

Safety of machinery

Step up to the new standards



EN 954-1

IEC 61508

EN 13849-1

EN ISO

EN 62061

Lenze

Standards increase | ready to face the future?

In the area of functional safety, the world of standards remains one full of change – in December 2011, EN ISO 13849-1 will completely replace EN 954-1. For machine and plant constructors this will mean changes affecting the certification of their products: Probability calculations will now be taken into account when defining safety.

The relevant safety-related parameters of individual components are an important factor when defining the overall performance levels of a plant.

Henceforth, mechanical engineers will be bound primarily by the requirements of three standards when designing and developing safe machines. As the comprehensive standard, the Machinery Directive (MD) 2006/42/EC defines the requirements to be met if a machine is to be put to market in the European Economic Area. Harmonised with the MD are EN ISO 13849-1 and EN 62061, both of which address issues of functional safety. The new MD 2006/42/EC will become legally valid from the start of 2010.



International
Organisation for
Standardization

ISO 13849-1



International
Electrotechnical
Commission

IEC 62061



European Committee
for Standardization

EN 13849-1



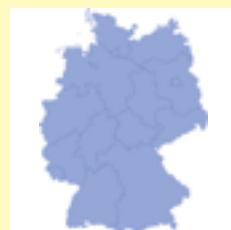
European Committee
for Electrotechnical
Standardization

EN 62061



Deutsches Institut
für Normierung

DIN EN 13849-1



Verband der Elektro-
technik Elektronik und
Informationstechnik

DIN EN 62061



Lenze responded at an early stage to this transition. One of the steps taken by the company was to implement the changes in the requirements of standards at product level, in order to provide mechanical engineers with the best possible support. Following is an overview of the certification of functional safety in line with the new standards.

Overview | a time of change for the world of standards

Machinery Directive (MD) 2006/42/EC to replace MD 98/37/EC

The new MD 2006/42/EC replaces the previously valid MD 98/37/EC. The new standard is universally applicable for machinery, replaceable equipment, safety components, load handling devices, chains, ropes and lifting straps, detachable cardan shafts, incomplete machines (partial machines) and service elevators carrying people and/or goods. Once the building of a machine is complete, mechanical engineers confirm that requirements have been taken into account themselves by affixing the CE mark to the machine. Once a machine bears the CE mark, it can be put to market in the European Economic Area.

EN ISO 13849-1 and EN 62061 – Application ranges

Another very important standard in the field of machine and systems engineering is EN 62061. This standard addresses the functional safety of safety-related electrical, electronic and programmable electronic control systems. How will these be affected by the new standard EN ISO 13849-1? What similarities do the application ranges of the two standards share and what makes them different?

As indicated above, the scope of EN 62061 is limited to electrical, electronic and programmable electronic control systems. As such, the standard cannot be applied to hydraulic, pneumatic or electromechanical safety-related control elements, for example. Conversely, EN ISO 13849-1 can be applied to the safety-related parts of

control systems and all types of machine – regardless of the technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.).

The application ranges of EN 62061 and EN ISO 13849-1, which will serve as a direct successor to EN 954-1, overlap considerably. This common ground has to do with the origins of both standards:

EN 62061 was derived from IEC 61508 for engineering. It was intended to close the gap left by EN 954-1, which did **not** take into account the specific requirements to be met by programmable electronic (in other words, microprocessor-based) systems with safety functions. As the standards committees set about developing IEC 61508, its original purpose was extended to include the application range of discrete electrics and electronics. Consequently, it developed into a comprehensive standard addressing virtually all types of safety-related issue. Standards described as “sector-specific” were then derived from this umbrella standard for individual sectors. EN 62061 for engineering is one such sector standard.

EN 62061 and EN ISO 13849-1 – Similarities

Regardless of whether a mechanical engineer chooses to work in compliance with EN ISO 13849-1 or EN 62061 – the deterministic approach of EN 954-1, with its consideration of structures, no longer suffices. Furthermore, probability calculations now need to be made in order to verify the reliability of the designs of the safety-related parts of machine controls.

