Probabilities in Safety of Machinery – Part 1: Risk Profiling and Farmer Matrix

Armin Bornemann
Deckel Maho, Pfronten, Germany

Yannick Froese
Fachhochschule Frankfurt am Main, University of Applied Sciences, Germany

Luca Landi
Department of Engineering, University of Perugia, Italy

Heinrich Mödden
German Machine Tool Builders´ Association (VDW), Frankfurt am Main, Germany

ABSTRACT

The new control system standard ISO 13849-1 deals with the theoretical probabilities of hypothetical individual events; however, it avoids depicting them as relative frequencies. For the practical design engineers, a relative frequency approach is a more comprehensible form, because with the relative frequency a reconciliation with statistically acquired data is possible. This article closes some explanatory gaps caused by the one-sided emphasis on theoretical probability. In doing so, four contributions are provided in the context of field experience:

1. the concept of probability and the basic principles of distribution functions are elucidated using an “hourglass analogy”,
2. fitting of an empirical Weibull distribution in order to evidence the theoretical requirements,
3. risk profiling method: plausibly stretched “risk snapshots” integrated to a “risk film” over the machine’s lifetime,
4. proposals for a probabilistically founded dimensioning of enclosure.

This part 1 shall serve for a better understanding of the probabilistic concept, in particular for ongoing discussions of the merging of IEC 62061 & ISO 13849-1 into IEC/ISO 17305 in the Joint Working Group (JWG 1). Part 2 addresses more the practical design of machine tools and the corresponding standardization work of ISO/TC 39/SC 10 and before in CEN/TC 143. Together, part 1 and 2 are also intended to connect the world of International Standardization with the network of International Probabilistic Research, e.g. ESREL. For the sake of comparison with reality, a separate third paper of Günnel et al. (2014) shows empiric findings of field data analyses.

REFERENCES

EN ISO 13849-1, 2008. *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*. Berlin, Germany; Beuth Verlag GmbH.

IEC/ISO 17305, *Safety functions of control systems*, Joint Working Group 1 (draft 2014)

Montgomery, D. et al. 2010. *Engineering Statistics.* Wiley; 5 edition

Günnel, B. et al. 2013. *EN ISO 13849-1 – New quantitative requirements for Functional Safety in the machine tool industry,* ESREL 2013

Günnel, B. et al. 2014. *Proven in use in the machine tool industry for demonstrating the quantitative Functional Safety according to EN ISO 13849 1,* ESREL 2014

EN ISO 12100, 2010. *Safety of machinery – General principles for design – Risk assessment and risk reduction*. Berlin: Beuth Verlag GmbH.

The European parliament & the council of the European Union 2006. *Machinery Directive 2006/42/EC.*

Meyna, A. & Pauli, B. 2010. *Zuverlässigkeitstechnik - Quantitative Bewertungsverfahren*. Munich: Carl Hanser Verlag.

E. Uhlmann, et al. 2012. *Sicherheit an Werkzeugmaschinen: Die Bedeutung der trennenden Schutzeinrichtung für die Risikoreduktion an Werkzeugmaschinen,* ZWF Jahrgang 107, Hanser Verlag

IEC 62061, 2005. *Safety of machinery - Functional safety of electrical, electronic and programmable control systems for machinery.* Berlin: Beuth Verlag GmbH.

ISO/CD 16090, 2014. *Machine tools — Safety — Milling machines (draft international standard)* Berlin, Germany; Beuth Verlag GmbH.

Probabilities in Safety of Machinery – Part 1: Risk Profiling and Farmer Matrix

Armin Bornemann
Deckel Maho, Pfronten, Germany

Yannick Froese
Fachhochschule Frankfurt am Main, University of Applied Sciences, Germany

Luca Landi
Department of Engineering, University of Perugia, Italy

Heinrich Mödden
German Machine Tool Builders´ Association (VDW), Frankfurt am Main, Germany

The new control system standard ISO 13849-1 deals with the theoretical probabilities of hypothetical individual events; however, it avoids depicting them as relative frequencies. For the practical design engineers, a relative frequency approach is a more comprehensible form, because with the relative frequency a reconciliation with statistically acquired data is possible. This article closes some explanatory gaps caused by the one-sided emphasis on theoretical probability. In doing so, four contributions are provided in the context of field experience:

1. the concept of probability and the basic principles of distribution functions are elucidated using an “hourglass analogy”,
2. fitting of an empirical Weibull distribution in order to evidence the theoretical requirements,
3. risk profiling method: plausibly stretched “risk snapshots” integrated to a “risk film” over the machine’s lifetime,
4. proposals for a probabilistically founded dimensioning of enclosure.

This part 1 shall serve for a better understanding of the probabilistic concept, in particular for ongoing discussions of the merging of IEC 62061 & ISO 13849-1 into IEC/ISO 17305 in the Joint Working Group (JWG 1). Part 2 addresses more the practical design of machine tools and the corresponding standardization work of ISO/TC 39/SC 10 and before in CEN/TC 143. Together, part 1 and 2 are also intended to connect the world of International Standardization with the network of International Probabilistic Research, e.g. ESREL. For the sake of comparison with reality, a separate third paper of (Günnel et al. 2014) shows empiric findings of field data analyses.

1 INTRODUCTION

1.1 *Practical application problems*

The one-sided polarisation of ISO 13849-1 towards theoretical probabilities is a disadvantage, because the relative frequencies would enable the theory to be objectively verified. For the practical design engineer, a reconciliation with statistically acquired data or experimental results is necessary, as well as with subjective empirical values, e.g. by enumerating the relevant events (in the numerator) with regard to the total quantity of all events (in the denominator). This fraction is the original definition of a probability (see e.g. Montgomery), and it is a realistic introduction to probability theory, as also shown by the study of VDW (German Machine Tool Builder Builders Association) on operational dependability (Günnel et al. 2014). At the German Social Accident Insurance Scheme (BAuA 2010), the accident figures are recorded as frequencies, too, (with histograms), and they show two important results:

a) a continuous improvement in safety due to decreased relative frequencies,

b) an almost constant mutual relative percentage content of frequencies for individual degrees of seriousness (accident pyramids).

1.2 *Probability*

Mathematically viewed, probability has its unique definition within an axiomatic calculus. Yet, it is not at all clear what the term probability means, if it is applied to a non-mathematical situation (Main 2012).

As far as machine tools’ safety is concerned, the terms “probability” or “likelihood” have not very often been used in developing the former product safety standards in CEN/TC 143. Their worldwide unique state of the art was established on a deterministic approach of the kind “identify hazard + compensate it with a bundle of safety measures = a safe machine” and is well-tried for more than a decade, now. Only when a second disconnecting channel in the control chains was discussed, the probability of a simultaneous failure of both channels was considered negligibly low. In contrast to this, since 2011 ISO 13849-1 made probability a key term in the standardization world. Most of the experts in the former deterministic approach are still in uncharted waters, when discussions circle around obviously different meanings of probability.

Here, in excerpted form only, the various manifestations of probability and certain fundamental relationships are explained: Probability as a theoretical value according to Laplace and Pascal is:

$$P(A) = \frac{number\ of\ events\ relevant\ for\ A}{number\ of\ all\ possible\ events} \qquad (1)$$

e.g. rolling the dice $P(get\ a\ 6) = 1/6.$ (2)

Probability as a relative frequency, e.g. of an experiment, according to von Mises:

$$F_{rel} = \frac{m(\ number\ of\ registered\ elements)}{n(number\ of\ all\ elements\ of\ a\ sample)} \qquad (3)$$

Linking the two probability definitions with Bernoulli’s Law of Large Numbers:

$$\lim_{n\to\infty} F_{rel} = P(A) \qquad (4)$$

According to Bayes, probability can also mean a degree of personal belief, which however varies between different persons.

A well-defined mathematical fundament for calculating with probabilities was established by Kolmogorov. E.g. the first axiom postulated that every random event *A* has a probability *P(A),* where:

$$0 \leq P(A) \leq 1 \qquad (5)$$

Kolmogorov’s Third Axiom on additivity, by the way, forms the basis for risk profiling, which is being proposed by the VDW for the superposition of individual “risk snapshots” to form a “risk film”; see below.

It needs no further explanation that the probability of mutual understanding can get very low, if students of Laplace and von Mises come across students of Bayes, even if they all apply the same mathematics of Kolmogorov.

For practical reliability engineering, the relationship between an experimentally determined histogram and an empirical density is very important and it has been compiled in very easily comprehensible form e.g. in Montgomery: several practical examples are adduced to explain how Bernoulli’s Law of Large Numbers can be used to proceed from experimentally determined frequencies to theoretical probabilities and vice versa. In doing so, distribution functions can be derived, e.g. the normal distribution curve of Gauss.

ISO 13849-1 uses the Exponential distribution as a basis for describing the safety related reliability, without pointing it out. The probability of failure is then $F(t) = 1 - e^{(\lambda \cdot t)}$

In doing so, the failure rate λ plays an important role, several roles respectively, and it a priori assumes pure random failures. For the scope of the standard, which is „safety related parts of control systems“, this is a very simple comparison standard. It fits quite well, if a constant failure rate λ can be suggested, e.g. for electronical products, which can be connected to the horizontal part of the „bathtub curve “. In the VDW’s study on operational dependability, by contrast, the Weibull distribution is used, because at machine tools the failures are not purely random, but the failure rate rises as the operating hours increase (as a consequence of wear and tear, ageing).

For the purpose of practical understanding, here the concept of probability and the basic principles of distribution functions are elucidated using an “hourglass analogy”. This could help to improve the discussion about safety, in which the term “probability” still is mainly used in the sense “degree of belief” and not scientifically founded, but just subjectively emphasized.

