Safety in control systems according to EN ISO 13849-1

Machine Safety - Jokab Safety products

Power and productivity
for a better world™

New 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. With this document we aim to provide an introduction to the standard and its application in conjunction with our products.

Introducing the new standard

The generation change for standards on safety in control systems introduces new concepts and calculations for machine builders and machine users. The EN 954-1 standard (categories) is being phased out and replaced by EN ISO 13849-1 (PL, Performance Level) and EN 62061 (SIL, Safety Integrity Level). Although the deadline for using EN 954-1 is set to 31/12/2011, it is beneficial to start applying the new standards as soon as possible as many new standards no longer refer to EN 954-1.

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 great if you have previous experience of the categories. EN 62061 defines the structures slightly differently.

Customer requirements

If the 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 document 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 document 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 level the PL 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 a failure that knocks out 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 the 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 the calculation tool

With the freeware application SISTEMA (see page 16) 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 safety PLC or Vital safety controller. Not only is it easier to make calculations, but above all it is easier to ensure a higher level of safety.

We develop innovative products and solutions for machine safety

We make it easy to build protection systems. Developing innovative products and solutions for machine safety has been our business concept since the company started in Sweden in 1988. Our vision is to be “Your partner for machine safety - globally and locally”.

Many companies, both in Sweden and abroad, have discovered how much easier it is to build safety and protection systems using products and guidance from us. The goal of our development is to ensure a high safety level (PL e). This is to help our customers create safe workplaces, regardless of who is assessing the risk level.

Experience

We have extensive experience in the practical application of regulations and standards from both authorities and manufacturing operations. We represent Sweden in the standards body for machinery safety and we work daily with the practical application of safety requirements in combination with production requirements. You can utilise our expertise for training and advice about the new Machinery Directive, risk analysis and safety in control systems.

Systems

We supply everything from a safety solution for a complete protection system installed on individual machines or entire production lines. We combine production requirements with safety requirements for production-friendly solutions.

Products

We have a complete range of safety components that make it easy to build protection systems. We develop these innovative products continuously, often in collaboration with our customers.

Contents:

Page 2 Introduction
Page 4 Work method according to EN ISO 13849-1
Page 8 Case study using RT9
Page 10 Case study using Vital
Page 12 Case study using Pluto
Page 14 What defines a safety function?
Page 16 SISTEMA
Page 17 Safety relay, Vital or Pluto?

Terms as specified in EN ISO 13849-1

PL Performance Level
Divided into a to e

PL_r Required Performance Level
(The required performance level for a particular safety function)

$MTTF_d$ Mean Time To Dangerous Failure is divided into Low, Medium and High

B_{10d} Number of cycles until 10 % of the components have a dangerous failure (for pneumatic and electromechanical components)

T_{10d} Mean time until 10 % of the components have a dangerous failure
(Component operating time is restricted to T_{10d})

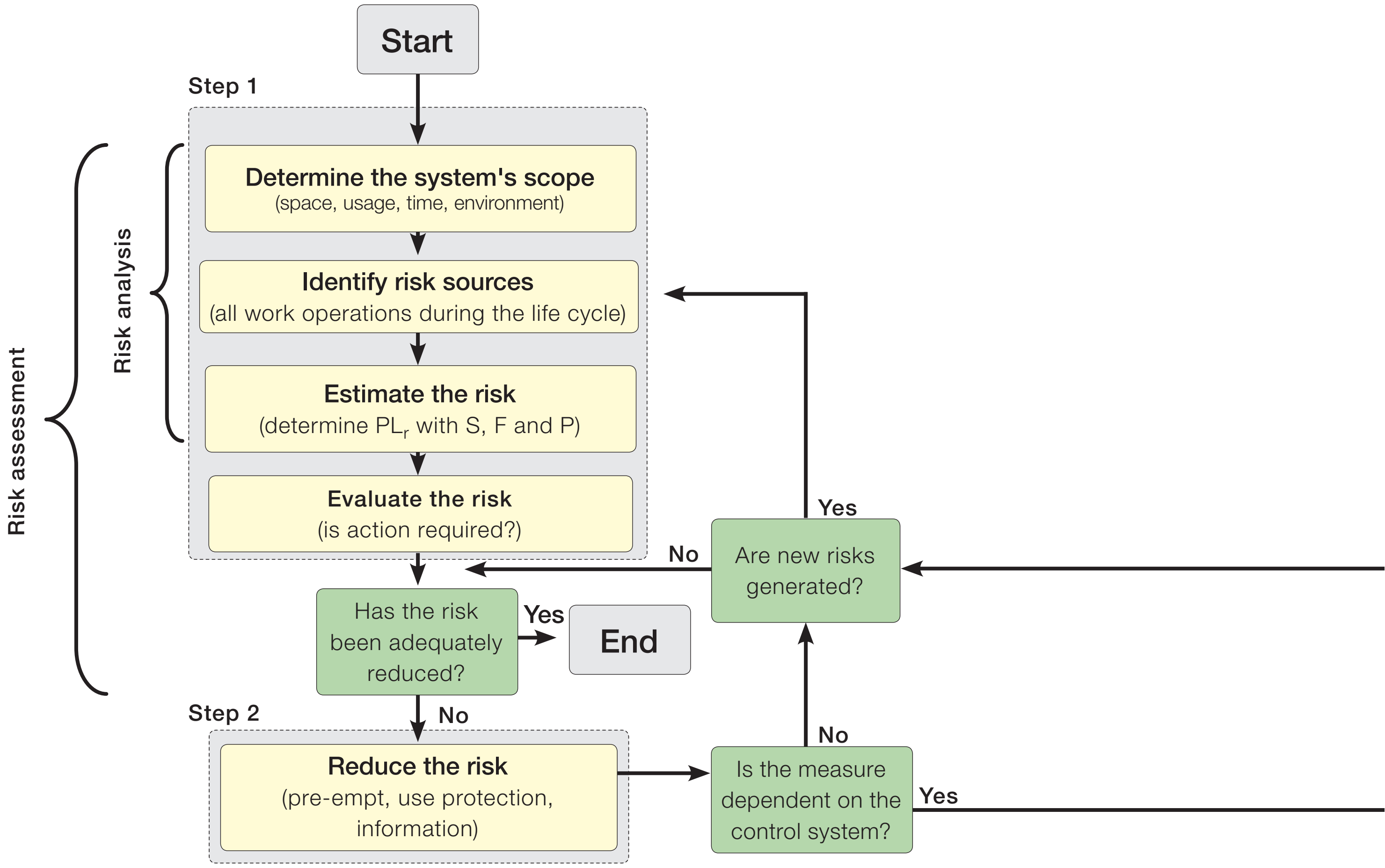
CCF Common Cause Failure

DC Diagnostic Coverage
Divided into Low, Medium and High

PFH_D Probability of Dangerous Failure per Hour
(Average probability of dangerous failure per hour)

The description and example in this document show how the product works and can be used. This does not mean that it satisfies the requirements for all types of machines and processes. The purchaser/user is responsible for the product being installed and used in line with applicable regulations and standards. We reserve the right to make changes to the product and product sheet without prior notice.

Working method as specified in EN ISO 13849-1


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
Has the risk been adequately reduced?
Yes
End
No
Step 2
Reduce the risk
(pre-empt, use protection, information)
Is the measure dependent on the control system?
Yes
No
Are new risks generated?
Yes
No

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. The EN ISO 12100 standard (combination of EN ISO 14121-1 and EN ISO 12100-1/-2) stipulates the requirements for the risk assessment of a machine. 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, severity), frequency of exposure to the risk (F, frequency) and the possibility you have of avoiding or limiting the injury (P, possibility). 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:

S1	bruises, abrasions, puncture wounds and minor crushing injuries
S2	skeletal injuries, amputations and death
F1	less frequently than every two weeks
F2	more often than every two weeks
P1	slow machine movements, plenty of space, low power
P2	quick machine movements, crowded, high power

By setting S, F and P for the risk, you will get the PL_r Performance Level (required) 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.

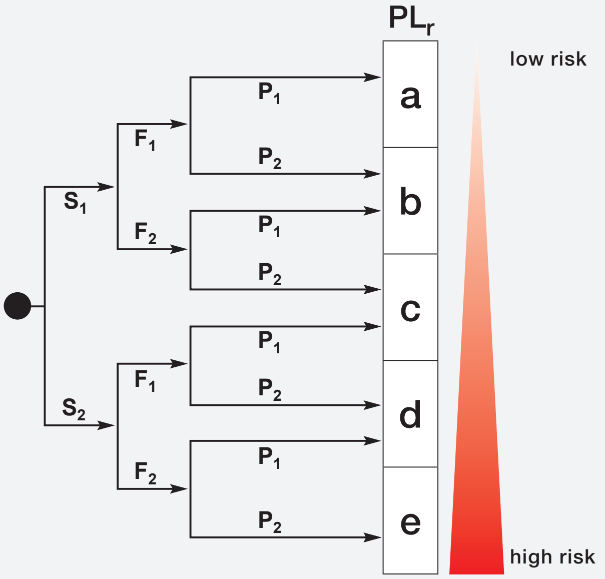
Risk estimation

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



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. (For example, reduce power, avoid interference in the danger zone.)

