Where Manufacturing begins

CECIMO input to European Commission's Machinery Directive Working Group meeting of December 7/8 2009

Brussels 25 November 2009

Concerning: Application of ISO 13849 *Safety of machinery – Safety-related parts of control systems* and its modified risk graph being not in accordance with ISO 14121 *Risk assessment*

CECIMO wants to draw the Commission's attention on the difficulties encountered when applying ISO 13849 as it causes **severe problems for manufacturers, customers and type C standardisation committees due to the risk graph being not in accordance with ISO 14121.**

Unless resolved, these difficulties will affect all types of CNC machines with a proven safety record, introducing a significant obstacle for machine tool builders wishing to demonstrate their CE compliance with the new Machinery Directive and harmonised standards. The need to resolve the difficulties is now urgent for machinery designers. Early guidance is therefore needed from Guidelines to the new Machinery Directive on how this may be addressed in terms of standards development and future CE enforcement.

CECIMO Machine Tool Builders request a fundamental and in Europe harmonized resolution to the question of how to carry out the risk assessment and how to record it in the technical documentation as now explicitly required by the new Machinery Directive 2006/42/EC [1] (cf. Appendix I, first, third and fourth bar).

Under Machinery Directive 98/37/EC, it became accepted practise to derive risk assessments and the required safety measures from the type C standards. Delays in the revision of the standards have now created a real problem for manufacturers, as the presumption of conformity of type C standards for a transition period is no longer valid in some cases. Therefore the need to identify alternative means of achieving alignment with the higher level standards is becoming increasingly urgent: ISO 14121 [2] as the standard that superseded EN 1050 and ISO 13849 [3] as the replacement for EN 954. Apparent contradictions between two standards are already leading to serious misunderstandings and uncertainties – not only on the part of manufacturers and their customers, but also among occupational safety experts and type C standardisation committees. Therefore CECIMO requests postponement of the withdrawal of EN 954.

<u>General description of the problem:</u>
The new approach to systematic derivation of requirements relative to the safety of control system components, i.e. the "performance level required, or PL_r" of ISO 13849 is a root cause of the difficulties. Within the context of risk assessment, EN 954 remains fully compatible with risk assessment standard EN 1050, as both standards put the relative probability of the hazardous event into perspective. The requirements are also qualitative in both cases. Various technical solutions are authorised if they can be well justified. A "rift" between the risk standards has now developed: while the 'A' standard ISO 14121 continues to assess risk considering the relative probability of occurrence of a hazardous event, the 'B' standard ISO 13849 assumes a 100% probability that the hazardous event will occur rather than assigning a relative value. This problem is masked in ISO 13849, as Appendix A simply makes the following claim about the new risk graphs: "*The risk assessment procedure is based on ISO 14121 …*" But this claim is false because the risk assessment parameters of ISO 13849 are

Avenue Louise 66 B-1050 Brussels
T +32 2 502 70 90 F +32 2 502 60 82
filip.geerts@cecimo.eu
www.cecimo.eu

limited to severity of harm (S1/S2), exposure of persons to the hazard (F1/F2) and the possibility of avoiding or limiting the harm (P1/P2), while ISO 14121 explicitly incorporates an additional parameter. The additional parameter is defined in ISO 14121 section *7.2.3.3. "Occurrence of hazardous events",* which states:

The occurrence of a hazardous event influences the probability of the occurrence of harm. Factors to be taken into account when estimating the occurrence of a hazardous event are, among others:
a) reliability and other statistical data;
b) accident history;
c) history of damage to health;
d) risk comparison.