1.3 *Hourglass Analogy*

Detailed explanations of the basic probabilistic principles involved are provided e.g. in Montgomery. With a simplified model of an hourglass as an analogy, the basic concepts will be briefly outlined here; since with an hourglass the survival probability as “1 minus the probability of failure”
$R(t) = 1 - F(t)$
can be very vividly explained, because in the analogy it corresponds to the sand remaining in the glass. How are the various forms of a distribution function, namely:

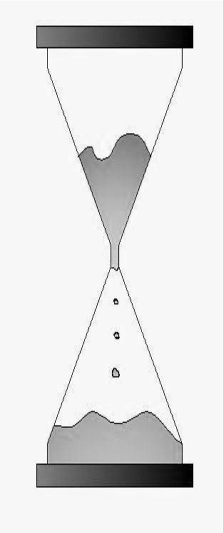
- density function $f(t)$
- failure probability $F(t)$ or survival probability $R(t) = 1 - F(t)$
- failure rate $\lambda(t)$

depicted in the hourglass analogy?

Fig. 1 illustrates how the “distribution function of an hourglass” is developed from the density function. The basic assumptions required here are that per time unit approximately n grains of sand trickle through and there are a total of N grains in the glass (for the precise functioning of an hourglass are reference is given below).

All formulae apply only for $0 < t \leq N/n$, because at $t^* = N/n$ the hourglass has run empty.

Formulae (6)



$$f(t) = \frac{n}{N}$$

Density function

$$F_d(t) = \int_0^t f(\tau) \cdot d\tau = \frac{n}{N} \cdot t$$

Probability of failure

$$R_d(t) = 1 - \frac{n}{N} \cdot t$$

Probability of survival

$$\lambda(t) = \frac{f(t)}{R_d(t)} = \frac{\frac{n}{N}}{1 - \frac{n}{N} \cdot t}$$

Failure rate

Figure 1: Analogy to distribution functions with trickling sand

The definition of the PFH$_d$ (Probability of Failure per Hour) as the average of the (dangerous) density function over an interval T shows that it corresponds quite well to the hourglass analogy. Fig. 2 shows an illustrating graphic, comparing the PFH$_d$-values of two different density functions, see also table 1 right column.

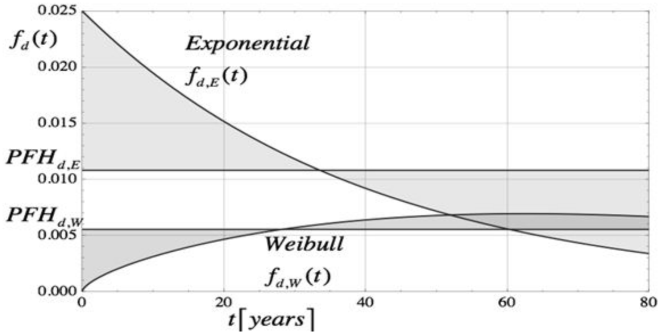


Figure 2: Comparison of PFH$_d$ for Exponential and Weibull Distribution

$$PFH_D = \frac{1}{T} \cdot \int_0^T \left(\frac{dF_d(t)}{dt} \right) \cdot dt = \overline{f}_d(t)$$
$$= \frac{1}{T} \cdot \int_0^T f_d(t) \cdot dt = \frac{F_d(t)}{T} \qquad (7)$$

2 CRITICISM OF THE PERFORMANCE LEVEL

The PFH$_d$ value is the crux of the matter in the studies of ISO 13849-1 and a “average variable in the kind of a frequency domain with the dimension [1/hour]”. It is used not only for the quantifications, but also for the decision tree for determining target values as “performance level required” (PL$_r$, which is divided into PFH$_d$ value ranges), see table 1. As explained above, an Exponential distribution is here assumed. For the example of “radioactive decay”, it is true that in each second a fixed percentage of the atomic nuclei present in the substance will decay; the fewer nuclei are still present, the more slowly their number will decrease. This is not the case with the reliability of machine tools: the initial results from the VDW’s studies on operational dependability show a significant deviation of the field data from an Exponential distribution (defining a temporally unchanging failure rate), because a time-dependence of the failure behaviour is clearly discernible. Against this background, during field data analysis criticism was voiced concerning the assumptions of a constant failure rate. As an improved model for the real failure behaviour, the Weibull distribution was chosen, which is able to factor in a failure rate rising to a maximum after a certain time period.

Table 1: Classification of Performance Level (ISO 13849-1)

Performance Level	Average probability of a dangerous failure per hour PFH$_d$ [1/h]
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

In the VDW’s first study on the operational dependability of lathes, a Weibull distribution was approximated from field data for the clamping function of a lathe, with the following parameters: α=0.000443 and β=1.64. For the empiric analysis, at the end of the available time series it was accumulated that *F(t)* =1, which is an assumption on the safe side. The curve for the empirical failure probability is shown separately in Fig. 3. It needs to be mentioned that all events influencing the reliability are incorporated in the empiric data, safety-related and non-safety-related events. How the separation of the safety-related share can be conducted by means of a fault tree, is explained in another ESREL 2014 paper of VDW (Günnel et al. 2014).

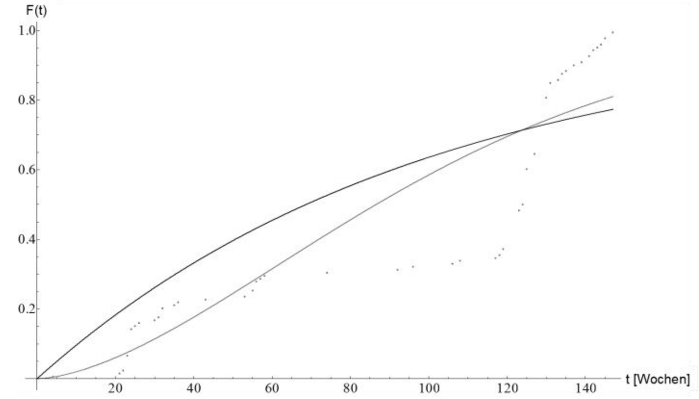


Figure 3: Empirical and theoretical failure probabilities for the clamping function of a lathe (Günnel et al. 2014)

3 CRITICISM OF THE RISK MODEL AS SET OUT ON ISO 13849-1 AND CORRECTIONS

The phenomenon “risk” obeys a necessary causation. According to the ISO 12100 standard, which is meant to explain the Machinery Directive (MD) 2006/42/EG for the practical design, the risk assessment is the combination of risk analysis and risk evaluation. Risk analysis subsumes specifying the machine’s limits (e.g. spatial and temporal limit), identifying the hazards involved, and estimating the extent of damage and the probability of its incidence. The risk $\mathfrak{R}$ is thus defined as a two-dimensional variable (damage severity S and expected frequency EF) which due to the EF element features a time-dependence:

$$\mathfrak{R}=S*EF \textit{ where } \mathfrak{R}=\mathfrak{R}(t) \qquad (8)$$

Unfortunately, the risk increase due to time duration or number of repetitions of single hazards is not yet considered plausibly in ISO 12100.

Starting with the risk estimate, the risk assessment is used to decide whether, after executing the measures involved, the goals for risk reduction have been achieved.

For this purpose, the machine is divided into spatial and temporal limits, in accordance with 5.3.3./4 of the above-mentioned standard. In the risk assessments so far publicly available for machine tools, analysis concentrates on individual hazardous situations/events, typical for specific machines, in which the machines are being used (i.e. man-machine-interaction, MMI). The modes of operation concept provide a standardized pattern for typical operator actions. From there, so called “stretched risk snapshots” can be derived as an abstracted MMI-model, which is needed as in input for the decision tree of ISO 13849-1. When this is done, the risk elements of ISO 12100 with regard to failure rates as “frequently based target values” are oddly compressed in ISO 13849-1, and the time slices of individual situations in relation to the machine’s entire lifecycle is not plausibly recorded. For example, no distinction is drawn at all as to whether individual “risk snapshots” are frequently repeated or occur very rarely, although the risk content in the total risk for a particular machine is crucially determined thereby.

In order to cover the temporal limits appropriately in the risk assessment, in chapter 4 a VDW-proposal is explained for grouping together the individual “risk snapshots” in a holistic risk profile (the “risk film”). This proposal covers all relevant phases of the life-cycle (20 years in accordance with ISO 13849-1) of the machine tool involved together with their time slices t_j (as a weighting factor in the with $PFH_d \cdot t_j$ approximated exponential distribution). In doing so, realistic risk proportions are made available for risk assessment in accordance with ISO 12100. The aim of this “untangling” of the compressed risk elements in ISO 13849-1 is to enrich the current discussion in the standardisation working groups, in particular in sub group 5 of the “Joint Working Group” for the merging into IEC /ISO 17305.

A risk model that considers only $\mathrm{PFH_d}$ value ranges (without considering the time duration) is not plausibly congruent with the definition of risk in ISO 12100. This is because the relative frequency F_{rel} is closely dependent on the observation time t concerned, as can clearly be seen in Fig. 1 and Fig. 2; it is always the integral of the density function:

$$F_{rel}(t) = \int_0^t f(\tau) \cdot \mathrm{d}(\tau) \qquad (9)$$

This is a probability in the sense of a relative frequency.

In a recent publication (G. Gigerenzer), too, the misunderstandings and misdirections in risk estimation are vividly illustrated as “risk incompetence”, which can be manifested even by high-ranking experts, if the risk is represented other than with relative frequencies in the Time Domain. Against this background, the risk definition provided in ISO 13849-1 can be seriously questioned in regard to the $\mathrm{PFH_d}$ value ranges, because the time-dependence of the expected frequency of severity levels is not explicitly dealt with in the decision tree (called “risk graph”) in Appendix A. Instead, the time-dependence is “accommodated” implausibly in risk parameter F, which is to be estimated out of the respective hazardous situation/event. Even recent discussions in the ISO working group in March 2014 for the ISO 13849-1 Amd 1 could not bring about a plausible definition of the parameter F, since it refers to the temporal ratio of hazardous exposure (which is plausible) *and in addition* to the frequency (*which is not plausible*). This risk model is therefore unsuitable for machine tools, because risk studies for machine tools must not simply ignore the temporally highly variable factor of man-machine interaction. It is precisely here that the greatest risk reductions can be achieved on the basis of defined access modalities within operating mode concepts, simply because the duration of the operator's exposure to hazard is minimised; temporally and spatially, e.g. with two-hand-control from a safely designed operator position. In the product standards for machine tools, there are detailed descriptions of how with the aid of fixed and movable guards the hazards resulting from random failures in the control chains can as far as possible be "kept away" from the operator. For risk assessment of machine tools, then one needs a "variable in the time domain", i.e. a reconciliation of:

- estimated expectable frequencies (EF) and corresponding severity levels (S)
  and
- tolerable limits for EF and S combinations.

