WHITE PAPER

ISO 13849: Why implementing a redundant contactor is a wise investment

This white paper outlines the basic safety principles and importance of the B10d value and the benefits of using redundant safety-rated contactors according to the ISO 13849 safety standard.

Safety challenges in the industry

The study of safety function failure in the industry has proven that contact welding is a common problem. Opening a circuit creates an arc each time it's opened. Combined with high short circuit currents or high loads, in some situations the conducting metal can reach its melting point and the two contacts can stick together. The contactor or switch will then never open.

The use of redundant contacts might seem extreme, but without redundancy the machine will never stop. Contactors are an affordable device. Implementing a second redundant contactor is a wise investment that could prevent a catastrophic event.

About the ISO 13849 safety standard

The ISO 13849 – Safety of Machinery Package provides the safety requirements and guidance on the design and integration of safety related parts of control systems. It specifies the characteristics to identify the performance level required for carrying out safety functions and should be applied, regardless of the technology and energy used.

ISO 13849-1 covers general principles for design, and provides safety requirements and guidance on the principles of design and integration of safety-related parts of control systems.

ISO 13849-2 focuses on validation. It specifies the procedures that should be followed for validating by analysis or tests, the safety functions of the system, and the category and performance level achieved.

In Part 1, the design of the safety system is based on the risk assessment of the process. This risk assessment identifies the safety functions required to mitigate risk and the performance level these functions need to meet to adequately mitigate the identified risks. The performance level of a function is determined by the architectural characteristics of the safety function (classified according to categories), the Mean Time to Dangerous Failure (MTTFd) of the components and system, and the average diagnostic coverage implemented in the system. The principle is that not only should the control system be able to perform the safety function to a level that will mitigate the identified risk, but also do so in the presence of a failure.

Applications under the ISO 13849 safety standard

Many machine manufacturing facilities use automated processes with loads that are in motion. These moving parts always require a risk analysis to determine the appropriate measures to protect workers from hazards. After this analysis is conducted, it's necessary to assess the type of protection that's needed and determine the level of performance required for the application. The level of danger, the probability, the frequency and the possibility of avoidance will be decisive in the choice of the required circuit.

Ideally, machine designers should use fixed guards or lock out/tag out (LOTO) strategies to ensure safety. However, there are certain situations where LOTO can't always be applied effectively, especially when interventions are frequent and repetitive.

When a machine requires human intervention to remove a jam condition or load the product, a strategy involving a monitored removable guard or a light curtain must be adopted. In addition, everything must be connected and monitored by a safety control circuit.

How to determine the required performance level

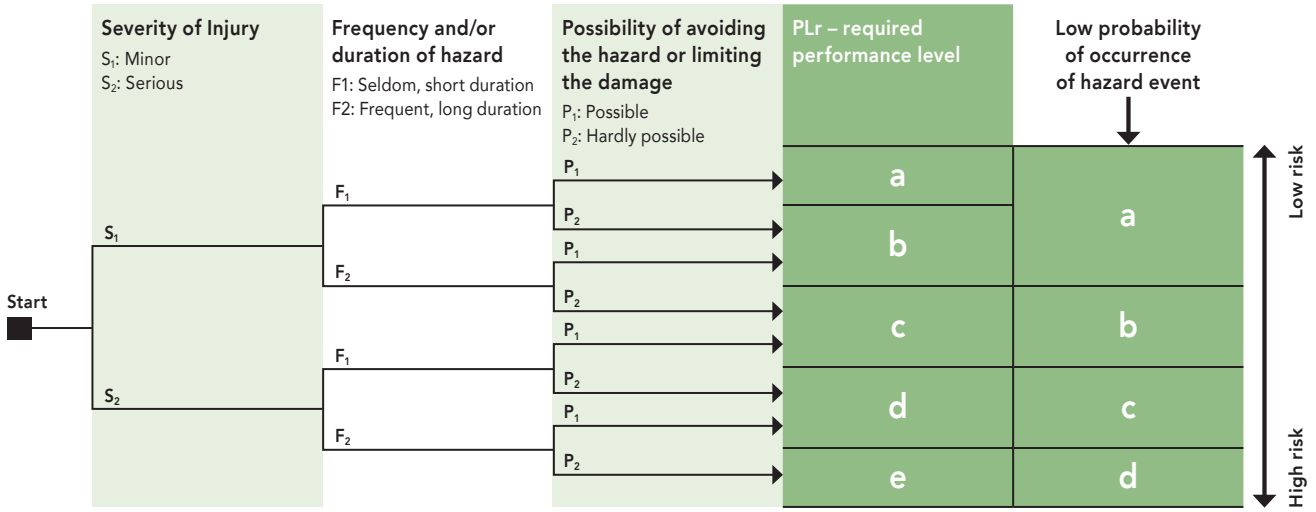
For example, at a food machine manufacturer, a worm screw feeding a machine must be accessible for cleaning and removing a jam in operation. During both procedures, jog must be allowed, making padlocking impossible since power needs to be applied to the motor to perform jogging of the motor. Working at normal speed with an open guard isn't an option, as the power of the motor and the screw could crush the hand of the operator. In addition, this procedure is required to be performed several times per shift. However, the screw works at low speed in inching mode and a horn and a light beacon warns the operator before their departure.

