IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Do safe drive controls also require safe position encoders?

1 Problem

In order for machines to be operated safely, safety functions are often required for the limitation of rotary and linear speeds, axis positions, etc. Frequency converters with integrated safety functions are used for this purpose, or safety PLCs, tachometric relays and similar components. The associated sensor technology for the detection of axis positions or rotary angles on spindles generally takes the form of position encoders with sine/cosine interfaces. These products are also increasingly available in safe versions intended for use in a specified Performance Level (PL) or SIL[1]. What advantages do safe sine/cosine position encoders offer over conventional products? What aspects need to be considered when "unsafe" encoders are used? These questions will be discussed with reference to an example safety function:

SF1, "limitation of a rotary spindle speed in setup mode"

This function is to be implemented in Performance Level PL d in accordance with EN ISO 13849-1 [1].

2 Implementation of the SF1 safety function

The SF1 safety function is to be implemented by the use of one or two rotary encoders together with a frequency converter with the integrated safety function of SLS (safely limited speed). Figure 1 shows the corresponding safety-related block diagram (selection of the operating mode is a safety function in its own right and is not therefore shown). The diagram consists of a subsystem G (rotary encoder) and an encapsulated subsystem T1 (frequency converter).

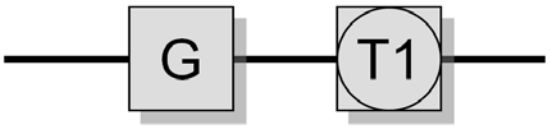

Figure 1: SF1 – safety-related block diagram

Encapsulated subsystems are components for which the manufacturer states the PL/SIL and the PFH[2], where applicable in conjunction with requirements concerning the products' use. The frequency converter T1 possesses interfaces for two sine/cosine encoders, and is able to perform fault-detection measures. The design of subsystem G is not clear, since it could be implemented by a range of architectures.

[1] SIL: Safety Integrity Level
[2] PFH: Average probability of a dangerous failure per hour

Before these architectures are considered however, the possible faults of rotary encoders must be determined. Component faults and their impacts upon the safety function ultimately constitute the basis for determining whether a single conventional rotary encoder is sufficient for attainment of PL d, whether two conventional rotary encoders are required, or whether safe rotary encoders must be employed.

2.1 Possible faults in rotary encoders

Figure 2 shows a cutaway view of a typical rotary encoder.

Figure 2: Rotary encoder (source: Fritz Kübler GmbH)

The encoder shaft, bearings, disc, electronics, housing and connector are visible. The functional structure of the encoder is shown in Figure 3.

