White paper

PRACTICAL SAFETY SOLUTION FOR SETUP MODE

SAFETY EVALUATION OF A REDUNDANT ROTARY ENCODER WITH USE OF A SAFETY MINI CONTROLLER

SCHMERSAL
THE DNA OF SAFETY

CONTENT

WHITE PAPER

PRACTICAL SAFETY SOLUTION FOR SETUP MODE

Safety evaluation of a redundant rotary encoder with use of a safety mini controller based on an example safety function and its quantification in Sistema

For setup mode or troubleshooting on machinery, the ‘Safely limited speed with opened guard door’ safety function is extremely relevant. The following white paper from the companies Schmersal and Wachendorff presents an example safety solution involving a redundant rotary encoder and a safety controller and evaluates the solution in accordance with EN ISO 13849.

Authors: Christian Lumpe, Product Manager for Controllers, Schmersal Group, and Steffen Negeli, Product Manager & Technical Sales, Wachendorff Automation GMBH & CO KG

INITIAL SITUATION

Let us consider a typical production line as might commonly be found in the packaging industry.

The operator will typically be protected from expected hazardous movements by an enclosure. Access to the danger zone is provided by a guard. From the perspective of machine safety, a minimum requirement is for the operator to not be in danger when the guard is opened, i.e. the drive should be unable to move. The possibility of bringing the system to a halt with an emergency-stop button should also be considered, in most cases.

Fig. 1: Production line in the packaging industry

To simplify setup of the production line or troubleshooting, it is often a good idea to configure the system in such a way that the hazardous drive system is allowed to run at a reduced speed, even with the guard door open.

In addition to the

- ‘Protection against unexpected start-up’ and
- ‘Halt with emergency-stop device’ safety functions, an additional safety function must also be considered,
- namely ‘Safely limited speed (SLS*) with opened guard door’

*Safely Limited Speed – in accordance with EN ISO 61800-5-2

SAFETY OF MACHINERY – THE EN ISO 13849 STANDARDS

We will apply the EN ISO 13849 standard to our example machine so we can determine and verify the required level of safety. When compared to DIN EN 62061, this standard has the benefit of being easier to handle, provided the technical implementation complies with certain formalisms.

Part of the concept of EN ISO 13849 is being able to demonstrate the capability to execute a specified safety function under the predictable conditions. This capability is expressed using the 'Performance Level (PL)', which corresponds to a probability of failure. The standard specifies five PL stages, which are labelled 'a' to 'e' in the ascending order of effectiveness and capability to reduce the risk. In contrast, there is an evaluation of the risk of a machine, which usually uses risk graphs to illustrate a target Performance Level, the so-called PLr (r = required).

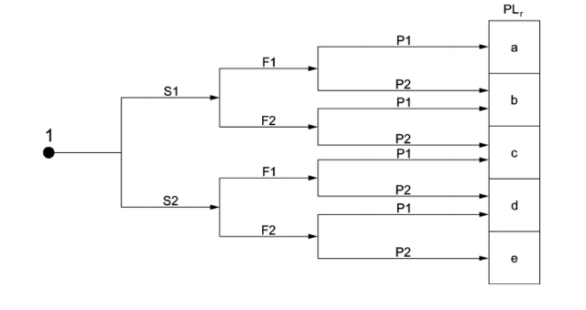

Fig. 2: Risk graph © Beuth Verlag

The risk evaluation for the example machine in this white paper has produced a PLr of d. This PL can be implemented in a number of ways. The standard provides an initial assessment with the following overview.

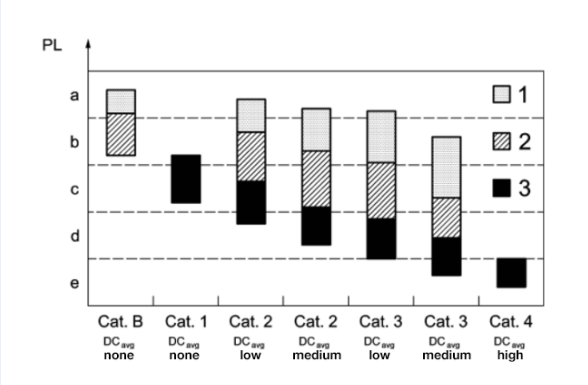

Fig. 3: Possible combinations of categories, MTTFD and DC
© Beuth Verlag

Category 3 is usually suitable for technical implementation as it allows dispensing with a test channel, which would be required in category 2. This testing is often difficult to implement, especially with mechanical systems. Category 3 requires single-fault safety, which can usually be achieved with a consistent two-channel configuration.