According to ISO 13849-1, this situation has an S2 severity with an F1 frequency and a P1 possibility of avoidance. Therefore, the required performance level is D, meaning a security system must meet this level of performance.

Required Performance Level (PLr) According to ISO 13849-1

This standard also uses a risk graph to determine the required safety level. The parameters S, F and P are used to determine the magnitude of the risk.

The result of the procedure is a "required performance level" (PLr).



To build a system with a performance level D, it's critical to design a safety function that considers all components. If not, the result will be no better than the weakest link in the chain.

According to ISO, the five fundamentals of performance level are: Structure, Reliability, Diagnostic, Resistance and Process.

Performance Level				
CATEGORY	MTTFd	DC	CCF	TEST
Structure	**Reliability**	**Diagnostics**	**Resistance**	**Process**

Once the level of performance has been determined, it's possible to meet the requirements for each fundamental to maintain the required level of performance.

5 fundamentals for establishing the required level of performance

1. Structure

The first fundamental focuses on structure of the control system, based on how many elements are used to build the control strategy. The structure refers to standard En 954-1, where the architecture of the security system was dictated according to five categories (B, 1, 2, 3 and 4). This approach has been integrated into ISO 13849 to become one of the five fundamentals for establishing a security function.

Category	Summary of Requirements
B	Safety-related parts of control systems should achieve their functions, and should withstand expected stress (vibration, EMC, etc).
1	**Category B +** Use of well tried safety components.
2	**Category B +** Safety function(s) shall be checked at appreciation intervals.
3	**Category B +** A single fault does not lead to the loss of safety function. Where practicable, a single fault shall be detected.
4	**Category B +** A single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to the loss of safety function.

Structures B and 1 are non-redundant and their level of reliability is based on the choice of components. Category 2 is similar to B and 1, but includes a test function that verifies the operation periodically. Structures 3 and 4 are redundant and include a plausibility function.

In a redundant system, the component set is simply duplicated and a verification function is added. Two inputs are evaluated and compared – and if one of the two is in a different state, the function will be disabled and restarting the function will not be allowed. The same will be done for the output elements. If one of the two outputs has a fault, the function will not be reset.

2. Reliability

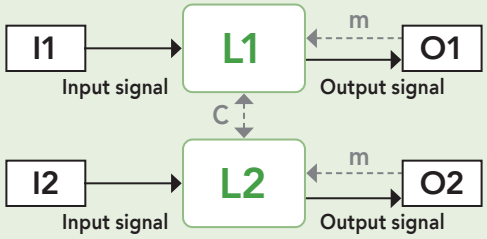
Reliability is an important basis because the redundancy of two unreliable components doesn't help to reduce the probability of dangerous failure – a breakage compromises the safety function (SRP CS). The standard therefore regulates the level of reliability, or MTTFd per maximum hour, depending on the level of performance targeted.

3. Diagnostic Coverage

Diagnostic coverage is the frequency at which the verification of entry and output is done. The standard also regulates the type and level of diagnostic coverage according to the level of performance to be achieved.

The table below indicates the relationship between the level of three key parameters (Structure, Diagnostics, Reliability) and performance level, a band of probability of dangerous failure.