2. Use protection and/or safety devices. (For example, fences, light grids or control devices.)

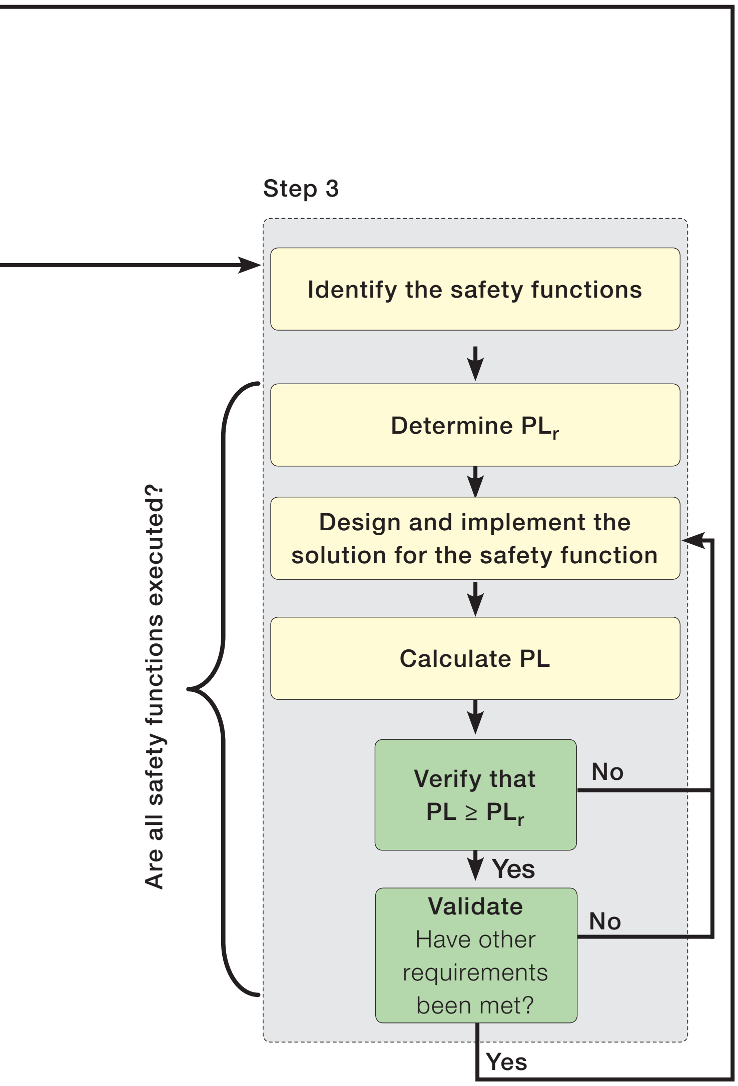
3. Provide information about how the machine can be used safely. (For example, in manuals and on signs.)

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.

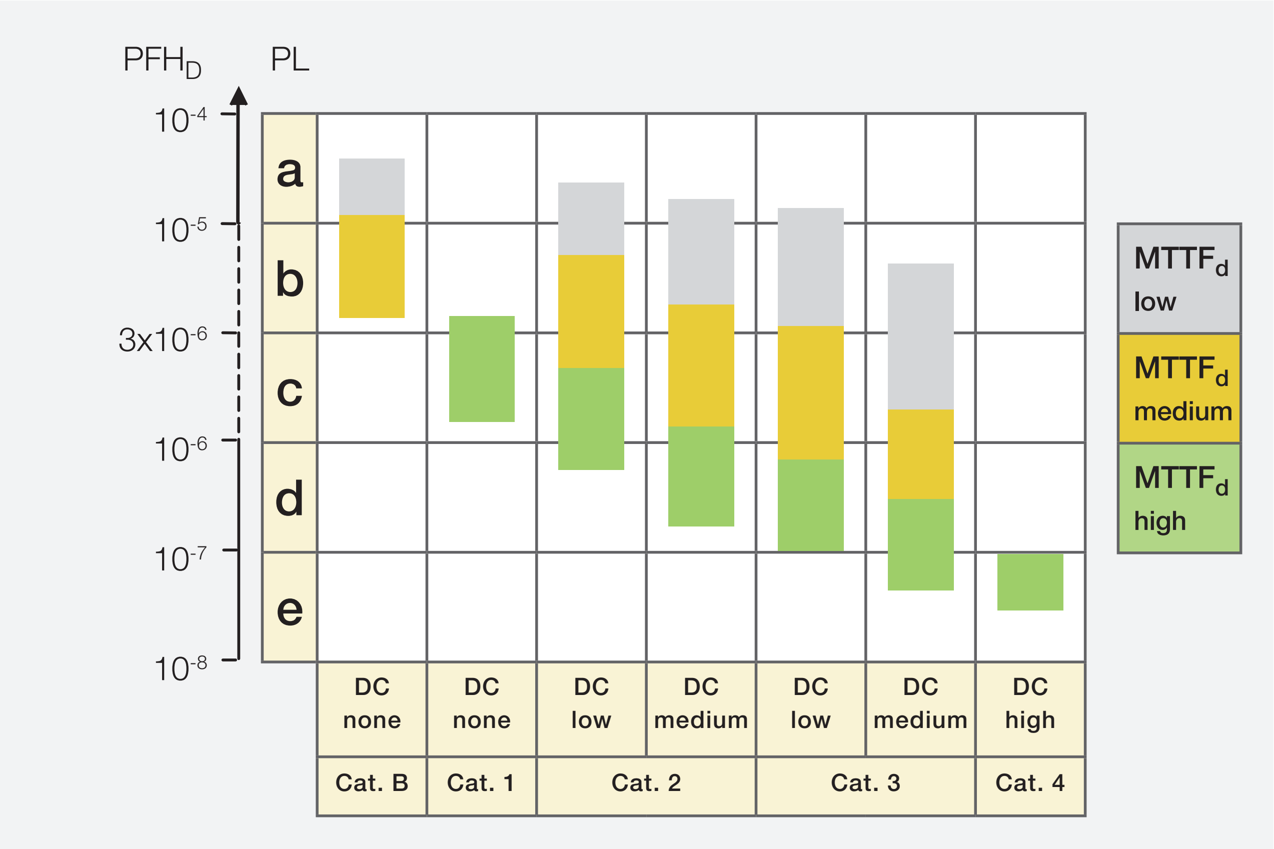
Step 3 - Design and calculate the safety functions

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.



Step 3
Identify the safety functions
Determine PL_r
Design and implement the solution for the safety function
Calculate PL
Verify that $PL \geq PL_r$
No
Yes
Validate Have other requirements been met?
No
Yes
Are all safety functions executed?



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.

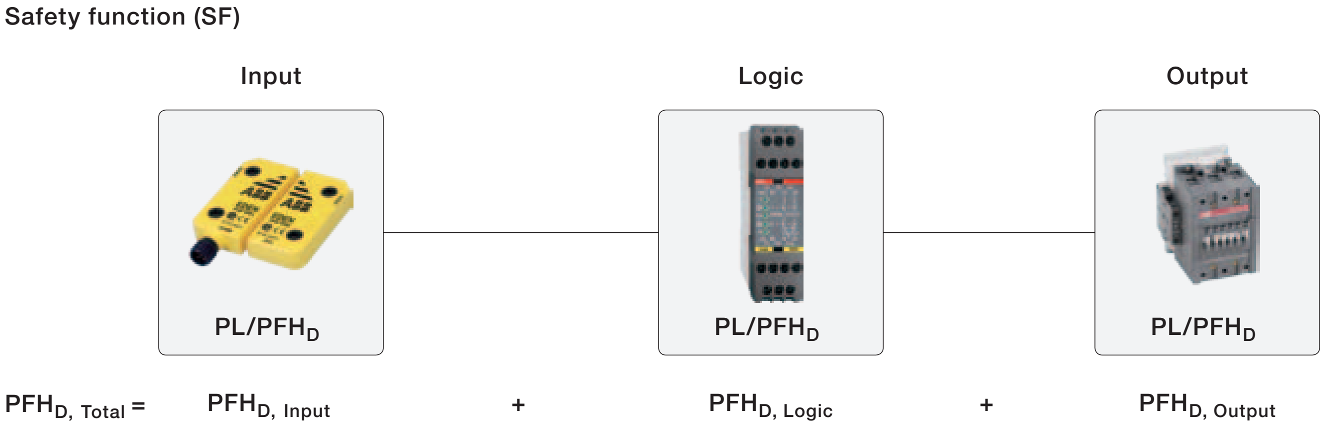
PL calculation in Step 3

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 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 output devices (such as contactors and valves) you do not usually specify a value as it depends on how often the component will be used. You can then either calculate yourself according to EN ISO 13849-1 or use the pre-calculated example solutions such as those from ABB Jokab Safety.

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 yourself 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.



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 contacts with positive opening operation.

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:

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

Where

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

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 nop= 17,520 cycles.

With a B_{10d}=2·10^6 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 facing 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.

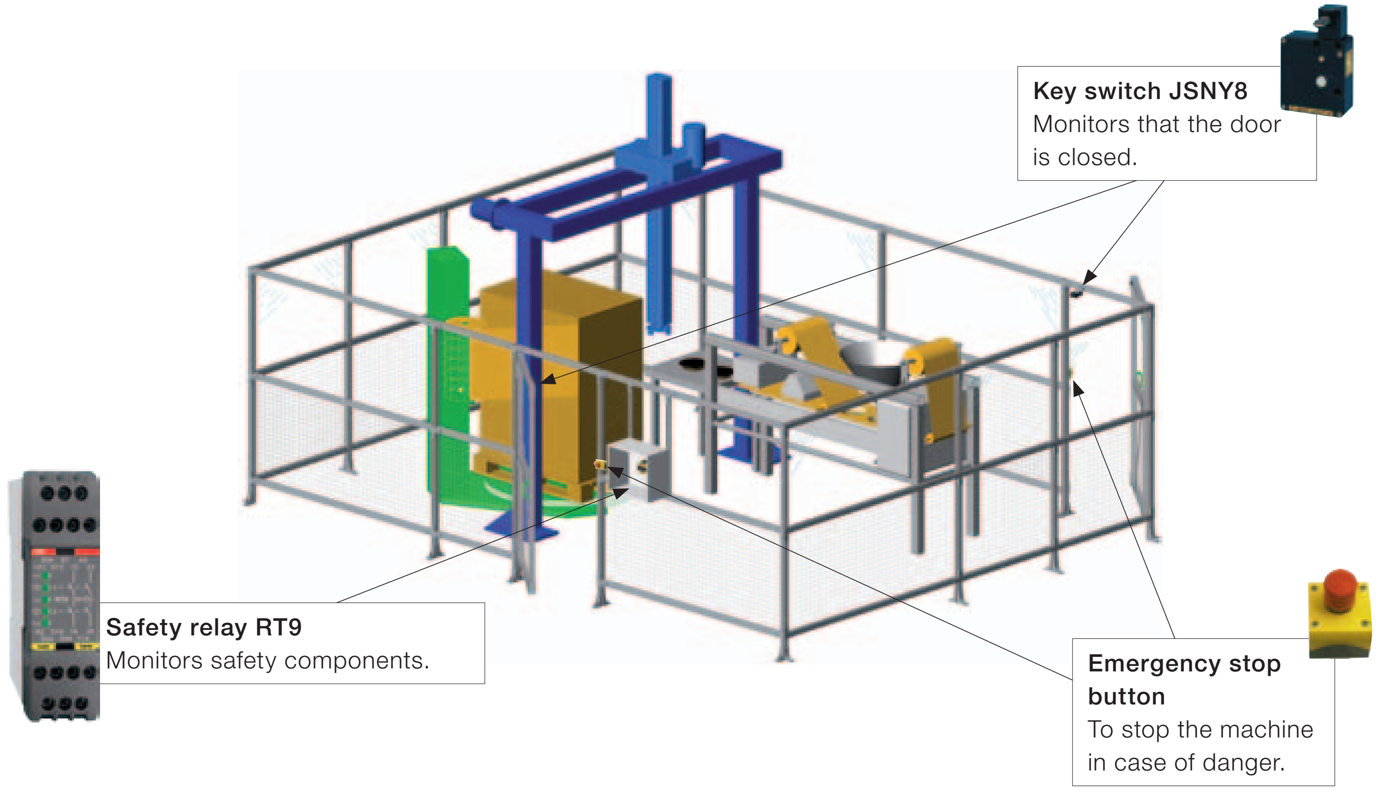
A software specification must be prepared to ensure that you can check the functionality of the program. It is also important to divide the program into modules that can be tested individually. Paragraph 4.6 and Appendix J of EN ISO 13849-1 specify requirements for safety related software.

