Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
*Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird*
*Annals & Proceedings of DAAAM International 2011*

# INFLUENCE ON THE FAILURE PROBABILITY

**BLECHA, P[etr] & PROSTREDNIK, D[aniel]**

***Abstract:*** *The evaluation of the probability of failure of a safety function is the basis for an approval procedure for machines which constitute a danger for their operation. This article demonstrates a few aspects of this evaluation and advocates an adjustment of the current evaluation procedures*
***Key words:*** *functional safety, risk, simulation, diagnosis*

## 1. INTRODUCTION

Together with a higher degree of autonomy of automated systems the danger is increased that a malfunction of a machine harms the health of people or causes considerable damage. The operator very often can only act in a limited manner as the processes are very rapid or automated to such a high degree that there is no local operator.

From the beginning machines and safety were two closely linked terms. A machine represents for the person / operator not only an aid in increasing his productivity but also a danger due to the forces of the machine. There was therefore, even at the beginning of the industrialisation, the need to reduce the dangers resulting from the function of the machine. The term "workplace safety" has led to the implementation of a series of mechanical and electro-mechanical engineering designs which served to protection of the operators health and continue to do so to this day.

The application of programmable logic controllers for the control of machines brought the principle of the "parallel safety " ( in parallel to the programmable controller a safety circuit in conventional relay technology was often provided ). With the development of the micro processor and with it ever more powerful PLCs, respectively the trend to decentralisation, and more functions in the software, the parallel safety circuits soon reached their limit. One was confronted with the question how a safe and therefore reliable function could be achieved with the relatively unreliable electronics.

Safety can only be accomplished with the reliability of the required function. The task is to ensure the safety of the complete system by intelligently linking unsafe electrical and or/electronic and / or programmable electronic elements.

## 2. OVERVIEW

The problem led during the 1980s and 1990s to a series of theoretical papers which discussed the functional safety of machines, respectively systems. The term "probabilistic view" was introduced. These papers led to several national and international standards being published. In particular VDI 803 should be mentioned which, after several revisions, was published as IEC standard (IEC 61508, 2010), which can be considered as the most important standard with regard to functional safety.

The European Community formulates the basic requirements on functional safety in the "Machine Directive "(Directive 2006/42/EC, 2006) . Simplified, it can be said that the manufacturer (or the seller of the machine in the EU) is under the obligation to carry out a risk analysis and to furnish proof that measures which reduce the risk to an acceptable level are implemented.

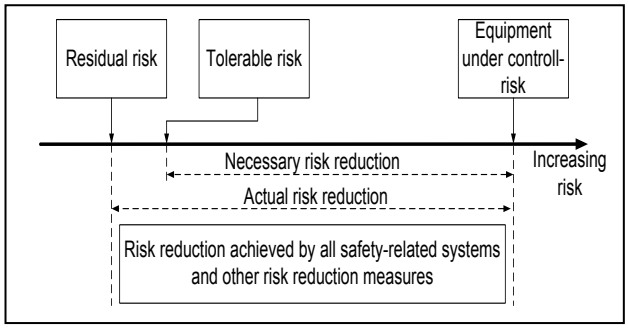


Fig. 1. Risk reduction – general concepts

## 3. MATHEMATICAL PROOF OF SAFETY

Under the assumption that the device for the reduction of risks does not suffer from any systemic faults (the systemic faults are to be eliminated, respectively to be minimized by the strict adherence to defined development processes) the failure of the safe function is caused by the random failure of a component of the device. Not every failure of a component will, however, lead to a failure of the safety function, as the device can fail in such a manner that a safe condition is taken up. A safe condition is considered as the condition under which no danger emanates from the technological device.

Example: The access to the tool of a machine tool is protected by a door which is locked while the machine / tool is in motion, in order that the operator is not exposed to any danger. The failure of the door lock in such a way that it cannot be opened is from a safety point of view no failure as the device for the risk reduction is still operative . It can be seen that safety is often in contradiction to availability.

In a formal manner we distinguish between four types of failures ( Fig.2 ). The rate $\lambda$ ( per hour) expresses the probability with which the actual failure will take place. The determination of the rate for a certain failure mode is based on the actual function of an element of the examined failure scenarios, the empirical value of the failure rate ( fit) of the individual components and stress factors which have an influence on the actual element of the system.

The proximity to reality of the determined values for the individual rates ($\lambda$ ) influences in a considerable manner the total failure probability of the safety function.

Apart from the rates, the calculated probability is at the same time the function of the Proof Test Interval T1 (h) and the Mean Time To Restoration MTTR (h). For multi-channel systems which are used when there are increased requirements