From Meyna, the double-logarithmical Farmer diagram according to the Farmer graph (Farmer 1967) of Fig. 4 is explained in this context. A linear line represents a certain risk, comprising all possible combinations of EF and S of this risk. As regards machine tools, the S-axis could be normed to a maximum of one fatal accident, which can be considered - the very rarely occurring – worst case of injury. In the Farmer diagram, the individual steps for the risk reduction can be shown either as effect-related (reduced severity levels) or as cause-related (reduced frequencies) or as a mixture of the two; see Fig. 4 for the example of a flat-grinding machine with a primary wheel guard and an additional enclosure.

With the aid of the 3-step method of the Machinery Directive (or ISO 12100) in its specific implementation for machine tools, the effect of risk reduction can be illustrated as a vectorial variable, as described in VDMA Standard Sheet 34189; see the generalised principle in Fig. 4, starting with the "naked machine" by means of various measures:

1. increase in inherent safety of the machine functions, in accordance with the technology-dependent state of the art
2. fixed or movable guard with interlocking and guard locking within an operating mode concept
3. instructive safety (operating instructions and training)

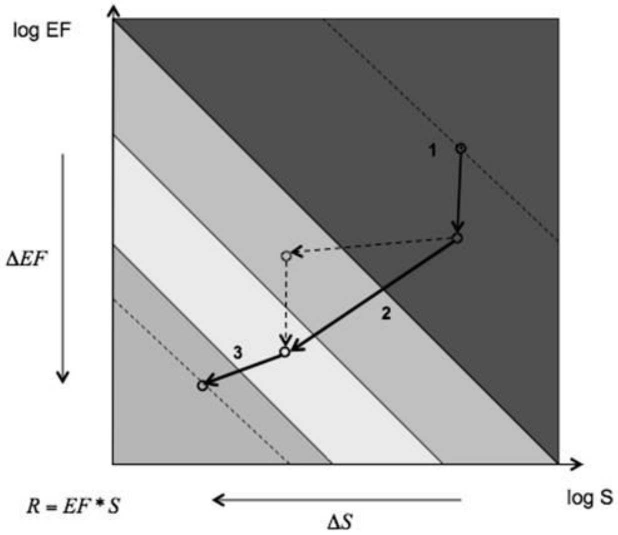


Figure 4: Theoretical risk reduction using the 3-step method acc. to ISO 16089 with primary wheel guard

The functional safety plays a role only in the inherent safety of the machine functions and in the interlocking of the enclosure. With the third step a tolerable risk can be achieved, if the instructions for the intended application are followed by the user. Otherwise, only step 1 provides a risk reduction and an orange of even red risk range may put the operator in jeopardy, e.g. when defeating safeguards.

When applying ISO 13849-1, a case distinction drawn between a:

- Pure safety function pure (e.g. two-hand control with dependable stopping of the drives) and a
- technology-dependent machine function (e.g. tool clamping)

has so far not been defined.

The typical feature of a machine function is that the design engineer is in any case targeting a high level of reliability in order to optimise the machine's availability for the owner's benefit. The safety-related reliability (functional safety) is here always improved as well, because safety is a subset of the overall reliability/availability, since a failure of functional safety will be given full statistical weight in quantifying the dependability or availability of the machine concerned. A machine function can become a safety function if it has to be safely shut down when guard doors are opened, e.g. a gravity-loaded vertical axis. It is clear that in this context time slices of the man-machine-interaction have to be factored in, because in the case of highly automated machines the transition to the safety function should have a far smaller time slice than the operation as a machine function. In fact, the trend to automation is going into this direction at least during the last decade.

Another unresolved discussion related to ISO 13849-1 is about the “overlapping of hazards”. On the one hand side, safety functions are looked at very closely in order cope with every conceivable imponderability in the relevant control chain. On the other hand, these detailed dissections are not interpreted as regards the superposition of individual safety functions, i.e. a plausible composition that refers to the proportions of single effects is completely missing. This seems to be a considerable gap in the ISO 13849-1 on its way to probabilistic professionalism. As a consequence, the possible influence of an required increase of “Performance Level” on an improved operational safety is completely overestimated. This is at least true for machine tools, for which fixed and moveable guards within a safely defined modes of operations concept are the dominant risk reduction strategy. Uhlmann, Meister & Mödden are explaining the situation in detail (2012).

4 VDW’S PROPOSAL FOR RISK PROFILING

The overall machine risk is in the VDW’s proposal totalled as a risk profile comprising the estimated individual contents of plausibly stretched “risk snapshots”, as explained in VDMA Standard Sheet 34189, over:

- *all man-machine-activities and*
- *all hazards potentially caused by control system errors of*
- *all relevant machine components*
- *over all lifetime phases*

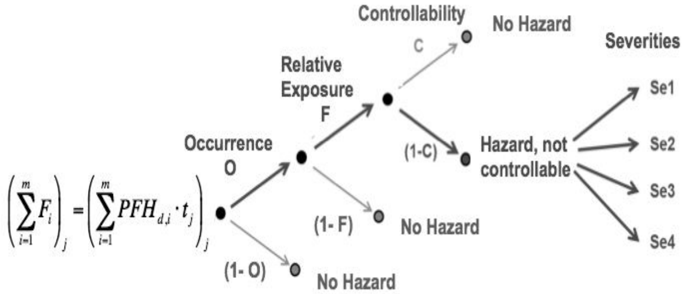


Figure 5: Risk path diagram, cause and effect relation,

In order to overcome the obstacles explained in chapter 4, VDW proposes an improved risk model in the Time Domain. Thereby, individual hazardous situations/events of man-machine interaction are modelled as (timely stretched) “risk snapshots” in order to follow ISO 12100, 5.5 (risk estimation), whereas the assumptions were made on the safe side for:

- the extent of damage in accordance with ISO 12100, 5.5.2.2 (Parameter S in accordance with accident statistics) and probability of occurrence of a damage in accordance with 5.5.2.3, with the influencing factors:
- ➢ hazard exposure in accordance with 5.5.2.3.1 (Parameter F: activity-related),
- ➢ probability of occurrence for the hazard in accordance with 5.5.2.3 (Parameter O: situation-related): the parameter O is in the risk profiles of the VDW mostly set to a value of 1, because the effects that reduce the probability of occurrence of damage are separately argued as a time share adducing a variable man-machine interaction. This is different from the utilization of parameter O in part 2 of this paper, because the “roof” of type A and B standards does not offer an explicit consideration of the time effect on the risk.
- ➢ avoidability or controllability in accordance with 5.5.2.3.3 (Parameter C: operating-mode-dependent)
- and further relevant aspects in accordance with 5.5.3.

For a “risk snapshot”, the connection between “cause” and “effect” can be depicted with the aid of the path diagram for mutually independent elements (O, F and C) in Fig. 5:

a) The probability of a hazardous failure in all safety-relevant control chains *i=1* to *m* for the MMI activity *j=1 to n* concerned $\sum_{i=1}^{m}\left(PFH_{d,i} \cdot t\right)$ as a possible “cause”

and

b) The probability or relative frequency of an operator’s injury with discrete severity levels Se 1 to Se 4 (in accordance with IEC 62061) as a possible “effect”.

The result of the severity-level prognosis is directly dependent on risk parameters O_j, F_j and C_j. In order to arrive at the severity levels, the distribution of the severity levels Se 1 to Se 4 is connected with a histogram typical for machine tools (i.e. accident pyramids of the BAuA).

$$\Re_j = S_j \cdot F_j \cdot (1 - C_j) \cdot O_j \cdot \left\lfloor \sum_{i=1}^{m} (-PFH_{d,i} \cdot t_j)_i \right\rfloor_j \qquad (10)$$

Individual safety functions, with their expected frequencies are added together to form a superimposed failure probability $\sum_{i=1}^{m}(-\mathrm{PFH}_{d,i}\cdot t_j)_i$, and multiplied by an occurrence probability O_j for the materialisation of a hazard.

The totalling function of the total risk $\mathfrak{R}(T)$ over all j = 1 to n risk snapshots during the time period $T=\sum_{j=1}^{n}\Delta T_j$ is obtained by totalling the snapshots with their temporal weighting in the approximated exponential function:

$$\mathfrak{R}(T)=\sum_{j=1}^{n}\mathfrak{R}_j(\Delta T_j) \qquad (11)$$

$$\mathfrak{R}(T)=$$

$$\sum_{j=1}^{n}\left[S_j\cdot F_j\cdot(1-C_j)\cdot O_j\cdot(\sum_{i=1}^{m}PFH_{d,i}\cdot t_j)\right] \quad (12)$$

In this way, a plausible relationship is established between the multiplicity of causes (control system failures) and the bandwidth of possible effects (hazards and expectable severity levels) in the context of the highly time-variable man-machine interaction. The risk reductions can thus also be depicted in a time domain as an enclosure with interlock and locking in the context of an operating mode concept. This is what the product standards for machine tools are dealing with very successfully since more than a decade.

The risk profiling gives an interesting insight in the ongoing discussions about the "overlapping of hazards". The detailed dissections of single safety functions are dealt with in superposition (Kolmogorov's Third Axiom), and a plausible composition considering the proportions of single effects is introduced by this paper. This should not be neglected.

