Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 69 (2014) 1242 – 1250

Procedia Engineering

www.elsevier.com/locate/procedia

24th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2013

Determination and Improvement of Performance Level of Safety Function of Emergency Stop for Machinery

Jiří Zahálka*, Jiří Tůma, František Bradáč

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

Abstract

This article focuses on the calculation of performance level (PL) by standard ISO 13849-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design [1]. Requirements of current standards are discussed and a typical composition of emergency stop is presented. Safety parameters of components and their determination and calculation are shown. The steps to determine the performance level for safety function of emergency stop along with a proposal to improve the reliability of existing systems are outlined.

Keywords: Performance Level; safety function; reliability; backup

1. Introduction

When designing any machinery, designers have to take into account a large number of different criteria. One of them is safety of machinery and compliance with the requirements for performance level (PLr) of each safety function. It is necessary to comply with PLr not only with newly designed systems but also with the existing ones. [5] This article deals with calculation and estimate of the performance level PL for safety function of emergency stop according the standard ISO 13849-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design [1]. A designed safety function must comply with PLr determined according to the standard ISO 12100 Safety of machinery – General principles for design – Risk assessment and risk reduction [2]. According to the standard IEC 61508 [3] we can use another approach to assess the safety function by setting SIL

* Corresponding author. Tel.: +420-728-648-425
E-mail address: zahalka@fme.vutbr.cz

doi:10.1016/j.proeng.2014.03.115

(Safety Integrity Level). [6] An important problem is the case of non-compliance of PLr according to the standard. This article discusses the possibility of increasing the reliability of the system that can be used in design stage of machinery.

Nomenclature

B_{10D}	Number of operating cycles after which 10 percent of population of components will have failed dangerously
d_{op}	Mean operating time in days per year
DC	Diagnostic Coverage
DC_{avg}	Average Diagnostic Coverage
h_{op}	Mean operating time in hours per day
ISO	International Organization for Standardization
$MTTF_D$	Mean Time to Dangerous Failure
n_{op}	Number of operating cycles per year
PFH_D	Probability of Dangerous Failure per Hour
PL	Performance Level
t_{cycle}	Mean time between two consecutive cycles

2. Description of safety function

The system which performs the safety function consists of input, logic and output parts. The input parts detect the external signals and forward them to logic parts of the system where they are evaluated. The output parts provide a required intervention; in this case it is an emergency stop of every dangerous machinery movement, the so-called stop-category 1, i.e. all movements are stopped and the power supply of the machine is disconnected. An example of structure and connection of the components can be seen the following scheme in Fig. 1:

- Input parts: Emergency Stop Pushbutton
- Logic parts: Safety Logic Module
  Control Unit
- Output parts: Motor Modules
  Contactors

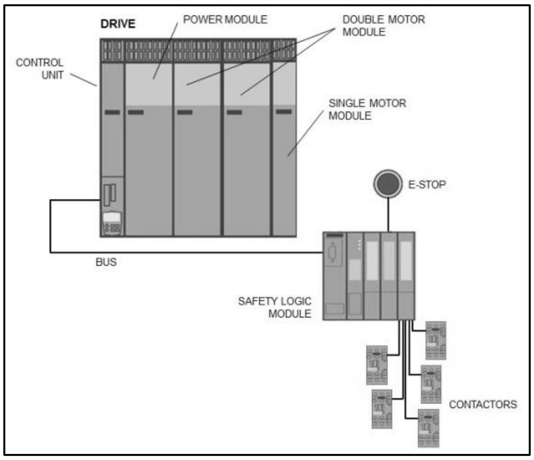

Fig. 1. Scheme of safety function.

The whole system operates as follows. As soon as the machine operator pushes the emergency stop button, the signal goes to the safety logic module which evaluates the signal. It can proceed from the safety logic module via fieldbus to a control unit which controls output parts of a low voltage converter – these can be single motor modules or double motor modules (single motor modules used to drive a spindle, double motor modules used to drive motions in the respective axes, e.g. X/C or Y/Z). The signal can also proceed from the safety logic module to contactors, which can disconnect e.g. a chip conveyer, a bar feeder, and a pump for cooling the tools. It is suitable to place one contactor in front of each asynchronous motor (contactors 3, 4 and 5) and two contactors at the beginning of wiring. This connection guarantees a disconnection of all three motors even if one of contactors 3, 4 or 5 failed. This approach meets the condition necessary to achieve higher performance levels (PLd, PLe), i.e. safety functions must operate via two independent channels.