STANDARD COMPONENTS IN SAFETY FUNCTIONS

A rotary encoder can be used to measure speed. The market offers a number of certified devices for safety applications. Depending on the application, it can be worthwhile to use standard components as well – whether for cost reasons, as the additional effort required for the manufacturer is reflected in the price of the components, or because standard components offer a better solution to the applicative issue.

The required verification regarding the suitability of the solution for safety applications is more easily achieved with components that have already been certified, as the manufacturers of these components guarantee compliance with the respective standards. It does, however, remain the responsibility of the operator to ensure correct installation taking into account the anticipated ambient conditions of the machine, including the temperature and EMC.

If standard components are used in a safety function, the machine designer or integrator of the component is responsible for evaluating their suitability for the safety application. The following text serves as an aid, but does not in any way replace an independent application of the relevant standards and directives.

STRUCTURE OF THE SAFETY FUNCTION

Which components are involved in the safety function? In addition to the rotary encoder, which is used to detect the speed, the evaluation logic, such as the PSC1 safety controller from Schmersal, and the drive system itself, usually the monitoring of the guard door has to be part of the considerations, as this is what normally activates the SLS function. Of course, there may be other solutions, but the further procedure will nevertheless be identical.

In the structure above, consideration of the rotary encoder for speed detection is of particular relevance. The other components are safety components – consequently, the overall PL is obtained by simply adding the individual values together.

The simplest approach to achieving the two-channel system required would be to use two separate encoders, which would need to be fitted at different locations in order to be mechanically two-channel. In practice, however, this is often time-consuming and complicated. Hence, it is more practical to only have to use one mounting location. The rotary encoder from Wachendorff combines these two properties. It comprises two completely independent encoders employing different technologies in a single enclosure. This enables straightforward installation. Moreover, the internal redundancy satisfies the requirements of category 3.

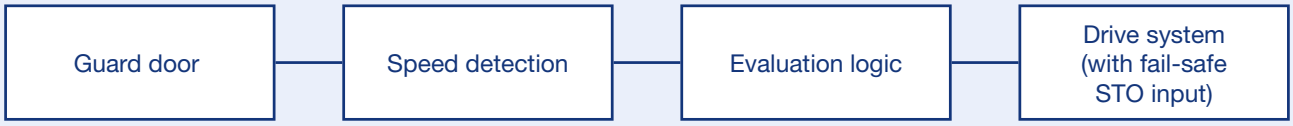

Fig. 4: Structure of the safety function

STRUCTURE OF A REDUNDANT ROTARY ENCODER

In principle, a redundant rotary encoder comprises two fully autonomous standard rotary encoders, which means that the electronic part of the rotary encoder can be viewed as a two-channel system. Only the mechanical structure, comprising a shaft and bearing assembly, is single channel in its design. The standard for electrical drive systems, EN 61800-5-2, provides for consideration of the error case when the mechanical link between the rotary encoder and the drive system is lost. In many cases, error exclusion is required as the controller cannot necessarily detect such errors. This error exclusion can be achieved with appropriate dimensioning of the attachment elements and by using a 100% reliable mechanical link (e.g. with a free-running, positive locking joint between the shaft and the drive system using a keyway and key).