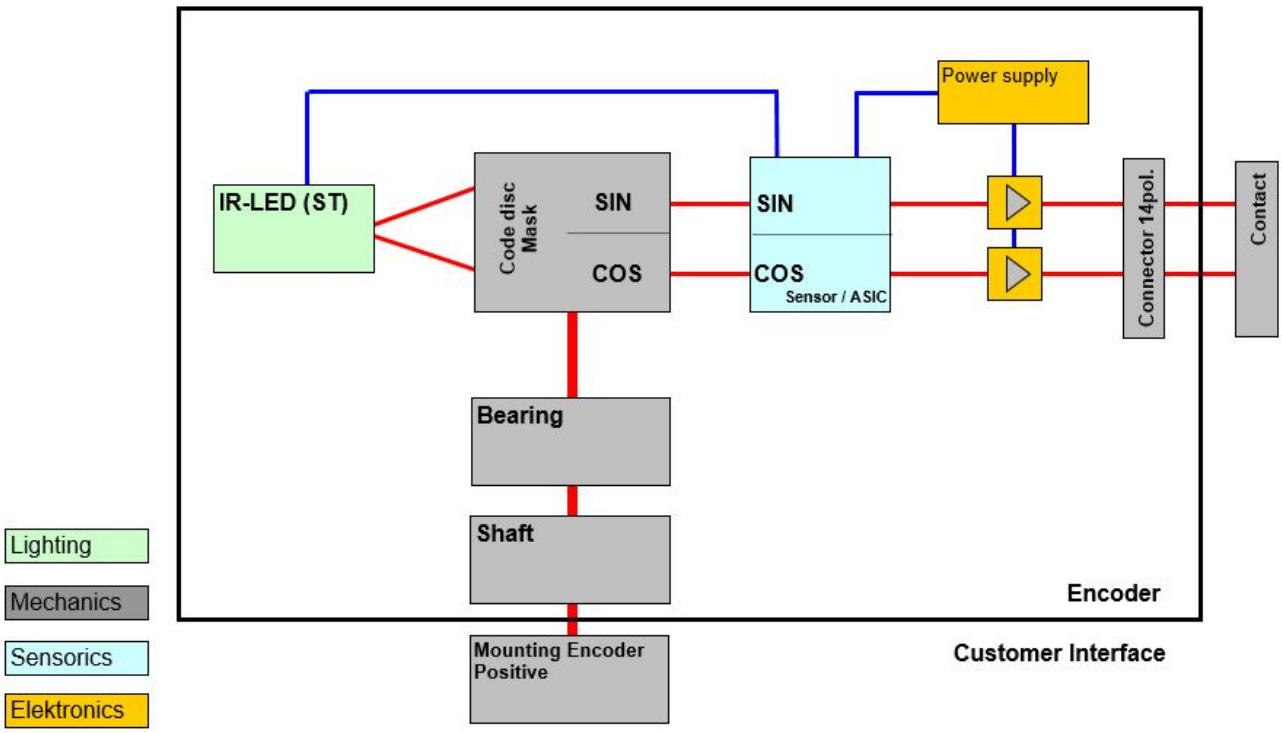

Figure 3: Structural arrangement of a sine/cosine rotary encoder (source: Fritz Kübler GmbH)

As this diagram shows, some of the functional elements of the rotary encoder are of single-channel design, others two-channel – assuming that sine and cosine are treated as two separate channels[3] (this will be discussed in more detail below). It is immediately apparent that mechanical faults on the shaft, bearings or disc could simultaneously affect the sine and cosine channels. Should for example the encoder shaft become detached from the motor shaft, changes in the motor position no longer lead to a (correct) change in the sine/cosine signals. Unless additional measures are taken, this fault cannot be detected in the frequency converter connected to the encoder[4], since the signals output by the encoder are still within the permissible range. Other component faults lead to falsification of sine and/or cosine output signals (see [2], Table D.16) which can be detected in the frequency converter by monitoring for $\sin^2(\varphi) + \cos^2(\varphi) = 1$.

2.2 SF1 with the use of conventional rotary encoders

The Performance Level required for the desired safety function, "SF1, limitation of the rotary spindle speed", is PL d. The encoder subsystem must therefore also satisfy at least PL d. PL d is possible in the designated architectures of Category 2 and Category 3 in accordance with [1].

Table 1: Requirements for Category 2 and 3 subsystems for use in PL d

Requirements for PL d	Category 2	Category 3
Basic principles ([3], Tab A.1, D.1)	Mandatory	
Well-tried principles ([3], Tab A.2, D.2)	Mandatory	
***MTTF*$_d$ of each channel**	High	Medium to high
Component faults	Testing at suitable intervals	• A single fault must not result in loss of the safety function • A single fault is detected wherever possible by reasonable means
DC	Low to medium	
CCF	Measures must be taken, see Annex F in EN ISO 13849-1	
Systematic failure	Measures must be taken, see Annex G in EN ISO 13849-1	
PFH	≥ 10^{-7} to < 10^{-6} per hour	

$MTTF_d$	Mean time to a dangerous failure
DC	Level of diagnostic coverage
CCF	Common-cause failure
PFH	Average probability of a dangerous failure per hour

[3] Sine and cosine signals are generated in the same optoelectronic ASIC. Owing to their signal form and phase difference, they can however be treated as separate channels; all dangerous component failures are detected by testing for $\sin^2(\varphi) + \cos^2(\varphi) = 1$.