3. Determination of performance level of safety function

Step 1 – Hazard identification and risk assessment (comply with ISO 12100 Safety of machinery – General principles for design – Risk assessment and risk reduction [2])

The standard ISO 12100 [2] defines the terminology and methodology used to achieve safety of machinery. [7] In the first step of performance level determining, it is important to identify dangers that may occur in case of safety function failure; in this case the safety function of emergency stop in stop-category 1. The dangers resulting from failure are abrasions, fractures, amputation of extremities or scalping. In successive steps, it is necessary to determine the severity of injury (S), frequency and/or duration of exposure (F) and possible prevention of danger (P).

There are serious injuries (S2). Although the operator is protected by protective coverage, when setting up the machine, changing the tools or changing the workpiece, the operator is exposed to danger (F2). Furthermore the operator is threatened by a chip conveyor, bar feeder and other moving parts. Prevention of danger is possible (P1). From this determine parameters results requirement performance level PLr d (by the graph in Fig. 2). However, there are may be differences between risk estimations from different analysis groups. [8]

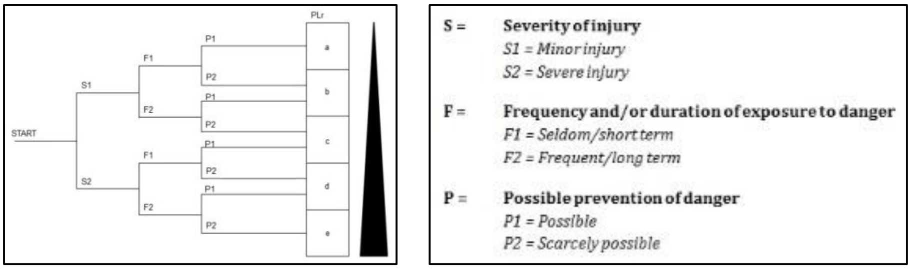

Fig. 2. Graph for determine PLr [1].

Step 2: Determination of architecture of safety function

Determining the suitable architecture is a very important step in designing a safety function because the method of connection affects the category by ISO 13849-1 [1]. Therefore it also means that the category affects the resultant performance level. To meet higher levels of PL we need to use architectures for category 3 or 4, i.e. a two-channel control (both channels are shown in Fig. 4).

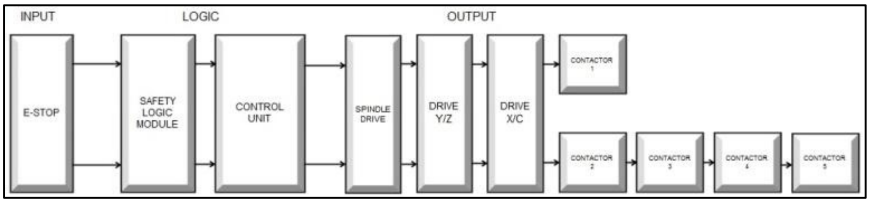

Fig. 3. Architecture of safety function.

As it is evident from Fig. 3 and 4, the condition to comply with PLd is accomplished and the safety function is controlled by a two-channel path. This means that the signal from the emergency stop pushbutton passes by a two-channel path through the safety logic module to the control unit and contactors. Disconnecting of the other peripheries (chip conveyer, bar feeder, tools cooling) is solved redundantly. The first method of how to disconnect peripheries is via contactors 1 and 2 (contactors 1 and 2 are placed at the beginning of wiring). The second method is via contactors 3, 4 and 5 (each contactor is placed in front of each asynchronous motor). This connection responds to categories 3 and 4 by ISO 13849-1 [1]. Categories 3 and 4 have the same architecture but their values of $MTTF_D$ and DC are different. In category 4 $MTTF_D$ has to be high (≥30 years) and DC has to be high (≥99%).

