Say 'NO' to safety reliability calculations

A White Paper presented by:
Mike Garrick
Product Marketing Lead Specialist
INTERFACE Relays
Phoenix Contact
P.O. Box 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300
Fax: 717-944-1625
Website: www.phoenixcontact.com

Say "NO" to safety reliability calculations for safe motor control

Key concepts:

- EN 954-1 will be replaced by EN ISO 13849-1.
- Proper device safety certifications will simplify machine design and lessen responsibility.
- Commonly used electromagnetic/safety contactors will require additional effort to incorporate into safety circuits for motor control.
- New hybrid safety starter technology reduces machine safety design effort.

Introduction

Machine safety standards are changing and this will affect machine builders who export into the European Union. It also affects those who use the risk analysis and safety categories defined in EN 954-1 "Safety of Machinery-Safety Related Parts of Control Systems." Associated with this change is additional manufacturer responsibility due to the requirement of "functional safety."

This paper will review the effect of these changes in regard to a simple safety design strategy and will introduce readers to a new safety motor starter technology that is pre-certified to meet the new safety standards, removing the need for additional safety reliability calculations.

Background

EN 954-1 is the safety standard that originally defined the machine control safety categories that OEM machine builders exporting machines to the European Union (EU) must adopt. It will become obsolete in the near future. Machine builders will now have the choice between two international "Functional Safety" standards to embrace in regard to their machine safety designs: EN IEC 62061 and EN ISO 13849-1. This change is happening due to the complexity of safety circuits, including the use of control components within safety circuits and ambiguous parts in the risk assessment. EN 954-1's deterministic approach did not compensate for the reduction of systematic failures found in today's complex functional safety schemes. This need has driven machine safety to migrate to different standards.

ISO 13849-1, entitled "Safety of Machinery – Safety-related Parts of Control Systems – Part 1: General principles for design," is the first choice for machine builders.

The abstract for this standard from the International Organization for Standardization (ISO) states:

> "ISO 13849-1 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery. It does not specify the safety functions or performance levels that are to be used in a particular case. ISO 13849-1:2006 provides specific requirements for SRP/CS using programmable electronic system(s)."

It's expected that machine builders will migrate without too much difficulty toward the ISO 13849-1. This standard builds on and recycles information from EN 954-1. Safety categories, along with the new elements of Mean Time To Failure Dangerous ($MTTF_d$), Common Cause Failures (CCF) and Diagnostic Coverage, will be used to formulate the new safety categories, called "performance levels."

Safety categories range from Category B to Category 4. Performance levels will range from performance level "a" to the highest performance level of "e." The new standard takes a probabilistic approach to determining performance levels, as opposed to the EN 954-1's deterministic approach. Calculating the performance level during the design stage will require some additional information.

Please note that all of the design thoughts using the safety categories from EN 954-1 can be built upon to determine the performance level. The safety category is combined with the new aspects of MTTFd, Diagnostics Coverage and Common Cause Failures to reach an accurate performance level. When looking at safety-rated components that are not electromechanical, a simple cross table can be used to estimate the performance level. (See Table 1.) Electromechanical parts will need the proper calculations to verify the exact performance level.

Table 1. Safety categories compared to performance levels

Safety category per EN 954-1	Equivalent performance level per ISO 13849-1
Category B	Performance Level a
Category 1	Performance Level b
Category 2	Performance Level c
Category 3	Performance Level d
Category 4	Performance Level e

Second choice is IEC 62061 "Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems." This standard must be used in conjunction with IEC 61508, which is the functional safety set of general rules to design a machine safety system.

Using the IEC 62061/61508 will present many unknowns to the designer. "Safe Failure Fraction," Hardware Fault Tolerance and Probability of Failure on Demand will all need to be supplied by the vendor or calculated by the machine safety designer.

It is common opinion that machine builders will migrate toward the ISO 13849-1 instead of the IEC 62061. This belief is due to the fact that the knowledge gained in EN 954-1 can be used or "recycled" in ISO 13849-1. Safety categories are actually part of the equation to determine a performance level, therefore providing a known starting point.