Nor is this serious deviation from ISO 14121 remedied by the overall designation of Appendix A of ISO 13849 "*Determination of required performance level (PLr)*" as merely "informative" because the standardising main part of ISO 13849 makes the following statement in the identically titled section *4.3 "Determination of required performance level (PLr)*": *"A required performance level (PLr) must be determined and documented for each safety function selected that is implemented by means of an SRP/CS (cf. Appendix A)."*

By using the modal auxiliary verb "must", this linkage establishes the risk graph as a quasi-normative obligation – especially given that no other standard describes an alternative method by means of which the "PLr" could be derived from the individual risk elements. Previous efforts by standardisation committees to apply ISO 13849 in their attempts to revise type C standards led to endless discussions and they created a schism between occupational safety representatives and machine design experts. Sometimes those involved in the revision work are no longer able to engage in constructive discussion. Meanwhile constructors and type C standardisation committees are becoming utterly perplexed, because although the pure mathematical modelling appears to be internally consistent, it does not correspond to practical reality (type C standards and the machines built in conformance with them). This results from a flagrant undervaluation of tried-and-tested safety engineering design principles specified in the type C standards when the risk parameter "Occurrence of hazardous events" from ISO 14121 is simply ignored.

Detailed description of the problem:

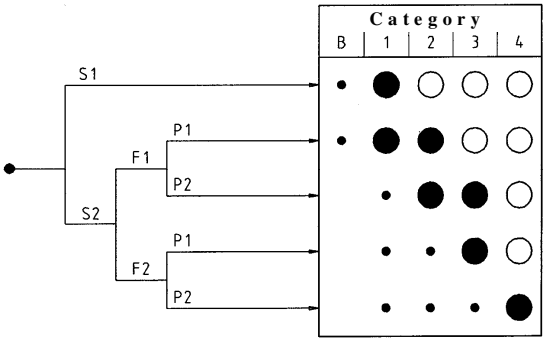

Figure 1: "Old" risk graph of EN 954

Black circles:
Preferred categories

Small dots or empty circles:
Alternative categories that must be justified, e.g. use of tried-and-tested components.

As a possible reason for selecting an alternative category, EN 954 (Appendix B.1) cites the combination of:
a) tried-and-tested hydraulic or electromechanical components (category 1) and

b) electrical and electronic systems (category 3 and 4).
It is precisely this recommendation that has been followed for all type C standards for machine tools (CEN / TC 143). Machine tools in Europe are built according to tried-and-tested safety engineering principles in exactly this way. As an important result, studies show that in Germany accident rates have been reduced by half on machine tools since the first machinery directive went into effect (cf. Figure 2). Surely similar results can also be found in other EU countries.