Step 3: Determination of parameters of each components of safety function

For a correct and complete calculation of performance level, it is necessary to know safety parameters of each component used in safety function. These parameters can be found on manufacturer website or in products catalogue. The parameters we are interested in are mainly the mean time to dangerous failure ($MTTF_D$), the probability of dangerous failure per hour (PFH_D), the number of operating cycles after which 10 percent of population of components will have failed dangerously (B_{10D}) and diagnostic coverage DC.

Step 4: Calculation of mean time to dangerous failure ($MTTF_D$) for each channel and diagnostic coverage (DC)

If we know $MTTF_D$ of each component, we can calculate $MTTF_D$ for the first and second channel. If we do not know this parameter, we can always use formulas 1 or 3 to calculate $MTTF_D$ of components. Formula no. 1 will be used if we know B_{10D} value and the number of operating cycles per year n_{op}. n_{op} is calculated using formula no. 2 (there we need to determine the mean operating time in days per year d_{op}, the mean operating time in hours per day h_{op} and the time between two consecutive cycles t_{cycle}). Formula no. 3 is used when we know PFH_D of each component. Another method of how to calculate $MTTF_D$ is in annex C in ISO 13849-1 [1]. The channels of safety function are illustrated in Fig. 4. The activation channel 1 has the same result – namely emergency stop in stop-category 1.

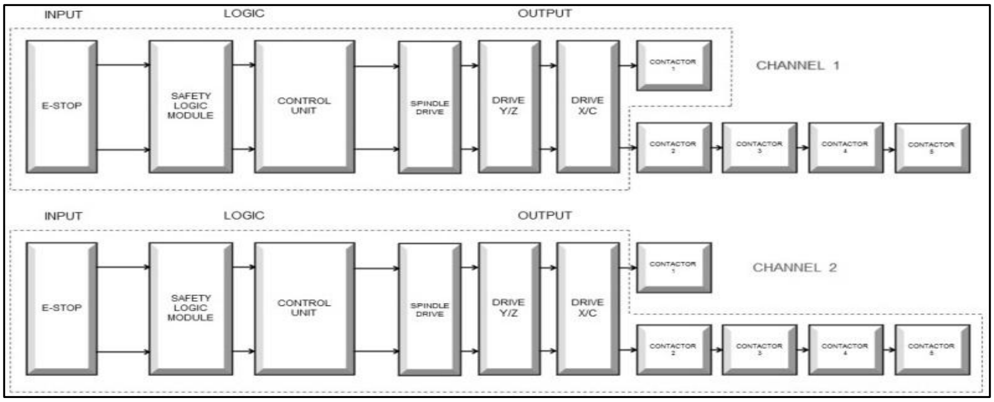

Fig. 4. Two channels of safety function.

$$MTTF_D = \frac{B_{10d}}{0{,}1 \times n_{op}} \tag{1}$$

where: MTTF$_D$ is mean time to dangerous failure
B$_{10d}$ is number of operating cycles after which 10 percent of population of component will have failed dangerously
n$_{op}$ is number of operating cycles per year

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cyklu}} \tag{2}$$

where: n$_{op}$ is number of operating cycles per year
d$_{op}$ is mean operating time in days per year
h$_{op}$ is mean operating time in hours per day
t$_{cycle}$ is time between two consecutive cycles

$$MTTF_D = \frac{1}{8760 \times PFH_D} \tag{3}$$

where: MTTF$_D$ is mean time to dangerous failure
PFH$_D$ is probability of dangerous failure per hour

$$MTTF_D = \frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \frac{1}{MTTF_{D3}} + \ldots.. + \frac{1}{MTTF_{Dn}} \tag{4}$$

where: MTTF$_{D1\ldots n}$ is mean time to dangerous failure for each component

If we have identified all MTTF$_D$'s of all components in the safety function, we need to calculate MTTF$_D$ for each channel and then for the whole safety function. From this result we will see if MTTF$_D$ is low, medium or high.

