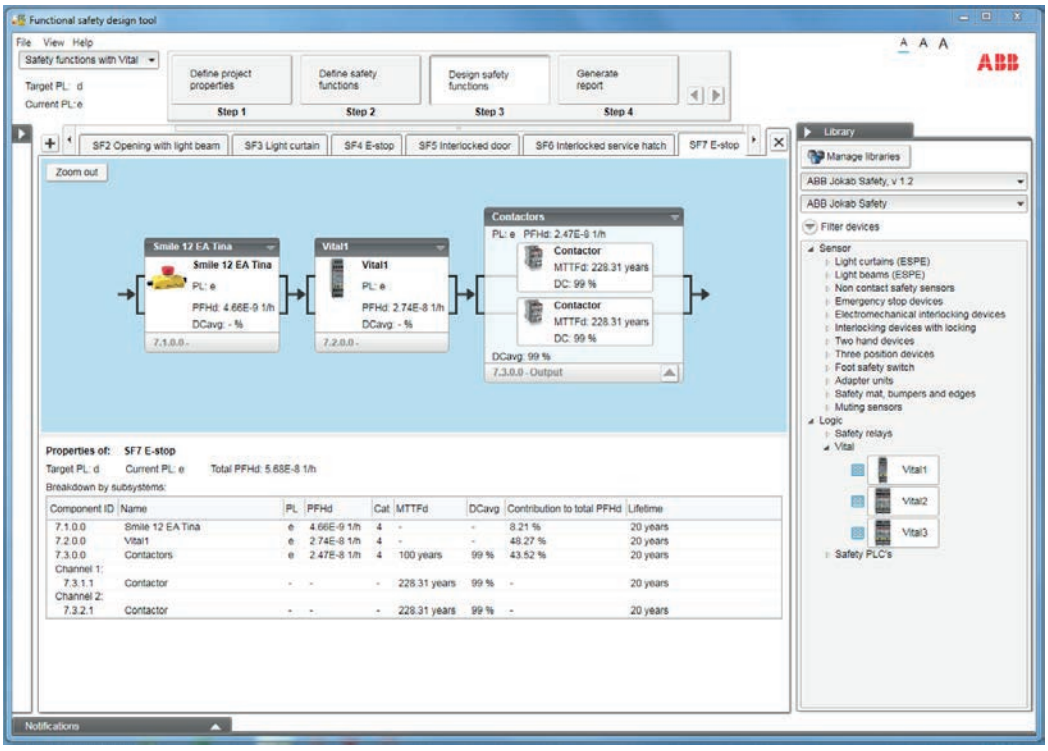
Tools for determining performance level (PL)

Tools to simplify the process of safety function design
FSDT is an ABB software for determining PL and SIL of safety functions and generating technical documentation. The tool helps simplifying the process of safety function design, verification and documentation. It supports the compliance of the requirements of both EN ISO 13849-1 and IEC 62061 as well as the European Machinery Directive. FSDT is freeware and can be downloaded from the ABB website.

Another commonly used software tool for the calculation of PL according to EN ISO 13849-1 is SISTEMA, developed by IFA (The Institute for Occupational Safety and Health) in Germany. With SISTEMA it is possible to “build” safety functions, verify them and generate the technical documentation required. The tool is freeware and can be downloaded from the IFA website.

To simplify the use of FSDT and SISTEMA with our products we have created a library containing all of our safety products.

2TLC172300D0201



Applying IEC/EN 62061

If a safety function is designed in accordance with IEC/EN 62061, the level of reliability is expressed as the Safety Integrity Level, SIL. There are a total of 4 levels, but in the IEC/EN 62061 standard SIL 3 is the highest level. SIL is similar to PL (performance level) and uses the same PFH_D (probability of dangerous failure per hour) to express the reliability of components and systems.

Safety Integrity Level, SIL	Probability of dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

There is a method in IEC/EN 62061 for assigning the Safety Integrity Level.

Severity (Se)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2
1				(OM)	SIL1

Cl=Fr+Pr+Av
OM=Other Measures

The severity of injury that can occur is divided into four levels. Class is the addition of the values of frequency (Fr, stated as a value between 1 and 5, where 5 represents the highest frequency), probability that a dangerous event will occur (Pr, stated as a value between 1 and 5, where 5 represents the highest proability) and the possibility of avoiding or limiting injury (Av, stated as a value of 1, 3 or 5, where 5 represents the least chance of avoiding or limiting an injury).

The safety function that is to be designed must at least fulfill the SIL that has been assigned to it in the risk assessment. The safety function consists of a number of sub-elements. Example: a door is interlocked by a non-contact sensor which is in turn monitored by a Pluto safety PLC, with outputs that break the power to two supervised contactors. The sensor is sub-element 1, Pluto is sub-element 2 and the two supervised contactors are sub-element 3. If in the assessment it has been established that SIL2 shall be used, every individual sub-element in the safety function must fulfill the SIL2 requirements. And the safety function must in its entirety fulfill the SIL2 requirements.

Definition of protective safety in accordance with IEC/EN 62061
"Function of a machine whose failure can result in an immediate increase of the risk(s)"

If the SIL requirements are not fulfilled in any of the sub-elements or by the safety function in its entirety, a re-design must be made.

Finally
This is just a brief introduction to the EN ISO 13849-1 and IEC/EN 62061 standards. You are welcome to contact us for more information and we are happy to guide you in how to apply the standards to our products.

The information given in this document is not intended to replace the standards - we strongly encourage you to purchase the standards if you are working with machine safety.

ABB b.v.
Electrification Business Area
George Hintzenweg 81, 3068 AX Rotterdam
P.O. Box 301, 3000 AH Rotterdam
Phone: 088 26 00 900
E-mail: nl-tech-EP@abb.com

abb.nl/lowvoltage
abb.nl/jokabsafety

Follow ABB via:
ABB Electrification NL
ABB Electrification
ABB-Benelux
Electrification NL

1SPC801342X0201 / 02.21