This paper's focus on ISO 13849-1 is based on the assumption that ISO 13849-1 will be more popular.

Safety-related components of a control function

To understand how to take advantage of proper product selection for machine safety control circuits to meet the ISO 13849-1 standards, the designer must first understand what safety control components are involved. Safety control functions can be broken down into three main components:

• Input – Inputs receive signals to enable the control to recognize an unsafe event. A common example of an input device is a light curtain.
• Logic – Monitors the input and output, determining the proper course of action to ensure safety. The logic element could be a simple safety relay, safety controller or a safety PLC.
• Output – Is the power control element that ensures safety. For example, it might stop motion. In a motor control safety circuit, this element could be a simple electromechanical or safety contactor.

Figure 1 below shows a very commonly used safety system. A light curtain (input) is being monitored by a safety relay (logic). When the light beam is broken, the safety relay will shut off the safety contactor (output) to effectively stop the hazardous motion. Referring back to the safety control function components, the input is the light curtain. As an input device, light curtains will be available pre-certified to ISO 13849-1 with a designated

performance level. In this example, it is shown as Performance Level "e" (PLe). The logic in this example circuit is a safety relay, which is also available pre-certified for use in a PLe safety circuit. The output in this example is a standard electromechanical or safety contactor, which will not have a designated performance level. This is due to the fact that safety contactors are electromechanical devices with a wide range of application. Manufacturers cannot anticipate usage, therefore a performance level value per the ISO 13849-1 will need to be calculated.

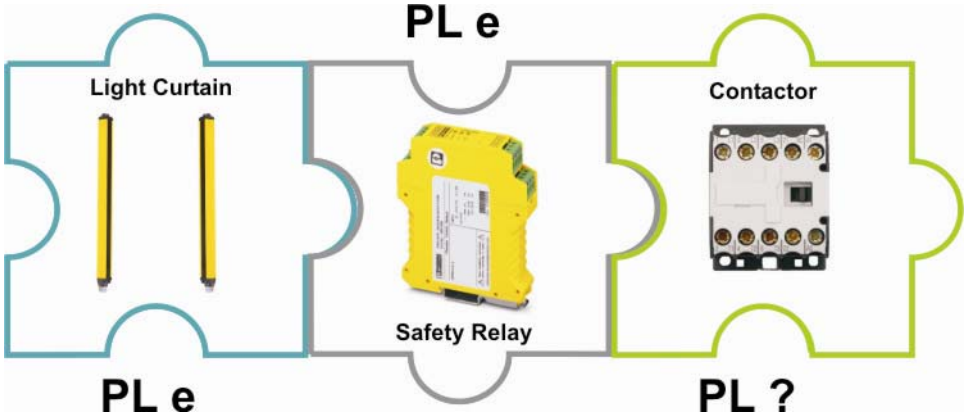

Figure 1. Safety circuit rated for Performance Level "c"

The designer must calculate the performance level of the contactor or safety contactor in order to rate the overall performance level of the safety circuit. Along with knowing the safety category, which in this case for a single safety contactor is safety category 2, the safety designer must obtain the Diagnostic Coverage (DC) value, evaluate the Common Cause Failures (CCF) list and calculate a value known as the Mean Time to Failure Dangerous ($MTTF_d$).

DC is identification of all online tests and diagnostics. Obtaining the DC value for a safety contactor itself is straightforward. It can be supplied by the manufacturer or can be found in Annex E of ISO 13849-1. For a single channel, safety category 1 circuit DC is not required. Note that the single safety contactor deems this contactor as single channel safety category 1 device due to the requirements of safety category 2 not being met. Note: There is no redundancy or test allowing safety category 1 to be excluded.

CCF is a list of prevention methods found in Annex F of ISO 13849-1. For each prevention method used, points are awarded. After going through the list, the designer adds up all of the points for each supported prevention method. If the sum is equal to or greater than 65 points, then the CCF prevention is approved. Note that CCF is not relevant for single channel circuits. For a single channel safety category 1 circuit, CCF is not required. Note that the single contactor deems this circuit as single channel safety category 1 device due to the requirements of safety category 2 not being met.