Calculation MTTF$_D$ for channel 1:

$$\frac{1}{MTTF_{D\_1}} = \frac{1}{MTTF_{D_{E-STOP}}} + \frac{1}{MTTF_{D_{SLM}}} + \frac{1}{MTTF_{D_{CU}}} + \frac{1}{MTTF_{D_{SD}}} + \frac{1}{MTTF_{D_{DYZ}}} + \frac{1}{MTTF_{D_{DXC}}}. + \frac{1}{MTTF_{D_{C1}}} \tag{5}$$

Calculation MTTF$_D$ for channel 2:

$$\frac{1}{MTTF_{D\_2}} = \frac{1}{MTTF_{D_{E-STOP}}} + \frac{1}{MTTF_{D_{SLM}}} + \frac{1}{MTTF_{D_{CU}}} + \frac{1}{MTTF_{D_{SD}}} + \frac{1}{MTTF_{D_{DYZ}}} + \frac{1}{MTTF_{D_{DXC}}}. + \frac{1}{MTTF_{D_{C2}}} + \\ + \frac{1}{MTTF_{D_{C3}}} + \frac{1}{MTTF_{D_{C4}}} + \frac{1}{MTTF_{D_{C5}}} \tag{6}$$

Calculation overall MTTF$_D$ for safety function:

$$MTTF_D = \frac{2}{3}\left[MTTF_{D\_1} + MTTF_{D\_2} - \frac{1}{\frac{1}{MTTF_{D\_1}} + \frac{1}{MTTF_{D\_2}}} \right] \tag{7}$$

To determine the performance level, it is necessary to determine the overall diagnostic coverage DC. The diagnostic coverage is the ratio of the probability of detected dangerous failures to the probability all dangerous failures. The diagnostic coverage is calculated by the formula no. 8.

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \frac{DC_3}{MTTF_{D3}} + ... + \frac{DC_n}{MTTF_{Dn}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \frac{1}{MTTF_{D3}} + ... + \frac{1}{MTTF_{Dn}}} \tag{8}$$

where: DC_n is diagnostic coverage of each components
$MTTF_{Dn}$ is mean time to dangerous failure for each component

Table 1. Table for determine of diagnostic coverage [1]

DIAGNOSTIC COVERAGE	
SIGNIFICATION	RANGE
0	DC < 60%
LOW	60% ≤ DC < 90%
MEDIUM	90% ≤ DC < 99%
HIGH	99% ≤ DC

Step 5: Estimate for common cause failures (CCF)

The last step before PL verification is to determine the precaution against failures having a common cause. It is suitable to use the standard ISO 13849-1[1] for this purpose, specifically its appendix F and tables F1 and F2, where it is possible to determine the overall point value of precaution against CCF. These precautions depend mainly on the system protection against various environmental impacts, overvoltage, overcurrent, way of communication, etc. A maximum of point count is 100; however it is necessary to exceed the limit of 65 pts.

Step 6: Verification of performance level (PL)

From the calculated values ($MTTF_D$ and DC_{avg}) and from the category we can find out if it meets the requirement for performance level PLr. To perform this, we can use the following table for verification of PL.

Table 2. Table for verification of PL [1]

Category	B	1	2	2	3	3	4
DC_{avg}	0	0	low	medium	low	medium	high
$MTTF_D$							
low	a	uncovered	a	b	b	c	uncovered
medium	b	uncovered	b	c	c	d	uncovered
high	uncovered	c	c	d	d	d	e

4. Proposal for procedure of how to increase the reliability of the designed system

If the situation occurs where the performance level is calculated using the above mentioned procedure and it is found out that it does not comply with legislative requirements, it is necessary to modify the system. In the phase of design, there is a high probability that this situation occurs because our intention is to design the system as simple as possible, as cheap as possible and with low number of elements. There are two possibilities of how to improve the reliability and trouble free function. It is possible to increase the reliability of the existing system without adding other elements. Another method is to improve the reliability by adding other elements (system backup), see Fig.7.

The first rule of reliability (the lesser the number of elements the lesser is the probability of their failure) was used during the initial draft. Another possibility is to use the elements with increased reliability but it means a higher price. To avoid the use of more expensive components, we can modify working conditions of elements, i.e. eliminate the sources of vibrations, humidity, dust and temperature. This also often extends the lifetime of elements.

