21st International Conference **ENGINEERING MECHANICS 2015**
Svratka, Czech Republic, May 11 –14, 2015
Paper **#052**, **pp. 368–369**

Issues with Determination of Mean Time to Dangerous Failure and Diagnostic Coverage in Safety Functions of Machine Tools

Jiří Zahálka[a]*, František Bradáč[b], Jiří Tůma[c] , Miloš Synek[d]

Brno University of Technology, Technická 2896/2, 616 69 Brno, Czech Republic

[a]zahalka@fme.vutbr.cz, [b]bradac@fme.vutbr.cz, [c]tuma.j@fme.vutbr.cz, [c]synek@fme.vutbr.cz

Keywords: functional safety, mean time to dangerous failure, diagnostic coverage

Abstract: Safety is currently a widely discussed topic in the design and construction of machine tools. Similarly important is the area of functional safety. This article focuses on determining the mean time to dangerous failure and diagnostic coverage in safety function of machine tools. Legislative requirements (2006/42/EC [1]) and requirements of current standards (EN ISO 13849-1 [2], EN 62061 [3]) are discussed. The current state of calculating the mean time to dangerous failure and diagnostic coverage and the shortcomings of current approach is presented. A new methodology for determining of mean time to dangerous failure and diagnostic coverage is outlined.

Introduction

The functional safety is part of the overall safety that depends on the electrical, electronic and programmable electronic systems. The area of functional safety is important from the perspective of protection of worker's health, the environment and property protection and we are also committed to comply with the valid EU legislation. Legislative documents and technical standards provide support and guidance for manufacturers of machine tools how to ensure and assess functional safety. However as shown below, neither of these technical documents can provide a hundred percent support; when solving these issues there appear to be gaps in their interpretation. This article is devoted to these gaps and suggests guidelines how these issues can be solved.

Formulation of the issue with determining of MTTF$_d$ and DC in safety function

As already indicated in the introduction, in functional safety standards the deficiencies can be found; these lead to different results of analyses of functional safety. Let us consider the following specific case. We will evaluate a safety emergency stop function in category 3, according to ISO 13849-1 [2] and from the analysis we will obtain the values MTTF$_d$=24 years and DC$_{avg}$=62 %. The required parameter PLr (Required Performance Level) will be "d" for this safety function. If we use the PL table 7 of ISO 13849-1 [2] for evaluation, we obtain PLc; the requirement PLr is not satisfied and the safety function would have to be further improved. If the same standard ISO 13849-1 [2] is used with the table in Annex K.1, it can be seen that the PLd is reached using the same input parameters. To evaluate the results of the functional safety analysis of the machine’s equipment, e.g. SISTEMA software can also be used. In this case, PLd is provided in SISTEMA software; i.e. the PLr value is also satisfied. However with other parameters completely opposite results can be achieved. Another important problem in the current methodology for determining the level of functional safety is counting of cycles of individual components, which are also active in a number of safety functions. In the construction of the current machine tools, we nearly always find the components that carry out more of these functions at a time; i.e. one component performs e.g. 3200 cycles per year in one particular safety function. A reliability level of this safety function is therefore calculated on the basis of this number of operating cycles. Calculation is carried out as if there was only this particular safety function on the machine. However, the same component can also be found in another safety function, which performs e.g. 6400 cycles per year. This is again calculated only with the number of cycles concerning the particular function. The fact that these functions can interact is not included at all. It is obvious that these numbers of operating cycles must be added up since one particular component performs in these three functions in total 9600 operating cycles per year. The mean time to dangerous failure is therefore shortened (equation C.1 in [2]), and so is the mean time to dangerous failure of all three safety functions, in which the component occurs. This reduction of total $\mathrm{MTTF_d}$ is not insignificant. In practice, the average of the summation of operating cycles leads to a reduction of $\mathrm{MTTF_d}$ by 20 years. Similarly to $\mathrm{MTTF_d}$, these issues also affect the calculation of diagnostic coverage (DC), which can be calculated according to formula E.1 in [2].

Summary

The above text refers to and describes two different issues that have a significant impact on the accuracy and consistency of evaluation of the level of functional safety of safety functions implemented in machine tools. The first problem is the quantity and inconsistency of methods which could be used to evaluate the resulting level of functional safety. Thus, the manufacturers can virtually choose their own method of final evaluation, which will ensure that the implemented safety function will meet legislative requirements. These different approaches are four in total. EN ISO 13849-1 standard [2] offers three approaches (Fig. 5, Tab. 7 and Tab. K. 1); the fourth approach is provided by SISTEMA software, which, according to its developers, offers "*refined analysis method for the performance level*" [4].

Another problem described in this article touches upon the actual determination of $\mathrm{MTTF_d}$ for each safety function as one of the important parameters for obtaining the final PL. Here the current legislation is "benevolent" and allows the evaluation of each safety function separately. It also, among others, allows achieving of significantly better results of the respective analyses. How to deal with this ambiguity is proposed in the following solutions. At the beginning of each analysis of functional safety of the machine tool it is necessary to perform an inventory of all the components implementing safety functions. This is followed by the selection of all components that perform simultaneously more functions and the sum of their working cycles from all safety functions is calculated. It is supposed that only this method can ensure a correct determination of PL.

Acknowledgement: This work has been supported by Brno University of Technology, FME, Czech Republic (Grant No. FSI-S-14-2401).

References

[1] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:cs:PDF

[2] EN ISO 13849-1, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

[3] EN 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

[4] M. Huelke, M. Hauke, J. Pilger, SISTEMA: a Tool for the Easy Application of the Control Standard EN ISO 13849-1. [online]. 2008. http://www.dguv.de/medien/ifa/en/pra/softwa/sistema/paper_e.pdf