$MTTF_d$ is a statistical value and does not reflect the actual component lifetime. To start calculating the $MTTF_d$, a B10 or B10d value must be obtained. $B10_d$ is the number of switching cycles whereby, statistically, 10 percent of components failed in a dangerous state. This value is either supplied by the manufacturer of the contactor or worse case values can be obtained from ISO 13849-1.

With this value, $MTTF_d$ can be calculated as follows:

$MTTF_d = B10_d/0.1*n_{op}$,
$n_{op} = (d_{op}*h_{op}*3600s/h)/t_{cycle}$

n_{op} is the average number of cycles per year.
d_{op} is the number of operating days/year
h_{op} is the number of operating hours/day
t_{cycle} is the cycle time in seconds

Solving the formula is as follows, assuming a $B10_d$ value of 2,000,000. (Value given in ISO 13849-1)

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 \frac{s}{h}}{t_{cycle}} = \frac{250d \cdot 16h \cdot 3600 \frac{s}{h}}{30s} = 480.000$$

$$MTTF_{dK} = \frac{B_{10d}}{0.1 \cdot n_{op}} = \frac{2.000.000}{0.1 \cdot 480.000} = 41.67 \text{ years} = \text{high}$$

MTTF has three different levels. Values outside of this table are not allowed. See Table 2.

Table 2. MTTF levels

MTTF level	MTTF Time Range
Low	3 to 10 years
Middle	10 to 30 years
High	30 to 100 years

With a known safety category of 1, no DC required and an $MTTF_d$ value, a performance level "c" (PLc) can be derived from ISO 13849-1. See Figure 2.

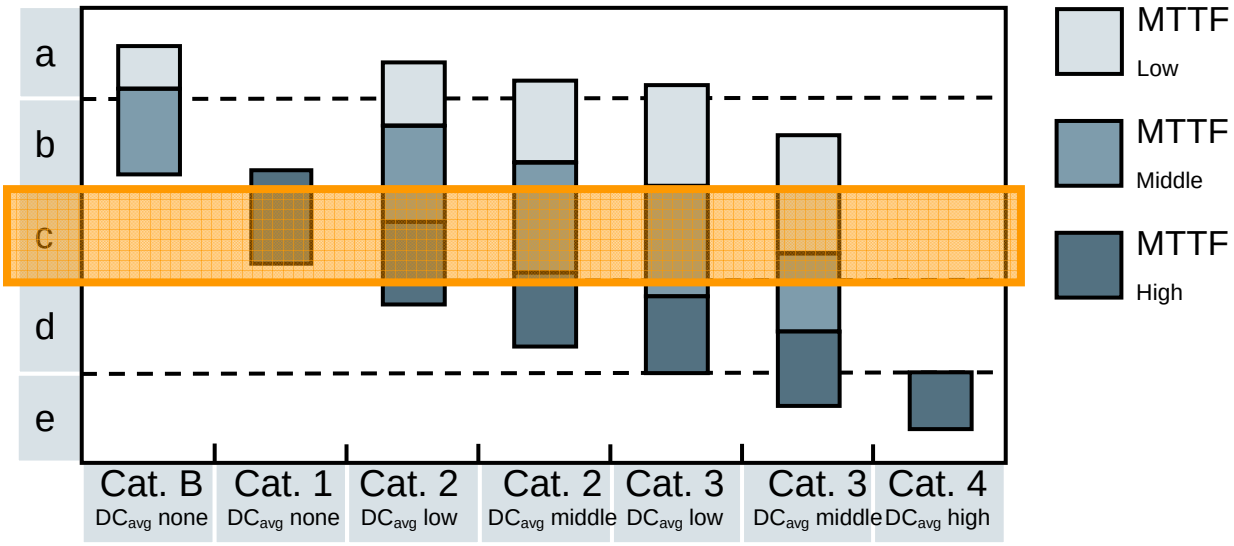

Figure 2. Performance level selection

With the use of one safety contactor in the Figure 1 example, the performance level is "c" circuit due to the single safety contactor being the "weakest link," if you will. This single safety contactor limits the overall safety rating of the safety control. If this is undesirable, a second safety contactor could be added for redundancy. This will bring the circuit up to at least a safety category 3. Safety category 3 warrants that the Common Cause Failures list is completed from Annex F of ISO 13849-1. If the score is above 65, then the design can continue. For a category 3