However to reach a higher performance level (PL d and e), it is suitable to use a two-channel control of safety function as it is shown in the example presented in this article (level d can also be reached through the connection in category 2 but it is necessary to use the testing device which controls the function of the system in periodic intervals, and simultaneously it must be ensured that this testing device is not a source of potentially dangerous situation). It can be achieved using the system backup, i.e. increase in reliability using the redundancy. There are two methods of how to create the system backup. The first method is to backup per systems, i.e. to create the second system which is the same as the first. In case of failure of the first system, the second system executes its function. The second method of system backup is to backup per elements. This kind of backup is more advantageous (also in case of the use with the same number of elements) because in case of system failure it is not necessary to substitute the whole system but only one element. Other possibilities are the use of fixed or substitution backup. The difference is in the character of backup elements. In case of fixed backup, the backup component has the same character; both of them have the same connection. In case of substitution backup, the backup element starts its operation only in case of failure of the first element to restore its safety function. A disadvantage in the second case is urgency of element failure detection, so another detection element is connected to the system. Today it is possible to buy a plenty of logical elements, which allows the control of function of other elements. It is possible to connect feedback contacts of contactors to the logic module, which can control its potential failures. To reach the performance level d, a flowchart in Fig.6 could be an inspiration.

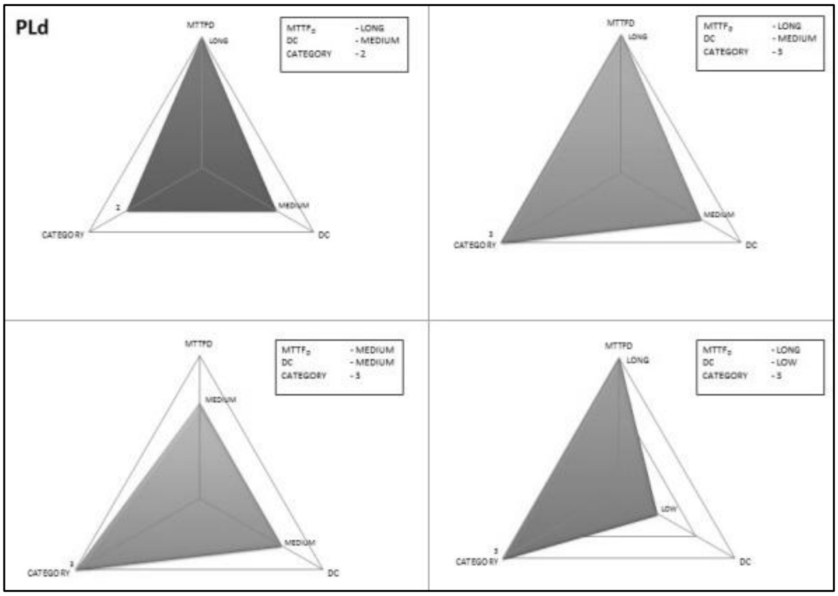

Fig. 5. Graphs of combination of MTTF$_D$, DC and category achieve PLd.

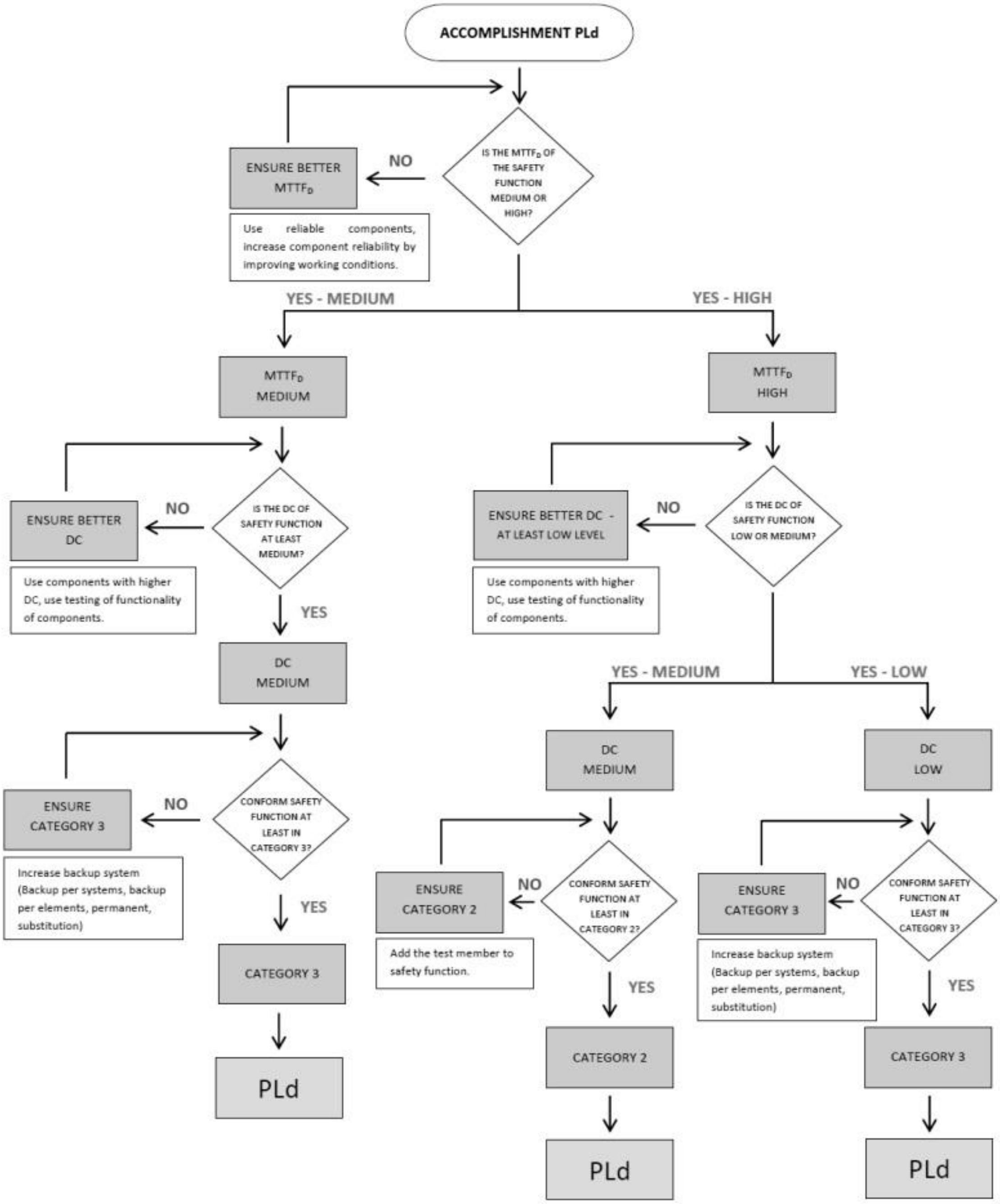
ACCOMPLISHMENT PLd
IS THE MTTF$_D$ OF THE SAFETY FUNCTION MEDIUM OR HIGH?
NO
ENSURE BETTER MTTF$_D$
Use reliable components, increase component reliability by improving working conditions.
YES - MEDIUM
YES - HIGH
MTTF$_D$ MEDIUM
MTTF$_D$ HIGH
IS THE DC OF SAFETY FUNCTION AT LEAST MEDIUM?
NO
ENSURE BETTER DC
Use components with higher DC, use testing of functionality of components.
YES
DC MEDIUM
CONFORM SAFETY FUNCTION AT LEAST IN CATEGORY 3?
NO
ENSURE CATEGORY 3
Increase backup system (Backup per systems, backup per elements, permanent, substitution)
YES
CATEGORY 3
PLd
IS THE DC OF SAFETY FUNCTION LOW OR MEDIUM?
NO
ENSURE BETTER DC - AT LEAST LOW LEVEL
Use components with higher DC, use testing of functionality of components.
YES - MEDIUM
YES - LOW
DC MEDIUM
DC LOW
CONFORM SAFETY FUNCTION AT LEAST IN CATEGORY 2?
NO
ENSURE CATEGORY 2
Add the test member to safety function.
YES
CATEGORY 2
PLd
CONFORM SAFETY FUNCTION AT LEAST IN CATEGORY 3?
NO
ENSURE CATEGORY 3
Increase backup system (Backup per systems, backup per elements, permanent, substitution)
YES
CATEGORY 3
PLd

Fig. 6. Flowchart achieve PLd.