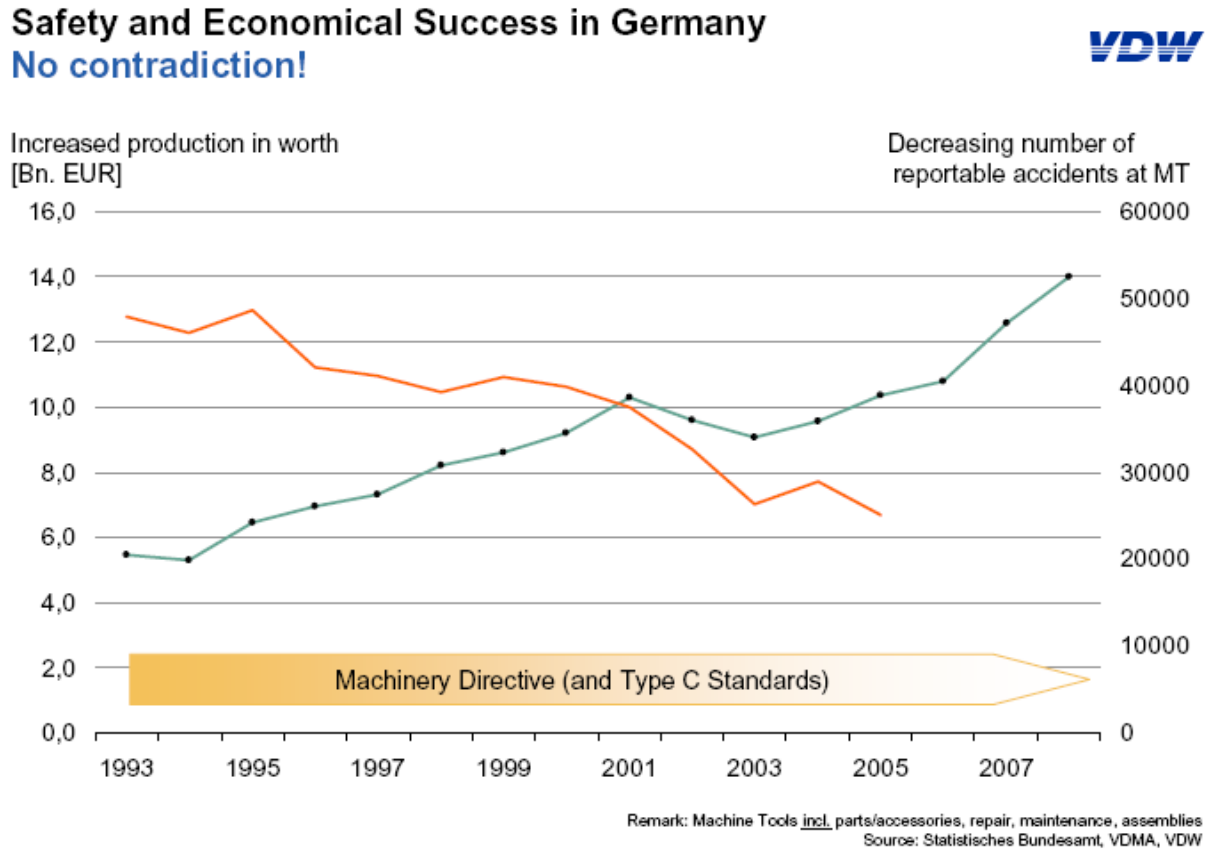

Figure 2: Accident figures on machine tools reduced by half since the first machinery directive

ISO 13849 casts serious doubt on the good result shown in Figure 2. A "rift" has just developed in the risk assessment methodology: EN 954 still states that the "quantitative determination of risk is generally difficult or impossible." By contrast, ISO 13849 adopts a thoroughly quantitative approach. The new risk graph is also now used to extrapolate quantitative results. EN 954 permitted a degree of qualitative latitude, the validity of which has been proven in machine tools. That latitude has now been eliminated from the risk graph. This represents a serious deviation from the new ISO 14121 standard. This can be seen as a triumph for "pure mathematics" as now there is no longer any "grey zone", but rather only "black/white" and "true/false". The connection to complex reality suffers considerably, however, under this theoretical simplification. The ability to make practical adjustments such as

envisioned by the EN 954 risk graph (Appendix B) no longer exists. Moreover, the structure of the risk graphs has been changed and the threshold specification values have also been ratcheted upward, as three new paths have been introduced: S1 and F1/F2 with P1/P2. There were only 5 paths before, whereas now there are 8 paths.

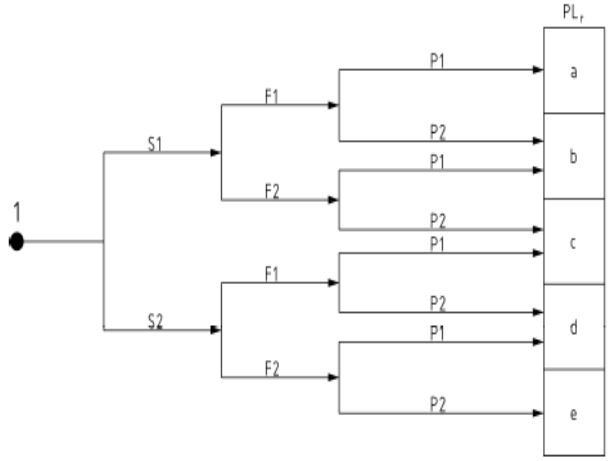

Figure 3:
Intensified risk graph
of ISO 13849.

