One big dilemma of the probabilistic approach of the standards ISO 13849-1, IEC 62061 and IEC 61508

Michael Schaefer, Michael Hauke, Ralf Apfeld, Thomas Bömer, Michael Huelke
IFA – Institute for Occupational Safety and Health of the German Social Accident Insurance
Alte Heerstr. 111, 53757 Sankt Augustin, Germany
Tel. +49 (0)2241 231 2640, Fax +49 (0)2241 231 2234, E-mail michael.schaefer@dguv.de,
http://www.dguv.de/ifa
In cooperation with
Expert committee "Mechanical engineering, manufacturing systems, steel construction"
(Fachausschuss Maschinenbau,Fertigungssysteme, Stahlbau – FA MFS)
Wilhelm-Theodor-Römheld-Straße 15
55130 Mainz-Weisenau, Germany

HAZARDS, SUPERPOSITION, PFH, SUPERIMPOSED HAZARDS, PROBABILISTIC APPROACH

ABSTRACT

In rare cases, at machines there are superpositions of hazards. In this context hazards are mainly caused by dangerous movements, but also other hazards such as laser-cutting or water-jet-cutting, should be considered.
This paper describes the content of a technical paper of the German Expert committee "Mechanical engineering, manufacturing systems, steel construction" (Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau – FA MFS) and IFA. By using the ideas of this paper it is possible to calculate and handle superpositions of hazards by using EN ISO 13849-1 [1] or EN IEC 62061 [2] in an easy way.

1 INTRODUCTION

The international standards for safety controls ISO 13849-1 [1], IEC 62061 [2] and IEC 61508 [3] have a so-called functional approach, which means that parts of control systems and subsystems perform safety functions.
For simple machines the safety function is simple too. If there is only one hazardous movement i.e. there is only one actuator, the world is pretty simple. To protect the operator, a safety function performed by one sensor, one logic and one output is sufficient.
Beside the severity of harm the residual risk of the individual operator is then related (not equal) to the probability of dangerous failure per hour PFH[1] of the safety function respectively of the equipment that performs the safety function.

Strung in a chain the total probability of failure per hour PFH_{total} is then the sum of the individual PFHs.

$$PFH_{total} = PFH_{sensor} + PFH_{logic} + PFH_{output} \quad (1)$$

But what if several dangerous movements act simultaneously on the operator?
To the pure doctrine the safety function may be much more extensive (this is shown in [4]).
Take for example two actuators existing simultaneously in one place; it is obvious that the PFH of a 2nd output should be added:

$$PFH_{total} = PFH_{sensor} + PFH_{logic} + PFH_{output\_1} + PFH_{output\_2} \quad (2)$$

Abstracted to n hazards in an effective range the total PFH then (with the same sensors and logic) yields in:

$$PFH_{total} = PFH_{Sensor} + PFH_{logic} + \sum_{i=1}^{n} PFH_{output\_i} \quad (3)$$

[1] For the sake of simple reading with the short form PFH the probability of dangerous failure per hour PFH or PFH_D is meant.

This mathematics is correct if one considers the hazards holistically.

Until PFH_{output_i} or n are small the overall PFH_{total} will be calculated playfully.
But this is unfortunately not the fact if a large number of hazardous movements exist in the exposure area. Then it is possible that the required level of risk reduction is no longer attainable by state of the art technologies.
This would lead e.g. in modern machine tools to an tightening of safety requirements, if one reflects on the old standard EN 954-1.
Using EN 954-1 a designer could cascade any number of sub-systems, if they all showed the same required fault behaviour and reasonable diagnostics.
This means the probability of occurrence of a fault was not considered by users of EN 954-1. The main question was, whether the occurrence of a single fault leads to loss of the safety-function or not. De facto it has never been considered that in a larger chain of subsystems a fault will appear more likely than in a smaller chain. For instance, in extreme cases, 100 Category-3-systems arranged in a chain again met the required Category 3.

The above approach of PFH-addition would also mean that many Category 1 parts yield no longer in a total required Category 1, since the probability of failure increases with the number of components.
These apparently simple observations have a great effect in practice and give rise to the following questions:
Should we switch back to old EN 954-1 not to increase safety requirements?
Should we use the approach of equation (3) because we need more safety and can this be justified by an increase of accidents?
Should we modify the risk tools of the standards to come to lower required SIL or PL_r?
Shall we decrease the PFH beyond the state of the art?
The presentation highlights this dilemma with the help of showing various examples and builds a bridge between scientifically correct approach and pragmatic approach.

