IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Safety functions to EN ISO 13849-1 where multiple overlapping hazards are present

1 The current situation

For many years, EN 954-1 [1] was applied for assessment of the safety of machine controls. This essentially involved the use of structural aspects, such as single-fault tolerance, for evaluation. With the appearance of EN 13849-1 [2], which replaces EN 954-1, calculation of the probability of dangerous failure per hour (PFH) of safety functions has entered the realm of machine construction.

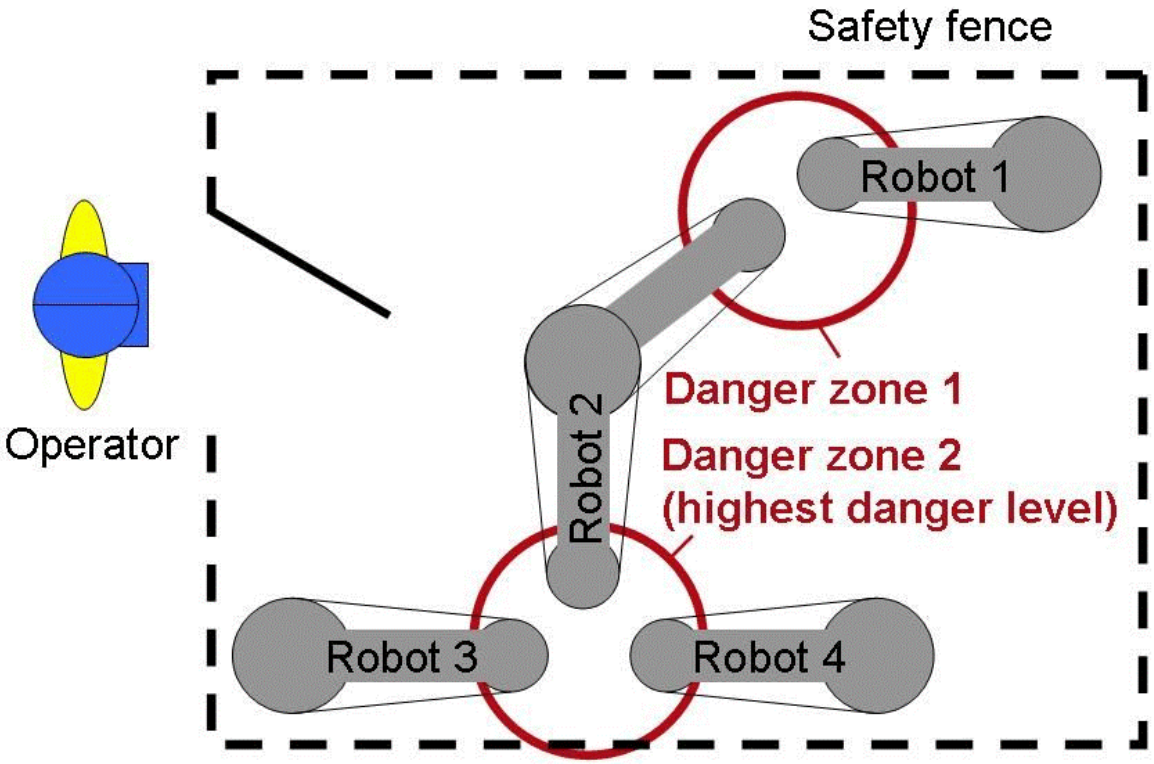
Safety functions are used to reduce risks on machines, for example by preventing motors from starting unexpectedly whilst a safety door is open. The requirements concerning the "quality" of a safety function are determined in the risk analysis by means of the required Performance Level, the PL_r. The Performance Level actually reached, or PL, must not be lower than the PL_r. Besides other aspects, the level of the PFH is particularly important here. The PFH indicates the probability of a controller failure occurring which could cause a safety function to fail and persons to be placed in danger. On simple machines, the safety functions are also relatively simple; in this case, the probabilities of failure of a small number of components must be combined to produce a PFH for a complete safety function. The task becomes more difficult on complex machines with numerous movements, particularly when multiple hazards may arise simultaneously. Multiple simultaneous hazards may for instance involve the possibility of several hazardous movements potentially injuring the operator at his or her location. Figure 1 shows two danger zones in a robot cell for which this is the case. The operator is required to enter the danger zones for part of the time during set-up. When the operator is present in danger zone 1, the movements of robots 1 and 2 constitute hazards; the same applies in danger zone 2 for robots 2, 3 and 4.