[4] One possible additional measure is for example a plausibility check in the frequency converter, provided no external forces apply, as for example on vertical axes. If the motor drive signal is known and a corresponding motor movement is anticipated, comparison with the motor position signalled by the position encoder can identify a discrepancy and therefore a fault. Application of this method is difficult in practice and it will not be considered further here, since it requires detailed knowledge of the frequency converter, control circuit, motor behaviour, etc.

Since, when conventional encoders are used, no safety-related product data are generally available from the manufacturer, users are responsible for demonstrating that the requirements to be met by the encoder subsystem summarized in Table 1 for the example discussed here are actually met [4]. The first problems emerge at this point: the documentation required for evaluation, such as component lists, failure data of the components used, FMEA, etc., is not likely to be available in full to users. The support of the encoder manufacturer is therefore generally required.

An essential aspect is the behaviour of the encoder subsystem when component faults occur, and when they are detected. This will be discussed in more detail below.

2.2.1 Category 3, two conventional encoders

Figure 4 shows the schematic circuit diagram and the safety-related block diagram. The encoder system is formed by two conventional rotary encoders. The sine/cosine output signals from encoder 1 are processed in channel 1 of the frequency converter, those from encoder 2 in channel 2. For detection of encoder faults, monitoring is performed for $\sin^2(\varphi) + \cos^2(\varphi) = 1$; should this criterion not be met, a fault response is triggered. The speed is determined from the encoder signals in a two-channel arrangement in channel 1 and channel 2. Cross-checking detects faults in the frequency converter and to some extent also in the encoder.

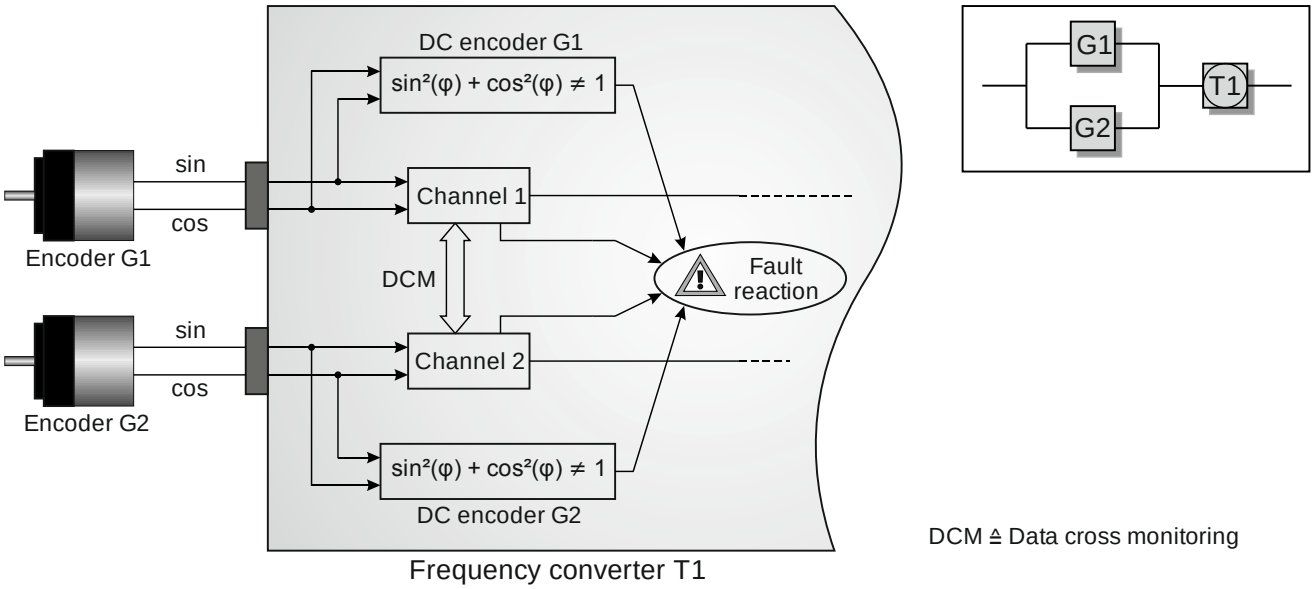

Figure 4: Two conventional rotary encoders and signal processing in the safe frequency converter T1

