IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Differences between using standard components or safety components to implement safety functions of machinery

Summary:

1. In principle, safety-related control systems can be implemented through the use of standard components, though safety components offer the advantage that the machine constructor's workload is reduced because the safety-oriented assessment and analysis of the components used is carried out by the producer of the safety components.

2. In order to achieve functional safety, the systematic integrity of components is to be taken into account in addition to the use of a suitable architecture (Category), the implementation of necessary fault detection and the consideration of failure rates/probabilities.

3. In general, the use of complex elements or subsystems of the same design (homogeneous redundancy) can be ruled out because questions of systematic integrity and the necessary detection of faults are often impossible to answer sufficiently.

The use of standard components (sensors, drive elements and control electronics) in safety applications is fundamentally possible according to EN ISO 13849. This is also the case if these components have not been categorized as safety components according to Annex V of the Machinery Directive 2006/42/EC.

In addition to the familiar basic framework of the Categories, the current standards EN ISO 13849 Parts 1 and 2 (Safety of machinery – Safety-related parts of control systems – Part 1: General design principles [1], Part 2: Validation [2]) also describe a probabilistic assessment of the functional safety achieved. Whereby there have been misinterpretations during the application of the standards in relation to the use of standard components.

Regarding the assessment of functional safety, the requirements in EN ISO 13849-1 compared to the previous standard (EN 954-1) have been expanded, in particular, with the probabilistic approach, i.e. the use of quantitative values for devices. These include, above all, the values for $MTTF_d$ (the mean time to dangerous failure of a channel in years), DC (Diagnostic Coverage in %) and CCF (evaluations of Common Cause Failures). Together with the circuit structure in the form of a Category, these probabilistic aspects should provide the Performance Level (PL), the new target criterion of EN ISO 13849-1 on application of the so-called simplified approach. The standards makers have not basically changed the basic element of the previous standard – the Categories – though they have been enriched with the above-mentioned additional criteria. The aspect of test frequency is still taken into account in the modeling for Category 2.

Some users of the standard falsely assume that the probabilistic aspects i.e. the calculated determination of the Performance Level, is sufficient for a safety-related validation. Whereby they sometimes ignore the consideration of systematic and environmental influences also required.

The Performance Level according to EN ISO 13849 also includes non-quantifiable qualitative aspects in addition to quantitative statements. Although the calculated proof of sufficiently low failure probability per hour can be provided, the systematic integrity is lacking because, for example, faults are still lying hidden in software or a component is simply not fit for purpose, so that the intended Performance Level, and thus sufficient risk reduction, is not achieved.

Those placing individual safety components on the market (sub-systems), constructed according to EN ISO 13849-1 and/or other standards, have already considered a number of requirements – to the benefit of the machine constructor. These could include, for example:

- observation of basic and well-tried safety principles,
- single fault safety,
- determination of the $MTTF_d$ and DC,
- CCF evaluation (failures resulting from a common cause),
- consideration of influences and environmental conditions that could lead to systematic failures,
- software requirements,
- Category and PL determination,
- documentation requirements.

If, on the other hand, machine constructors use standard components for the implementation of safety functions, they must assess compliance with safety-related requirements themselves. Given the currently valid measures required by the standards, this can involve considerable effort for them or even be, in some cases, practically impossible. Reasons for an assessment being difficult include, for example, the lack of producer information. In order to master systematic failures it is important that the components used (sensor, control system, etc.) operate correctly under all the operating and environmental conditions that can be expected and are foreseeable (temperature, humidity, vibrations, electromagnetic compatibility, optical interference such as reflections and ambient light, etc.) respectively that if there is a fault the machine is placed in a safe state. Environmental conditions must be taken into account in relation to the application just as much as the operational limits of components. In addition, the realisation and determination of a DC for a standard component may prove difficult if it cannot be run using external equipment.

It is impossible to define general rules on when certain standard components can be used in safety-related applications and when they cannot. In general, however, the use of complex sub-systems (e.g. Standard PLCs) with the same design (homogeneous redundancy) can be ruled out for the reduction of medium and high risks because questions regarding systematic integrity and the necessary detection of faults are often impossible to answer sufficiently. A standard controller could contain hidden design faults. If this were the case and a safety function is to be carried out in a hazardous situation, the use of two identical control systems would not help achieve the safe state of the machine. Safety PLCs now often also offer the advantage of a corresponding tool that supports the user during safety-oriented programming and parameterization (in particular in relation to errors and failures to be assumed during editing, compilation and download), and provides the necessary access protection.