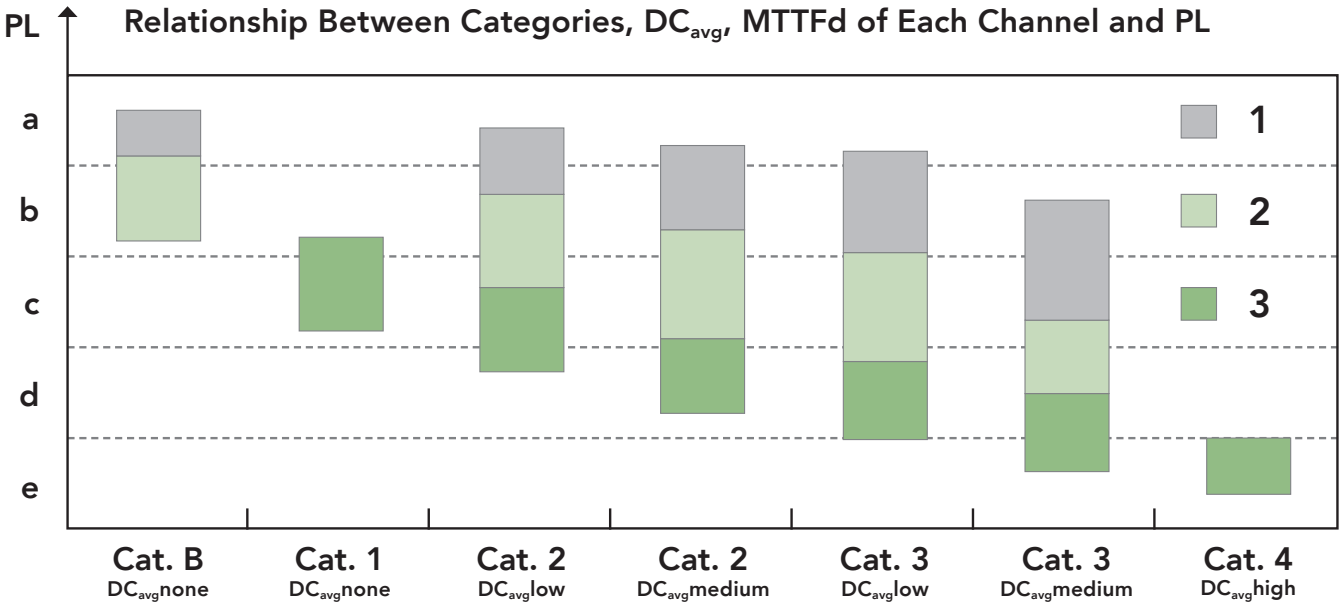
Configuration Applicable to Category 3 and Category 4



m = Monitoring
C = Cross monitoring

In Category 3, safety function may be lost due to accumulation of undetected faults.

The redundancy of architecture shown in these block diagrams can mean not just physical meaning but also internal logic from which the single fault tolerance is confirmed.



KEY
PL Performance Level
1 MTTFd of each channel = low
2 MTTFd of each channel = medium
3 MTTFd of each channel = high

It's possible to achieve the desired performance level by using different combinations of Structure, Diagnostics, Reliability.

For example, to reach a performance level D, there's the choice of a Cat 2 or Cat 3 structure. The non-redundant Cat 2 structure requires average diagnosis and a high MTTF. The diagnostic side is impossible to achieve with electromechanical components, such as a contactor. Checks require the opening of the circuit, which can't be done constantly without affecting contactor lifetimes and interrupting the process.

Therefore, a structure of Cat 3 should be considered. This isn't much more expensive than Cat 2, and it can be easy to create with currently available components. In addition, its redundancy meets the principles of control reliability in certain North American standards.

In this example, the parameters that must be followed include:

- Cat 3 structure
- A diagnosis of Low to Medium
- A MTTF from Medium to High

Diagnostic: How to assess the level of diagnosis

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

In this example application, two safety contactors can be used with linked contacts to evaluate the position of the power contacts via an NC auxiliary contact. This type of assembly achieves the requirements for an average diagnostic coverage range of 90% to 99%.