Category 3 requires single-fault tolerance, i.e. the incidence of a single fault must not lead to loss of the safety function. The architecture considered here is two-channel throughout; satisfaction of the requirement for single-fault tolerance should not therefore be a problem. Attention should however be paid to the mechanical coupling of the encoder to the movement in the machine that is to be monitored. A single fault must not simultaneously have dangerous effects upon encoder 1 and encoder 2. Alternatively, the two encoders can share the same mounting provided fault exclusion can be assumed for the movement/encoder coupling for at least one of the two encoders.

2.2.2 Category 3, a single conventional encoder

It can be seen clearly that in this architecture (see Figure 5), breakage of the connection between the encoder shaft and the drive shaft immediately results in undetected dangerous failure of the safety function, unless additional measures take effect in the frequency converter (e.g. comparison with anticipated behaviour).

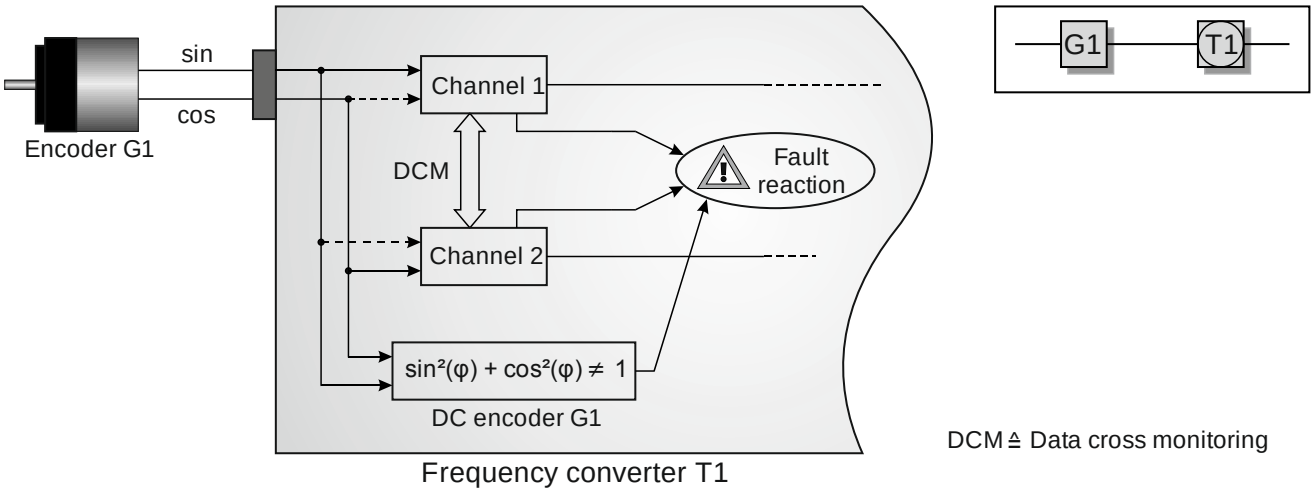

Figure 5: Subsystem G1 in Category 3 with a single conventional rotary encoder and signal processing in the safe frequency converter T1

Fault exclusion for the mechanical connection between the movement and the encoder is therefore absolutely essential. The encoder manufacturer must provide evidence of adequate strength for this purpose. Failure of the mounting causing the encoder enclosure to turn with the shaft may also have an effect upon the safety function, and must be considered (see [2], Table D.16).