safety circuit, the Diagnostic Coverage value is also required. DC can be obtained from Annex E of ISO 13849-1 or from the manufacturer. $MTTF_d$ will still need to be calculated for the redundant combination of contactors.

Figure 3 shows the approach using a "pre-certified" safety motor starter device. This example uses the CONTACTRON 4 in 1, a hybrid reversing motor starter that is safety rated for performance level "e" (according to ISO 13849-1) and safety integrity level 3 (according to IEC 61508). In this safety circuit, there are no weak links. When the manufacturer certifies every product as "PLe," it is easy to see that the overall safety rating for the entire circuit is performance level "e." In addition, the machine safety designer is confident that his safety circuit meets the requirements of the ISO 13849-1 standard and that there were no errors, wrong assumptions or safety reliability calculations.

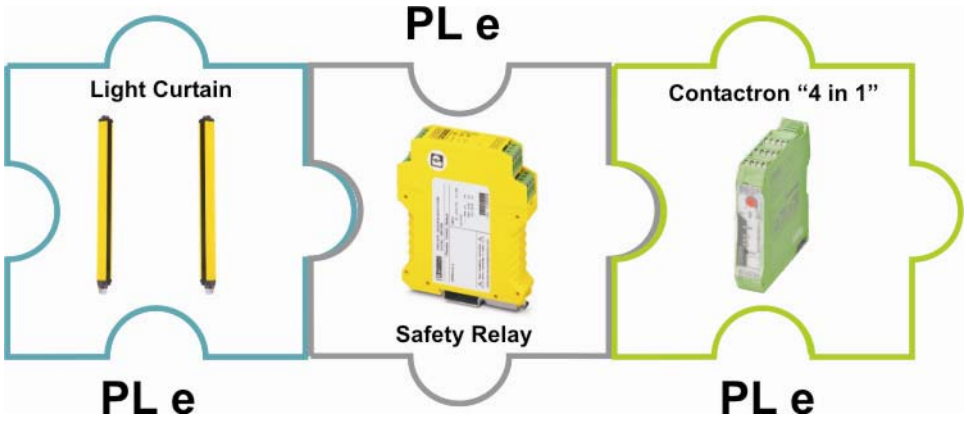

Figure 3. Safety circuit rated for performance level "e"

Summary

ISO 13849-1 will replace EN 954-1 as the preferred European standard for machine safety, affecting many machine builders outside of Europe. Using components with the proper safety certifications in regard to performance level (PL) or safety integrity level (SIL) will reduce engineering and lessen safety circuit liability. Properly rated components will have the required safety reliability data readily available from the manufacturer. In contrast, safety circuits based on safety category using redundant safety contactors will not have reliability data available. Unfortunately, manufacturers of safety contactors will not be able to supply the data required to document the level of safety, according to ISO 13849-1 or IEC 62061. This is due to the fact that safety contactors are an electromechanical device, and the manufacturers cannot anticipate the exact use. Therefore, manufacturers cannot generically present reliability data to determine the required degree of safety for a safety control circuit.

Once again, pre-certified devices will reduce design effort, reduce responsibility and ultimately reduce the machine builder risk.

About Phoenix Contact

Phoenix Contact is a world leader in electrical connection, electronic interface and industrial automation technologies. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 46 international subsidiaries, including Phoenix Contact USA in Middletown, Pa. Global sales exceed more than1 billion euro annually. Phoenix Contact's formal Integrated Management System is registered to ISO quality, environmental and safety standards (ISO 9001:2008,14001:2004 and 18001:2007).