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.

Example 1
Safety system using RT9

Protection layout for a packaging machine with low risks.



Key switch JSNY8
Monitors that the door is closed.

Safety relay RT9
Monitors safety components.

Emergency stop button
To stop the machine in case of danger.

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 hen both doors are closed and when the protection system has been reset.

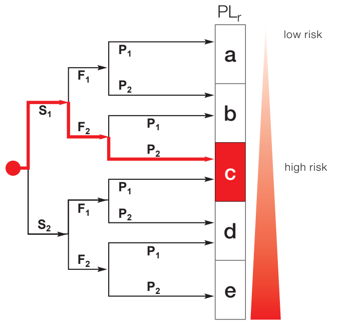
In the risk assessment it was established that the machine is to be operated in three shifts (8 hours per shift) 365 days a year. It is assumed that operational disturbances were resolved in less than one minute in the danger zone. This can be carried out two times per hour (F2). Unexpected start-ups are not deemed to cause serious injury but rather minor healable injuries (S1). The operator is deemed 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 · (3·8) hours/day · 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.

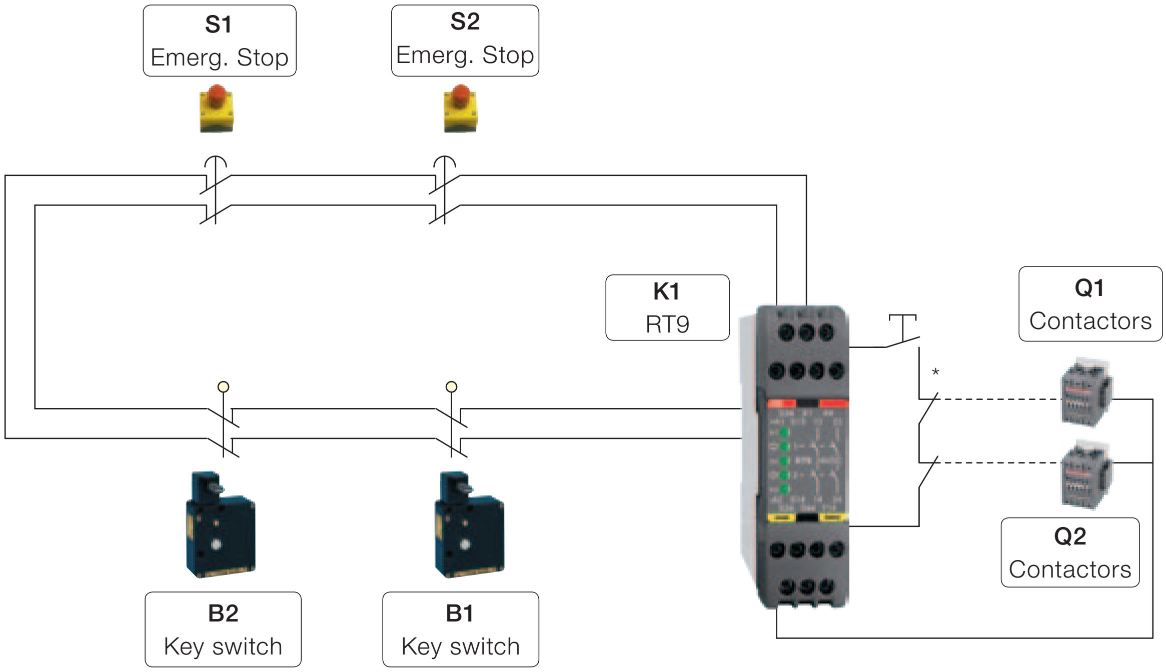
Step 2 – Reduce the risk

As protection, an interlocked door is selected with the key switch JSNY8. Downtime is short enough for the dangerous movement to have stopped before the operator can access it. The emergency stop is placed within easy reach, on both sides of the cell near the locked doors.



Assessment 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.



* Monitoring of contactors with K1

Step 3 - Calculate the safety functions

The starting block that is composed of double unmonitored contactors has been calculated at $2.47 \cdot 10^{-8}$. The safety functions are represented by block diagrams.

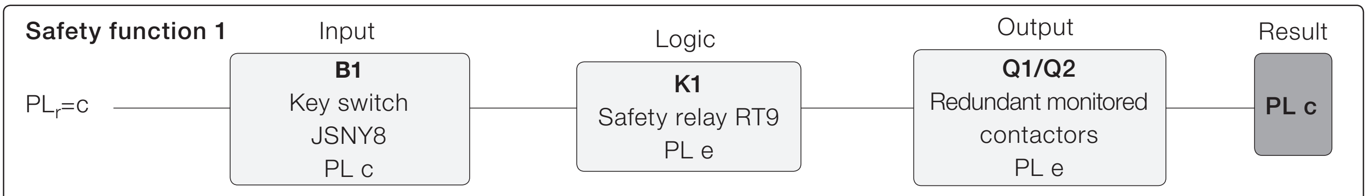
Safety functions 1 and 2 are identical. Therefore, only safety function 1 is shown.

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

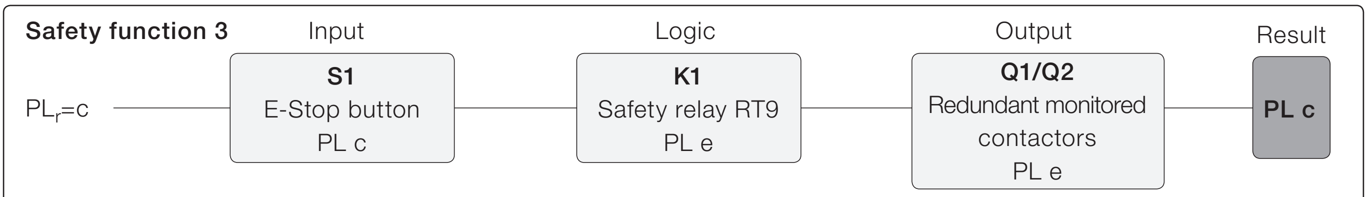
How safe is a mechanical switch?

A mechanical switch must be installed and used according to its specifications in order to be reliable.

- Life expectancy only applies if correctly installed.
- The locking head must be fixed so that it will not loosen.
- The environment around the lock housing must be kept clean.
- Two mechanical switches on a door can also fail for the same reason.



$PFH_{D,\ JSNY8} + PFH_{D,\ RT9} + PFH_{D,\ Q1/Q2} = 1{,}14 \cdot 10^{-6} + 9{,}55 \cdot 10^{-9} + 2{,}47 \cdot 10^{-8} = 1{,}17 \cdot 10^{-6} \longrightarrow$ **PL c**

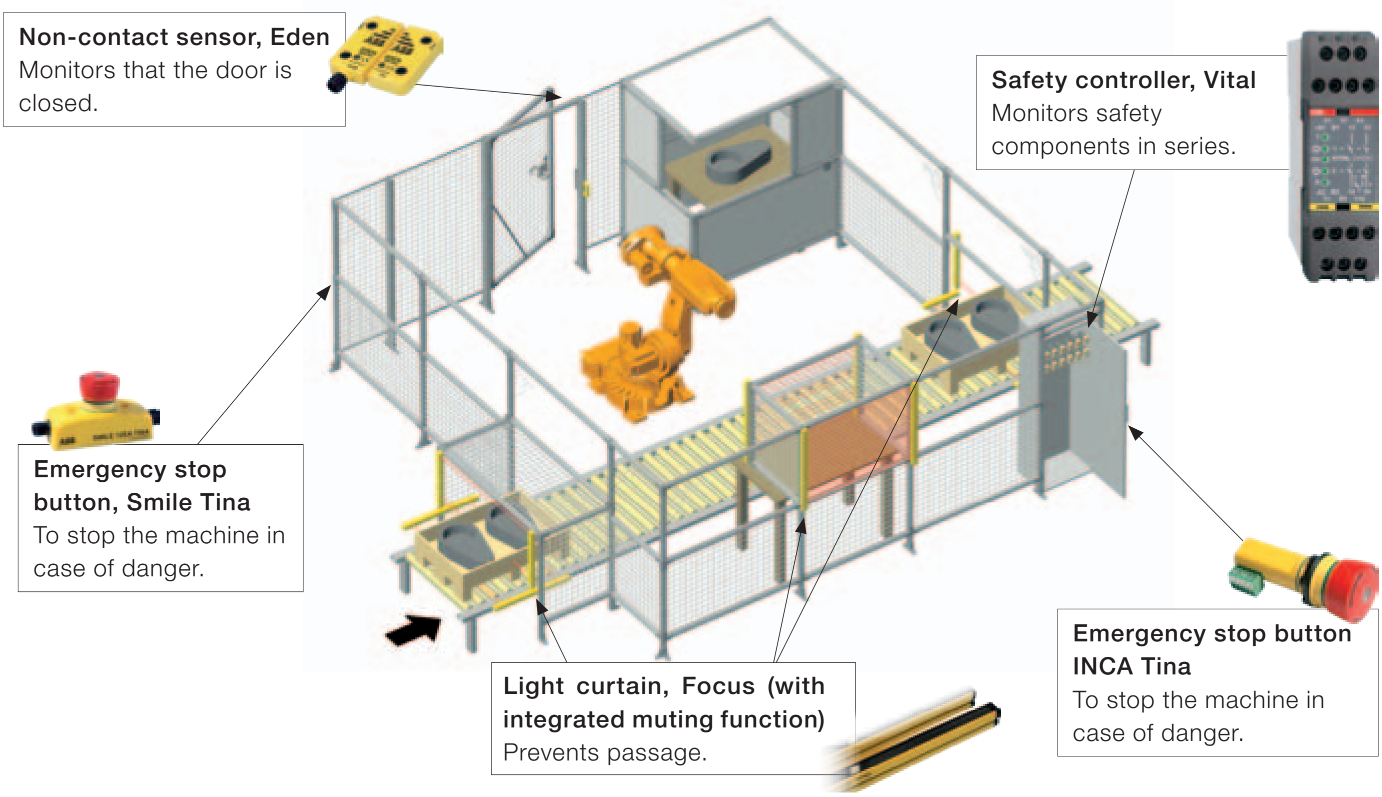


$PFH_{D} + PFH_{D,\ RT9} + PFH_{D,\ Q1/Q2} = 1{,}34 \cdot 10^{-6} + 9{,}55 \cdot 10^{-9} + 2{,}47 \cdot 10^{-8} = 1{,}37 \cdot 10^{-6} \longrightarrow$ **PL c**