Note: where the encoder is integrated into the control circuit of the motor, it could be assumed in the past that encoder faults caused by faulty motor commutation also resulted in fault detection via the process. However, modern control algorithms may at times operate in encoderless mode even when an encoder is connected; it can therefore no longer be assumed that faults will be detected quickly through disruptions in functioning of the machine.

Faults in the encoder and wiring faults are detected by monitoring for $\sin^2(\varphi) + \cos^2(\varphi) = 1$. Component faults can occur in which both sine and cosine channels fail dangerously (such as interruption in the power supply or wiring faults). This architecture is nevertheless able to satisfy the single-fault tolerance requirement for Category 3, since fault detection in the frequency converter by way of $\sin^2(\varphi) + \cos^2(\varphi) = 1$ is of high quality (DC ≥ 99%) and so fast (within the process safety time) that a dangerous state does not arise (see [5], Section 6.2.6). This structure does not satisfy the designated architectures of ISO 13849-1; the simplified method in the standard for calculation of the PFH, and therefore SISTEMA software, cannot be used in the first instance.

2.2.3 Category 2, one conventional encoder

If the encoder subsystem is implemented with only a single encoder and fault detection is not possible within the process safety time, a Category 2 solution may be possible. Figure 6 shows the schematic circuit diagram and the safety-related block diagram.

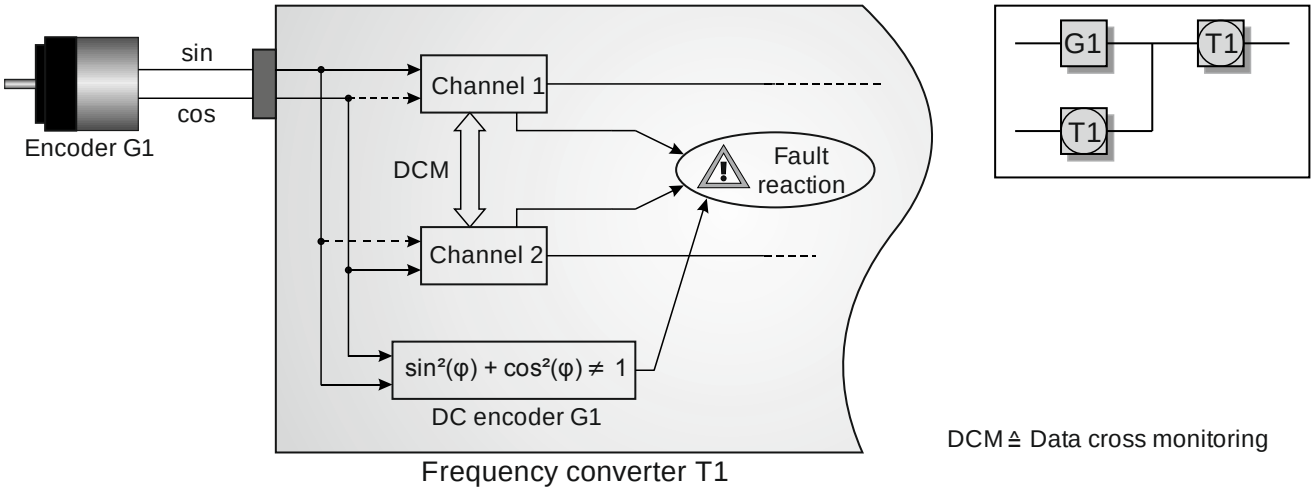

Figure 6: Subsystem G1 in Category 2 with a single conventional rotary encoder and signal processing in the safe frequency converter T1

Single-fault tolerance is not a requirement for Category 2; exclusion of mechanical faults is not therefore absolutely necessary. Strict requirements are however placed upon the $MTTF_d$ and the DC_{avg} for PL d. In the preceding example for Category 3 with a single encoder, a fault exclusion was assumed for breakage of the coupling between movement and encoder. This was the only means by which single-fault tolerance could be attained, since no measures whatsoever are available for fault detection. This mechanical fault can also not be detected in Category 2. The principle of Category 2 is however that the safety function is tested at reasonable intervals. This condition cannot be met, owing to the lack of a facility for testing. In the absence of fault exclusion for coupling of the movement and encoder, implementation of the "single encoder" subsystem is therefore also not possible in Category 2.