In order for unanticipated movements to be prevented, the drive motor torques are switched off, and the mechanical brakes engage. Despite all the safety precautions, a residual risk exists of, for example, a drive starting unexpectedly in the event of a fault. The probability of this happening is expressed by the PFH. To the machine operator, it is not relevant which of the drives injures him, but the sum of the individual probabilities of all moving machine parts [3]. This philosophy represents the state of the art in the area of hazardous substances at workplaces. For the machine construction sector however, it constitutes a new challenge, since summation of the individual PFH values results in the PFH for the entire safety function increasing, and ultimately possibly exceeding the permissible value for a safety function.

An additional difficulty arises when the risk analysis on the machine produces different PL_r values for the individual hazards. Safety functions with a PL_r of d are generally required for the risk reduction of hazardous robot movements. However, when tools which present additional hazards, such as for welding, water-jet cutting, laser beams, etc., are mounted on the robot arm, a different PL_r may be produced for them. How may these multiple simultaneous hazards be taken into account in the analysis?

In order to resolve this issue, a procedure is described below that has been developed jointly by the IFA and the expert committee machine construction, production systems, steel construction (FA MFS) [4]. The use of this procedure is worthwhile only in cases in which the PL_r for a safety function is not attained or risks with different PL_r levels exist.

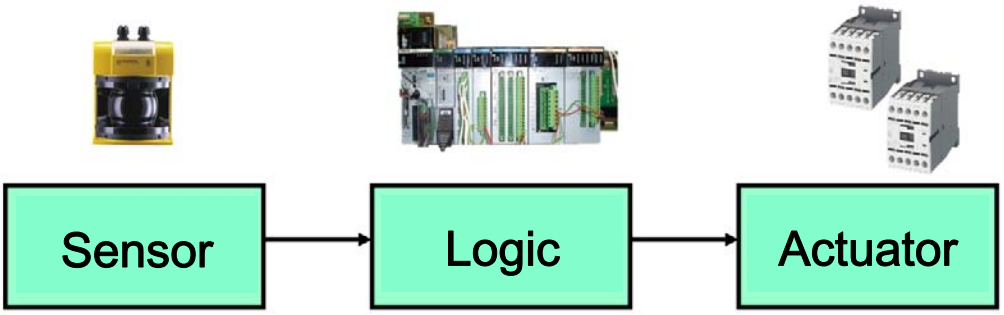
Figure 1: Robot cell with two danger zones



2 Procedure for handling simultaneous multiple hazards

Safety functions can generally be categorized as sensor, logic and actuator (see Figure 2).

Figure 2: A typical safety function arrangement



The probability of a dangerous failure per hour is then calculated as follows:

$PFH_{safety\ function} = PFH_{sensor} + PFH_{logic} + PFH_{actuator}$

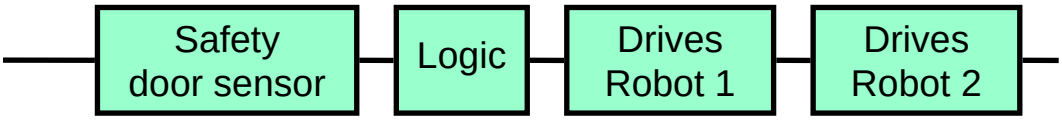
When multiple hazardous movements occur simultaneously, the PFH of all actuators capable of injuring the operator at his or her location must be considered.

For each danger zone, safety functions which provide an adequate risk reduction must then be defined. For the example in Figure 1, these could for example be:

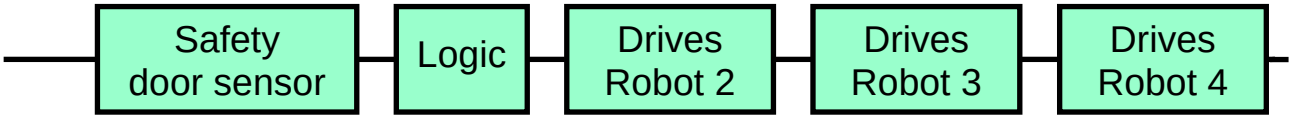
- SF1 Opening of the safety door leads to halting of all drives of Robots 1 and 2
- SF2 Opening of the safety door leads to halting of all drives of Robots 2, 3 and 4

Figure 3 shows the structure and calculation of the PFHs for these two safety functions.