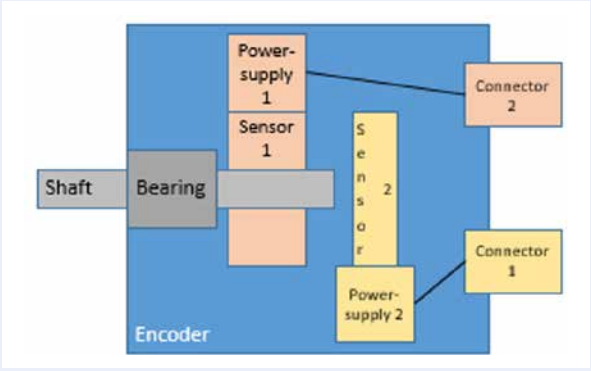

Fig. 5: Basic structure of a redundant rotary encoder

TYPES OF A REDUNDANT ROTARY ENCODER

As an example, Wachendorff offers three different types of redundant rotary encoders – the WDGR (incremental optical/incremental magnetic), WDGE (incremental optical/absolute magnetic) and WDGB (absolute optical/absolute mechanical). This ensures maximum flexibility in application and regarding the use of additional components as well as the option to choose from a comprehensive set of non-certified standard products. All three types rely on the principle of diversity, which means that the failure safety is increased by using different measuring principles and in so doing, as few components of identical construction as possible. The basic philosophy underpinning this procedure is that the different sensor platforms respond with varying degrees of sensitivity, or insensitivity, to malfunctions of different kinds and consequently, do not drop out concurrently, thus allowing the downstream electronic system to reliably detect this potential failure. Designing this approach, Wachendorff have used their range of tried-and-tested sensor systems developed over many years. In specific terms, the redundant standard rotary encoder provides divergent (magnetic and optical) signals, which are generated completely independently of each other, but which can nevertheless be correlated with each other. Even the supply voltage is available separately for each sensor unit. This refers to the optical and magnetic incremental rotary encoders, as well as to the magnetic absolute rotary encoders.

Fig. 5a: Redundant incremental rotary encoder WDGR by Wachendorff

‘SPEED DETECTION’ SUB-SYSTEM

The core of EN ISO 13849 is the calculation of a probability of failure of the controller solution. The purely mathematical approach, i.e. a calculation based on MTTFD values only, is not sufficient on its own. Rather, systematic and environmental influences must be taken into account, i.e. that the components have been designed for the application’s anticipated conditions.
As Fig. 3 shows, a PLr of d requires components with a high MTTFD value (mean time to failure dangerous) of more than 30 years at a minimum and/or a high-value diagnostic (DC - Diagnostic Coverage) of more than 90%. Considering the sub-system of encoder and evaluation alone, we get the following block diagram.

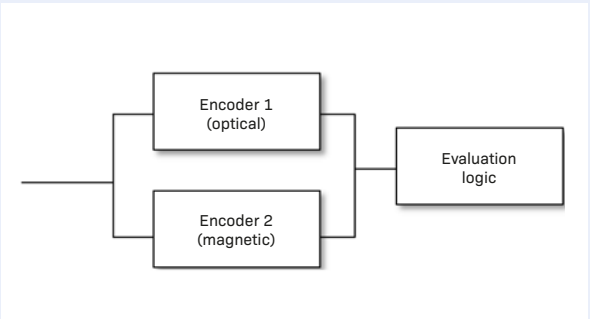

Fig. 6: Block diagram of the structure of rotary encoder and evaluation logic

As explained, category 3 requires a single-failure proofing, which is provided by the continuous two-channel capability of the speed/direction detection in the rotary encoder. The error coverage (DC) that is required is not integrated into the encoder, but must be covered by the evaluation logic.

The PSC1 series of safety controllers from Schmersal is a pertinent example. If required by the application, as many as twelve axes can be reliably monitored, with the rotary encoders connected easily via D-sub interfaces. By cross comparing the two encoder signals or, in case of sin-cos encoders, by evaluating the relationship $\sin^2+\cos^2=1$, errors can be detected and a response to the error initiated.

Figure 7a:
PSC1 safety controller

In addition, the SafePLC2 programming tool for the PSC1 integrates function blocks for the main monitoring functions, such as SLS, SOS or SCA, in accordance with DIN EN 61800-5-2. These can be easily integrated into the safety logic program, as illustrated by the following image of the programming logic in our example safety function.