The advantage of using Category 3 acc. to [1] as shown in the block diagram (Figure 1) can be found in the independent implementation of the safety function through the individual channels. Influences that could lead to a simultaneous failure of both channels (so-called systematic influences) would nullify the use of two channels (redundancy).

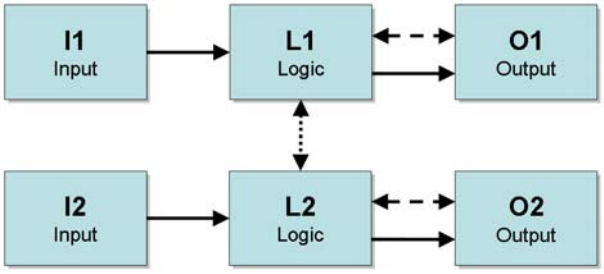

Figure 1: Category 3 shown in block diagram form

The BGIA Report 2/2008e on functional safety of machine control systems [3] examines this topic in Section 6.3.10 under the aspect of requirements regarding the embedded software (SRESW, safety-related embedded software, e.g. firmware) of standard components. The considerations found there, e.g. the evaluation of diversity, can be generalized to some extent. Table 1 (Table 6.5 from [3]) provides an overview of the recommendation.

Table 1: Requirements regarding the SRESW of standard components

No.	PL	Category, redundancy	SRESW
1	a b	Category B/2/3	The basic measures for PL a to b apply. Two alternatives: i) Confirmation by the manufacturer, or; ii) Covered by development within a QA-system in accordance with relevant product standards; in this case, the manufacturer need not confirm the observance of the requirements to EN ISO 13849-1.
2	c d	Two components for two channels in Category 2/3 Diverse SRESW or diverse technology	Bonus by diversity of the SRESW or the technologies. The basic measures for PL a to b apply. Two alternatives: i) Confirmation by the manufacturer, or; ii) Covered by development within a QA-system in accordance with relevant product standards; in this case, the manufacturer need not confirm the observance of the requirements to EN ISO 13849-1.
3	c d	Two components for two channels in Category 2/3 Homogeneous SRESW	No bonus owing to diversity. The basic measures for PL a to b apply, and additional measures for PL c/d. The manufacturer must confirm that all requirements to EN ISO 13849-1 have been observed.

The realisation of safety functions by integration of safety components simplifies the probabilistic considerations e.g. in case of determination of the performance level according to [1]. The example shown below according to the standards example in figure H.1 points out that the quantification can be made up by simple addition of three values in best case.

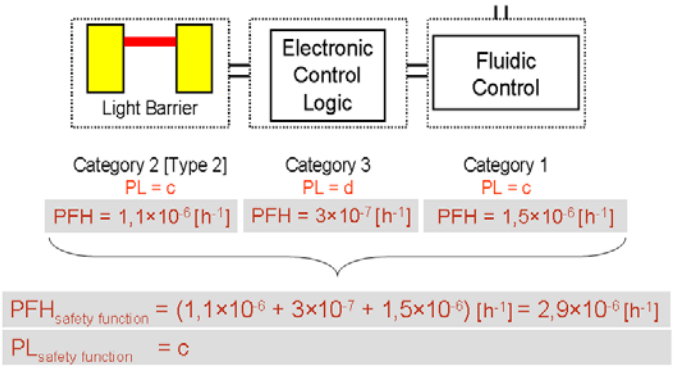

Figure 2: Linear combination of SRP/CS (with PFH-values) for the safety function „Stop actuator if light barrier is interrupted“.

If a standard exists for an application or a product, its requirements regarding the control and avoidance of failures must, of course, also be taken into account. The requirements of the EN 61496 series of standards are relevant if, for example, an optical sensor is involved.

Literature:

[1] EN ISO 13849-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (2008). CEN, Brussels 2008

[2] EN ISO 13849-2 Safety of machinery – Safety-related parts of control systems – Part 2: Validation for design (2008). CEN, Brussels 2008

[3] Functional safety of machine controls. BGIA Report 2/2008e. Publisher: German Social Accident Insurance (DGUV), Sankt Augustin 2008
Download at http://www.dguv.de/ifa/13849e

Authors: Thomas Bömer, Dr Michael Schaefer
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin