Technical Article

www.boschrexroth-us.com

Reliability is Required: New Safety Standard for Machine Control Systems

The safety of machine control systems is now evaluated according to reliability. In this respect, the new European Machinery Directive 2006/42/EC refers to a new standard – EN ISO 13849. This replaces the traditional standard for machine safety EN 954, bringing a whole new perspective on control system design.

The European Machinery Directive 2006/42/EC came into effect on December 29, 2009. As a result of its introduction, all manufacturers worldwide that market their machines in the European Economic Area are obliged to fulfill additional safety requirements. This directive is also accompanied and supported by an array of harmonized standards (Fig. 1). As well as the directive itself, machine manufacturers have to align themselves according to machine-specific product standards (Type-C standards), which in turn refer to the requirements of basis (Type-A standards) and generic safety standards (Type-B standards).

Machine safety begins with risk assessment

In accordance with the European Machinery Directive (EMD), a risk assessment must be carried out on every machine based on EN ISO 14121. If relevant risks are detected, measures must be taken to minimize these risks. For risk reduction the following sequence must be applied:

1. Avoidance by intrinsic design

2. Avoidance by safeguards

3. Avoidance by information for use

If a measure depends on a control system, then it performs a safety function. To ensure compliance with safety requirements by design of control systems, the EMD refers, in this case, to the EN ISO 13849. This standard deals with the design and integration of Safety-Related Parts of Control Systems (SRP/CS) independently from the technology used — as opposed to IEC 62061 (which is applicable for electro-electronic control systems). If a machine manufacturer does not use this harmonized standard, and damage occurs, it must be able to prove that its machine control systems at least comply with the requirements of the EMD.

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

The EN ISO 13849 is already valid and replaces the EN 954. Although the EMD still allows the application of the EN 954 in some special cases until December 31, 2011 (e.g. for turn key systems without machine specific standards), from the point of view of product liability, it is recommended to apply the EN ISO 13849. Furthermore, in cases where a Type-C standard already refers to EN ISO 13849, the new standard has to be applied.

The new standard introduces a new procedure for designing safety-relevant control systems. The statistical approaches promote a new mentality among the design engineers: the interoperability of different components from a control system now has to be considered from various safety engineering points of view. On one hand, for machines with established safety technologies, quantitative evidence will be generated with this new approach, demonstrating the safety levels reached. On the other hand, for machines with safety weak points, it provides clear recommendations showing how to improve these weaknesses. Therefore, this standard provides guidelines for systematically improving the machine safety. These also help to optimize the machine availability, by reducing its lifecycle costs.

EN ISO 13849 provides new perspective

The safety requirements for every identified safety function are described in the EN ISO 13849 in the form of the Required Performance Levels (PL_r). If these are not already specified in a machine-specific standard, the designer uses the risk graph of the EN ISO 13849. Based on questions about the impact, frequency, duration and also the possibility to prevent risks, the PL_r can be assessed on a scale of “a” to “e” — with “a” representing low risk and “e” representing high risk. The Performance Level (PL) is the characteristic used for safety-related design and the evaluation of control systems in accordance with the EN ISO 13849. It describes the contribution of the control system for risk reduction and it is defined in terms of the average probability of a dangerous failure per hour (PFH_d). This means that the safety of a control system is now evaluated according to its probability of failure (or reliability).

For the design of control systems, the EN ISO 13849 incorporated the system architecture from standard EN 954, which is now directly related to the PL (Fig. 2). The control categories differ according to whether they are single-channel or dual-channel, whether they have been designed with or without monitoring, whether they are resistant to systematic errors, and also in terms of their reliability values. Basically, the EN ISO 13849 offers the design engineers a greater freedom to find out the most cost-effective solution for achieving the PL_r. In accordance with the selected category, a circuit is designed and modeled within a safety block diagram. This safety model determines the way in which the individual components are considered in the PL calculation. This modeling means a whole new point of view with respectively

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

work packages, particularly for designers of complex systems with fluid power technology.

In addition to the control category, the component reliability plays an important role in the PL calculation. In order to apply a component in a safety function, the EN ISO 13849 requests a pre-condition that specific safety design principles are observed. For example, in accordance to the de-energization principle, the components must assume a safe state by a shutting off the power supply and maintaining this position by all the approved operating conditions (vibration, temperature, etc.; see product data sheet). If a product does not fulfill these safety principles, it is not suitable for safety functions based on EN ISO 13849. Depending on the technology, different reliability characteristics must be provided by the supplier, such as Mean Time to Dangerous Failure ($MTTF_d$) for hydraulic components, the B_{10} value for pneumatic components or PL (PFH_d) for electronic subsystems. These are statistically expected values, which depend heavily on the determination method and the operating conditions. For this case, there are generally three main methods for determining the required reliability characteristics:

Lifetime calculations (e.g. according to the Parts-Count or Parts-Stress methods):

These approaches are used to calculate the reliability of components, particularly electronic components, based on the lifetime characteristics (MTTF) of each part (e.g. resistors, capacitors etc.). Environmental conditions such as temperature play an important role here. The EN ISO 13849 recommends an $MTTF_d$ of 150 years for hydraulic components when the safety principles and the requirements of the EN 982 have been fulfilled. However, in the case of products which integrate more than one hydraulic component, the $MTTF_d$ has to be calculated using the Parts-Count method according to the EN ISO 13849. For example, for a combination of a pilot and a main valve, one would get a $MTTF_d$ of 75 years instead of 150 years.

Lifetime tests

B_{10} reliability characteristics (e.g. of pneumatic components), can be determined by means of lifetime tests. B_{10} is an expected value of the number of cycles until 10% of the components have exceeded specified limits (response time, leakage, switching pressure, etc.) under defined conditions. This statistical evidence relies heavily on the test conditions and the number of samples.

Lifetime from field data

If a sufficiently large database about the application of products in the field exists, the MTTF can be obtained from this. This lifetime characteristic represents an average of

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

over-all applications in the field. To ensure significant statistical evidence, it is very important to collect and evaluate the data in a careful manner.

The EN ISO 13849 takes only dangerous failure into account (i.e. failures which are dangerous for the machine safety). As the percentage of dangerous failure often cannot be identified directly, this standard assumes that 50% of all failures are dangerous: $MTTF_d = 2 \times MTTF$ or $B_{10d} = 2 \times B_{10}$. The $MTTF_d$ for the safety function of a machine is calculated using the Parts-Count procedure (Fig. 3). The German Association of Machinery and Plant Construction (VDMA), recommends to apply the software Sistema from the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA, which participated in the elaboration of this standard).

The diagnostics coverage (DC) is another factor affecting the PL. This specifies the proportion of dangerous failures that can be detected. In order to identify this diagnostic characteristic for a component, the user needs to know all types of dangerous failures, as well as the probability of their occurrence and their detection. This calculation is performed for special products. For standard components, the EN ISO 13849 provides a list of measures with typical DC values, e.g. DC = 99% for valves with direct position monitoring. However, it is very important that the position signal is processed appropriately in a higher-level control system. Finally, it is extremely difficult to specify a DC for components, as their measures rely on the complete processing of the diagnostic signals.

Performance level for more safety

Common Cause Failures (CCFs) are also taken into account in the EN ISO 13849. These denote failures on redundant units as a result of common events, such as high temperature. For this reason, specific requirements surrounding the resistance against CCFs must be observed for dual-channel control systems. The measures against CCFs (such as protection against overpressure/overvoltage) are evaluated using a table with different points for each applied measure, in which at least 65 out of 100 points must be achieved.

Finally, the EN ISO 13849 requires that measures for the control and avoidance of systematic failures are taken into consideration. Any software that has been created specifically must also satisfy the corresponding requirements. It must also be ensured that the basic and well-tried safety principles are also fulfilled in the design of the whole control system. Once the machine design is finished, the EN ISO 13849-2 prescribes a validation procedure to check that the planned safety functions have correctly been implemented and documented. This process includes examining the error lists: Can the assumptions regarding fault exclusions be confirmed? The

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

assumed categories must also be confirmed: Does the existing circuit actually represent the category for which the calculations were performed?

Guideline

Bosch Rexroth supports its customers, for example with its guideline “10 Steps to Performance Level”. This is available on the company’s website at www.boschrexroth.com/SAFETY**.**

Standards

EN ISO 13849 “Safety of machinery, Safety-related parts of control systems”, Part 1: “General principles for design”, Part 2 “Validation”

EN ISO 14121-1 “Safety of machinery — Risk assessment — Part 1: Principles”

EN 62061 “Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems” (IEC 62061)

EN 982 “Safety of machinery — Safety requirements for fluid power systems and their components — Hydraulics” (replaced by EN ISO 4413)

EN ISO 12100-1 “Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology”

Authors

Dr. Alexandre Orth (born 1978) coordinates the topic of “Reliability & Maintainability” in the Quality Methods department at Bosch Rexroth AG, Wurzburg, Germany. He is a member of several working groups on functional safety and reliability at the VDMA (The German Association of Machinery and Plant Construction) and ZVEI (The German Electrical and Electronics Industry).

Dr. Jürgen Barg (born 1951) is head of the electro-hydraulic drives sector in the Application Center at Bosch Rexroth AG, Lohr, Germany. He plays an active role on various standards committees and VDMA working groups about the European Machinery Directive.

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

Technical Article

www.boschrexroth-us.com

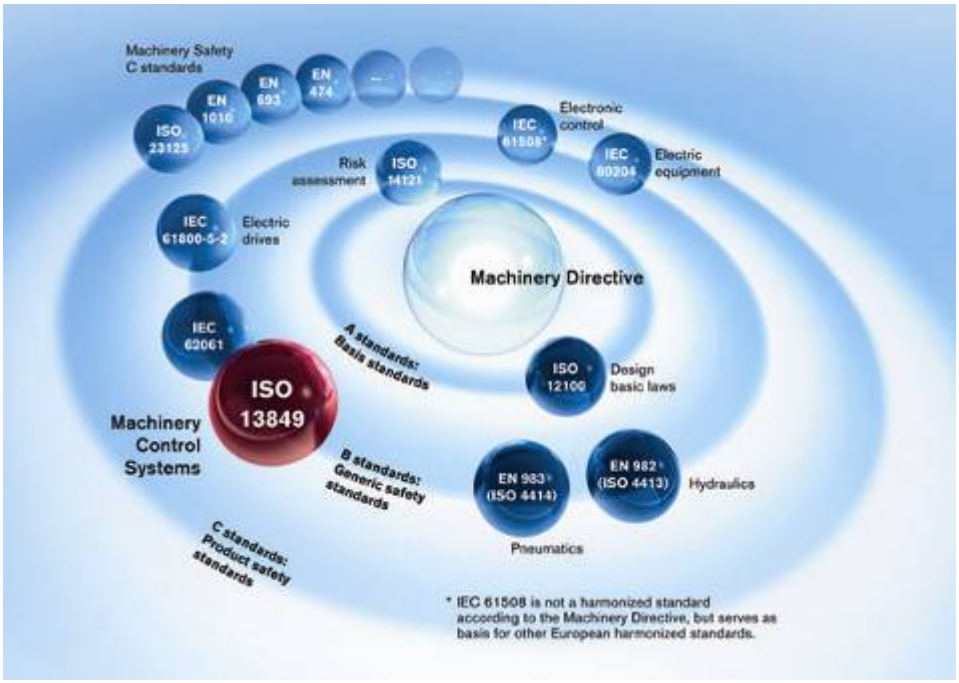

Fig. 1: Relationship between the European Machinery Directive and the harmonized standards

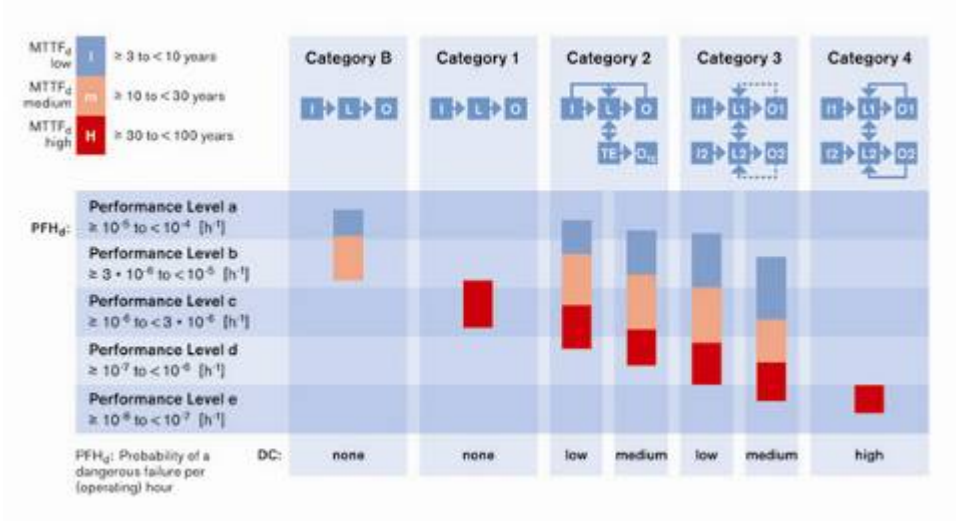

Fig.2. Relationship between the categories, diagnostics coverage level, $MTTF_d$ and PL in accordance with EN ISO 13849-1

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

Technical Article

www.boschrexroth-us.com

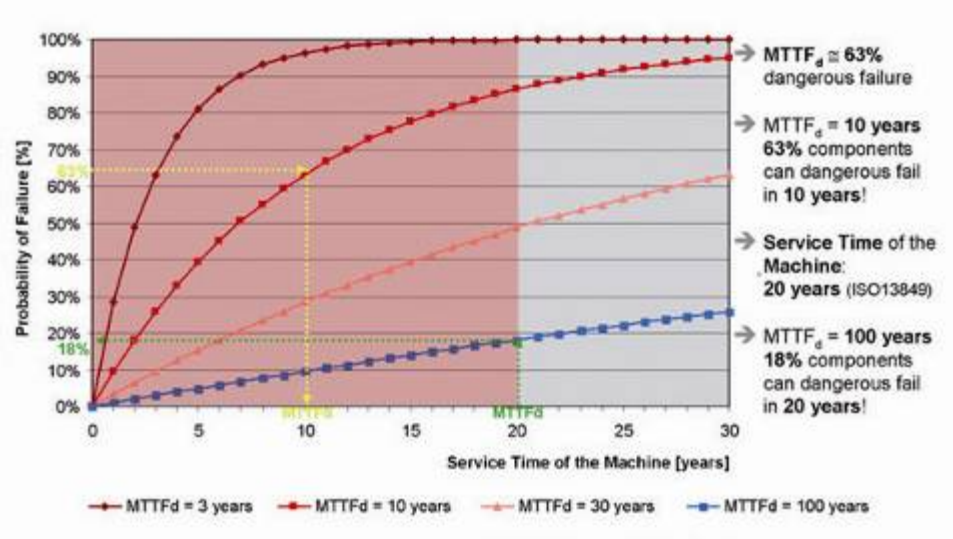

Fig. 3: The significance of $MTTF_d$ for the availability of a safety function. Example: $MTTF_d$ = 10 years (yellow) means that approx. 63% of safety function components may dangerously fail within 10 years. With $MTTF_d$ = 100 years (blue), 18% of components may dangerously fail during the machine's service time required by the EN ISO 13849 of 20 years.

Glossary:

PL (Performance Level): Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

PL_r: Required Performance Level

SIL (Safety Integrity Level): Safety Integrity Level (appropriated only for electronic control systems, see PL and IEC 62061)

MTTF (Mean Time To Failure): Statistic expected value of the mean time to failure

$MTTF_d$ (Mean Time To dangerous Failure): Statistic expected value of the mean time to dangerous failure

FIT (Failure In Time): Unit used to measure the failure rate of electronic components (1 FIT=$1x10^{-9}$/h)

PFH_d (Probability of Dangerous Failure per Hour): Probability of dangerous failure per hour (reference value for PL and SIL)

B_{10}: Statistic expected value of the number of cycles until 10% of the components have exceeded specified limits (response time, leakage, switching pressure, ...) under defined conditions

B_{10d}: Expected number of cycles until 10% of the components fail dangerously

T_{10d}: Expected value of the mean time until 10% of the components fail dangerously (maximal service time of a component).

T_M (Mission Time): Service life

DC: Diagnostic Coverage

CCF: Common Cause Failure

SRP/CS: Safety-Related Parts of a Control System

Dangerous failure: Failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

Technical Article

www.boschrexroth-us.com

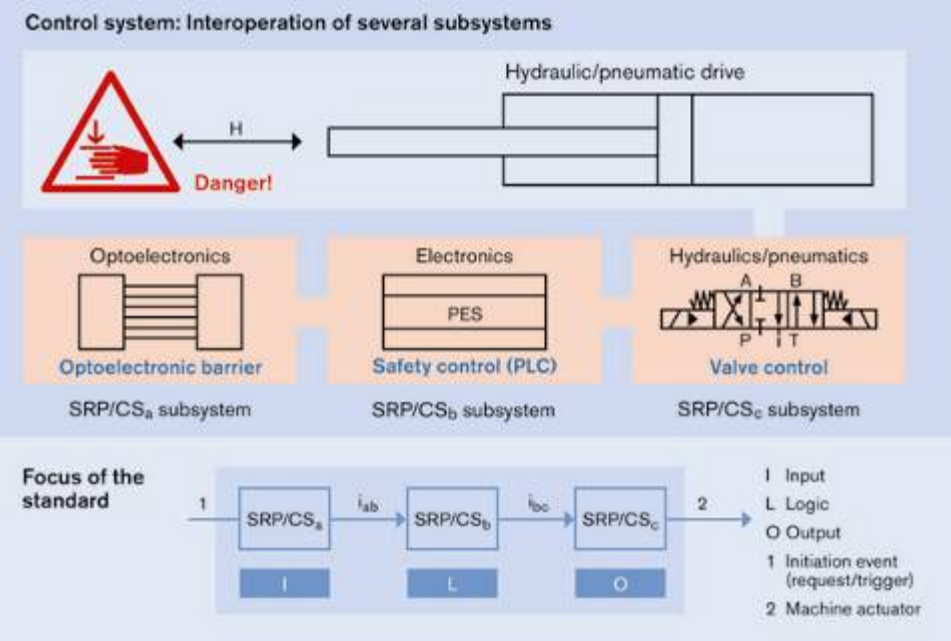

Fig. 5: Definition of Safety-Related Parts of a Control System (SRP/CS)

Bosch Rexroth AG is one of the world's leading specialists in the field of drive and control technologies. Under the brand name of Rexroth the company supplies more than 500,000 customers with tailored solutions for driving, controlling and moving. Bosch Rexroth is a partner for industrial applications and factory automation, mobile applications and renewable energy.
As The Drive & Control Company, Bosch Rexroth develops, produces and sells components and systems in more than 80 countries. In 2009 Bosch Rexroth, part of the Bosch Group, achieved sales of around $5.7 billion (4.1 billion Euro) with 34,200 employees.

For more information please visit: www.boschrexroth-us.com

###

(Magazine Note) Please Send Any Reader Inquiries To:

Alexandre Orth
Tel.: +49 (0)9352 18-1697
alexandre.orth@boschrexroth.de
www.boschrexroth.com/SAFETY

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com

Technical Article

www.boschrexroth-us.com

Contact for Journalists:
Bosch Rexroth Corporation
Negin Neghabat
5150 Prairie Stone Parkway
Hoffman Estates, IL 60192
Telephone (847) 645-3600
Fax (847) 645-3728
negin.neghabat@boschrexroth-us.com

Godfrey Public Relations
Todd Walter
40 North Christian Street
Lancaster, PA 17602
Telephone (717) 393-3831 ext. 133
Fax (717) 393-1403
twalter@godfrey.com