The reason for not achieving more than PL c with this solution is that you use one key switch per door. PL d could be achieved by using two key switches per door, but further action on the monitoring of each switch will be required as well. Note: If the risk assessment had shown that a serious injury, S2, could occur, the outcome would have been PL_r= e. This would have meant that the above solution was inadequate. For the emergency stop function, PL d can be achieved provided that certain failure exclusions can be made. These safety functions can be downloaded from our website as a SISTEMA project, www.jokabsafety.com.

Example 2
Safety system using Vital

Protection layout for a robot cell with high risks.



Non-contact sensor, Eden
Monitors that the door is closed.

Safety controller, Vital
Monitors safety components in series.

Emergency stop button, Smile Tina
To stop the machine in case of danger.

Light curtain, Focus (with integrated muting function)
Prevents passage.

Emergency stop button INCA Tina
To stop the machine in case of danger.

Step 1 – Risk assessment

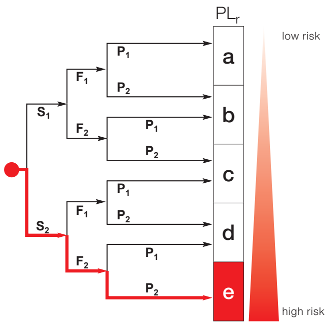
The workpieces are fed into the equipment and transported out again following an error-free test. With the help of a robot the workpieces are added to a machine for testing. Unauthorised workpieces are positioned by the robot for post-machining in a manual discharge station. The work that needs to be done in the robot cell is to correct operational disturbances for the test equipment and the conveyor belt (about once an hour), post-machining and 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 expected to cause serious injury (S2). The operator is deemed not to have the possibility of avoiding injury as the robot moves quickly (P2). The assessment for the safety function required for access to the machine is PL_r=e (S2, F2, P2).

The coming ISO 10218-2 standard for robot systems/cells specifies the requirement PL d for the safety functions to be used (if the risk analysis does not show a different PL). For the robot safety stop and emergency stop inputs, the requirement is at least PL d (according to the EN ISO 10218-1 standard). However, in this case risk assessment is PL_r= e.

Step 2 – Reduce the risk

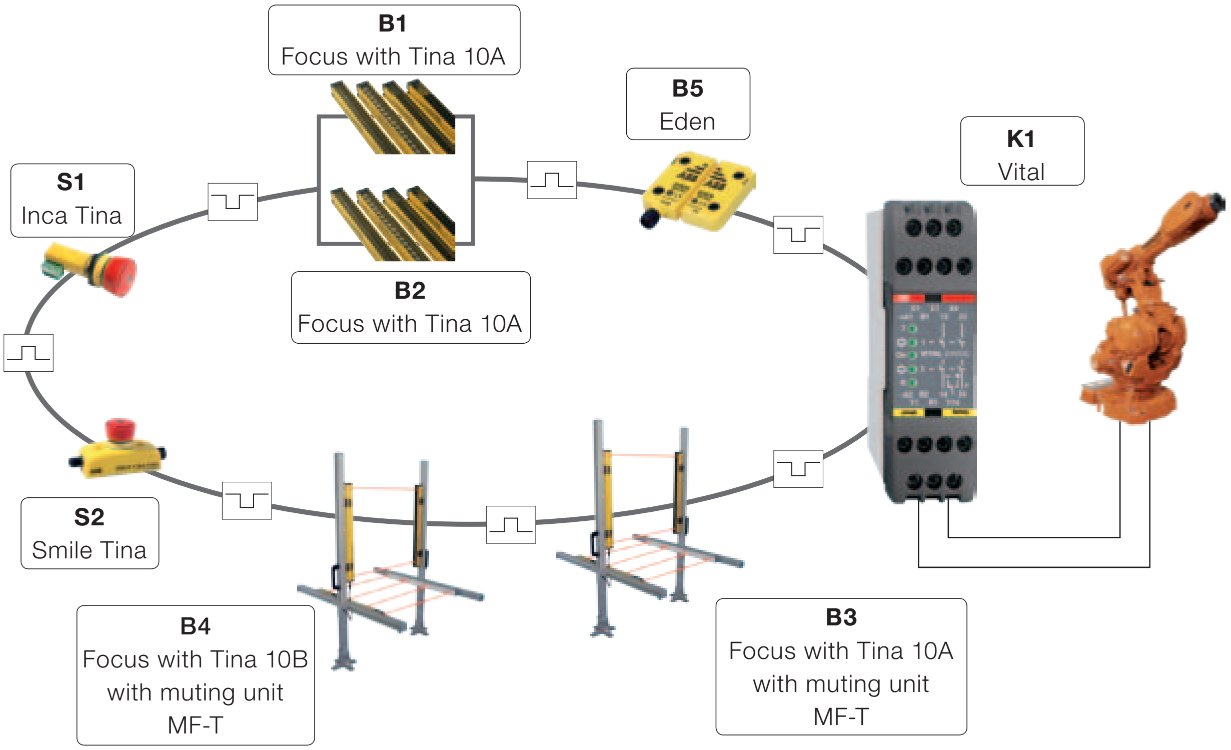
As protection, an interlocked door is selected with the Eden non-contact sensor. To protect against entering the cell the wrong way, transport of materials in and out is protected and provided with muting to distinguish between material and people. The emergency stop is also a safety function that is required. The power source to all hazardous machinery functions has to be cut using 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 loop, with PL e in accordance with EN ISO 13849-1.



Assessment of the PL_r required 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 $5.79\cdot10^{-8}$ (the value applies to ABB industrial robots with IRC5 controller). The safety functions are represented by block diagrams.

Safety function 3
When calculating the safety function the PFH_D- values for both the light curtain and the muting unit shall be included in the same function. See safety function 3 below.

Safety function 1	Input	Logic	Output	Result
PL_r=e	**B5** No contact safety sensor Eden PL e	**K1** Safety controller Vital PL e	**Q1** Machine stop input for robot, redundant PL e	**PL e**

$PFH_{D,\ Eden} + PFH_{D,\ Vital} + PFH_{D,\ Robot} = 4{,}5\cdot10^{-9} + 2{,}74\cdot10^{-8} + 5{,}79\cdot10^{-8} = 8{,}98\cdot10^{-8} \longrightarrow$ **PL e**

Safety function 2	Input	Logic	Output	Result
PL_r=e	**S2** E-Stop button Smile Tina PL e	**K1** Safety controller Vital PL e	**Q1** Machine stop input for robot, redundant PL e	**PL e**

$PFH_{D,\ Smile\ Tina} + PFH_{D,\ Vital} + PFH_{D,\ Robot} = 4{,}66\cdot10^{-9} + 2{,}74\cdot10^{-8} + 5{,}79\cdot10^{-8} = 9{,}0\cdot10^{-8} \longrightarrow$ **PL e**

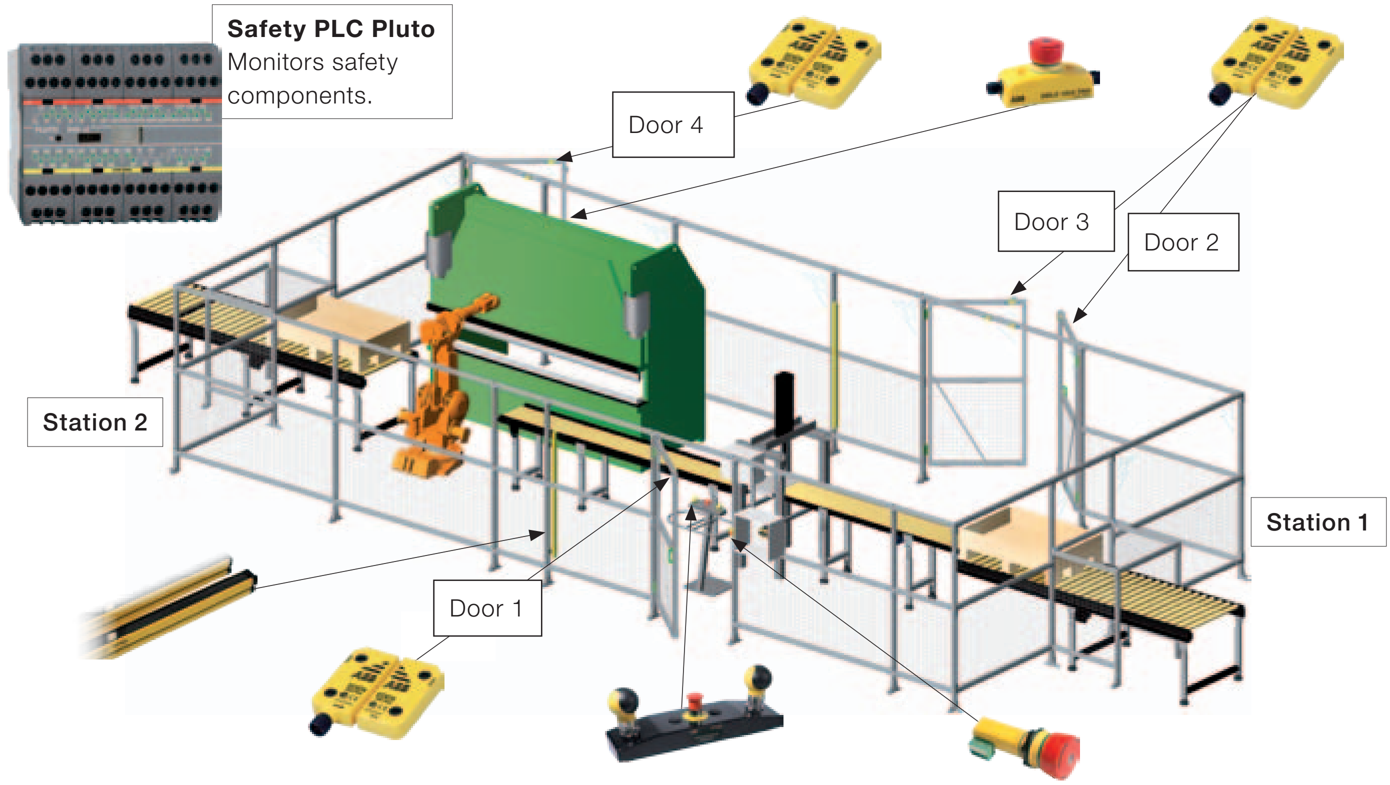
Safety function 3	Input		Logic	Output	Result
PL_r=e	**B4** Light curtain Focus PL e	Tina 10B PL e	**K1** Safety controller Vital PL e	**Q1** Machine stop input for robot, redundant PL e	**PL e**