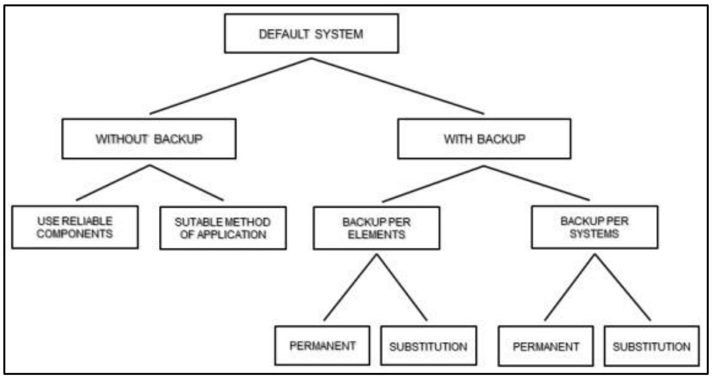

Fig. 7. Possibility of increasing the reliability of the designed safety function.

5. Conclusion

To reach contemporary legislative requirements, the designed machinery must be safe, i.e. it must also fulfill the requirements related to its safety. These requirements are governed by different standards for machinery. For example the standards for lathes are above all the following: ISO 23125 Machine tools – Safety – Turning machines [4], ISO 12100:2010 Safety of machinery – General principles for design – Risk assessment and risk reduction [2], ISO 13849-1:2006 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design [1]. The first standard establishes detailed safety requirements for lathes; the second defines a basic terminology and methods used for risk assessment of machinery and for achievement of safety. The last standard is a manual on how to assess the overall safety of safety function. It is also the main source for this article because the calculation and establishment of emergency stop performance level are based on it. This performance level determines the ability of designed system to fulfill the requested safety function. With sequence of steps described in this article, it is possible step-by-step to meet the established safety requirements. . This gives us the information if it is necessary to modify the system because of safety requirements.

This article shows different approaches to improvement of reliability and also performance level of safety functions. The major purpose of our research is to propose how to proceed in case of non-compliance with requested PLr level, which is necessary for reaching the highest levels of PL. This can be ensured via different kinds of backup. The result of our research was effort of a simplified form of decision about steps which leads to satisfy the PLd. This simplified form is a flowchart which can be useful during the design process of safety function.

Acknowledgement

This work has been supported by Brno University of Technology, FME, Czech Republic (Grant No. FSI-J-13-1937).

References

[1] ISO 13849-1:2006 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design.
[2] ISO 12100-1:2004 Safety of machinery – General principles for design – Risk assessment and risk reduction.
[3] IEC 61508-1:2010 Functional safety of electrical / electronic / programable electronic safety related system – Part 1. General requirements.
[4] ISO 23125:2010 Machine tools – Safety – Turning machines.
[5] Sabrina Jocelyn, James Baudoin, Yuvin Chinniah, Philippe Charpentier, Feasibility study and uncertainties in the validation of an existing safety-related control circuit with the ISO 13849-1:2006 design standard, Reliability Engineering & System Safety, Volume 121, January 2014, Pages 104-112, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2013.07.012. (Will be published).
[6] Rainer Faller, Project experience with IEC 61508 and its consequences, Safety Science, Volume 42, Issue 5, June 2004, Pages 405-422, ISSN 0925-7535, http://dx.doi.org/10.1016/j.ssci.2003.09.008.
[7] BLECHA Petr, System methodology of risk assessment in machine tools. MM Science Journal. 2008. http://www.mmscience.eu/archives/mmsj_2008_04_blecha.pdf.
[8] Marita Hietikko, Timo Malm, Jarmo Alanen, Risk estimation studies in the context of a machine control function, Reliability Engineering & System Safety, Volume 96, Issue 7, July 2011, Pages 767-774, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2011.02.009.