The two standards are harmonised under the Machinery Directive. As such, they have the legal advantage known as “probability of conformity” on their side. This means that the party putting a machine to market – in this case the mechanical engineer – is not under obligation to prove that the product concerned conforms to the directive requirements set out in the standards. If the mechanical engineer does not apply harmonised standards, what is known as “shifting of the burden of proof” comes into effect – in the event of an accident, this can make a very considerable difference.



Safety-related parameters of EN ISO 13849-1

- ▶ Category (structural requirement)
- ▶ PL: Performance level
- ▶ $MTTF_d$: Mean time to failure dangerous
- ▶ $B10_d$: Number of cycles at which 10% of a random tested sample of components suffering from wear failed as dangerous
- ▶ DC: Diagnostic coverage
- ▶ CCF: Common cause failure
- ▶ TM: Mission time

Safety-related parameters of IEC EN 62061

- ▶ SILCL: SIL claim limit
- ▶ PFHD: Probability of dangerous failure per hour
- ▶ T1: Life time
- ▶ λ : Failure rate ; for elements suffering from wear: B10 value
- ▶ SFF: Safe failure fraction
- ▶ T2: Diagnostic test interval
- ▶ β : Susceptibility to common cause failure
- ▶ DC: Diagnostic coverage

The safe machine | overview of the route to be followed

Step 1

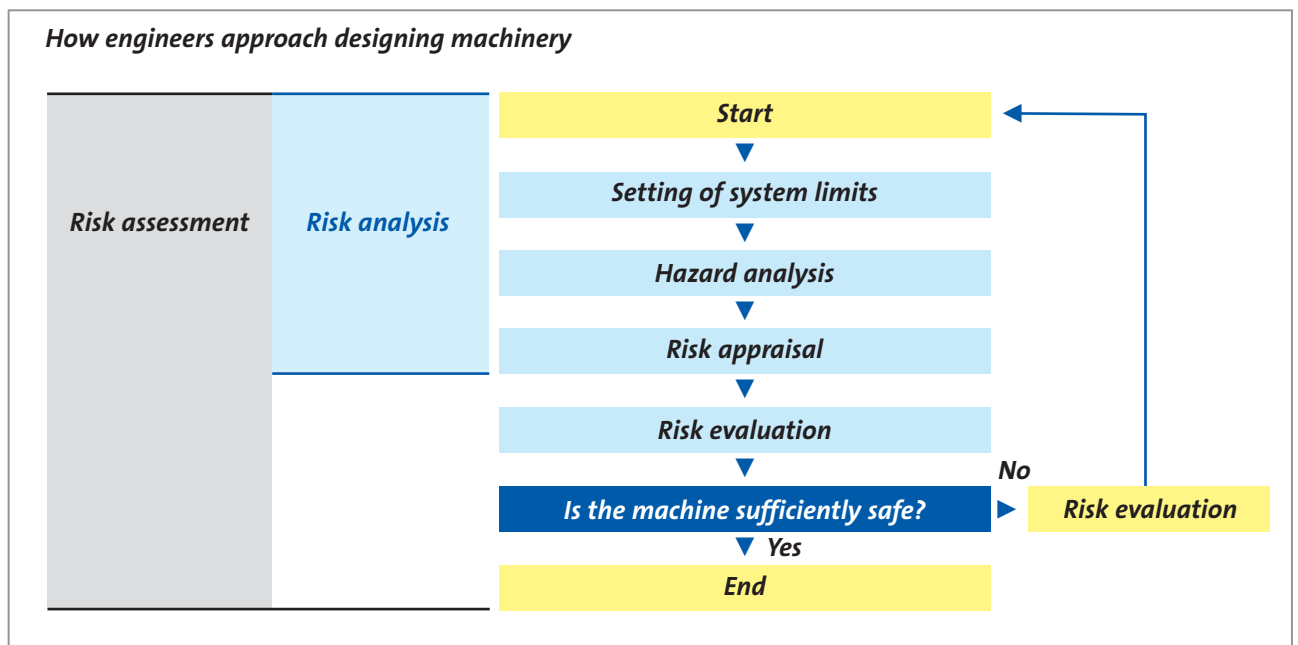
Risk assessment & evaluation in accordance with EN 1050/EN ISO 14121

When engineering a machine, the first question to be asked is what risks does it pose. It is fundamentally assumed that a hazard prevailing on a machine will cause damage sooner or later if protective measures are not taken.

All hazards which could be posed by a machine must therefore be identified (risk and hazard analysis) at a very early stage of the design and development of a machine. The results of this analysis are then used to assess the risk posed by each

hazard. Risk evaluation then follows, and the findings of this stage of the process are then used to make decisions about the need for risk minimisation.

To sum up in simple terms, the crux of the matter is to recognise dangers in advance, assess and evaluate the risk and reduce it to an acceptable minimum if necessary in order that – ultimately – a “safe machine” can be built.



Formerly EN 1050 and now EN ISO 14121: Hazard analysis, risk appraisal and risk evaluation

- ▶ Definition of the machine's limits and application as directed
- ▶ Identification of hazards and their associated hazardous situations
- ▶ Assessment of the risk posed by each hazard and hazardous situation identified
- ▶ Evaluation of the risk and making of decisions about the need for risk minimisation

Step 2

Minimising risk

If these initial steps identify a need for risk minimisation, the standards set out a hierarchy of measures for reducing the hazards to an acceptable level:

1. Design measure
2. Protective devices
3. User information

Safety in a machine must therefore be an integral part of the overall process as early as the design engineering phase. Designs and tests cannot just be “shoehorned in” when a problem affecting machine safety is identified.

The fact is that the safety of a machine has to be considered at all stages of its service life – from assembly taking in commissioning, through to the production period including production with operation and maintenance, and beyond to waste disposal.

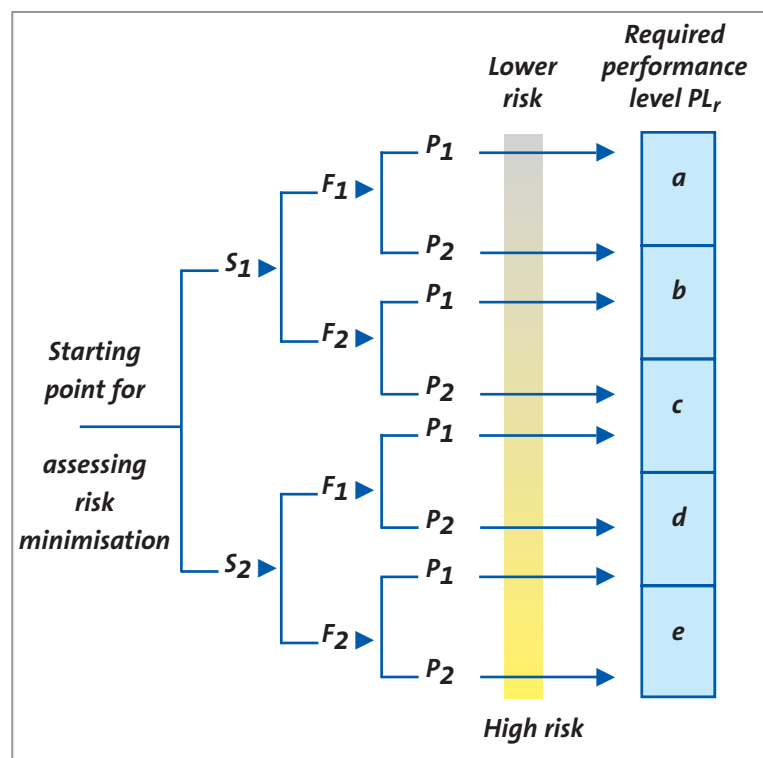
Like its predecessor standard, EN ISO 13849-1 uses a risk graph. However, unlike EN 954-1, the graph does not result in a category but a “PL_r” (performance level required). This is the gauge used to measure the actual performance level (PL) achieved following implementation of the defined safety functions with the various safety components (sensor – logic – actuator): The PL has to be greater than or equal to the original performance level required (PL_r).

PL refers to the ability of a safety-related part of a control system (SRP/CS) to perform a safety function designed to achieve the expected reduction in risk. Both quantitative and qualitative aspects are taken into account.

From the starting point, the following risk parameters have to be evaluated for each hazard identified in the risk and hazard analysis:

- ▶ S – Severity of injury (S1: slight, reversible/S2: serious, irreversible to fatal)
- ▶ F – Frequency (F1: seldom to infrequent/F2: frequent to continuous)
- ▶ P – Ways of avoiding the hazard or limiting the damage (P1: possible under certain conditions/P2: virtually impossible)

The evaluation ultimately results in the performance level required PL_r. If design measures can be taken to minimise the risk, the risk graph process (iterative method) is repeated. The aim is to achieve a lower PL_r for this previously more serious hazard – if this can be achieved, the risk will have been minimised successfully by means of a design measure.

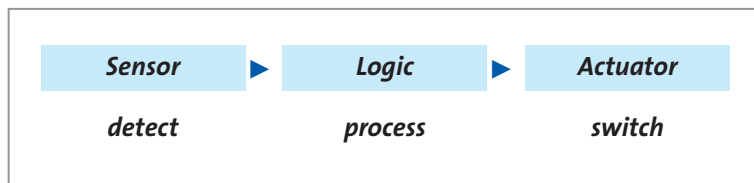


Risk graph from EN ISO 13849-1 for determining the performance level required PL_r

Step 3 Implementation in control systems

In many cases design measures are not sufficient and protective devices are needed in order to achieve risk minimisation. In this context, safety functions executed by SRP/CS (safety-related parts of control systems) are defined. SRP/CS include the entire safety chain with sensor (detect), logic (process) and actuator (switch).

Safety functions are defined on the basis of both the application and the hazard. They are often specified in a Type C standard (in other words, a product standard) which sets out precise specifications for special machines. In the absence of a C standard, the safety functions are defined by the designer of the machine. Typical safety functions are described in more detail in EN ISO 13849-1 Section 5.1 “Specification of safety functions”.



SRP/CS with sensor, logic, actuator

The safety functions for adjustable speed electrical power drive systems are not described in EN ISO 13849-1 but in the separate standard EN 61800-5-2.

Abbreviation	English designation	Function
STO	Safe torque off	No power is being fed to the motor, which can generate a rotation; stop category 0 to DIN EN 60204-1.
SS1	Safe stop 1	Motor decelerates; monitoring of deceleration ramp and STO following standstill or STO at the end of a deceleration time; stop category 1 to DIN EN 60204-1.
SS2	Safe stop 2	Motor decelerates; monitoring of deceleration ramp and SOS following standstill or SOS at the end of a deceleration time; stop category 2 to DIN EN 60204-1.
SOS	Safe operating stop	Motor stops and resists external forces.
SLA	Safely-limited acceleration	Prevents an acceleration value being exceeded.
SLS	Safely-limited speed	Prevents a speed value being exceeded.
SLT	Safely-limited torque	Prevents a torque/force limit value being exceeded.
SLP	Safely-limited position	Prevents a position limit value being exceeded.
SLI	Safely-limited increment	The motor moves at a specific increment and then stops.
SDI	Safe direction	Prevents the motor from moving in any direction other than that intended.
SMT	Safe motor temperature	Prevents a motor temperature value being exceeded.
SBC	Safe brake control	Safe control of an external brake.
SCA	Safe cam	A safe output signal is generated whilst the motor position is located in a specified range.
SSM	Safe speed monitor	A safe output signal is generated whilst the motor speed is lower than a specified value.
SAR	Safe acceleration range	The acceleration of the motor is kept within specified limit values.

Safety functions for adjustable speed electrical power drive systems to EN 61800-5-2

Specification of safety functions

The standard requires that a specification of functional requirements is drafted containing details about each safety function to be executed.

To this end, necessary interfaces with other control functions need to be defined and the required error responses specified. The performance level required PL_r also has to be defined as described above and documented in writing.

Step 4



Step 5

Determining the achieved performance level PL

The PL must be estimated for each selected SRP/CS executing a safety function. The following parameters are significant when determining the PL for an SRP/CS

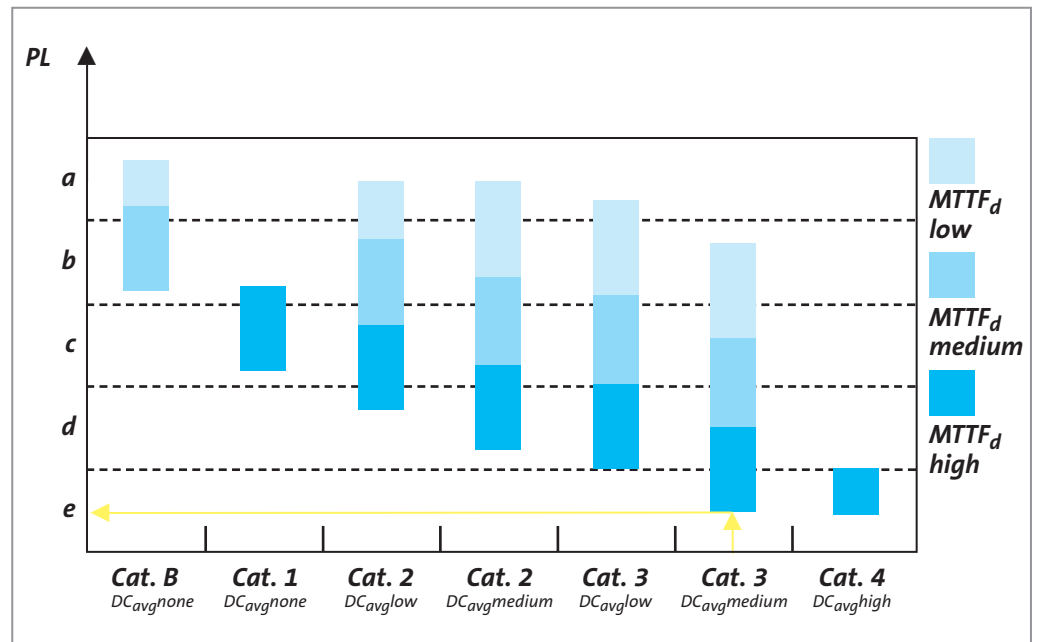
- ▶ The $MTTF_d$ value (mean time to failure dangerous) of individual components
- ▶ The DC (diagnostic coverage)
- ▶ The CCF (common cause failure)
- ▶ The structure (category)
- ▶ The behaviour of the safety function under error condition(s)
- ▶ Safety-related software
- ▶ Systematic errors
- ▶ The ability to execute a safety function under foreseeable ambient conditions

Standard EN ISO 13849-1 uses a graph to describe a simple way of estimating the PL. The graph illustrates the relationship between the familiar category from EN 954-1 and the new relevant safety-related parameters which are relevant.

- ▶ Category (Cat. B,1,2,3,4)
- ▶ DC_{avg} (none, low, medium, high)
- ▶ $MTTF_d$ (bars in the diagram: low, medium, high)

How can a safety component classified as Cat. 3 in accordance with EN 954-1 achieve the highest performance level PL e in accordance with the new standard EN ISO 13849-1?

Example: Cat. 3, a DC_{avg} of medium and an $MTTF_d$ value of high can achieve the highest performance level PL e.



Relationship between category, DC_{avg} , $MTTF_d$ of each channel and PL

The example shows that here too the standard is opening up ways of achieving the highest possible PL (PL e) with a component classified as Cat. 3 in accordance with EN 954-1, a “good” diagnosis in the component and “good” $MTTF_d$ values.

Back to the safety functions and the estimation of the achieved PL based on the graph:

Up until now the focus was on the safety function per se, whereby the function was required to achieve a required performance level (PL_r). This then had to be verified in turn with the achieved performance level PL, taking into account the relevant safety-related parameters.

What is new now is that a PL has to be defined for each safety function for each individual channel. This is relevant in the case of systems designed with redundancy, like those found in many applications, which require a “higher level of safety” (EN 954-1/Cat. 3 and higher applications).

Accordingly, for a system set up with redundancy, the relevant safety-related parameters for both disconnecting paths have to be made available.

More detailed information about determining the PL actually achieved appears in the chapter “SISTEMA, a software for practical PL determination”.



Step 6 Verification and validation

Verification and validation (V&V) are QA measures for the avoidance of errors during the design and implementation of safety-related parts of control systems (SRP/CS) which execute safety functions. Part 2 of EN ISO 13849 in particular deals with this subject in depth.

For each individual safety function, the PL of the associated SRP/CS(s) must match the “performance level required”. The PLs of the various SRP/CSs forming part of a safety function have to be greater than or equal to the performance level required of this function.

If a number of SRP/CSs are interconnected, the definitive PL can be determined using Table 11 from the standard.

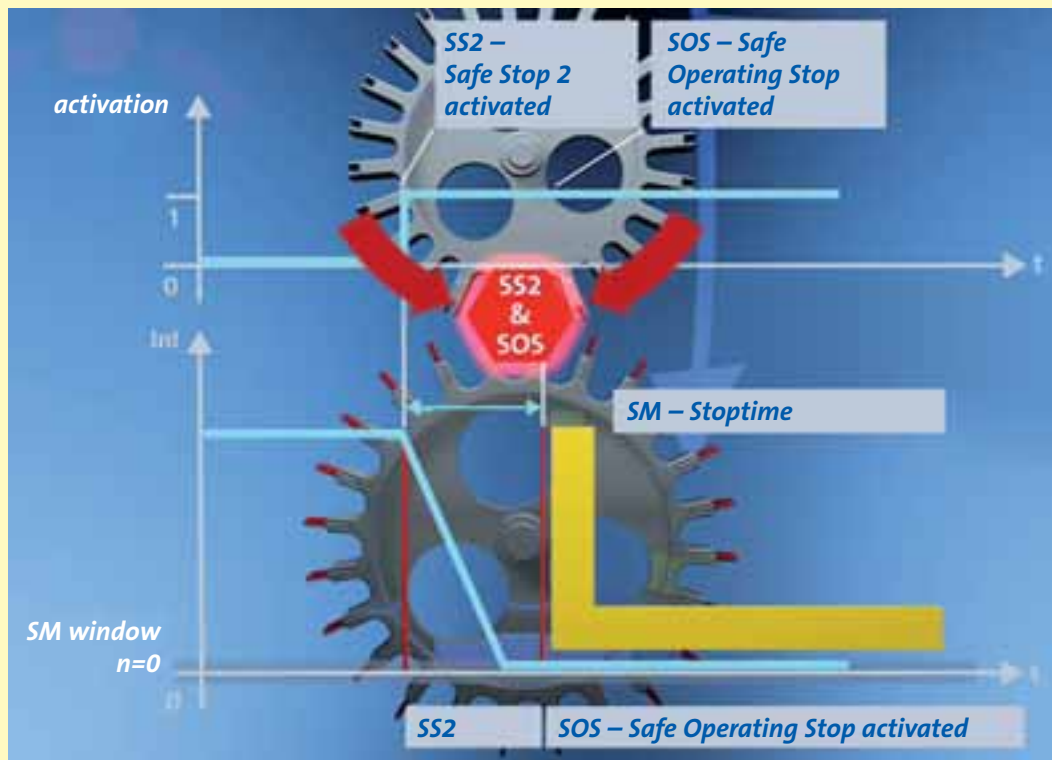
The design of a safety-relevant control function has to be validated. Validation must show that the combination of safety-relevant parts for each safety function meets the applicable requirements.



PL _{low}	N _{low}	▶	PL
a	>3	▶	None, not permitted
	≤3	▶	a
b	>2	▶	a
	≤2	▶	b
c	>2	▶	b
	≤2	▶	c
d	>3	▶	c
	≤3	▶	d
e	>3	▶	d
	≤3	▶	e

Note: The values calculated for reference purposes are based on reliability values for the mid-point of each PL.

Table 11 of EN ISO 13849-1: Calculation of the PL for series connection of SRP/CSs involved in a safety function



Functional safety engineering | by Lenze

Lenze's products with functional safety engineering are already certified in accordance with the new standards.

At Lenze we have already had our products with functional safety engineering certified in accordance with the requirements of the new standards as a matter of course. For example, the TÜV Rheinland has confirmed that the frequency inverters in the 8400 series with the "Safe torque off/STO" safety function and the servo inverters in the 9400 series with high-grade functions such as "Safely-limited speed/SLS" have achieved the highest performance level PL e.

