EN ISO 13849-1

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:

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})

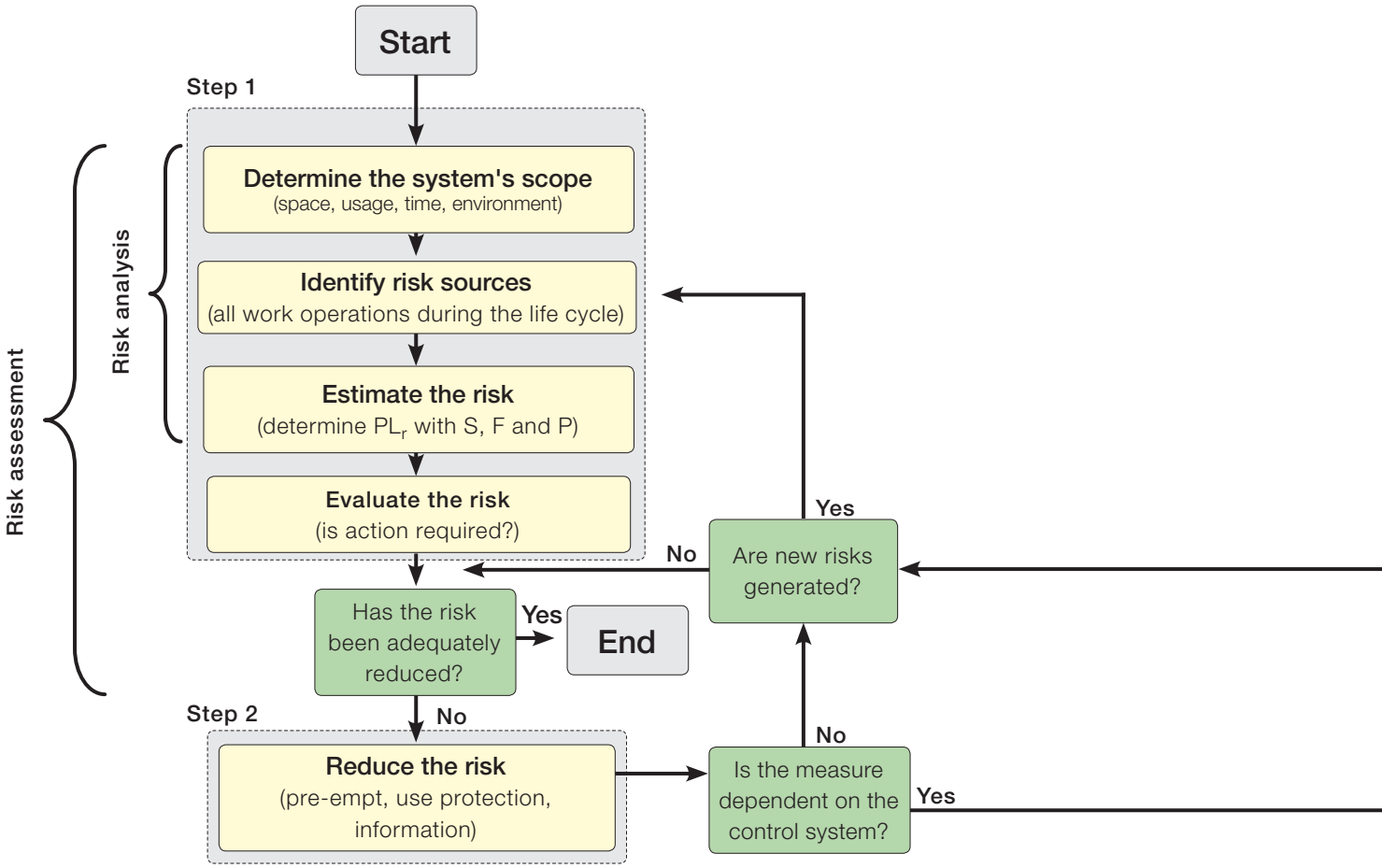
CCF Common Cause Failure

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



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

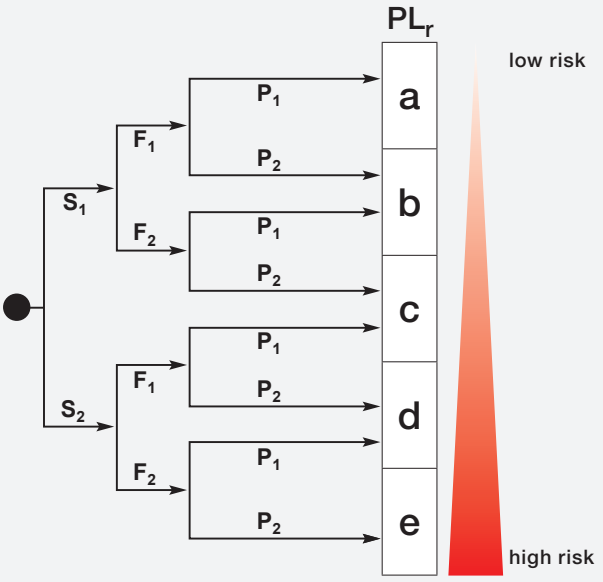