The PLr is clearly assigned to the parameters S, F and P.

The parameter "Occurrence of hazardous events" from ISO 14121 is ignored, however.

Alternatives allowed by EN 954 have been eliminated.

Difficulties in the revision of standards:

Whereas harmony existed earlier between EN 1050 and EN 954, there is now a lack of harmony between the ISO 14121 and ISO 13849 standards – and this is a fundamental problem in the CEN revision process. With the new turning machines standard ISO 23125 [4], WG 3 of CEN/TC 143 managed to make the adjustments from "categories" to "performance levels" without major objections from the occupational safety side. WG 3 successfully submitted a result that respects the tried-and-tested state of the art in turning machines. Their success was also no doubt attributable to the fact that the occupation safety experts likewise lacked in-depth experience with the application of ISO 13849. But the remaining groups of CEN/TC 143 began discussing basic principles, thereby casting doubt on the determinations of WG 3. The entire issue essentially hinges on "consistent" application of the risk graphs on the one hand, and the retention of tried-and-tested design principles in machine tools on the other. Here the tenet "no significant accident events due to control system failure" plays a major role.

The differences in requirements between ISO 13849 and EN 954 has been recognized in several CECIMO countries. The broader controversies including the link between ISO 14121 and ISO 13849 have been fought out mainly in Germany. Uncertainties are already spreading, however, where other CEN members are involved. It is reasonable to assume that the difficulties will continue to grow if ISO member states are included as planned via the "Vienna Agreement", i.e. the adoption of CEN standards also as ISO standards. Here there is an urgent need for the preparation of timely clarification so that the revision work that has already started in the WGs of CEN / TC 143 can be completed effectively. The standardisation committees depend on the willingness of industry experts in order to develop practice-based standards.

CECIMO machine tool builders have already been intensely involved with sample calculations according to ISO 13849. As example, German industry has a record of 5 years calculation. Companies now want to refer to this standard in order to present safety as an advantage. But this requires some

explanations and adaptations in order to re-establish harmony with ISO 14121.

Summary of all individual issues related to the application of ISO 13849:

In addition to problem no. 1 "Unforgiving risk graph", however, there are also several other issues of no less importance concerning the application of ISO 13849 that still need to be clarified.

Problem no. 2 "Modelling": There is confusion as to how safety functions as described in type C standards – and actually implemented safety functions – should be modelled. A safety function generally comprises a process chain from sensor to actor. Type C standards cover a large number of safety functions, e.g. the secure clamping of tools and workpieces. In applying ISO 13849, however, it soon became apparent to everyone that the safety function designations in type C standards are of no use when trying to apply ISO 13849. The following example from machine tools standard ISO 23125 illustrates the modelling problem. For automatic operation, this standard lists the requirement:

ISO 23125, section 5.11, 7)

"Control system of tool clamping and workpiece clamping; PL_r = b"; for Manual Intervention Mode PL_r = c is required.

In order to be able to meet this requirement with the probabilistic calculation methods of ISO 13849, three separate safety functions must be calculated. This can be seen from the results of a research project entitled "Functional safety in machine tools", which VDW started together with the employers' liability insurance association (BG) in March 2009 following a four-year preliminary investigation ([5] and [6]).

Three safety functions for tool clamping

- SF1, safe limited speed (SLS): When the rotational speed limit n_{max} specified by the manufacturer (depending on the type of operation) is exceeded, the machine executes a controlled shutdown of the tool spindle. PL_r = d.
- SF2, prevention of start-up in case of improperly clamped tool: In the event of improper clamping, the tool spindle is prevented from starting. PL_r = c.
- SF3, tool clamping while the tool spindle is rotating: For spindle speed n > 0, the unit prevents the tool from being released. PL_r = c.