The risk profiling method is also intended to trigger a public discussion, particularly in the relevant standardisation bodies. For instance, in sub group 3 of the JWG 1 for the into IEC /ISO 17305, several machine examples have been discussed, for turning, grinding and milling machines, showing the significant risk reduction of guards, Fig. 8 to 12 are taken as examples from them. In addition, a presentation on this topic was given during the VDW's Technology Day at the METAV in March 2014. Furthermore, a comparison between different risk scoring systems (not yet compared e.g. in ISO / TR 14121-2) is feasible with the risk profiling, when a comparison object is selected, e.g. a machine as in fig. 8.

This risk snapshot, however, occurs more than once during a machine's service time (mission time), as a consequence a grouping of equivalent risk snapshots occurs. The factor with which the j-th snapshot has to be weighted over the exponential function as a group is reflected in the time slices; see Fig. 6, Fig. 7 and Fig. 9.

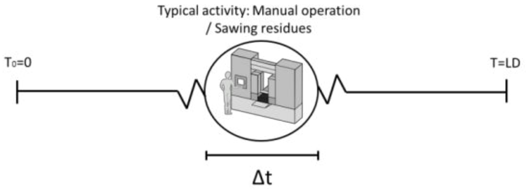


Fig. 6: Individual risk snapshots within the service time (mission time)

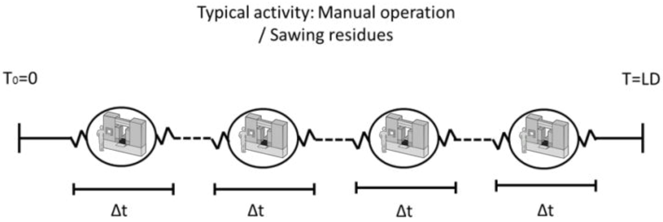


Fig. 7: Repetition of risk snapshots and supsumption in a group as a a time share within the lifetime service time (mission time)

A practically useful risk model has to be able to depict the case that a reduction of activities with a comparatively increased risk of injury leads overall to a reduction in the total risk involved for the machine concerned. For example, for machine tools "offline setup" (instead of usual setup at the machine) is being developed using a 1-to-1 simulation model of the actual machine at a PC. This enables the risk to be significantly reduced by downsizing the amount of repeated activities during setup, see Fig. 10 with operation mode 2 (OM 2) as a significant risk share with 37,5%. This cannot, however, be argued with the risk model of ISO 13849-1, because it does not deal at all with a reduced repetition frequency of critical situations, although this reduction (in the author's view) is the most important element in risk reduction for machine tools.

The result of the supsumption into groups of theequivalent risk snappshots of a time allocation overthe service time (mission time) for the machine shown in Fig. 8 may resemble the diagram in Fig. 9.

Fig. 8: Example of a CNC milling machining center (5 axes)

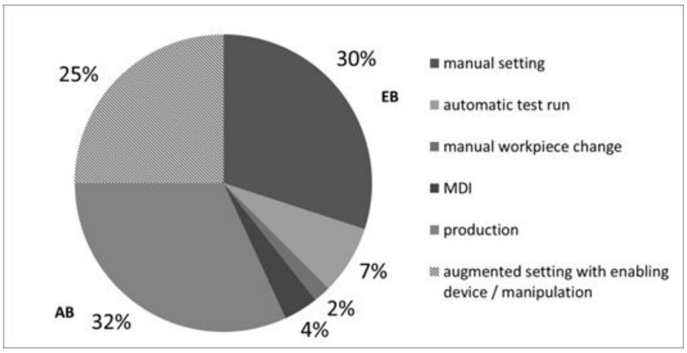


Fig. 9: Time slices of different operating modes (AB=automatic mode, EB=setup mode, SBA= Special operating mode).

The time shares of installation and troubleshooting are not listed, because these shares are relatively unimportant for the risk assumption caused by control failures on the other hand they represent accidents focuses caused by other reasons.

Furthermore, the cost-benefit ratio is for VDW companies an important issue in what is anyway a very predatory competition with low-price machines. This is another reason why a profiling method has been developed in the form of a Farmer Matrix and a two-dimensional Pareto diagram; see Figs. 10 and 11 below.

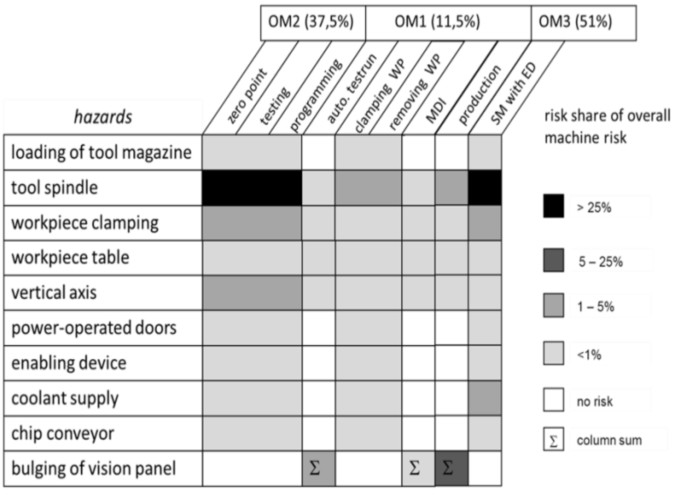
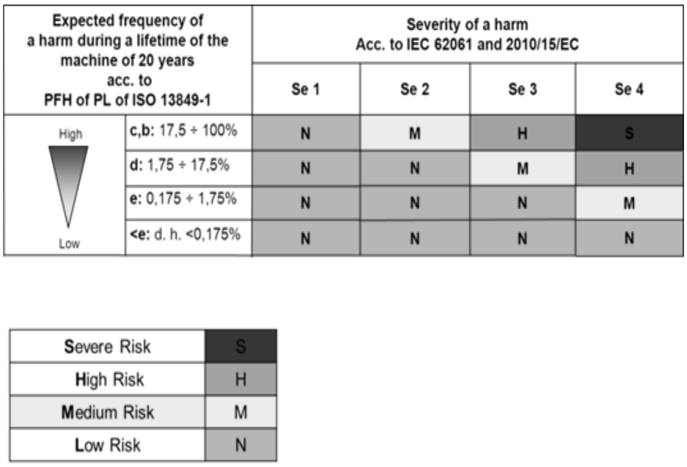


Fig. 10: Two-dimensional Pareto diagram for the risk of a milling machine being used for its intended purpose, with a program test and enabling device in accordance with ISO 16090.

The risk presentation formats in Figs. 10 and 11 enable the design engineer to reduce the risk as best as possible, relating proposed additional efforts to the benefits obtained. Parameter studies are possible, answering the question: Which efforts leads to the highest risk reduction? Or the question (see Fig. 12: Is the special operation mode really the "lesser evil" compared to defeated safeguards (manipulation)?



Expected frequency of a harm during a lifetime of the machine of 20 years acc. to PFH of PL of ISO 13849-1		Severity of a harm Acc. to IEC 62061 and 2010/15/EC			
		Se 1	Se 2	Se 3	Se 4
High	c,b: 17,5 ÷ 100%	N	M	H	S
	d: 1,75 ÷ 17,5%	N	N	M	H
	e: 0,175 ÷ 1,75%	N	N	N	M
Low	<e: d. h. <0,175%	N	N	N	N

Severe Risk	S
High Risk	H
Medium Risk	M
Low Risk	N

Fig. 11 (below): Proposal for a Farmer Matrix for comparing accumulated risk estimates

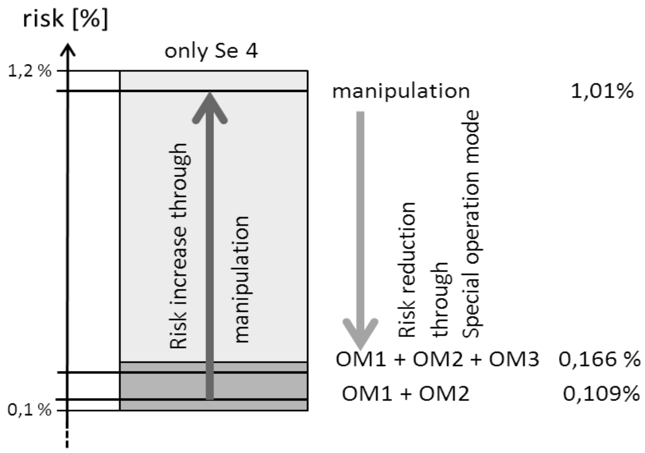


Fig. 12: Risk comparison with standardised references for severity level Se 4

5 PROBABILISTICALLY FOUNDED GUARD DIMENSIONING

The safety of a machine tool depends very much on the impact resistance of fixed and moveable guards (enclosure with vision panels). In the current product standards a non-probabilistic approach is still the basis for empiric tests to determine the required guard thicknesses. However, in reality all design variables are random variables, which can be described with statistical methods. The deterministic approach does not consider very unlikely events, but, it is desirable to know, what the probability P for a perforation event is, when the dimensioning is in compliance with the standard requirements: Is the probability tolerable? The probabilistic requirements for the functional safety can be directly compared with the requirements for the guard dimensioning, because both serve the same goal: operator protection. As a first step, it could be evaluated, how the deterministically defined state of the art in product standards performs in the probabilistic domain, i.e. if the impact resistance and the impact energy are being considered random variables.

Out of the density functions for the impact resistance R and the impact energy E, the probability P of a perforation event can be calculated. If e.g. impact resistance and impact energy follow a standard distribution, the relevant mean values and standard deviations can be empirically derived. The difference of both density functions, the „limit state function“ is again a standard distribution, of which the mean and standard deviation are functions of the input functions. The failure probability is the negative area element of the integrated limit state function. It is equivalent to the intersection area of the density functions of impact resistance and impact energy, see figure 13 and Montgomery. To start with, in Berlin and Tokio this approach is being studied for grinding machines, indicated in the CNC-Arena.