Figure 3: Structure and PFHs of the safety functions SF1 and SF2



$PFH_{SF1} = PFH_{Sensor} + PFH_{Logic} + PFH_{Rob1} + PFH_{Rob2}$



$PFH_{SF2} = PFH_{Sensor} + PFH_{Logic} + PFH_{Rob2} + PFH_{Rob3} + PFH_{Rob4}$

Each robot has several drives, each with its own PFH. Summation of the individual probabilities may lead to the permissible PFH value being exceeded and the PL_r (the required PL) not being reached. If calculation was performed in accordance with the simplified method of EN 13849-1 and the PFH is only slightly too high, Markov modelling [5] may be performed instead. In this method, the estimations performed in EN 13849-1 are avoided. These always err on the side of caution, and can produce higher PFH values. The Markov modelling method is however very complicated, and EN 13849-1 employs a simplified approach for this very reason. Even when the Markov method is used, however, machines exist which execute numerous hazardous movements in a confined space, which leads to the permissible PFH being exceeded.

In the risk analysis, safety functions for risk reduction have been defined and a PL_r assigned to them. However, on complex machines with numerous actuators, an adequate risk reduction provided by safety functions cannot be demonstrated mathematically. Does this mean that these machines are too dangerous, and may not therefore be built? Practical experience suggests otherwise, since an elevated accident rate is not observed. But: how can quantitative proof be furnished?

3 The compromise

In the past, when EN 954-1 was applied, only parts of safety functions were considered. For example, the machinery standards contained provisions such as:

- Monitoring of the safety door position in Category 1 – Sensor
- Signal processing in Category 3 – Logic
- Hydraulic valves in Category 1 – Actuator

A summarizing analysis of a complete safety function was not performed, much less simultaneous analysis of multiple hazards. This procedure has in no way been associated in practice with increased accident rates. It would therefore appear to be both beneficial and permissible to limit safety functions to:

- Discrete hazards
- Movements of a single machine part

The machine manufacturer is able to do this during risk analysis/risk assessment. The danger zone must be defined in consideration of the proper actions to be performed by the operating personnel and the extent to which parts of the body are at risk. The movements of machine parts within the danger zone constitute the relevant hazards in this case. Individual machine parts may be moved by multiple drives. In this case, all components capable of bringing about a hazardous movement of the machine part under analysis must be considered during definition of the safety functions, and subsequently during calculation of the PFH. For the example of the robot cell shown in Figure 1, the new approach yields the following safety functions:

- SF1: Opening of the safety door leads to halting of all drives of Robot 1
- SF2: Opening of the safety door leads to halting of all drives of Robot 2
- SF3: Opening of the safety door leads to halting of all drives of Robot 3
- SF4: Opening of the safety door leads to halting of all drives of Robot 4

The robot is regarded here as a single machine part the movements of which present a danger to the operator. However, although each safety function still always contains multiple drives, it contains only those of a single robot. The PFH of the safety functions is therefore substantially lower.