The model is thus unclear and contradicts the intensification of the risk graphs, which no longer allow any latitude for interpretation. Why are the "PLr" specifications so harsh when the model for the calculation is relatively arbitrary? So the use of ISO 13849 methodology to set industry-specific standards for the quantification of safety functions is a challenge, because when the requirements are intensified the conditions that satisfy them must also be clear. The calculation models must be consistent otherwise the calculated performance levels are not comparable. Previous discussions have shown that the responsible employees' liability insurance associations must be consulted during the modelling process. This contradicts the conformity evaluation procedure of the new Machinery Directive 2006/42/EC, which stipulates that the conformity evaluation remains within the exclusive purview of the manufacturer (non-Appendix-IV machinery). Notwithstanding this, there are even differences of opinion among the various employees' liability insurance association offices.

Problem no. 3 "Interaction of individual residual risks": How to handle interactions among multiple residual risks remains unclear. When retooling in the workspace, for example. Although it makes sense to sum up all of the quantitatively determined residual risks, this leads to such bad overall results that they cannot satisfy the risk graph criteria: the possibility of reaching PL_r = d is already excluded when either four individual functions with PL = d are combined or when a sub-function can only contribute PL = c (e.g. a hydraulic valve).
What is the logical consequence? Perhaps the machines should be redesigned? Should the available control system components be made ten times safer? Should a new generation of control system technology be developed? This seems ridiculous, as the available control system technology is already demonstrating a high safety level – as evidenced by the continuous reduction in accident rates (Figure 2). Moreover, control system failures cause only a minor share of the total accidents reflected in those reduced accident rates. The manipulation of safely designed machinery is a far more influential factor [7].

Problem no. 4 "Lack of characteristic data": Some of the required characteristic data are indeed available, e.g. major control system and component suppliers provide the characteristic data for high-quality safety products. But characteristic data are missing for commonly used control system components that do not expressly provide increased reliability – many of which are still used by those same suppliers. And some of the characteristic data are missing for the many mechatronic components used in machine tools controlled by central control systems: e.g. mechanical clamping units (turning chucks, collet chucks) and brakes, fluid power systems (hydraulics and pneumatics) and advanced electrical clamping concepts. Nor can these characteristic data be gathered in the short time remaining. Procuring test specifications for hydraulic valves is a tedious undertaking, for example, even for medium-sized assemblies.
The use of estimations for the preliminary evaluation of control system structures is a major source of insecurity. Customers become irritated, for example, when the final results are not completely released until later, possibly necessitating technical revision. The effect is similar when delayed final results force changes to operation (access modes) and maintenance (replacement intervals). Moreover, legal problems can arise if an estimate has been made for components used at a specific point in time but actual values have been published thereafter.

Overall problem:
Taken together, these four problems lead to an undervaluation of commonly accepted, tried-and-tested design principles (i.e. accident rates reduced by half, minor role of control system failures). This casts doubt on both the successful type C standards and the machines built according to them. Manufacturers can expect legal problems as well as problems with their customers.

Proposed solutions:
The problems presented here all involve the risk assessment that the new Machinery Directive emphasizes. As a result of that emphasis, the risk assessment becomes very important for the manufacturer's technical documentation. Type C standardisation committees are affected to the same degree. The new guideline of the new Machinery Directive 2006/42/EC already envisions two sections for explaining the risk assessment process:

Guideline, 2006/42/EC, §163 Risk assessment

Guideline, 2006/42/EC, §164 Risk assessment and harmonised standards

So far those sections refer exclusively to ISO 14121. There is still an opportunity to remedy this

deficiency prior to the publication of the new guideline by also mentioning ISO 13849. The link between ISO 14121 and ISO 13849 must also be presented unambiguously. The guideline must show how these standards harmonise with one another. To that end, the guideline must expressly mention the risk parameter "*Occurrence of hazardous events*" from ISO 14121 and highlight its significance for design principles whose safety engineering aspects have been tried and tested. At the same time, the guideline must rectify the "quasi-normative" and "dogmatic" character of the risk graphs from ISO 13849, which are ostensibly only "informative".