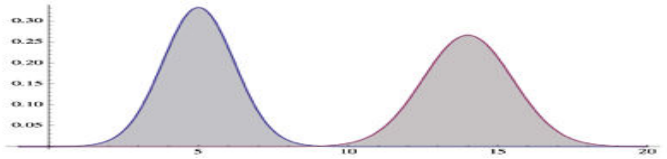


Fig. 13: Intersection of two density functions

6 CONCLUSION

When comparing probabilistic theory and practice, the question arises, how the designer should consider a quantifiable tolerable risk in a responsible way. The deliberations above show that a quantitative risk assessment does not necessarily mean the numerical verification of the compliance with a tolerable limit. Due to the multi-dimensional variability of the man-machine-interaction as illustrated in the risk profiling in chapter 4, a precise proof is not feasible. However, showing the relative proportions of the risk reduction effects following the 3-step-method of ISO 12100 is much more important than giving an absolute value, which anyway depends on many subjective estimations. In doing so, estimates on the safe side that are summed up provide again a safe estimate. So, the essential effects become visible (see Fig. 10) and reproducible parameter studies can be conducted in a relatively objective manner (see Fig. 12). This enables the designer to justify that he derived a best possible design in the boundaries of technically available and economically acceptable means.

Depending on the specific aspects of a technology, numerically different tolerable risks develop as the significant differences in accident statistics of wood working and metal working machines clearly indicate, although the technologies are very similar except for the machined material (BAuA, 2010).

The best possible reference for a tolerable risk is the state of the art in well-tried product standards as ISO 16090 (before EN 12417). An increase of the requirements in the standard needs to be justified plausibly, and an appropriate consideration of the economic risk in Global competition is indispensable, not only in (small and medium) enterprises, but also from the Health and Safety experts.

Proving a tolerable risk can become a challenge, if product standards are not available. Then plausible probabilistic methods can be an useful argumentation platform, because the term „probability“ in the law can be applied mathematically correct.

For the sake of comparison with reality, a separate third paper of Mödden & Günnel (ESREL, 2014) shows empiric findings of field data analyses.

Finally, a revealing oral statement on the quantitative consideration of safety, given by Dr. Heinrich Mushardt in 2013, an honoured VDW senior designer for machine tools, who retired recently, shall be quoted here:

„Under the obligation, to keep records of design analyses and to deal with potential hazards in a numerically plausible way, the designer can elude the allegation of culpable negligence. However, the completeness of analyses and the correctness of the decisions presumably can only be reviewed in case of damage. The numerically small values and the multitude of possible causes (for a hazardous effect) are located in the statistically limit range of small numbers. Statistically founded conclusions are not easy to obtain, when customers’ requirements lead to a trend towards individual „one-off“ designs. This causes scepticism whether the practical application of ISO 13849-1 can bring about significant improvements for the safety of machine tools. Risks due to foreseeable human behaviour shall be excluded, but there are also a not foreseeable misuse, technical failures and working errors. On this background, it should not be forgotten how rare severe injuries at machine tools occur altogether, and that if one severe accident happens, unforeseeable events or unforeseeable misuse of possibly criminal conduct play a major role but NOT primarily a lack of functional safety.“

7 REFERENCES

EN ISO 13849-1, 2008. *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*. Berlin: Beuth Verlag GmbH.

IEC/ISO 17305, 2014. *Safety functions of control systems*, Joint Working Group 1 (draft 2014)

Montgomery, D. et al. 2010. *Engineering Statistics.* Wiley; 5 Edition

Günnel, B. et al. 2013. *EN ISO 13849-1 – New quantitative requirements for Functional Safety in the machine tool industry,* ESREL 2013

Bundesministerium für Arbeit und Soziales 2010. *Sicherheit und Gesundheit bei der Arbeit 2010, Unfallverhütungsbericht Arbeit*, BAuA

B.Günnel et al. 2014. *Proven in use in the machine tool industry for demonstrating the quantitative Functional Safety according to EN ISO 13849 1,* ESREL 2014

EN ISO 12100, 2010. *Safety of machinery – General principles for design – Risk assessment and Risk reduction.* Berlin: Beuth Verlag GmbH.

The European parliament & the council of the European Union 2006. *Machinery Directive 2006/42/EC.*

Gigerenzer, Gerd 2013. *Risiko – Wie man die richtigen Entscheigungen trifft,* C.Bertelsmann, in English: *Risk Savvy, How to Make Godd Decisions*, Penguin New York

Meyna, A. & Pauli, B. 2010. *Zuverlässigkeitstechnik - Quantitative Bewertungsverfahren*. Munich, Germany; Carl Hanser Verlag.

E. Uhlmann et al. 2012. *Sicherheit an Werkzeugmaschinen: Die Bedeutung der trennenden Schutzeinrichtung für die Risikoreduktion an Werkzeugmaschinen,* ZWFJahrgang 107 Hanser Verlag

VDMA Einheitsblatt Nr. 34189 2013. *Steuerung von Werkzeugmaschinen – Risikobeurteilung, Draft 2013*

IEC 62061, 2005. *Safety of machinery - Functional safety of electrical, electronic and programmable control systems for machinery.* Berlin, Germany; Beuth Verlag GmbH.

METAV 2014 press release *VDW-Technology Day "Safe ty engineering for metal-cutting machining"*

ISO/CD 16090, 2014. *Machine tools — Safety — Milling machines (draft international standard)* Berlin, Germany; Beuth Verlag GmbH.

CNC-Arena:http://www.cnc-arena.com/de/emagazine/01-2014/, see page 24.

Bruce W. Main, 2012 *Risk Assessment – Challenges and Opportunities* ,Ann Arbor, USA; design safety engineering inc.

F.R. Farmer, 1967. *Containment and sitting of nuclear power plants - Siting criteria — A new approach* International Atom Energy Agency, Vienna, Austria

Probabilities in Safety of Machinery – Part 2: Theoretical and Practical Design

Armin Bornemann
Deckel Maho, Pfronten, Germany
Yannick Froese
Fachhochschule, Frankfurt am Main, University of Applied Sciences
Luca Landi
Department of Engineering, University of Perugia, Perugia, Italy
Heinrich Mödden
German Machine Tool Builders Association, Frankfurt am Main

ABSTRACT

As stated in part 1 of the article, standard ISO 13849-1 deals with the theoretical probabilities of hypothetical individual events and the possibility of reconciliation of this theoretical approach with empiric field data is partly neglected.

In part 2 the problems arising during the real design of SRP/CS (Safety Related Part of a Control System) of machines are addressed on the background of relevant safety standards. Using the informative theoretical appendix A of ISO 13849-1 to determine the Performance Level required (PLr) may cause sometimes technically impracticable requirements, which are far beyond the state of the art in existing type C standards. For the sake of connection between theory and practice, the probability of occurrence of a hazardous situation must be taken into account in order to appropriately consider the required risk reduction of a SRP/CS in the context of the three-step-method of ISO 12100. For this purpose two practical solutions are provided:

1. a methodology for PLr definition for safety functions considering a realistic probability of occurrence of hazards, using a hybrid approach of ISO 13849-1 and IEC 62061.

2. a "table based" methodology for the design of machine tool control system considering all the realistic "occurrences" as stated also in the "new" ISO/TR 14121-2.

The selected safety function for 2.) is very similar to the safety function "prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece" of the standard ISO 16090-1. This safety function was chosen in another paper of Günnel, Mödden for ESREL 2014. Therein, the analysis of field data of real milling machines shows that a reliability between PL=a and PL=b is actually being achieved with state of the art design. This finding connects quite well theory and practice of state of the art milling machines.

Those contributions are extracted from the work during the ISO/TC 39/SC 10/WG4 works (ISO/CD 16090 for milling machines).

REFERENCES

EN ISO 13849-1, 2008. *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*. Berlin, Germany; Beuth Verlag GmbH.

IEC 2012. *IEC 62061:2005 + A1:2012. Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.* International Organization for Standardization, Geneva, Switzerland

.

ISO, 2012a. *ISO/TR 14121-2 - Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods.* . International Organization for Standardization, Geneva, Switzerland

ISO 2014. *ISO/CD 16090 - Machine tools safety — Machining centres, Milling machines, Transfer machines — Part 1: Safety requirements.* International Organization for Standardization, Geneva, Switzerland.

B.Günnel et al.2014. *Proven in use in the machine tool industry for demonstrating the quantitative Functional Safety according to EN ISO 13849 1,* ESREL 2014

Probabilities in Safety of Machinery – Part 2: Theoretical and Practical Design

Armin Bornemann
Deckel Maho, Pfronten, Germany
Yannick Froese
Fachhochschule, Frankfurt am Main, University of Applied Sciences
Luca Landi
Department of Engineering, University of Perugia, Perugia, Italy
Heinrich Mödden
German Machine Tool Builders Association, Frankfurt am Main

ABSTRACT As stated in part 1 of the article, standard ISO 13849-1 deals with the theoretical probabilities of hypothetical individual events and the possibility of reconciliation of this theoretical approach with empiric field data is partly neglected.

In part 2 the problems arising during the real design of SRP/CS (Safety Related Part of a Control System) of machines are addressed on the background of relevant safety standards. Using the informative theoretical appendix A of ISO 13849-1 to determine the Performance Level required (PLr) may cause sometimes technically impracticable requirements, which are far beyond the state of the art in existing type C standards. For the sake of connection between theory and practice, the probability of occurrence of a hazardous situation must be taken into account in order to appropriately consider the required risk reduction of a SRP/CS in the context of the three-step-method of ISO 12100. For this purpose two practical solutions are provided:

1) a methodology for PL_r definition for safety functions considering a realistic probability of occurrence of hazards, using a hybrid approach of ISO 13849-1 and IEC 62061.