$PFH_{D,\ Focus} + PFH_{D,\ Tina\ 10} + PFH_{D,\ Vital} + PFH_{D,\ Robot} = 2{,}5\cdot10^{-9} + 4{,}5\cdot10^{-9} + 2{,}74\cdot10^{-8} + 5{,}79\cdot10^{-8} = 9{,}2310^{-8} \longrightarrow$ **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 that is represented in the robot cell.

Example 3
Safety system using Pluto

Protection layout for a machining tool and industrial robot with high risks.



Step 1 – Risk assessment

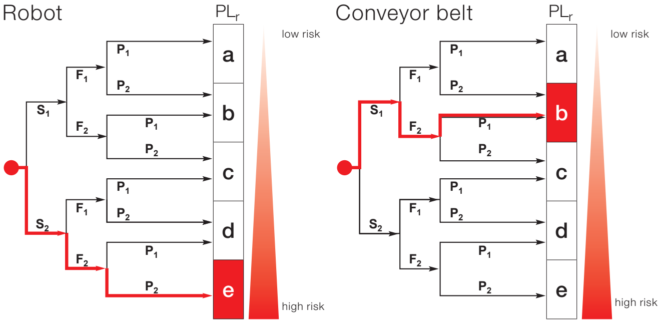
The workpieces to be machined are fed into the cell through a conveyor belt and positioned by the operator in the pneumatic machining tool in station 1. The operator starts station 1 manually. The pneumatic machining tool performs work on the workpiece in station 1. The operator then places the machined workpiece on the conveyor belt for transfer to station 2. The robot then takes the workpiece that is placed 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, for example, to address operational disturbances in the press and the robot (a few times a week, F2).

Unexpected start-ups of the robot are expected to cause serious injury (S2). The operator is deemed not to have the possibility of avoiding injury as the robot moves quickly (P2). The assessment for the safety function required for access to station 2 is PL_r=e (S2, F2, P2). This assessment would still be the same in respect of the press. For the safety function for the risks associated with the conveyor belt, the assessment S1, F2, P1 is made giving PL_r= b.

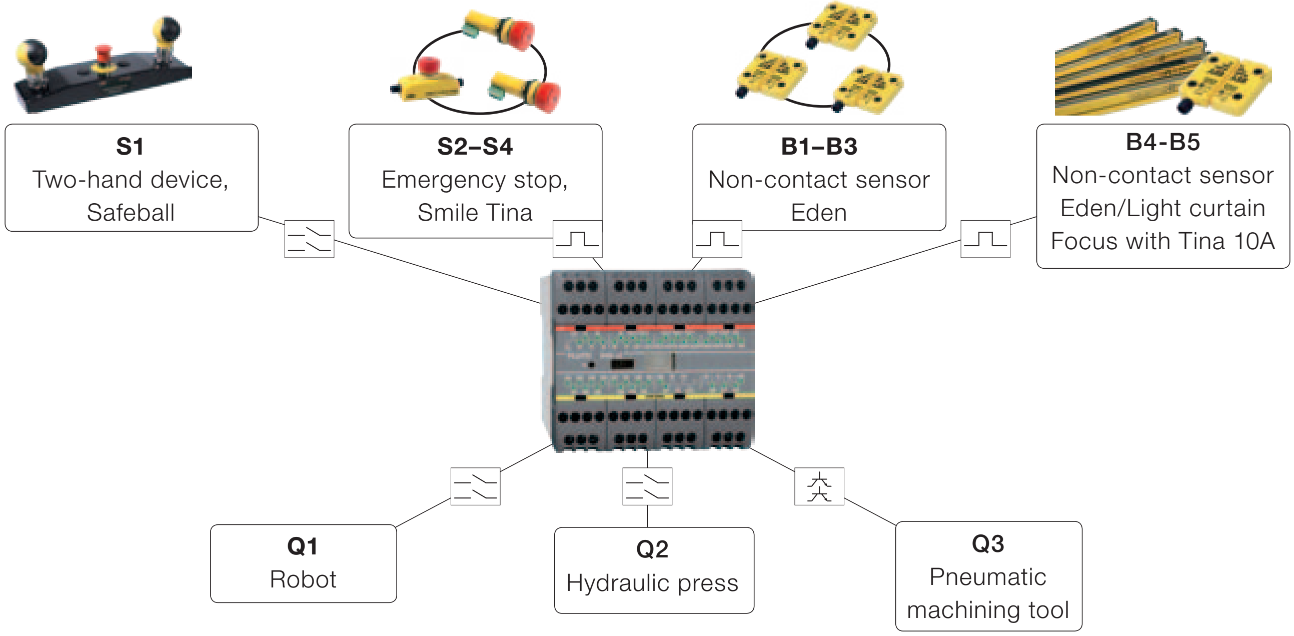
Step 2 – Reduce the risk

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 (Focus) and a non-contact sensor at door 4 (Eden) protects the entry. If the door is opened or the light curtain is breached, station 2 stops in a safe manner. By opening doors 2 and 3 (also monitored by Eden) the conveyor belt and the pneumatic machining tool will stop safely. Manual reset must always be done after actuation by any safety device.

When the protection system requires a number of safety devices and that multiple machines must be checked, safety PLC Pluto is the most effective solution. If the protection system also has to work by zones and in different modes of operation, this is another compelling reason to use Pluto. With Pluto, PL e can be achieved regardless of the number of connected safety devices.



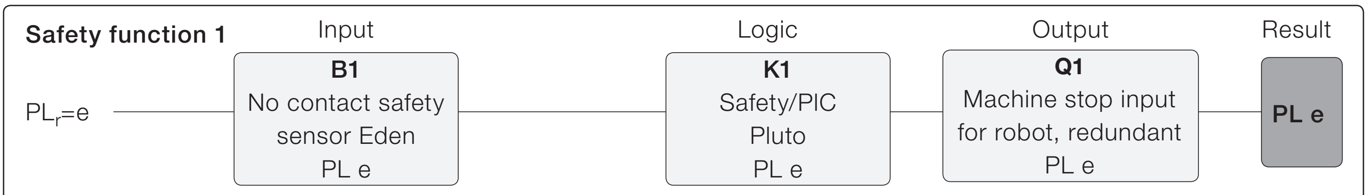
PL_r= e for the robot and hydraulic press and PL_r=b for the conveyor belt.


S1
Two-hand device, Safeball
S2–S4
Emergency stop, Smile Tina
B1–B3
Non-contact sensor Eden
B4-B5
Non-contact sensor Eden/Light curtain Focus with Tina 10A
Q1
Robot
Q2
Hydraulic press
Q3
Pneumatic machining tool

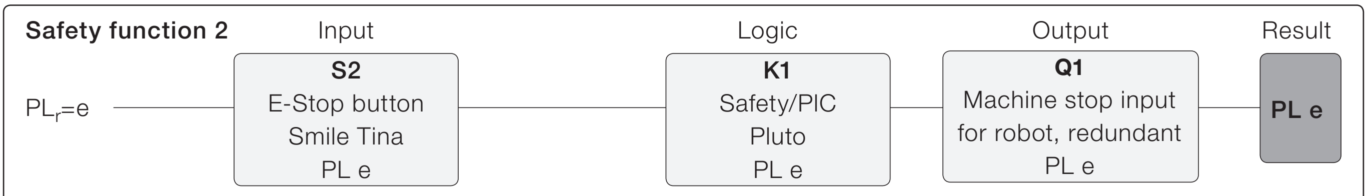
Step 3 - Calculate the safety functions for the robot cell

The $\mathrm{PFH_D}$-value for the robot's safety stop input is $5.79 \cdot 10^{-8}$ (the value applies to ABB industrial robots with IRC5 controller).