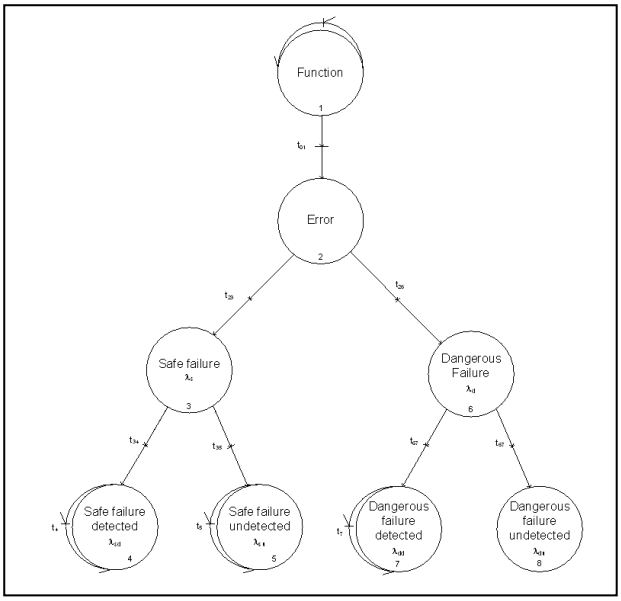


Fig. 2. Failure mode possibilities

on safety , the independence of the channels has to be taken into consideration. The function can be expressed in the following formula:

$$PFD\ (PFH) = f\ (\lambda_{dd},\ \lambda_{du},\ T1,\ MTTR,\ \beta) \qquad (1)$$

Börcsök analyses the theoretical background of the function (1) in his book (Börcsök, 2004).

## 4. QUESTIONS

The engineer is confronted with the application. Each of the function parameters signifies a series of predominantly constructive measures which are also to be designed from a economical point of view. A potential redesign which may become a requirement in the last phase (after carrying out the mathematical proof) can have a considerable impact on cost. The safety engineer is therefore confronted with the question as to how the individual parameters influence the total failure probability.

Our point of view is limited for a proposal of a technological equipment. Although the published theses are relevant generally for all systems evaluated by IEC61508, the central point of our interests is the automated cutting system, e.g. combination of a cutting machine with a robot system.

Parameter MTTR (Mean time to restoration) reflects the exchange parts philosophy and the requirements on training, respectively the equipment for the service personnel. The shorter this interval is selected the more and better trained service personnel has to be made available The service personnel also has to be provided with a larger number of exchange parts.

Parameter $T_1$ ( Proof test interval) expresses the interval in which the self tests of the system are to be carried out. They represent a loss of performance and in particular a reduction of the system response time.

Parameters $\lambda_{dd}$ and $\lambda_{du}$ are influenced by the application of components with a low failure rate, by a sophisticated design, but in particular by the diagnostic depth, i.e. the ability of the system to recognize its own failures. A larger diagnostic depth requires additional components, which in turn means a higher failure rate.

Parameter β ( common cause failures) is the better the more "separated" the channels of a system are designed. This, however, represents higher cost, e.g. by providing separate supplies, or separation.

In the course of an analysis the individual influencing factors were mathematically examined under the assumption of an actual system. The standard simulation methods were used (Jerz & Tolnay, 2006). Their influence on the total result of the failure probability of a safe function is shown in Fig.3.

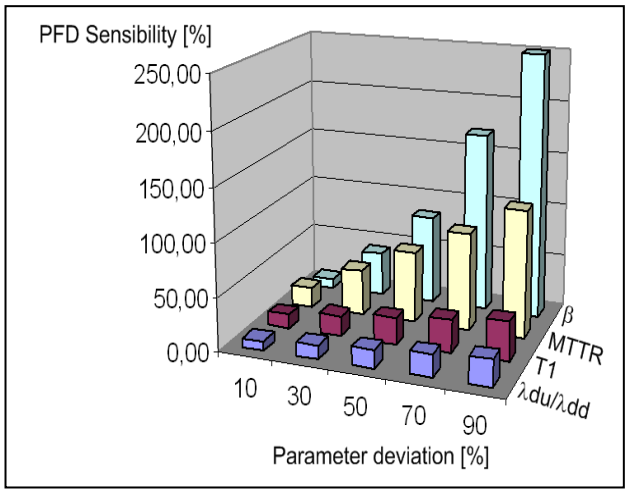


Fig. 3. Sensibility of probability of failure on demand of a safety function

## 5. CONCLUSION AND FUTURE

The normative work ( in particular IEC 61508) treats in a complex manner the minimization of systemic faults, it defines exact mathematical processes for the quantitative determination of the probability of failures of a safety function, but does not give any exact targets for the determination of the rates for the individual failure modes.

From a point of view of the authors a supplement to the actual standards is required to allow a uniform determination of the individual rates for all four failure modes in order to be able to compare the mathematical results.

The determination of the factor β is defined by means of a quantitative analysis in the standards, however, this method allows for a very wide interpretation.

It can be seen from the analysis that the factor β influences the calculated result in a significant manner. Here as well, a transparent procedure should be laid down in the standards.

In the next future the authors intend to concentrate their effort on a factor β. The target is to create and establish the methodology for an evaluation of factor β, that allows better quantification of probability of failure of a safety function.

## 6. REFERENCES

Briolini, A. (1991). *Qualität und Zuvelässigkeit technischer Systeme,* Springer, ISBN 3-540-54067-9, Berlin

Börcsök, J. (2004). *Elektronische Sicherheitssysteme,* Hüthig, ISBN 3-7785-2939-0, Heidelberg

Jerz, V. & Tolnay, M. (2006) *Simulacia diskretnych systemov,* STU Bratsilava, ISBN 80-227- 2384-3, Bratislava

*** (2010) IEC 61508 -1 to 7 Functional safety of electrical electronical programmable electronic safetyrelated systems IEC Genf

*** (2006) Machinery Directive 2006/42/EC EC Brussel 2006