2) A "table based" methodology for the design of machine tool control system considering all the realistic "occurrences" as stated also in the “new” ISO/TR 14121-2 Those two contributions are extracted from the work during the ISO/TC 39/SC 10/WG4 meetings (ISO/CD 16090 for milling machines).

The selected safety function for 2.) is very similar to the safety function “prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece” of the standard ISO 16090-1. This safety function was chosen in another paper of Mödden, Günnel for ESREL 2014. Therein, the analysis of field data of real milling machines shows that a reliability between PL=a and PL=b is actually being achieved with state of the art design. This finding connects quite well theory and practice of state of the art milling machines.

1 INTRODUCTION

The design of Safety Related Parts of the Control System (SRP/CS) it is one of the emerging problems of the new standard requirements related to Machinery Directive (European Parliament and the Council of European Union, 2006).

The leading standards are ISO 13849-1:2008 and IEC 62061:2005 respectively from a “mechanical and electronic point of view”.

If compared with the older “European standard~~s~~” (EN 954-1:1996), the basic reliability concept of categories and design of systems with a given hardware fault tolerance has been rewritten in terms of reliability calculation.

Now the SRP/CS has to be designed using a validation procedure that requires a minimum reliability to be acquired in terms of Mean Time to Dangerous Failures ($MTTF_d$)

Also other very important concepts have been developed in the new standards mentioned above. Such as the requirement of a Diagnostic Coverage (DC) and the design of systems which considers the Common Cause Failures (CCF). Trying to summarize with an understandable simplification, using the new standards a good architecture on the SRP/CS (for example doubled channels) is no longer sufficient to achieve the required minimum reliability.

The acronyms for the overall design safety concepts of the two standards are: PL (Performance Level, ISO 13849-1) and SIL (Safety Integrity Level, IEC 62061).

As it will be explained in detail in the next paragraphs those two different concepts, whose full calculation are performed in different ways, are comparable in terms of Average Probability of Dangerous Failure per Hour (PFH_D, expressed in terms of 1/h).

The main problem of those two "safety views", often sharing the same components on a real machine, is the result~~s~~ of risk assessment (see also Part 1 of this paper). The minimum PFH_D required for assuring a sufficient level of safety may be different if the calculation it is performed using the SIL or PL concept, because ISO 13849-1 is cutting at $MTTF_d$ at 100 year and IEC 62061 is doing it with 150 year.

And if some technologies are used for SRP/CS, e.g. pneumatic or hydraulic, only the PL concept according ISO 13849-1 is still valid for the full design process, but often both are valid.

The PL_r (required) needs to be derived from the risk assessment with the three-step-method of risk reduction according to ISO 12100:2010.

The Machine Directive only requires a risk assessment, but does not specify as it shall be done. Moreover also the ISO 12100, type A standard, specifies the principles of risk assessment and does not specify any method to do it.

In the following paragraphs some methods useful to calculate PL_r, in full accordance with the risk assessment principles of ISO 12100, will be presented. In the first paragraph, an hybrid method ISO 13849-1 - IEC 62061 will be presented. In the second paragraph, a table method covering all the phase necessary to perform the risk estimation for a general safety function of a SRP/CS will be shown.

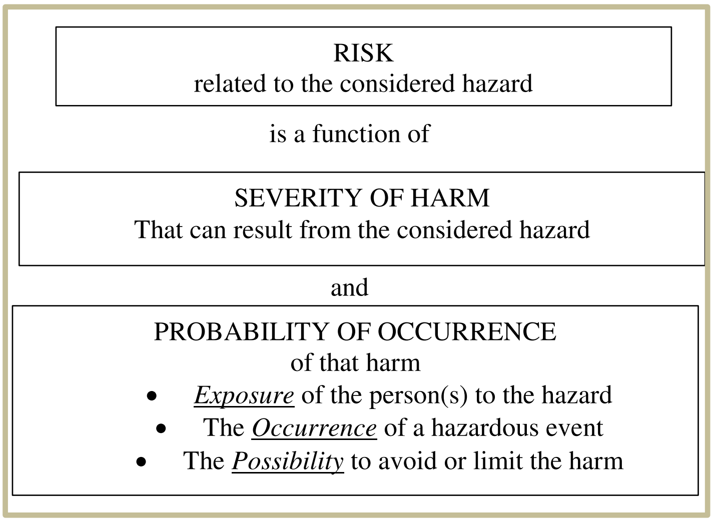
2 DEFINITION OF THE PL_R

Trying to merge the two different approaches of the two already mentioned standards, some preliminary consideration on the definition of a hazard occurrence probability in ISO 12100 has to be done.

2.1 *The "occurrence problem" on ISO 13849-1*

If somebody sees the element of risk of the figure 1 ISO 12100, one can notice that the overall probability of occurrence of the harm depends on (see part 1 of the paper):

1. exposure,
2. occurrence of hazardous event,
3. possibility of avoiding or limiting the harm.



RISK
related to the considered hazard

is a function of

SEVERITY OF HARM
That can result from the considered hazard

and

PROBABILITY OF OCCURRENCE
of that harm

- *__Exposure__* of the person(s) to the hazard
- The *__Occurrence__* of a hazardous event
- The *__Possibility__* to avoid or limit the harm

Figure 1. Elements of risk according to ISO 12100

If one looks at the definition of Occurrence (point 5.5.2.3.2 of the ISO 12100), the relevant factors that influence the probability of occurrence of harm are:

1. reliability and other statistical data,
2. accident history,
3. history of damage to health,
4. comparison of risks.

The standard says clearly that *__those factors__* *__shall be taken into account__*.

Looking at informative Annex A of ISO 13849-1, concerned with the contribution to the reduction in risk made by the SRP/CS, amazingly, an explicit provision of the occurrence parameter is missing.

The method given here provides, as stated in ISO 13849-1: *"only an estimation of risk reduction and is intended as guidance to the designer and standard maker in determining the PL_r for each necessary safety function to be carried out by an SRP/CS".*

In our opinion this definition it is too conservative and some of the already mentioned relevant factors of ISO (e.g. real accident history) cannot be taken plausibly into consideration.

To give an example, we are looking at the safety function (SF) of limited speed monitoring – maximum spindle speed during some modes of safe operation (MSO) for milling machines (ISO CD/16090, 2014, table J.2. paragraph 2). Among experts, there are no accidents known due to this risk. If the occurrence of a hazard is not taken into account, no risk reduction can be done. The same is true, if a real harm related with this risk never occurs in the operational field. The point is that the machines are designed the last 10-15 years with high safety standards and the technology has been changed in the drive control system. Before this has been done, some accidents had occurred. This evidence/lack of injuries can be researched, for example, on national accident institution surveillance reports (e.g. INAIL 2013). From the ”experience point of view” the theoretical severity of the harm is high, but in the “real world” we have no evidence of real accidents.

In the novel technical report ISO/TR 14121-2 (ISO 2012) the problem of *probability of occurrence of hazard* and its correlation with *probability of occurrence of harm* is clarified.

In point 5.4.3 of the ISO/TR it is clarified that occurrence of a real harm is a fundamental aspect to take into account and this occurrence is strictly connected not only with potential risk, but also with occurrence as stated in ISO 12100.

In all the risk estimation tools proposed in subsequent paragraph 6 of ISO/TR 14121-2 the occurrence is always taken into account.

For example if the risk graph method is used according to ISO 14121-2_2013, section 6.3.2, the occurrence is divided in three levels:

1. O1 – low
2. O2 –medium
3. O3 – high.

In IEC 62061 there are even 5 levels as defined in table A.3.

In ISO 13849-1 one cannot find any definition or any variations or levels.

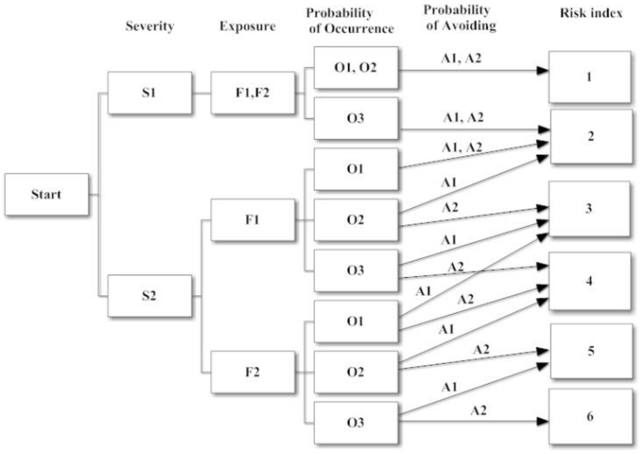


Figure 2. Risk graph from ISO/TR 14121-2

From statistical data on the market, usually we have data of occurrence of harm and not occurrence of hazard, which is different from a theoretical point of view. In other words, the SRP/CS designer has to be sure that there is no accident data recorded for a given SF, but this fact does not mean no occurrence of hazardous event. It only means that the designer managed to cope with the hazardous events by applying the right safety measures.

For instance usually we have designed and properly installed other protective measure (as guards) for a specific risk reductions (e.g. impact with moving parts) effecting also the SF risk estimation.

If the occurrence of hazard is low, the general hypothesis of reducing the risk index by one level appears to be a good compromise between the theoretical and the real application (see figure 2). This can be done, if you use the informative risk graph of ISO /TR 14121-2. On the other side, when the occurrence of hazard is high, the risk index is increased, if a possible severe injury is expected.

From the authors point of view, the entire machine tool is a very complex machine made of several hundreds or thousands of components and the correlation between different safety principles leading to a common risk reduction cannot be simply neglected, but needs to be considered properly (see chapter 4 of part 1 of the paper). If a very complex machine with several correlations between SF and other safety measures has to be taken into account, the designer has to take an overall view of the entire machine. The proposed risk estimation matrix method of ISO/TR 14121-2 (table 1), taking into consideration directly the overall probability of harm it is a quite realistic approach.