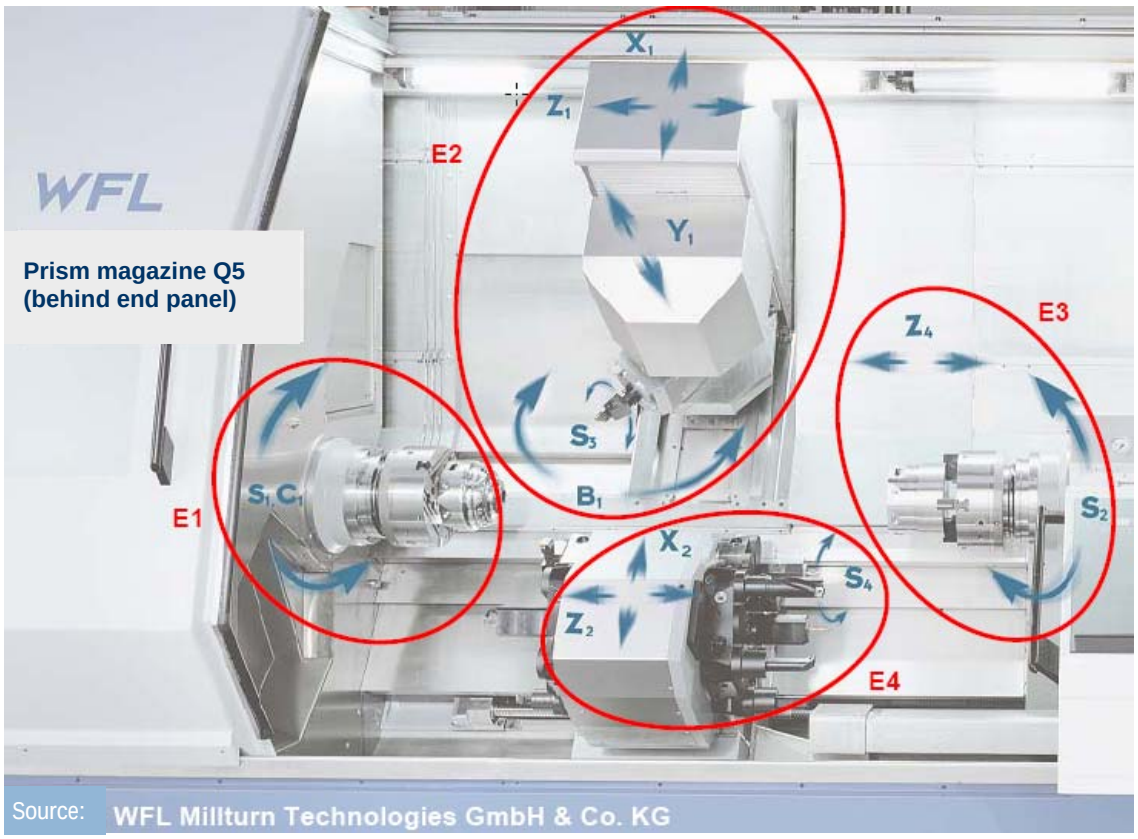
The principle presented here by which discrete hazards are considered also resolves the problem of simultaneous multiple hazards with different PL_r values. If a robot arm carrying a tool (such as a welding gun, laser beam or water jet) is assumed, an additional hazard exists over and above the hazardous movements. A further safety function, SF5, is required for risk reduction. It may be possible for this safety function to be implemented in a different Performance Level. In such cases in particular, it is advisable to consider only discrete hazards (of a machine part).

4 Example of a machine tool

Figure 4 shows a machine tool in the working area of which multiple simultaneous movements occur which present a danger to the machine operator, for example during set-up. In principle, almost all drives would have to be considered within a single safety function, since the ranges of their travel largely overlap, and the operator conducting set-up is required to intervene manually. The result is certain to cause the maximum permissible PFH to be exceeded. In this case, too, the itemized approach described above leads to a practicable solution. Four machine parts are defined the movements of which are analysed separately (refer to the markings in Figure 4):

- E1: Rotary (S1) and translatory (C1 for off-centre machining) motion of the left-hand workpiece spindle
- E2: Rotary (S3) and translatory (X1, Y1, Z1) motion and swivel motion (B1) of the milling spindle
- E3: Rotary (S2) and translatory (Z4) motion of the right-hand workpiece spindle
- E4: Rotary (S4) and translatory motion (X2, Z2) of a tool spindle (the tool turret is indexed; its rotary motion need not therefore be considered here)

Figure 4: Different discrete hazards, with reference to the example of a machine tool



Analysis of the four discrete hazards of machine parts thus yields four safety functions, SF1 to SF4, which result in a risk reduction for E1 to E4:

- SF1 considers movements S1 and C1
- SF2 considers movements S3, X1, Y1, Z1 and B1
- SF3 considers movements S2 and Z4
- SF4 considers movements S4, X2 and Z2

The design of the safety functions is dependent upon the mode of operation of the machine and the associated tasks that must be performed. The spindle could for example rotate at limited speed (safely limited speed, SLS); movements not required could be disabled (safe torque off, STO), and movements of axes could be made possible only in hold-to-run/inch mode. For all safety functions, the number of drives to be considered is reduced substantially compared to the integral approach, and the permissible PFH can be observed.

5 Literature

[1] EN 954-1: "Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design" (03/97). Beuth, Berlin (1997)

[2] EN ISO 13849-1:2007 "Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design" (12/08). Beuth, Berlin 2008

[3] Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) No 6, pp. 34-37 (in German)
http://www.dguv.de/ifa/de/pub/grl/pdf/2009_249.pdf

[4] Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachausschuss-Informationsblatt Nr. 047. Issue 5/2010. Published by: Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau, Mainz (in German)
www.bghm.de, Webcode 796

[5] EN 61508-5: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5:1998 and Corrigendum 1999) (11/02). Beuth, Berlin 2002

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