DC	
DENOTATION	**RANGE**
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

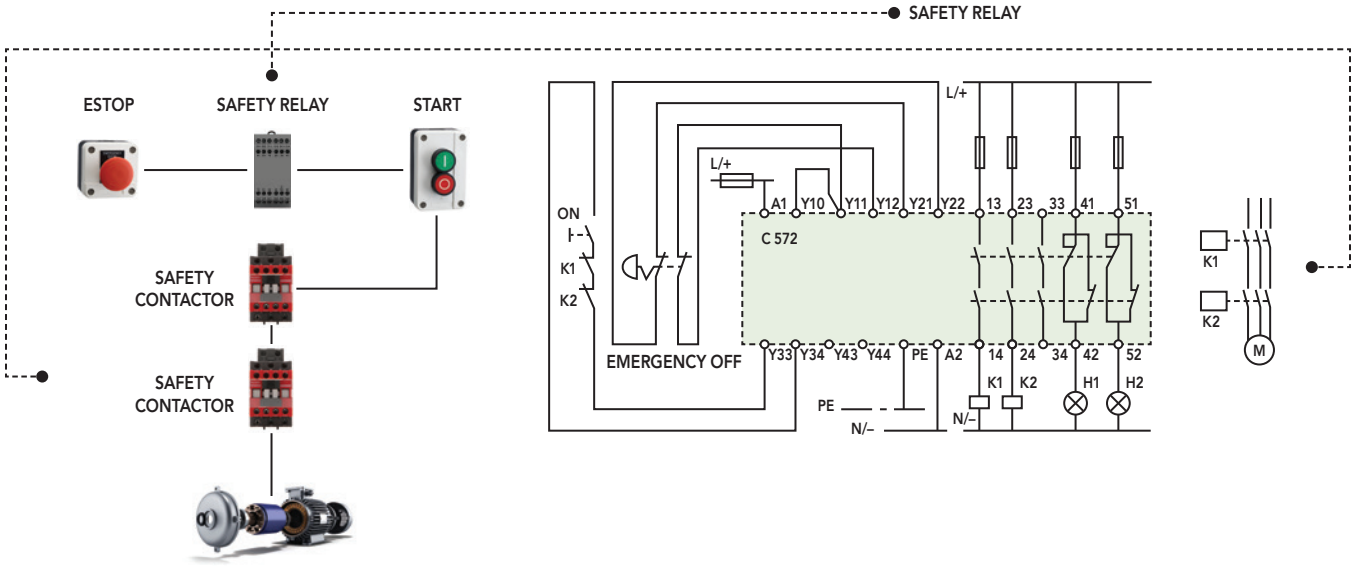
MTTFd

In a safety system, MTTFd is the calculation of how often a piece of equipment or safety system fails in a way that threatens the safety of workers, the environment or equipment. MTTFd is critical to the determination of the performance level of a safety system.

Contactor manufacturers like NOARK provide the B10d values for components, which indicates the number of cycles where 10% of the component fails to danger. MTTFd can easily be determined by the B10d value.

For example, if a motor is a 5HP, at 460 volts 3 phase, the number of operations per day is 200, 5 days weeks, and the control voltage is 24 VDC. The contactor that should be chosen is an Ex9CAD11B, from the Ex9CA series that's specially designed to meet the standard IEC 60947-4-1 and IEC 60947-5-1 (mirrored contacts and mechanically linked contacts).

The construction is such that if the power contacts are stuck or welded, the NC auxiliary contact attached won't change state. This ensures that the integrity of the logic of the circuit responsible for supervising the contactors is maintained. The relays must see a closed loop before a restart can happen. In the industry, this is called an external device monitoring (EDM) function. This is usually performed by the safety controller or a safety light curtain.



For example, in 200 operations per day, the calculation for the contactor's yearly operation will be:

52 weeks x 5 days x 200 = 52,000 operations per year

The B10d value published by NOARK for a contactor under load is 4075230. By dividing the yearly operation by the B10d value, the result is 78 years. This corresponds to a High level of MTTFd, according to ISO 13849-1:2015, which is compatible with the desired safety function.

ISO 13849-1:2015	
	YEARS
Low	3 ≤ MTTFd < 10
Medium	10 ≤ MTTFd < 30
High	30 ≤ MTTFd < 100

4. Common Cause of Failure (CCF)

The fourth fundamental states the system must be resistant to the most common failures. For categories 2, 3 and 4, the system must obtain 65 points. The table below can help calculate the worth of each measure.

Measure Against CCF		
CAUSE		**SCORE**
1	Separation / Segregation	15
2	Diversity	20
3	Design / Application / Experience	
3.1	Protection against over-voltage, over-pressure, over current, etc.	15
3.2	Components used are "WELL TRIED"	5
4	Assessment / Analysis	5
5	Competence / Training	5
6	Environmental	
6.1	Pertaining to the power source for electrical and fluid power EMI, RFI, Filtration, Drainage, Dirt Entry (All according to Manufacture's Specifications)	25
6.2	Temperature, Humidity, Dust, Shock, Vibrations	10

Common measures include separation of redundant signals, use of NO and NC contacts at the input, and use of certified components according to the correct voltage and current. Protection against transient over voltage and electromagnetic interference is also required. It's critical to follow temperature, humidity and environmental specifications, and to implement proven components and state-of-the-art techniques.

5. Process

The final step is to document the process and test the function. Once everything is working flawlessly, it can be put into service.

Summary

Because contact welding is a common problem, implementing a second redundant contactor is a wise investment that could prevent a catastrophic event. Order the ISO 13849 standard to become familiar with more details of how to realize a safety function.

About NOARK

NOARK Electric is a global supplier of low-voltage electrical components for specialty manufacturing industries. We strive to provide our customers with high-quality products at an affordable price, backed by a five-year limited warranty. We are committed to becoming a leader in cost-effective components through the development of innovative products and continuous improvements, while demonstrating integrity, trust and honesty.

NOARK Electric North America
(626) 330-7007
na.noark-electric.com • nasales@noark-electric.com