Table 1. Risk estimation matrix from ISO/TR 14121-2

Prob. of	Severity of harm			
occurence of harm	Catastrophic	Serious	Moderate	Minor
Very likely	High	High	High	Medium
Likely	High	High	Medium	Low
Unlikely	Medium	Medium	Low	Neglig.
Remote	Low	Low	Neglig.	Neglig.

2.2 *Element of risk in different standards and technical reports*

Before the merging project IEC/ISO 17305 is providing concrete results, we have at first to summarize the different meanings of risk element of ISO 13849-1 and IEC 62061.

2.2.1 *Severity (S or Se)*

In ISO 13849-1 only two severity levels are used, and they are called S1 and S2, where S2 is severe injuries. In contrast hereto, in IEC 62061 four severity levels are used, which largely correspond to the four severity levels of EU Decision on general safety of products (Decision 2010/15/EU, called RAPEX), see table 2.

Comparing the severity, bruises and/or cut wounds without complications are classified as S1 in ISO 13849-1 (table A.1.), that corresponds only partially to the grouped severity levels Se1 and Se 2 of ISO 62061.

The severity levels Se 3 and Se 4 of ISO 62061 are, in accordance with Table A.1, largely congruent with severity level S2 of ISO 13849-1.

2.2.2 *Exposure (F or Fr)*

In ISO 13849-1 only two exposure levels are used, and they are called F1 and F2 (the F2 is frequent exposure, a very rough method which even tries to compress the duration of hazardous situations into a frequency, which is not plausible, as already stated in part 1 of the article).

In IEC 62061 five exposure (*Fr*) levels are used (Table A.2) with numerical values that can to be assigned.

2.2.3 *Possibility of avoiding the hazard – harm (P or Av)*

In ISO 13849-1 again only two probabilities of avoiding of hazard levels are used, and they are called P1 and P2 (the P2 is to be used, if there are no/little chances to avoid the hazardous situation).

In IEC 62061, we have a different theoretical contribution, here we have three levels of probability of avoiding or limiting harm (*Av*) not hazard (Table A.4) with three different numerical results possible from an overall estimation.

2.2.4 *Occurrence of hazard (Pr)*

In ISO 13849-1 is not possible to take an occurrence probability explicitly into account. Very different from this, in IEC 62061 we have five levels available. As regards automatically controlled machines, especially the risk of unexpected start-up of a movement has to be taken into consideration in the context of the three-step-method of risk reduction of ISO 12100. Only then it is possible to estimate the occurrence probability that will be caused, if the SRP/CS fails. The intended use needs to be taken into consideration e.g. as regards the modes of operation (e.g. setup, manual or automatic working, maintenance). On the background of a kind of "naked" machine (i.e. only step 2 of 3 steps of risk reduction is considered), the occurrence probability of a hazard due SF failure cannot reasonably estimated. But, ISO 13849-1 tries to do exactly this, not surprisingly concluding that the occurrence probability rather should be equals to 1.

2.3 *A practical "partial merging" method for type C standards*

The risk classification method in accordance with IEC 62061 is of general validity, and not only restricted to electrical control systems. Therefore, it can also be applied to mechatronic control chains as ISO 13849-1 regards them. The requirement for a SF made of mechatronic components can thus be defined either with the informative decision tree, (wrongly called "risk graph") of ISO 13849-1, or with a risk classification in accordance with IEC 62061. Other parts of IEC 62061 however, for example the beta factors estimation for common cause failures, are not useable, when hydraulic and pneumatic systems are used.

In IEC standard the results of risk estimation leads to a class of probability of harm (not hazard) CL:

$$CL = Fr + \mathrm{Pr} + Av \qquad (1)$$

In table 2, the result of IEC 62061 is a SIL.

Table 2. SIL from IEC 62061

Severity	Class (Cl)				
(Se)	3-4	5-7	8-10	11-13	14-15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2.
1				(OM).	SIL1

So a defined PFH$_d$ value range dependent of a SIL is stated (see IEC 62061, table 3 below).

Table 3. PFH$_d$ and SIL

SIL	Probability of dangerous Failures per Hour (PFH$_d$)
3	$\geq 10^{-8}$ *to* $< 10^{-7}$
2	$\geq 10^{-7}$ *to* $< 10^{-6}$
1	$\geq 10^{-6}$ *to* $< 10^{-5}$

The resulting PFH$_d$ value range is likewise defined in ISO 13849-1 Table 3, table 4 below.

Table 4. PL from IEC 13849-1

PL	Average probability of dangerous Failures per Hour (1/h)
a	$\geq 10^{-5}$ *to* $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ *to* $< 10^{-5}$
c	$\geq 10^{-6}$ *to* $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ *to* $< 10^{-6}$
e	$\geq 10^{-8}$ *to* $< 10^{-7}$

From the tables 3 and 4 we can conclude that because the value ranges of PFH$_d$ are largely congruent, the risk graph and the risk classification can be plausibly linked to each other. The PFH$_d$ parameter is a common mathematical platform between ISO 13849-1 and IEC 62061 (assuming that also the IEC 62061 definition is an "average", as illustrated in part 1 of this paper).

The PL=a has no correspondence with SIL.

In the figure 3, the result of the decision tree of ISO 13849-1 is a PL_r.

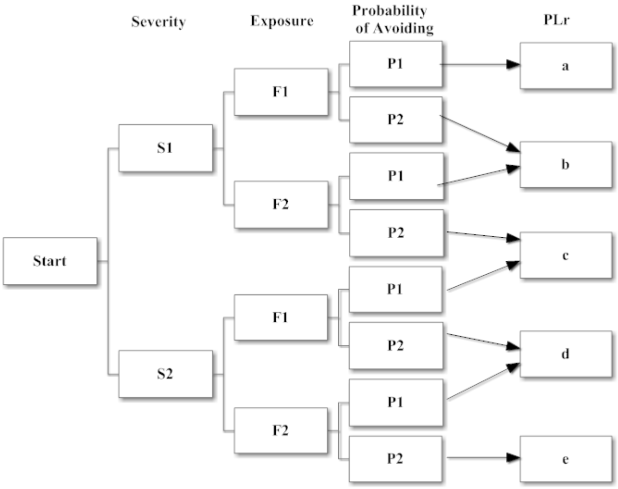


Figure 3. PL_r from IEC 13849-1

A SIL 1 is equivalent to PL=b and PL=c. Only for injuries with a lower severity of S1, PL=b can be derived, since for a severity of S2 at least PL=c is demanded. SIL 1, however, subsumes the entire PFH_d value range of PL = b and PL = c.

SIL 2 is completely equivalent to PL=d and SIL 3 is fully equivalent to PL=e.

Furthermore, IEC 62061 provides, as we have already seen, more "levels" for each parameters and the overall CL, see equation 1 and table 2 above. This enables a substantially more realistic and more accurate assessment of the risk reduction to be achieved by the SRP/CS than in ISO 13849-1.

The requirement for SIL 1 is, in accordance with table 2 detailed for the following combinations and risk classes:

- severity level Se 3 with CL 8-10,
- severity level Se 2 with CL 11-13,
- severity level Se 1 and CL 14-15.

On the basis of these requirements of SIL 1, the following case differentiations are derived for the minimum PL_r:

Se 1 and CL=14, SIL 1 → $PL_{r,min}$ =b
Se 1 and CL=15, SIL 1 → $PL_{r,min}$ =c
Se 2 and CL=11, SIL 1 → $PL_{r,min}$ =b
Se 2 and CL =12 or 13, SIL 1 → $PL_{r,min}$ =c
Se 3 and CL=8 or 9 or 10, SIL 1 → $PL_{r,min}$ =c because injuries of Se 3 are irreversible and comparable to S2 in ISO 13849-1, and there PL=c (S2, F1, P1) is the lowest possible PL.

In IEC 62061, below SIL 1 "other measures" must be provided at least (OM in table 2). We have also a very important note to table 3 point 5.2.4.2 in the IEC 62061. If we have less than SIL 1 from risk estimation, the minimum requirements are the ones of category B of ISO 13849-1.

The requirement of OM is, in accordance with table 2, detailed for the following combinations and risk classes:

Se 1 and K=11-13, AM → $PL_{r,min}$ =a
Se 2 and K=8-10, AM → $PL_{r,min}$ =a
Se 3 and K=5-7, AM → $PL_{r,min}$ =a

In addition to $PL_{r,min}$ =a, the wording "other measures" of IEC 62061 is used. Following this approach, the IEC 62061 OM + ISO 13849-1 PL=a become a kind of "safety integrity performance level" with the sum of the requirements of both.

In our opinion, this hybrid approach gives excellent results on removing the very rough risk estimation of ISO 13849-1 (see also Hedberg & others, 2011).

Example 1: the following example shows the difference that could be found using the direct approach of ISO 13849-1 instead of the hybrid one presented. The SF function being analysed here is *limited speed of spindle due to tool* being applied in different modes of safe operation (MSO).

When exceeding the maximum processing speed of the tool, a controlled stopping of the tool spindle shall takes place according to IEC 60204-1:2009, 9.2.2 depending on the technique applied.

Usually the maximum processing speed shall be provided in the tool parameters of the tool management (manual human data input).

The risk estimation of ISO 13849-1 leads for long stays during some operation to: S2- F2 -P2 and then to PL=e. This is often far away from both, and from the state of the art of all the tooling machine technologies and from technical achievability.

If the risk estimation of IEC 62061 is used, we can find: CL=Fr + Pr +Av=4+1+5=10 with a possible severity Se=4 we have a SIL 2 and then with the partial merging approach PL=d. Then we have to define, if we have to use a category 2 or 3 system, because a PL=d can be designed in both ways. But when fixed or moveable guards are in operation (for example full enclosure with interlocked guards and guard locking during automatic machining), one can have longer stays according to IEC 62061, because the severity Se=3 is sufficient.