2.3 SF1 with the use of a safe rotary encoder

All necessary safety-related data for safe encoders are stated by the manufacturer; they therefore constitute an encapsulated subsystem (see Figure 7).

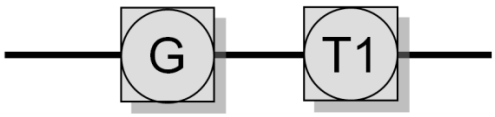

Figure 7: SF1 – safety-related block diagram

Only the following is then necessary for the SF1 safety function considered here:

- Select an encoder that is suitable at least for use in PL d
- Calculate PFH_{SF1}: $PFH_{SF1} = PFH_{encoder} + PFH_{T1}$
- Check whether the fault detection stipulated on the data sheet for the encoder is performed by the frequency converter T1

2.4 What is different for PL e?

If the SF1 safety function assumed in the example is to satisfy the requirements for Performance Level PL e, the requirements for the encoder subsystem differ from those for PL d as follows:

- $MTTF_d$: medium/high → high
- DC_{avg}: low/medium → high
- If the function is implemented in Category 4, attention must be paid to the possible accumulation of undetected faults.
- The information in ISO/TR 23849 [6] on the application of fault exclusions must be considered.

A sufficiently high $MTTF_d$ can – as always – be achieved only by the use of a suitable encoder.

Should checking for $\sin^2(\varphi) + \cos^2(\varphi) = 1$ fail unnoticed, the next fault may lead to dangerous failure of the safety function. This is not permissible in Category 4. Further measures are therefore required, such as redundant performance of monitoring, testing of the efficacy of monitoring, use of two encoders, etc.

As described in 2.2, fault exclusion for the coupling between the movement and the encoder is required for single-encoder systems. ISO/TR 23849 [6] places constraints upon the application of fault exclusions in PL e and SIL 3, stating that it is not generally the rule. If the encoder is suitably mechanically overengineered, this is however also permissible in PL e/SIL 3 (see [2], Table D.16).

3 Guidance for selection

The conclusions from the discussion in the above paragraph are shown in Figure 8 diagrammatically. The flow chart is intended to assist in the reaching of decisions on the use of safe or conventional encoders. It draws attention to performance of the measures that may be required.