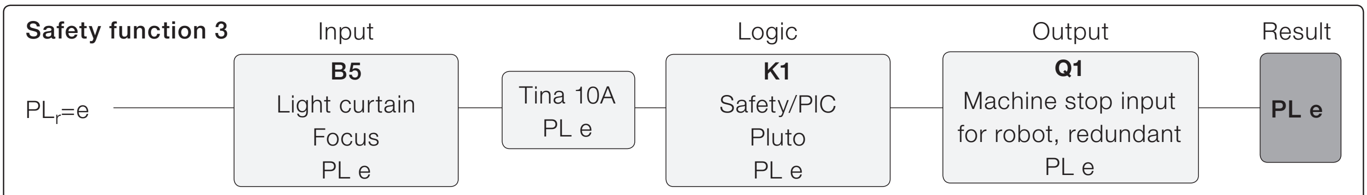
Only safety functions to help cut the power to the industrial robot are shown below. This is only a subset of the safety functions. When the power is to be cut to multiple machines in a cell, the safety functions can be defined in different ways depending on the risk analysis. The safety functions are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



$\mathrm{PFH}_{\mathrm{D},\ \mathrm{Eden}} + \mathrm{PFH}_{\mathrm{D},\ \mathrm{Pluto}} + \mathrm{PFH}_{\mathrm{D},\ \mathrm{Robot}} = 4{,}5 \cdot 10^{-9} + 2 \cdot 10^{-9} + 5{,}79 \cdot 10^{-8} = 6{,}44 \cdot 10^{-8} \longrightarrow$ **PL e**



$\mathrm{PFH}_{\mathrm{D,\ Smile\ Tina}} + \mathrm{PFH}_{\mathrm{D,\ Pluto}} + \mathrm{PFH}_{\mathrm{D,\ Robot}} = 4{,}66 \cdot 10^{-9} + 2 \cdot 10^{-9} + 5{,}79 \cdot 10^{-8} = 6{,}46 \cdot 10^{-8} \longrightarrow$ **PL e**



$\mathrm{PFH}_{\mathrm{D,Focus}} + \mathrm{PFH}_{\mathrm{D,\ Pluto}} + \mathrm{PFH}_{\mathrm{D,\ Robot}} = 5{,}02 \cdot 10^{-9} + 2 \cdot 10^{-9} + 5{,}79 \cdot 10^{-8} = 6{,}49 \cdot 10^{-8} \longrightarrow$ **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 that appear in the robot cell.

What defines a safety function?

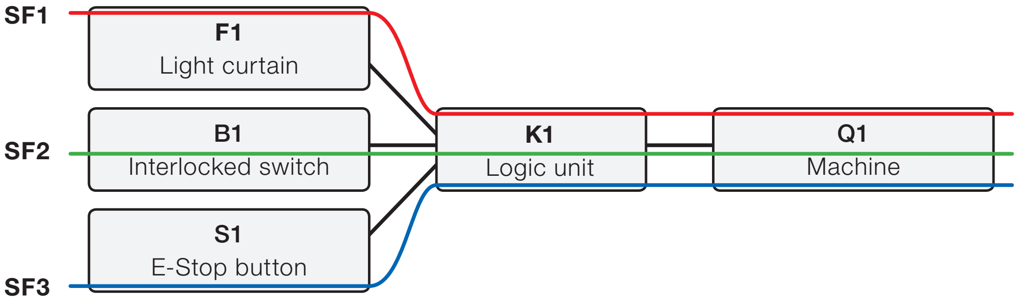
Calculating that you have achieved the PL_r that is required is not difficult, especially if you use “pre-calculated” safety devices and logic units. But what parts should then be included in each safety function? This must be resolved before you start calculating phase. To summarise in simple terms you can say that each safety device gives rise to a safety function for each machine that is affected by the safety device in question. Three safety devices that all cut the power 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, the 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:

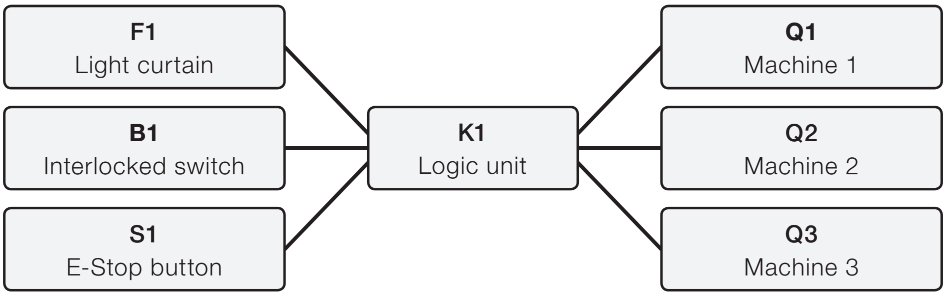
SF1: $PFH_{D,\ F1} + PFH_{D,\ K1} + PFH_{D,\ Q1} = PFH_{D,\ SF1}$
SF2: $PFH_{D,\ B1} + PFH_{D,\ K1} + PFH_{D,\ Q1} = PFH_{D,\ SF2}$
SF3: $PFH_{D,\ S1} + PFH_{D,\ K1} + PFH_{D,\ Q1} = PFH_{D,\ SF3}$



Multiple safety functions for multiple machines in a cell

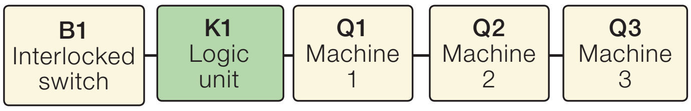
More commonly, several machines in a single cell/zone are to be protected by multiple safety devices. The following figure illustrates the interconnection schematically for an example. Each of the machines Q1 – Q3 is shut down separately and independently of K1.

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 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:



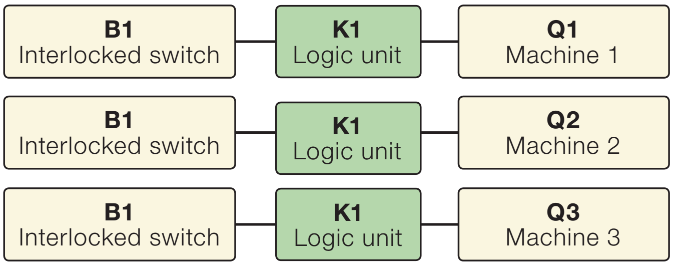
For the full safety function to be performed you require all the components to be working. Note that if B1 or K1 has a dangerous malfunction, the entire safety function is disabled. However, if for example machine Q1 has a dangerous malfunction, and is not shut down, machines Q2 and Q3 will still be 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:
www.dguv.de/ifa/de/pub/grl/pdf/2009_249.pdf
www.bg-metall.de/praevention/fachausschuesse/infoblatt/deutsch.html
(No 047, Date 05/2010)

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.

Examples of safety functions from Case Study 3 - safety PLC Pluto

The risk assessment for the safety functions needed for the risks associated with the robot was S2, F2, P2, which resulted in PL_r=e. The same assessment was made for the hydraulic press: PL_r=e. The assessment of the pneumatic machining tool is S2, F2, P1 giving PL_r= d due to the fact that the assessment is that there is the possibility of avoiding risk.

Interlock switch B1, Eden, is to cut the power to all machines in the danger zone:

- Robot Q1 ($\text{PFH}_{\text{D, Q1}} = 5.79{\cdot}10^{-8}$)
- Hydraulic press Q2 ($\text{PFH}_{\text{D, Q2}} = 8{\cdot}10^{-8}$)
- Pneumatic machining tool Q3 ($\text{PFH}_{\text{D, Q3}} = 2{\cdot}10^{-7}$).

Theoretical approach

If you use the practical approach the safety functions are as follows:

Robot:

$$\text{PFH}_{\text{D, B1}} + \text{PFH}_{\text{D, K1}} + \text{PFH}_{\text{D, Q1}} = 4{,}5{\cdot}10^{-9} + 2{\cdot}10^{-9} + 5.79{\cdot}10^{-8} = 6.44{\cdot}10^{-8} \longrightarrow \text{PL e}$$

Hydraulic press:

$$\text{PFH}_{\text{D, B1}} + \text{PFH}_{\text{D, K1}} + \text{PFH}_{\text{D, Q2}} = 4.5{\cdot}10^{-9} + 2{\cdot}10^{-9} + 8{\cdot}10^{-8} = 8.65{\cdot}10^{-8} \longrightarrow \text{PL e}$$

Pneumatic machining tool:

$$\text{PFH}_{\text{D, B1}} + \text{PFH}_{\text{D, K1}} + \text{PFH}_{\text{D, Q3}} = 4.5{\cdot}10^{-9} + 2{\cdot}10^{-9} + 2{\cdot}10^{-7} = 2.07{\cdot}10^{-7} \longrightarrow \text{PL d}$$

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

How would it have worked if you had used the theoretical approach? Would the safety function have achieved PL e?

All machines:

$$\text{PFH}_{\text{D, B1}} + \text{PFH}_{\text{D, K1}} + \text{PFH}_{\text{D, Q1}} + \text{PFH}_{\text{D, Q2}} + \text{PFH}_{\text{D, Q3}}$$
$$= 4{,}5{\cdot}10^{-9} + 2{\cdot}10^{-9} + 5.79{\cdot}10^{-8} + 8{\cdot}10^{-8} + 2{\cdot}10^{-7} = 3.44{\cdot}10^{-7} \longrightarrow \text{PL d}$$

In this case, the safety function would therefore have not achieved a total PL e, which was required for the risks associated with the robot and hydraulic press.

Conclusions

- Use the practical approach.
- 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.