2 Practical treatment of superimposed hazards

Superpositions of hazards are caused by the simultaneous interaction of several single hazards acting on one or more persons to be protected, body parts or limbs which reside in a place or which can reach areas (see Figure 1). A single hazard may be understood as a hazard caused by an individual motion of one part of a machine.

The consideration of individual risks is common practice in safety technology and is well-proven. Following the probabilistic approach of ISO 13849-1 or IEC 61508 [3, 4] respectively IEC 62061 and the risk assessment for a hazardous situation, the superposition of hazards shall be considered.

A final determination of the consideration for all hazardous situations and their single hazards can not be done at this point, as this should be left to the individual risk assessment by the machine designers. Commonly their knowledge and experience of risk assessments should be collected in machine-specific standards (e.g. European Type-C standards).

A problem is, that at hazardous areas with a high number of superimposed hazards sufficiently small probability of failure of all the parts of safety-related control systems (sensors, logic, multiple actuators) is hardly achievable and can be done only with very high mathematical effort (e.g. Markov modelling).

Also superimposed hazards with different necessary risk reductions (PL_r or SIL) increase the complexity of determining the probability of failure of safety functions, which in turn increase the effort of the calculation dramatically.

A detailed review of which hazards are superimposed in a specific area is essential. Here both the expansion of the vulnerable body parts and the operations as well as the possible movements of hazardous machine parts (e.g. electrical or mechanical interlocking of movements or only one direction possible) have to be taken into account.

Taking into account the above reasons the authors together with other German occupational safety experts developed a proposal for the practical treatment:

- Depending on the individual risk assessment, it is allowed in practice, to allocate safety functions to single hazards.

- However, multiple output switching elements (e.g. contactors, valves) which contribute to the risk reduction of the same individual hazard (e.g. movement of a single part of the machine) should all be considered together in one safety function.

Examples:

1. For the dangerous movement of a machine part, caused by the interaction of several drives, all drives shall be considered together in one safety function (e.g. a milling head in machine tools, which causes the same hazardous movement by translation of x-, y- or z-axis and the rotation of the milling head itself). See Figure 1.
2. Movements of a single multi-axis robot shall be considered together in one safety function (several robots will be considered in separate safety functions side by side).
3. A number of clamping devices which together hold a work piece shall be considered together in one safety function (if the failure of one clamping devices leads to a hazardous release).

Following this principle, that different hazards are treated in separate safety functions, superposition of hazards with different PL_r or SIL can always be considered separately (different safety functions).

3 Example of a machine tool

Referring to the example figure 1 shows the following four single hazards respectively superposition of hazards H_i:
H_1 Rotation (S1) of the left stationary spindle.
H_2 translation of the milling unit (X_1, Y_2, Z_3), pivoting movement (B_1) and rotation of the milling head (S_3).
H_3 translation (Z_4) and rotation (S2) of the right spindle.
H_4 translation (X_2, Z_2) of the lead screw and rotation of the tool changer (S4).

These four hazards result in the four safety functions SF1 to SF4. The safety function of SF1 comprises only one drive (S1) (single hazard). The safety function of SF2 comprises for example then the drives X_1, Y_2, Z_3, B_1 and rotation of the milling head S_3 (superposition of hazards).

Figure 1: Scheme of axes of a machine tool. S_i, B_1 are rotations, X_i, Y_i, Z_i are translations, C is not considered (Source: WFL Multiturn Technolgies GmbH & Co. KG, Austria, A-4030 Linz)

4 REFERENCES

[1] EN ISO 13849-1: Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (11.06) and Technical Corrigendum 1 (02.09)

[2] IEC 62061: Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems (01.05) and Corrigendum 1 (07.05) and Corrigendum 2 (04.08)

[3] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 0 to 7 (11.98 to 01.05)

[4] Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) Nr. 6, S. 34-37 (free download: www.dguv.de/ifa/13849)

5 WEB-LINKS

IFA – Institute for Occupational Safety and Health of the German Social Accident Insurance
http://www.dguv.de/ifa/13849

Expert committee “Mechanical engineering, manufacturing systems, steel construction”
http://www.bg-metall.de/index.php?id=97