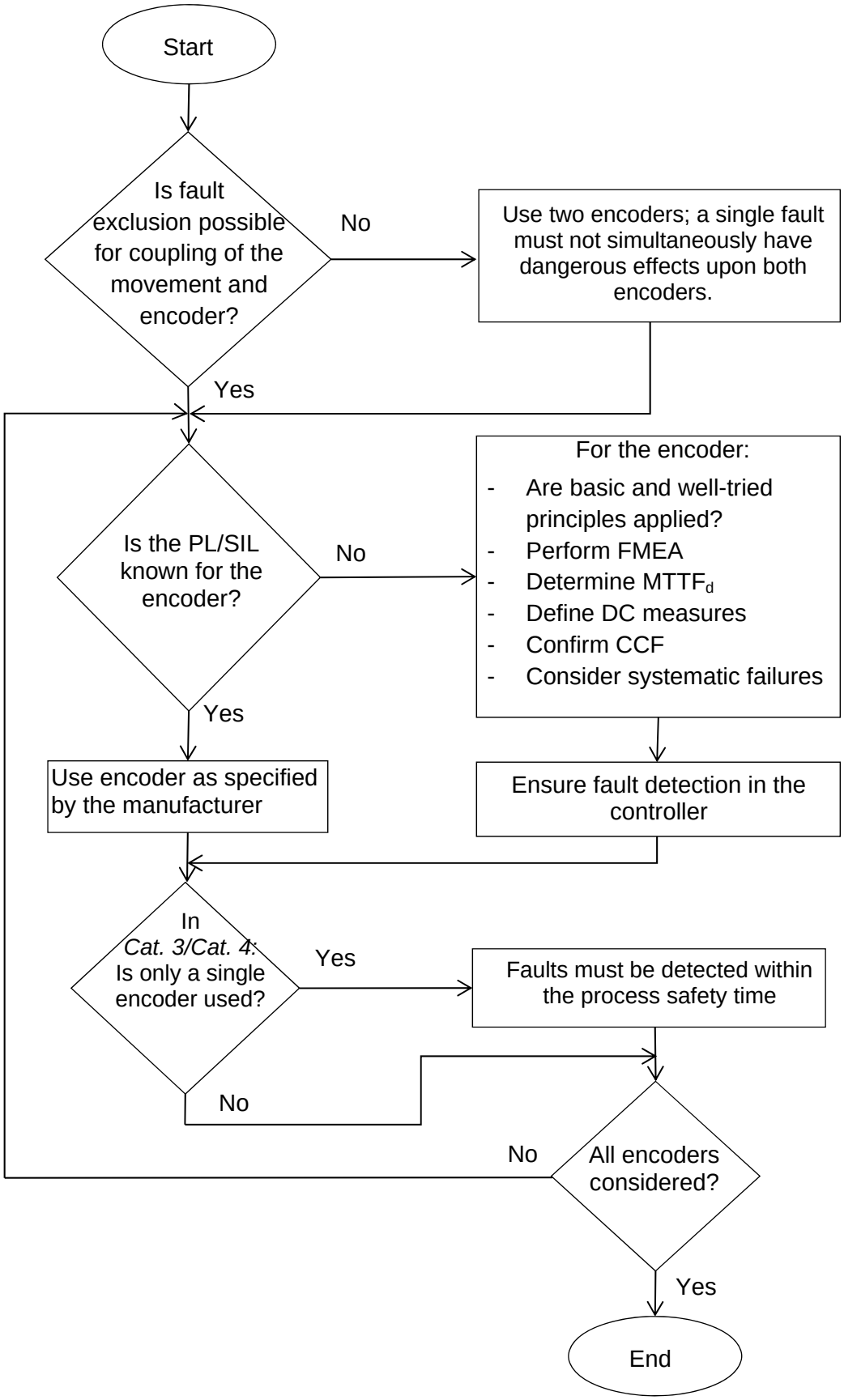

Figure 8: Use of safe or conventional encoders in PL c, d and e?

4 Summary

Conventional rotary encoders can in principle be used in safety functions. It must however be demonstrated in each case that the required Performance Level is satisfied. This requires detailed knowledge of the product, which generally entails support by the manufacturer. The fault exclusion for the coupling between the movement and the encoder that is required for single-encoder systems is particularly critical. In comparison, the use of safe encoders is much simpler, since all the necessary safety-related information is available.

5 Literature

[1] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (07.07). Beuth, Berlin 2007

[2] EN IEC 61800-5-2 (VDE 0160-150-2): Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (04.08). Beuth, Berlin 2008

[3] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (02.13). Beuth, Berlin 2013

[4] Bömer, T.; Schaefer, M.: Differences between using standard components or safety components to implement safety functions of machinery. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2011. www.dguv.de/webcode/m204554

[5] Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.: Functional safety of machine controls. BGIA-Report 2/2008e. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2009. www.dguv.de/webcode/e91335

[6] ISO/TR 23849: Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (05.10). Beuth, Berlin 2010

Author: Ralf Apfeld
Division 5: Accident prevention/product safety
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
Sankt Augustin