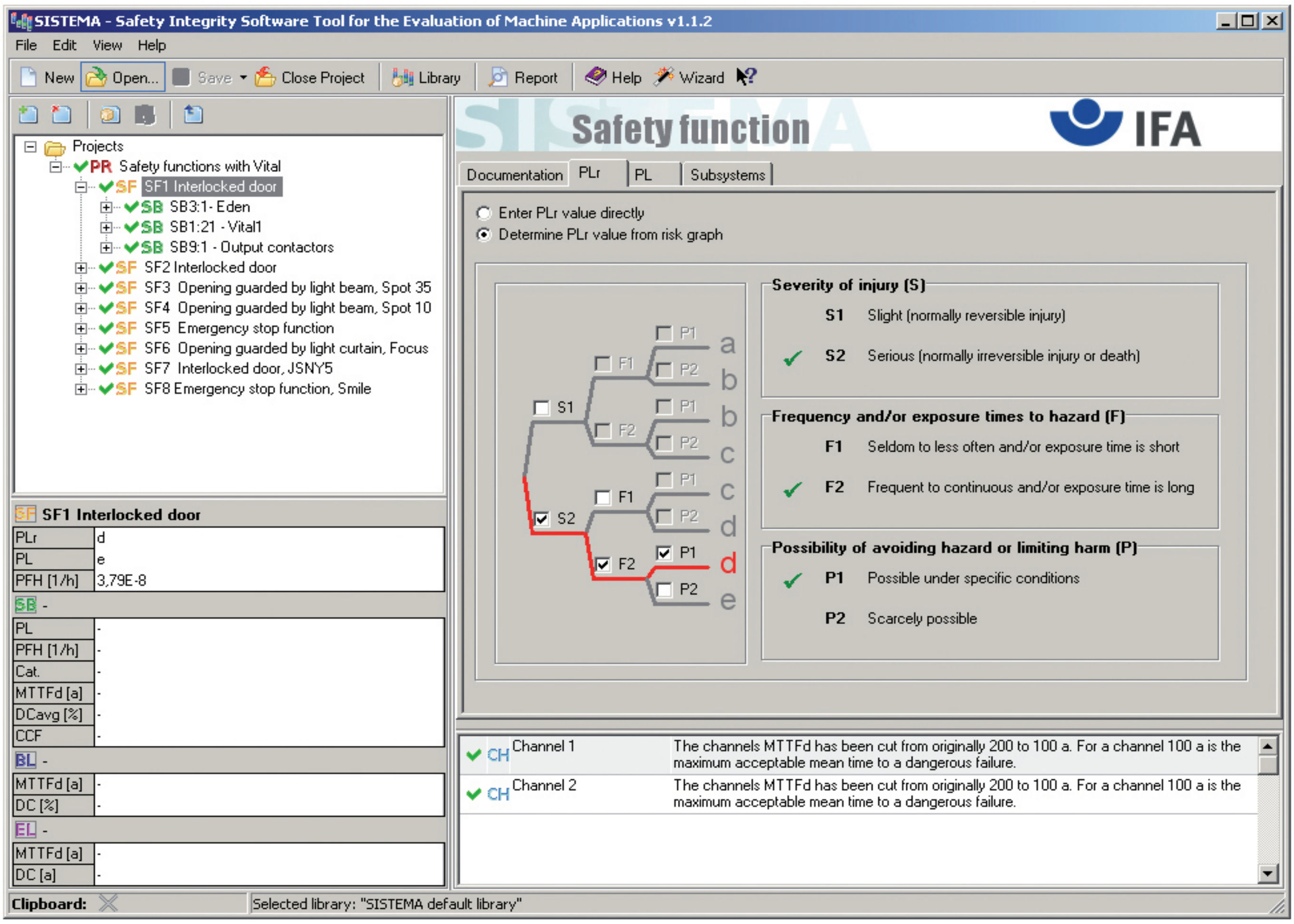
SISTEMA

A tool for determining performance level (PL) and generating technical documentation

EN ISO 13849-1 requires calculations. To do this in a manageable way a software tool provides excellent help. ABB Jokab Safety has chosen to use SISTEMA, a software tool developed by BGIA, now called IFA, in Germany. The tool is freeware and can be downloaded from the IFA website, www.dguv.de/ifa. With SISTEMA it is possible to “build” safety functions, verify them and generate the technical documentation required.

To work with SISTEMA in a rational way, we have developed a library of our products for download from our website www.jokabsafety.se. In order to have access to the latest version, visit this page periodically to check for updates and new releases.

To download SISTEMA go to www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp or search the Internet for “sistema”.



- Projects
  - ✓ PR Safety functions with Vital
    - ✓ SF SF1 Interlocked door
      - ✓ SB SB3:1- Eden
      - ✓ SB SB1:21 - Vital1
      - ✓ SB SB9:1 - Output contactors
    - ✓ SF SF2 Interlocked door
    - ✓ SF SF3 Opening guarded by light beam, Spot 35
    - ✓ SF SF4 Opening guarded by light beam, Spot 10
    - ✓ SF SF5 Emergency stop function
    - ✓ SF SF6 Opening guarded by light curtain, Focus
    - ✓ SF SF7 Interlocked door, JSNY5
    - ✓ SF SF8 Emergency stop function, Smile

SF SF1 Interlocked door

PLr	d
PL	e
PFH [1/h]	3,79E-8

SB -

PL	-
PFH [1/h]	-
Cat.	-
MTTFd [a]	-
DCavg [%]	-
CCF	-

BL -

MTTFd [a]	-
DC [%]	-

EL -

MTTFd [a]	-
DC [a]	-

○ Enter PLr value directly
● Determine PLr value from risk graph

☐ S1 ☑ S2 ☑ F2 ☑ P1

Severity of injury (S)

S1 Slight (normally reversible injury)
✓ S2 Serious (normally irreversible injury or death)

Frequency and/or exposure times to hazard (F)

F1 Seldom to less often and/or exposure time is short
✓ F2 Frequent to continuous and/or exposure time is long

Possibility of avoiding hazard or limiting harm (P)

✓ P1 Possible under specific conditions
P2 Scarcely possible

✓ CH Channel 1 The channels MTTFd has been cut from originally 200 to 100 a. For a channel 100 a is the maximum acceptable mean time to a dangerous failure.

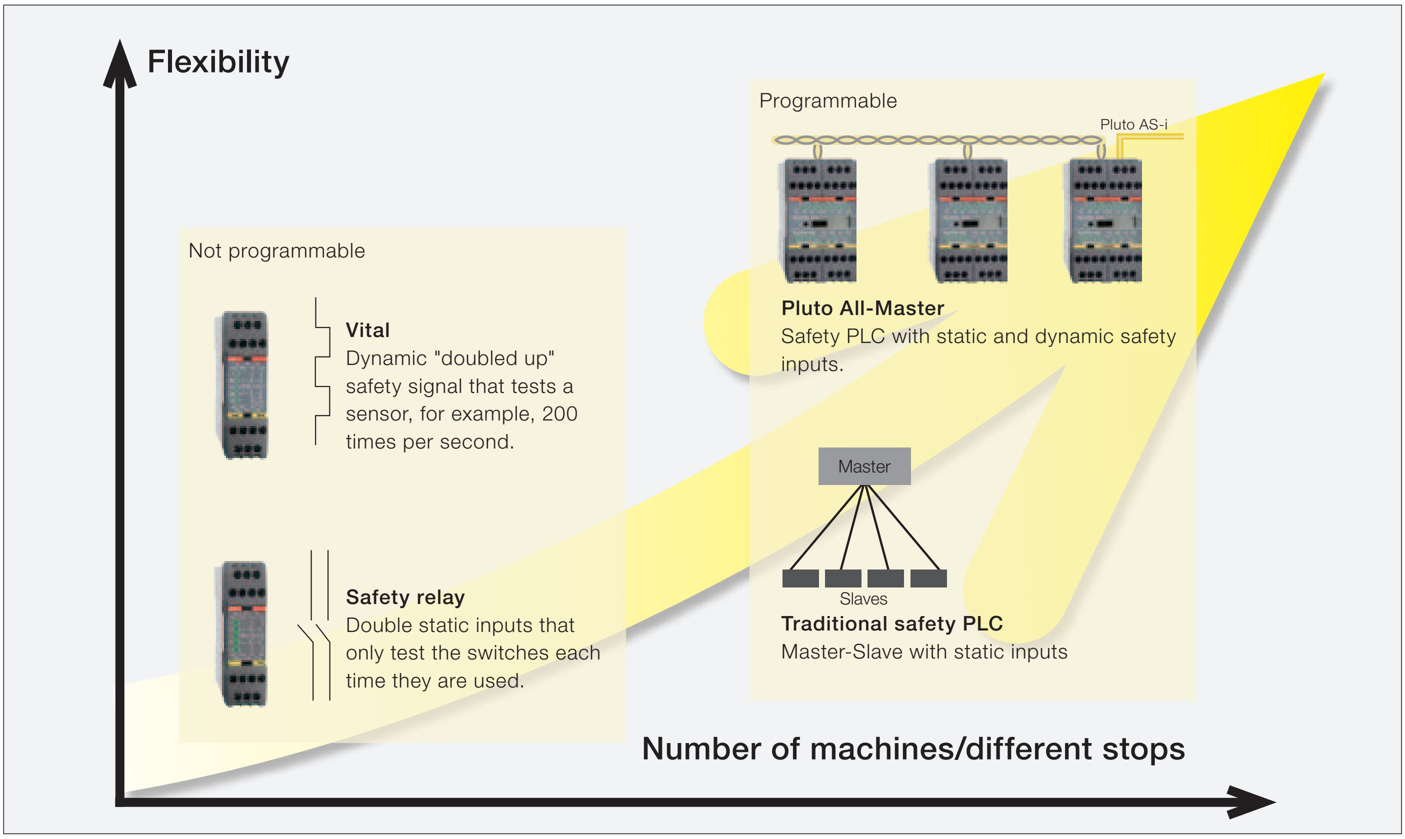
✓ CH Channel 2 The channels MTTFd has been cut from originally 200 to 100 a. For a channel 100 a is the maximum acceptable mean time to a dangerous failure.

Clipboard: Selected library: "SISTEMA default library"

Screenshot from SISTEMA.

Safety relay, Vital or Pluto?

Various benefits in comparison to EN ISO 13849-1


Flexibility
Programmable
Pluto AS-i
Pluto All-Master
Safety PLC with static and dynamic safety inputs.
Not programmable
Vital
Dynamic "doubled up" safety signal that tests a sensor, for example, 200 times per second.
Master
Slaves
Traditional safety PLC
Master-Slave with static inputs
Safety relay
Double static inputs that only test the switches each time they are used.
Number of machines/different stops

To achieve PL e using a conventional safety relay, such as RT9, you need to use both channels on the input side and only connect a single safety device. Under certain conditions PL d can be achieved by connecting multiple two-channel devices to a safety relay, but this is not a generally accepted method. Vital is a safety controller that allows you to connect and monitor a variety of safety components in series, and to achieve PL e to EN ISO 13849-1. The Vital module is based on a dynamic single-channel concept and can replace multiple safety relays. A similar solution, although more flexible, is safety PLC Pluto. Pluto, like Vital, is able to make use of dynamic signals to achieve maximum reliability.