The main difference between the two simplified risk estimation methods is that it is possible also to take into consideration positive field experiences, e.g. that no accidents are known among experts for a certain machine type with a specific SF and so even Pr=1 can be justified. The corresponding discussion is ongoing in the working groups of type C standards.

There are also some technical achievability problems with this SF, which will be considered in detail in the next paragraph.

3 A NOVEL TABLE METHOD FOR CONCISE RISK ESTIMATION OF A SAFETY FUNCTION OF A SRP/CS

From the machine builders point of view, a precise identification and explanation of all the SF's is needed in order to develop a model for both, the risk estimation and the quantification of the reliability (PL or SIL). However, in the current type C standards for machine tools, it is very difficult to find a precise identification and risk estimation for all the SF of a given machine.

Also some technical information of how to reach the required safety level is welcomed by machine designer (for example technical information based on state of the art of current machine on the market or technical achievability of a given PL).

A "technically design oriented" view leads to very detailed explanations of all the SF's, which could take several pages in the type C standard. The first ISO type C standard for machine tools with a small SF description is the ISO 23125:2010/Amd 1:2012 – Safety of turning machines. In this standard the main SF are described in a single page (see point 5.11 b) trying to give the main information on PL_r regardless of the different requirements for similar SF in different zones of the machine. For example in this standard the enabling device SF has always a PL_r=d requirement, this is a very simplified approach.

It is clear that this simple table is not satisfactory at all, not even for a simple analysis: the PL_r of the SF depends on the kind of the control chain which builds the SF and it also depends on the risk reduction of an enabling device. So a realistic risk estimation has to consider all the factors of paragraph 2 of this paper for all the different risk reduction effects of an enabling device. Moreover this has to be done in all the specific applications, e.g. in every mode of operation there needs to be a specific requirement in a type C standard. Moreover an enabling device has always to fulfil at least two different safety functions: a "safe stop function", if it is released and "protection of unexpected movement", if the enabling device is not used.

Trying to summarise the main requirements for a methodology for SF requirement of a general type C standard, at least the following tasks have to be taken into consideration:

- identical SF in different zones of the machine (for example work zone, maintenance zone, tool magazine, tool changer) may lead to different required performance level depending on the individual risk estimations,
- identical SF used in different modes of operation may have different required performance level depending on the individual risk estimations. For example some "other protective measure" as partial guards or safe operator position may affect the risk estimation for the SF (se parameter P),
- detailed explanation of the risk reduction of a safety function and according additional normative requirements.
- remarks for details of SF which are not requirements, but can help the designer in defining a safe machine control system,
- classification with the parameter S, F, P, as explained above and with plausible description of why it was been chosen,
- additional explanations needed as stated in paragraph 1.1 of this paper. All those factors may affect the PL_r from a theoretical formulation to a realistic one as already explained.

It is also very important to give a clear definition of the main quantities to be used, especially when different definitions can be used. For example the definition of *short* and *long presence* differs from one standard to another, so a clear definition of what is a short stay and what is long stay is very important for exposure parameter (see paragraph 1.2.2).

The resulting concise table method comprises two different tables:

- ***SF_table 1***: list of SF with numbering, designation and cross reference to the occurrence probability of hazards that can be found later in the SF_table2 (see table 5 below),
- ***SF_table 2***: table method for the concise risk estimation of every SF, see Table A.2, appendix A for the full table example.

Table 5. Example of SF_table1, numbering, designation and cross reference

No. of SF	Designation	Cross-reference to SF_table 1
SF 01	Safety-related stop function	1.5, 1.9, 4.1, 5.3, 9.1, 10.1,…
SF 02	Manual reset function	
SF 03	Start / restart function	15.4, 20.4
SF 04	Local control function	1.7, 15.5

These two tables will be proposed as normative (mandatory) for the new type C standards of milling machines ISO 16090-1.

Going back to example 1 of paragraph 2.3 the entire concise risk estimation in tabular method is presented in Table A.2 of appendix A.

The selected safety function is very similar to the safety function “prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece” of the standard prEN ISO 16090-1. This safety function was chosen in another paper of Mödden & Günnel for ESREL 2014. The analysis of field data of real milling machines shows that a reliability between PL=a and PL=b is actually being achieved with state of the art design.

3.1 *Typical demand rates of Safety functions*

To perform the necessary $MTTF_d$ calculation and subsequent PL quantification according to ISO 13849-1, it is very important to give to the machine builder the *typical demand rates* of SF. This additional table will be informative, because different demand rates are possible for different machine types.

The demand rates are divided into groups of machine depending from the category defined in the standard. For the milling machine standard, it will define 4 different groups of machines: from the simple group 1 (manual machines) to the group 4 (complex transfer and special purpose machines). See Appendix A for the full table example of demand rates.

4 CONCLUSIONS

In this part 2 of the paper, the problems arising during the real design of SRP/CS using exclusively ISO 13849-1 are addressed. Using an ISO 13849-1/IEC 62061 “partial merging” approach based on the PFH_d, which is a common mathematical basis in both standards, proper risk reduction requirements for the SRP/CS or SF can be found both in terms of PL or SIL.

A novel "table based" methodology for concise risk estimation utilizable in type C standards is presented. The selected safety function is very similar to the safety function “prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece” of the standard ISO 16090-1. This safety function was chosen in another paper of Mödden & Günnel for ESREL 2014. The analysis of field data of real milling machines shows that a reliability between PL=a and PL=b is actually being achieved with state of the art design. This finding connects quite well theory and practice of state of the art milling machines.

Those two contributions are extracted from the work during the ISO/TC 39/SC 10/WG4 meetings (ISO/CD 16090-1 for milling machines).

5 REFERENCES

Decision 2010/15/EU. *Commission Decision of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System ‘RAPEX’ established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC* (the General Product Safety Directive) (notified under document C(2009) 9843)

EN 1996. *EN 954-1 - Safety of machinery — Safety-related parts of control systems - General principles for design.* International Organization for Standardization, Geneva, Switzerland.

IEC/ISO 17305 2014. *Safety functions of control systems*, Joint Working Group 1 (draft 2014)

European Parliament and the Council of European Union, 2006. *Directive2006/42/EC on machinery safety.* International Organization for Standardization, Geneva, Switzerland.

Hedberg, J; Söderberg A. & Tegehall J, 2011. *How to design safe machine control systems – a guideline to EN ISO 13849-1*, SP Technical Research Institute of Sweden, SP REPORT 2011:81, ISBN 978-91-87017-14-8, ISSN 0284-5172.

IEC 2012. *IEC 62061:2005 + A1:2012. Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.* International Organization for Standardization, Geneva, Switzerland.

INAIL 2013. *7° Italian report on surveillance on the market*, Inail, Rome. Can be found and downloaded in Italian: http://www.ispesl.it/informazione/eventi/DTS/20137Rapporto.pdf

ISO 2008. *ISO 13849-1 - Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2010. *ISO 12100 Safety of machinery - General principles for design - Risk assessment and risk reduction.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2012a. *ISO/TR 14121-2 - Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods.* . International Organization for Standardization, Geneva, Switzerland

ISO 2012b. *ISO 23125:2010/Amd 1:2012 - Machine tools - Safety - Turning machines - Amendment 1.* International Organization for Standardization, Geneva, Switzerland

ISO 2014. *ISO/CD 16090-1 - Machine tools safety — Machining centres, Milling machines, Transfer machines — Part 1: Safety requirements.* International Organization for Standardization, Geneva, Switzerland.

B.Günnel et al. 2014. *Proven in use in the machine tool industry for demonstrating the quantitative Functional Safety according to EN ISO 13849 1,* ESREL 2014

APPENDIX, TABLE METHOD FOR RISK ESTIMATION OF A SF OF A SRP/CS

Table A.1. Example of concise risk estimation of a SF, from ISO 16090:2014 (draft)

No.	Subject	No of SF	Explanation of safety function effect, other requirements*	Remarks **	Classification according to ISO 13849-1:2006	Additional explanation see ISO 12100:2010, 5.5.2.3.2	PLr
2	**Tool Spindle and tool Clamping Device**						
2.2	Tool Clamping	SF 16	***Limited speed - maximum processing speed of the tool in MSO 1, MSO 2, MSO 3*** When exceeding the maximum processing speed of the tool (see 3.6.1) a controlled stopping of the tool spindle takes place according to IEC 60204-1:2009, 9.2.2 depending on the technique applied. The possible input of the maximum processing speed (see 3.6.2) shall be provided in the tool parameters of the tool management.	Fault incident may occur unexpectedly in MSO 2 or MSO 3. Incorrect input of tool parameters is most common source of failure. Tool data may be provided manually as well as by a central control level of the machine. The maximum permitted processing speed depends on constructive limitations of the spindle, the clamping means and the size, mass and unbalance of the specific tool. These limitations are given by the manufacturer of the machine.	**S2**: – **F1:** In MSO 2 or MSO 3 short presence*** in hazard zone and limited speed depending on the mode of safe operation, (see 2.3 in this table). In MSO 1 protection by guards. **P2:** –	Rotational speed parameters may be provided by manual data input or Rotational speed parameters may be provided by a central control level of the machine State of the art is PL=a (technical achievability, see separate paper Mödden, Günnel 2014). Accidents in MSO 2 or MSO 3 due to lack of functional safety are not known.	PLr=a

* In this column only normative requirements, no explanations

*** Remarks are not mandatory, here additional information can be provided

** In this case the "short stay" in the hazardous zone is defined as less than 1 hour accumulated during a 8 hours shift, not more than 10 minutes per exposition (see IEC 62061:2005, table A.2).

Table A.2. Examples of typical demand rates of Operations and SF

		Machine group			
No.	Function	Group 1, number of operations	Group , number of operations	Group 3, number of operations	Group 4, number of operations
1	Mean operating time in days per year (d_{op})	300	300	300	300
2	Mean operating time in hours per day (h_{op})	8	8	16	24
3	Emergency STOP	Once per day	4 - times per day	Once per week	Once per week