By setting S, F and P for the risk, you will get the PL_r Performance Level (required) that is necessary for the risk source.

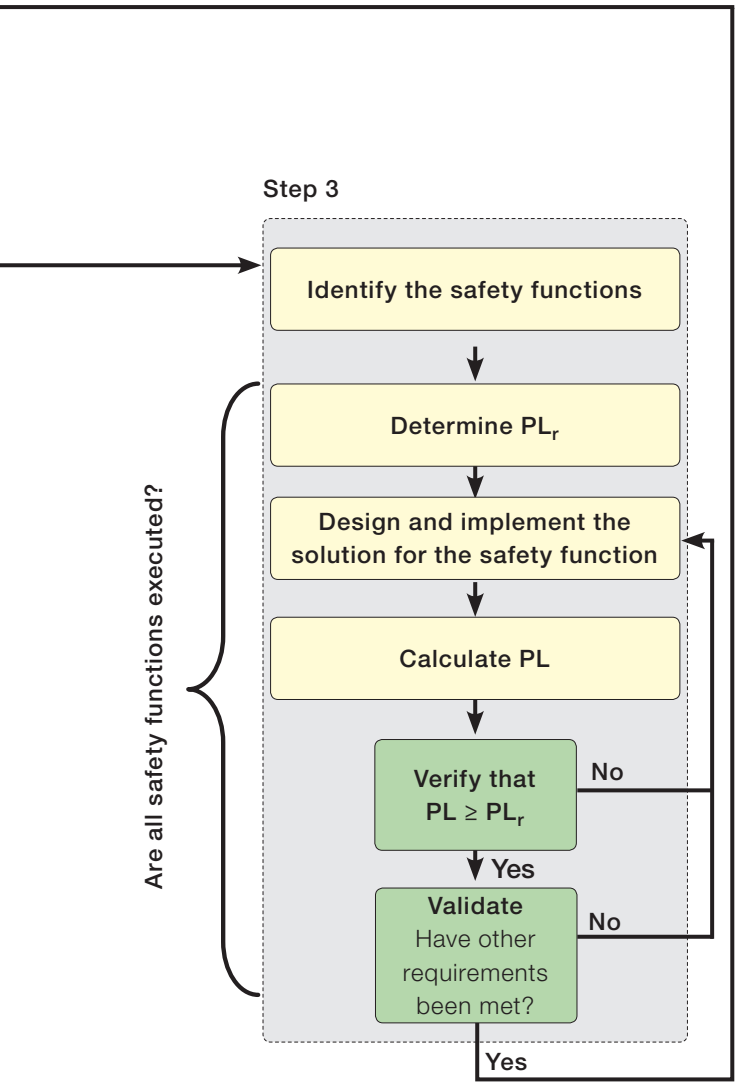
Finally, the risk assessment includes a risk evaluation where you determine if the risk needs to be reduced or if sufficient safety is ensured.

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.