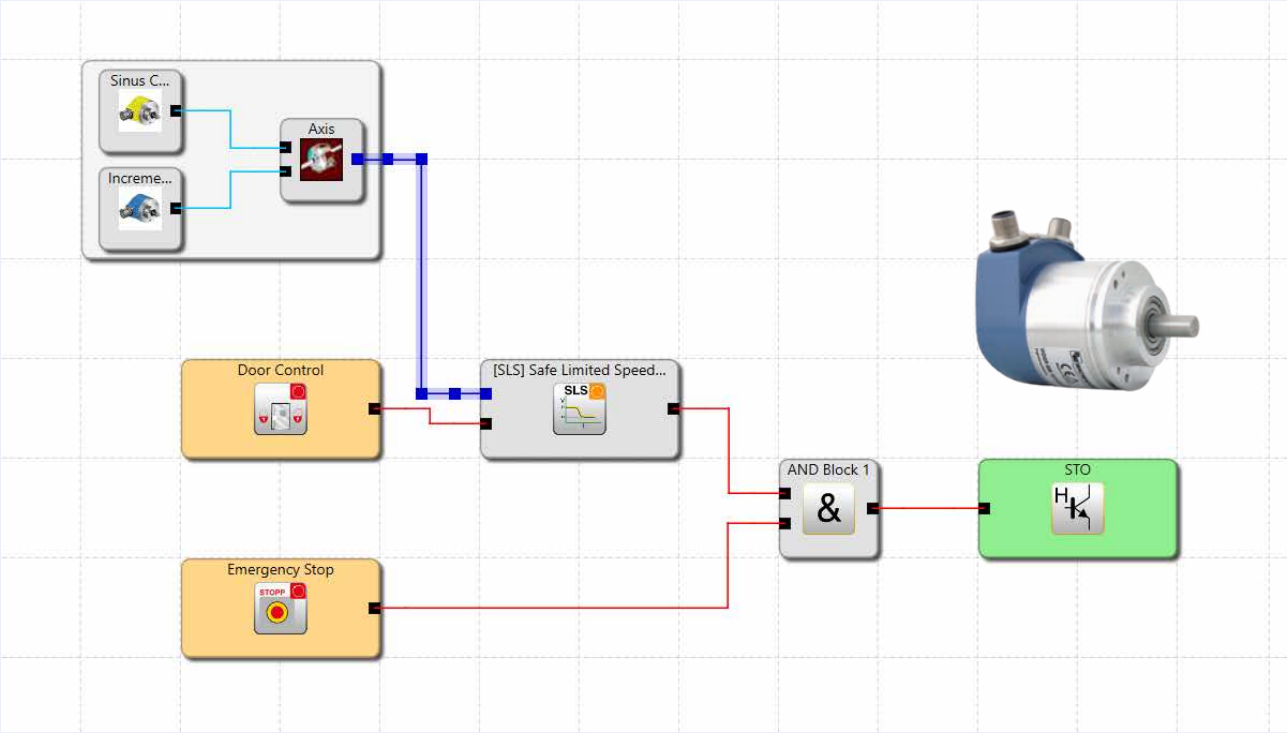

Fig. 7b: Programming in SafePLC2

Thanks to this straightforward programming, the likelihood of errors is minimised and the traceability of the program in terms of validation or in the event of extensions to the machine is simplified. A necessary parametrisation of the encoder path, such as the resolution, can be carried out intuitively within dialogue windows.

ERROR EXCLUSION REGARDING THE MECHANICAL LINK BETWEEN SHAFT AND ENCODER

Particular attention should be given to the mechanical link between the encoder and the drive system, which is by design a single-channel configuration. The latter necessitates an error exclusion for this link since a single error here would lead to a hazardous situation.

The standard permits these kinds of error exclusion, provided that they are documented and substantiated (EN ISO 13849-1, sec. 7.3). In terms of mechanical error, reference is typically made to suitable over-dimensioning. But what does ‘suitable’ mean in this regard? A look at EN ISO 61800-5-2 offers some insight in the form of table D.8, which provides information on the justification for error exclusion.

In addition to verification of the maximum bearing capacity of the link (mathematical or through testing), the standard also demands that a FMEA is carried out for this error exclusion.

→ FMEA (Failure Mode and Effects Analysis)
This involves evaluating the effects and probability of different failure modes and outlining how they are managed, i.e. the measures taken or the limitations that apply.

An FMEA could be designed as follows, for example:

FMEA Subject: Redundant-diverse encoder on small safety controller PSC1
26.02.2021
CHLU, DABR, LILBE, STNE, HAPO