Although an extension of the presumption of conformity of EN 954 will not solve the problems described here, it is still advisable to leave EN 954 in place until all of the issues relative to its replacement by ISO 13849 have been resolved. There actually is a tried-and-tested state of the art for machine tools: the type C standards with reference to EN 954. This would serve to "bridge" the presumption of conformity of type C standards until the all questions have been clarified concerning the type C standards for machine tools (which are currently being revised) and new industry-specific standards have been established.

Another crucial point is that the risk graphs of ISO 13849 have to be expanded within the meaning of ISO 14121 and an informative appendix has to explain the practical application of ISO 13849 for complex, real cases, e.g. retooling in the workspace. The relatively simple mathematical examples in the appendix of ISO 13849 and in BGIA Report 02/2008 [8] do not capture the complexity of real machines with highly cascaded mechatronic functionalities.

What must be avoided:
Given the sustained reduction in accident rates on machine tools, the undervaluation of generally accepted design principles as a result of new, probabilistic control system safety specifications cannot go unchallenged. The consequences would be obvious: the machines would have to become even more sophisticated and/or use even more reliable control system components. The additional costs associated with this would be disproportionate to the benefits – especially in view of the fact that the number of accidents caused by control system failures is anything but alarming when the machine tools are built according to type C standards. Moreover, this idea is hypothetical and thus not feasible as there are no "more reliable control system components" available on the market and "generally accepted design principles" for machine tools have matured over the course of decades and cannot be replaced by other principles overnight. The tool and workpiece clamping system shown in Figure 4 is a good example.

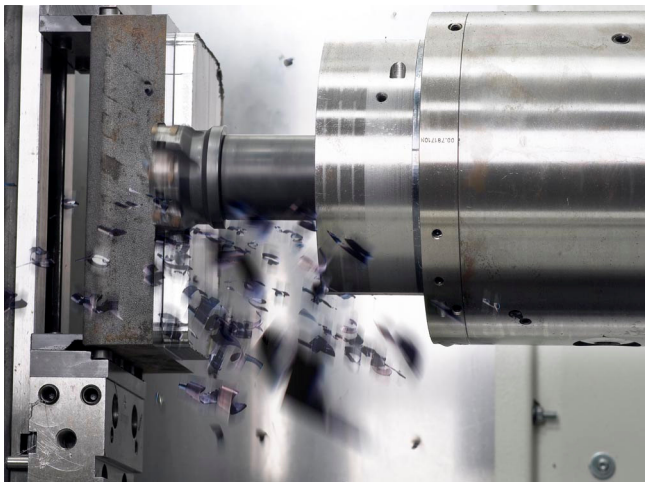

Figure 4: Design principles, the safety of which has been tried and tested in machine tools:

Left: Safe workpiece clamping

Right: Rotating milling tool, tool safely clamped in the drive spindle

No known accidents caused by control system failure in the past 24 years!

Source: VDW, Gebrüder Heller, Nürtingen

Literature:

/1/ Machinery Directive 2006/42/EC
/2/ Type A standard ISO 14121, "Risk assessment", predecessor EN 1050
/3/ Type B standard EN ISO 13849-1:2006, "Safety of machinery – Safety-related parts of control system safets", predecessor EN 954 ;
/4/ Type C standard ISO/FDIS 23125 "Safety of machinery – Turning machines"
/5/ VDW, "Functional safety in machine tools", *Branchenreport* (Industry report), October 2009
/6/ Sample calculation for safe workpiece clamping in turning machines, *FA Infoblatt* (Technical Committee Leaflet)
/7/ BGIA Report "Manipulation in machine tools"
/8/ BGIA Report 02/2008