Benefits of Vital

- It is possible to connect up to 30 safety components through a channel in line with PL e
- No programming required
- The option of combining various safety components (e.g. emergency stop button and door contact)
- Easy configuration of the circuit
- Electromechanical switches can also be used (with the addition of the Tina adaptation device)

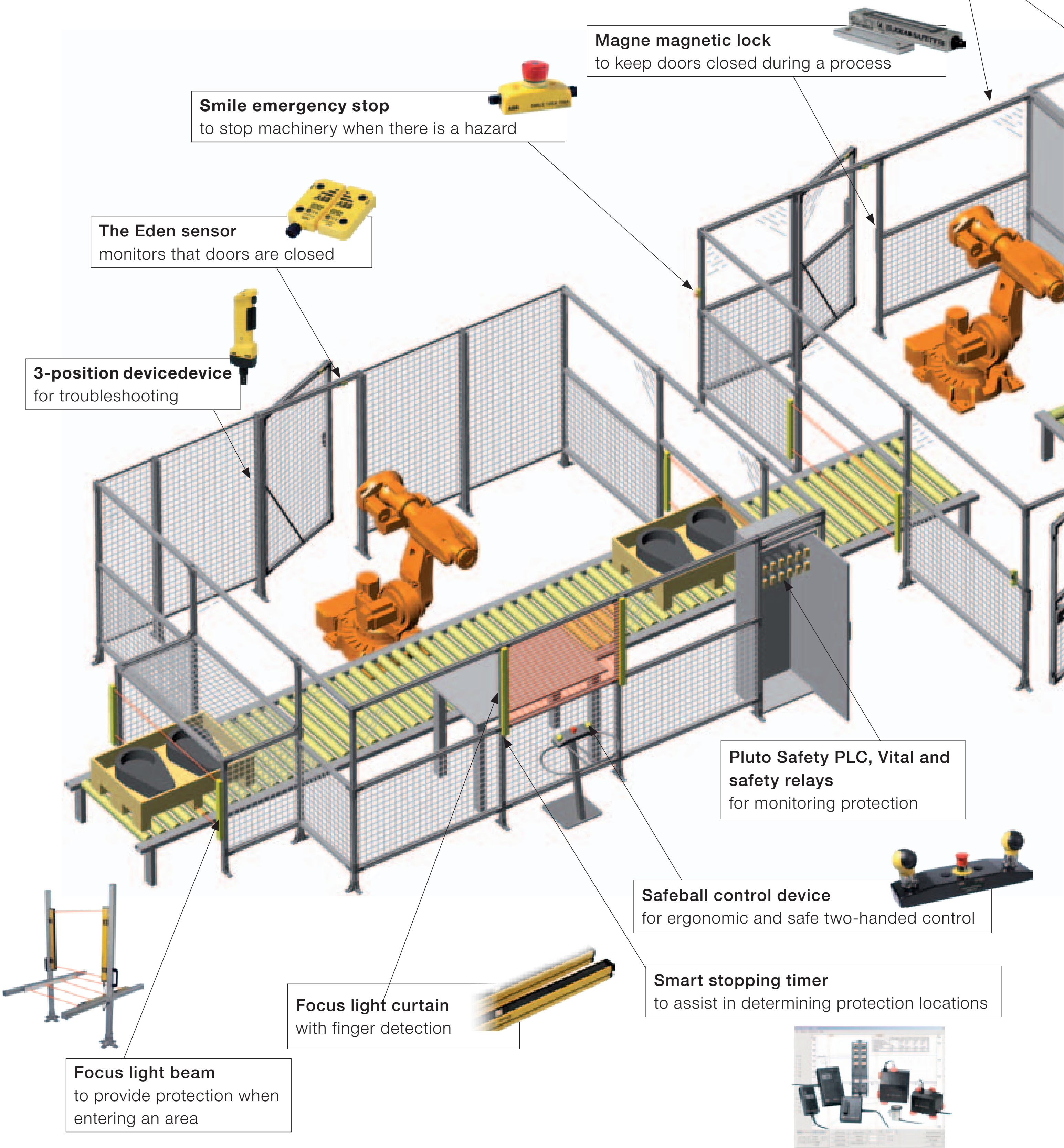
More than 70,000 Vital systems have been successfully installed.

Benefits of Pluto

- Pluto is an all-master-system with communications across a separate safety bus
- Greater flexibility facilitates the design of protection systems
- One software for all systems
- Easy programming for PL e by using function blocks (certified by TÜV)

More than 30,000 Pluto systems have been successfully installed.

Production-friendly safety systems from ABB Jokab Safety



Quick-Guard fencing system
prevents unauthorised access and offers noise reduction

Magne magnetic lock
to keep doors closed during a process

Smile emergency stop
to stop machinery when there is a hazard

The Eden sensor
monitors that doors are closed

3-position devicedevice
for troubleshooting

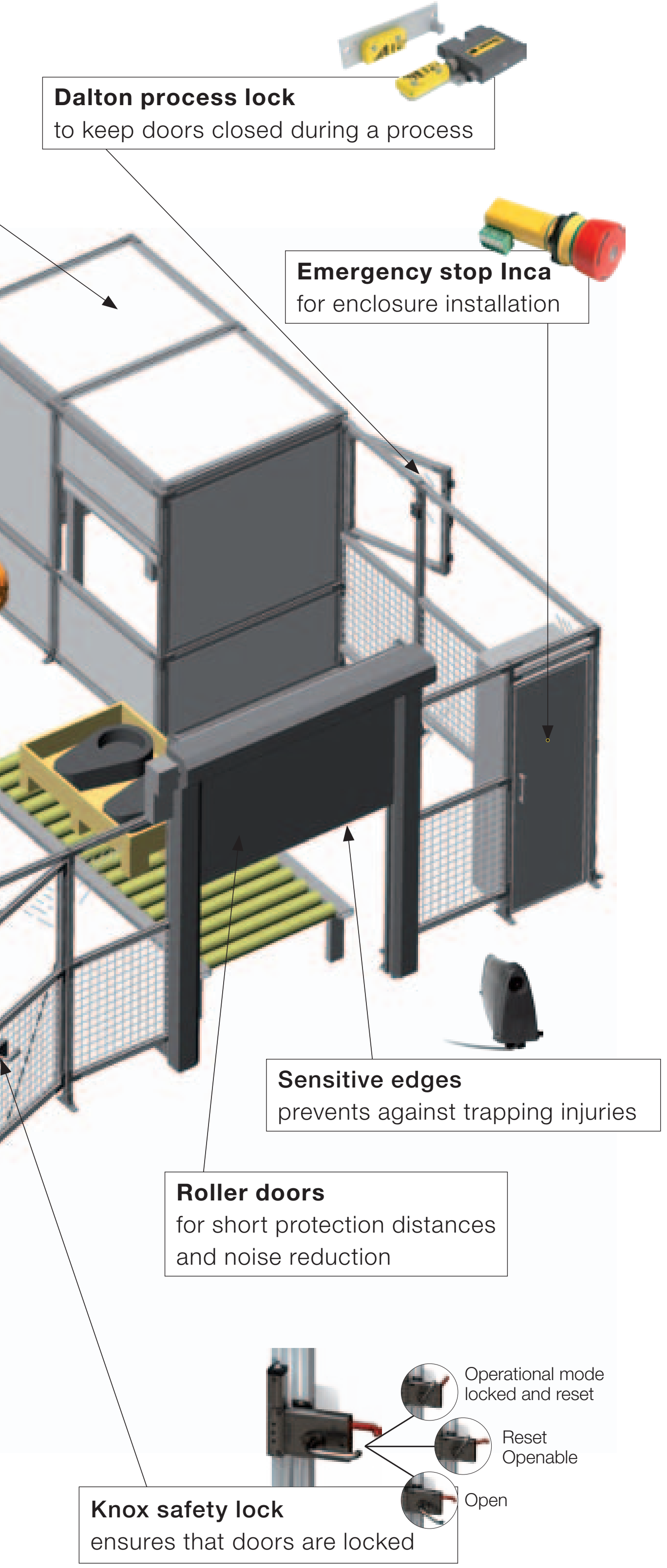
Pluto Safety PLC, Vital and safety relays
for monitoring protection

Safeball control device
for ergonomic and safe two-handed control

Smart stopping timer
to assist in determining protection locations

Focus light curtain
with finger detection

Focus light beam
to provide protection when entering an area



Dalton process lock
to keep doors closed during a process

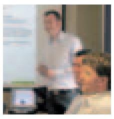
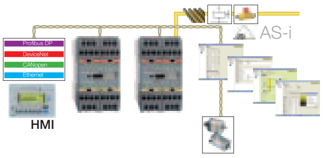
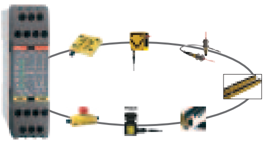
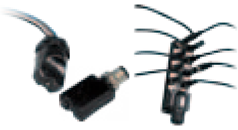
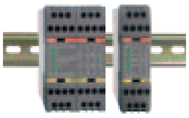
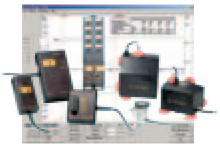
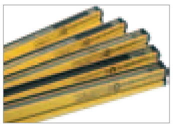
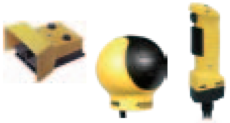
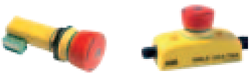
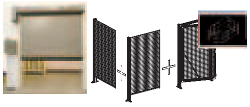
Emergency stop Inca
for enclosure installation

Sensitive edges
prevents against trapping injuries

Roller doors
for short protection distances and noise reduction

Knox safety lock
ensures that doors are locked

Product groups

	**Training & Advice** Practical application of standards and regulations, along with CE-labelling.
	**Pluto Safety PLC** A unique All-Master safety PLC for dynamic and static safety circuits.
	Pluto AS-i Programmable safety system AS-i where all units are connected to the same bus cable and the function of the unit is determined in the PLC program.
	**Vital safety controller** Dynamic safety circuit for multiple protection according to the highest safety category
	**Tina adapter units** Transformation of static signals to dynamic safety signals, etc.
	**Sadety relays** The market's most flexible safety relays for different protection purposes and categories.
	**Stopping time & machinery diagnosis** Used for stopping time measurement, annual maintenance and for trouble-shooting machinery.
	**Light curtain/light beam/scanner** Complete range of light beams, light curtains and scanners.
	Sensors/switches/locks Dynamic non-contact sensors, safety switches, magnetic switches and locks.
	**Control devices** Ergonomic three-position control units, two-handed control units and foot pedals.
	**Emergency stop devices** Emergency stop devices for dynamic and static safety circuits.
	Contact strips/Bumpers/Safety mats Sensitive edges bumpers and safetys mats.
	**Fencing systems/SafeCAD/Roller doors** A stable and flexible fencing system that is easy to install.

Contact us

ABB AB
Jokab Safety
Tel. +46 300-67 59 00
www.abb.com/lowvoltage

2TLC172003B02002 ABB Jokab Safety, 2011

Power and productivity
for a better world™