SCHMERSAL THE DNA OF SAFETY

No.	Component / Process	Function / Feature	Possible Error	B	Possible Error	Current / planned measures for error detection	E	Possible causes of errors	Current / planned measures for error prevention	A	RZ	Note
1	Connection Encoder-Shaft	Flange	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Connection is overloaded by excessive torque and thus loosens	none	10	1000	
				10		Fault exclusion	10		Oversizing for the application. Limit values are given in BA. Proof of loadability via calculation	7	700	Current solution with grub screwsnon flattening probably not suitable. Alternative connections are being examined
				10		Target/actual comparison	5			7	350	
	Connection Encoder-Shaft	Clutch	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed t	none	10	Connection is overloaded by axternal thrust	none	10	1000	
				10		Fault exclusion	10		Oversizing for the application. Note in BA. Recommendation if necessary	1	100	
				10		Target/actual comparison	5			1	50	
	Mounting encoder-machine	Bolting	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Connection loosens	none	10	1000	
				10		Fault exclusion	10		Correct dimensioning of the screws. Visual inspection, QEP	1	100	
				10		Target/actual comparison	5			1	50	
	Connection Encoder-Shaft	Grub screw	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Connection loosens	none	10	1000	
	Encoder	Detection of movement	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed on one channel	none	10	Damage due to e.g. vibration, shock, e.g. loosening of the pulse disc or the magnet	none	10	1000	
				10		Error detection in safety controller	1		Diverse encoder technologies	1	10	
	Encoder	Wiring	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Short circuits due to mechanical damage to the cables	none	10	1000	
				10		Error detection in safety controller	1		Separate cable routing	5	50	
	Encoder	Power-supply	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Power supply fails or overvoltage	none	10	1000	
				10		Error detection in safety controller plus supervision of power supply	1		Separate power supplies Prescribe PELV power supplies in manual	5	50	
	Encoder	Generating SSI-Signal	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Error in FW	none	10	1000	
				10		Error detection in safety controller	1		Diversity of encoder technologies at SSI/Incremental. With SSI different FW and HW realisation	2	20	
	Encoder	General	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	EMC	none	10	1000	
				10		Error detection in safety controller	1		Reference to compliance with environmental conditions in manual. Diverse structure	2	20	

Fig. 8: Example FMEA

Nevertheless, it is ultimately the responsibility of the design engineer, as is otherwise the case with the use of certified encoders, to ensure that the ambient conditions do not exceed the permissible values.

What still needs to be considered?

The following paragraphs discuss additional aspects that need to be taken into account in accordance with EN ISO 13849 to ensure that category 3 is satisfied.

■ Fundamental and proven safety principles

These must be observed for the mechanical aspects and for the electrical systems. This includes the use of suitable materials as well resistance to environmental stresses such as humidity or electromagnetic interference (EMC) or the over-dimensioning of mechanical links

■ CCF (Common Cause Failure)

In addition to calculating the probability of failure, measures to prevent failures with a common cause must also be implemented. This is to ensure that a single error cannot cause a concurrent failure of both channels, thereby creating a hazardous situation.

Potential measures to guard against a CCF are evaluated on a point scale in EN ISO 13849. Category 3 requires a minimum of 65 points in order to demonstrate sufficient consideration of errors with a common cause.

The following criteria are satisfied by the encoder system considered.

		Remark
Separation	15	Physical separation between signal paths by means of - Separate electrical structure - Separate power supply - Separate cable routing - Consideration of clearance/creepage distances
Diversity	20	Different technologies and/or physical principles
Competence	5	Designers' training to understand the causes and consequences of common cause failures
Ambient (mechanical -> environment)	10	Consideration of ambient conditions
Design/application/experience	15	Protection against overvoltage, overpressure, overcurrent, over-temperature, etc.
	65	

■ **Systematic failures**

The rotary encoder uses different physical principles (magnetic, optical) for the two channels, as well as mutually isolated and independent power supplies. Systematic failures in the software of the safety mini controller must be taken into account by the design of the software according the requirements of the standard (SRASW).

■ **$MTTF_D$**

The time until failure or error is given for both sensor systems as being significantly greater than 100 years. However, the standard requires a cap of 100 years. Consequently, the values for the encoder sub-system, even after symmetrisation of both channels, result in a $MTTF_D$ value of 100 years.

■ **DC**

The encoder itself does not have an error detection mechanism of any kind in the individual sub-channels, nor does it have an integrated, higher-level logic. The safety mini controller carries out error detection by means of a constant cross-comparison of the speed and direction information from the encoders. If the two values deviate from one another, the safe state is initiated. The 'Safe speed' safety function being considered is also a highly dynamic signal. The supply voltages of the two internal encoders are also monitored. The error detection rate is 99%.

As outlined above, a shaft breakage is excluded. Nevertheless, error detection can be accomplished via the safety mini controller, assuming that in the event of an error in the shaft link, the measured speed is lower than the actual speed.

If a higher-level field bus is used, the speed values can be read back from the safety controller and then directly compared with the values of the drive system control. If this option is not available, an additional signal – 'drive system running' – from the PLC can be used to execute a plausibility check at the mini controller.

This form of error detection does not, in principle, affect the category 3 requirement for single-failure proofing, but if an implementation is possible, this additional measure should be applied.

CALCULATING THE PL

If we consider the entire structure again, we get the following calculation with the following assumptions:

Guard monitoring: A type 4 safety switch is used in accordance with EN ISO 14119. The PFH_D value is specified by the manufacturer as 5.2E-10/h.

PES: The safety controller is certified for PLe. The PFH_D value is 1.38E-8.

STO: The probability of failure of the STO function is specified by the manufacturer of the frequency inverter as 3.2E-7 and corresponds to a Performance Level of d.

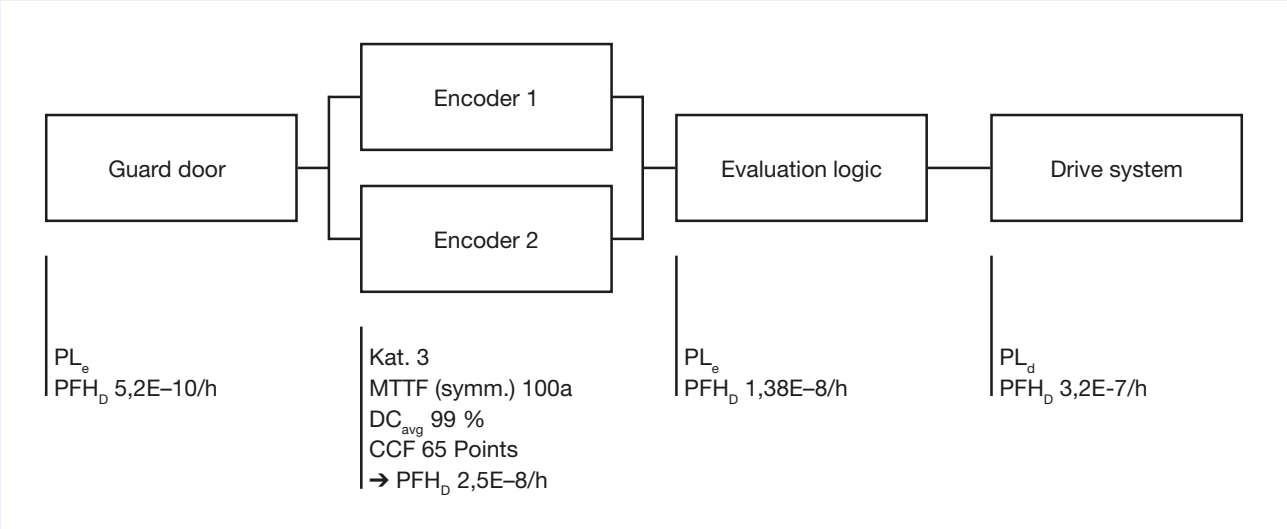

Fig. 9: Overall block diagram

CONCLUSION

The structure outlined allows for a Performance Level of d. The potential PL in our example is largely limited by the PL of the frequency inverter. Therefore, a high safety level can be achieved despite the partial use of standard components. In addition, the use of the redundant encoder simplifies installation.

Plus, the combination with the PSC1 safety controller facilitates additional safety functions such as an emergency stop or monitoring of additional safety circuits in a single device.

Authors:
Christian Lumpe
Product Manager for Controllers
Schmersal Group

Steffen Negeli
Product Manager & Technical Sales
Wachendorff Automation GMBH & CO KG

About the Schmersal Group:
The Schmersal Group is an international market leader in the challenging field of machine safety. With the world's most comprehensive range of safety switchgear products, the Schmersal Group develops safety systems and solutions for special requirements in a variety of user industries. Schmersal's tec.nicum business division offers a comprehensive service portfolio to complement the range of solutions offered by Schmersal.

Founded in 1945, the company is represented by seven manufacturing sites on three continents with its own companies and sales partners in more than 60 countries.

Contact:
K.A. Schmersal GmbH & Co. KG
Phone: +49 202 6474-0
info@schmersal.com
Möddinghofe 30
42279 Wuppertal
Germany

www.schmersal.com
www.tecnicum.com