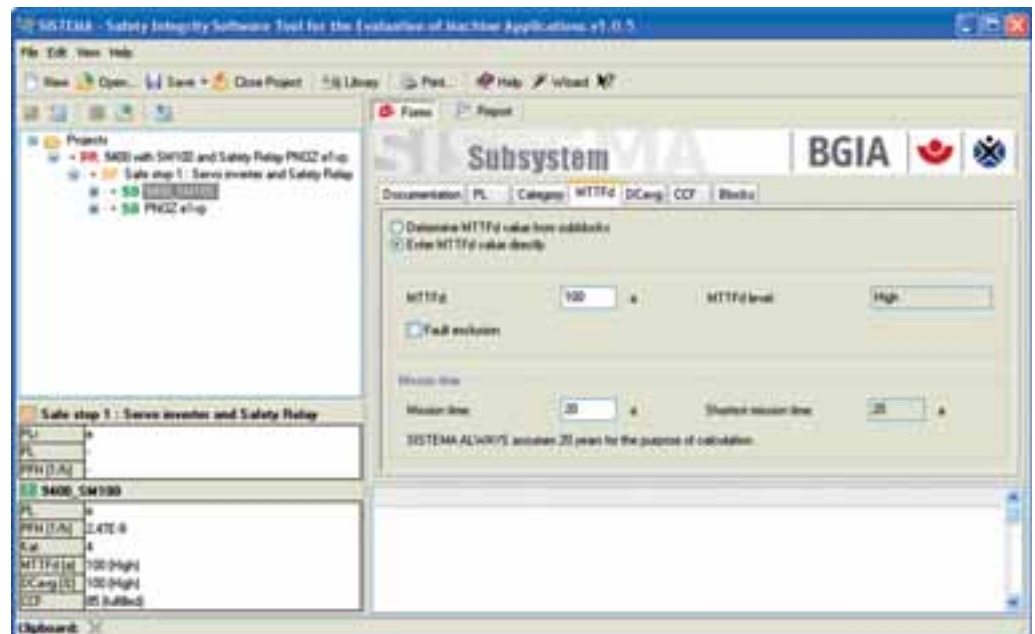
How does this benefit you?

Since Lenze products with functional safety engineering have already been certified by the TÜV, this will make obtaining approval for your overall

machine featuring the safety concept you have selected much easier. In providing the relevant safety-related parameters we are helping you to achieve a high level of safety engineering in your machine.

Software tool support BGIA's "SISTEMA" with the provision of libraries

"SISTEMA" is a software tool which is provided free of charge by the BGIA (Berufsgenossenschaftliches Institut für Arbeitsschutz, the Institute for Occupational Safety and Health) in St. Augustin, Germany. It is frequently used to determine the achieved performance level in a machine. Dialog boxes guide mechanical engineers through the process of creating their individual safety functions in a project and entering the safety-relevant parameters for the individual disconnecting paths.



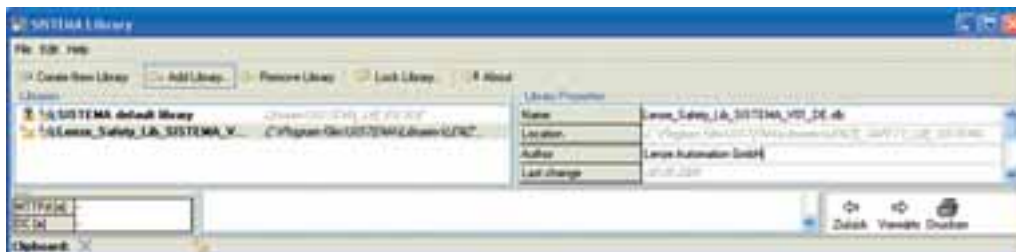
SISTEMA software tool for determining PLs to EN ISO 13849-1

The parameters for all components involved in the safety chain (sensor, logic, actuator) have to be entered. The tool then calculates the PL.

Lenze can provide you with user support for the SISTEMA tool in the form of a SISTEMA library containing all Lenze components which have already been certified in accordance with the latest standards.

How does this benefit you?

You integrate the Lenze library into your SISTEMA project and can use the Lenze products with functional safety straight away in your project: You no longer have to enter the individual safety-relevant parameters. This saves time and avoids erroneous entries – for safety's sake.



SISTEMA library with Lenze components

Lenze collaboration | TÜV Rheinland initiative

Creation of a databank available world-wide with valid entries of “safety-relevant parameters”

The TÜV Rheinland has started a joint venture committed to making available the relevant safety-related parameters (SI parameters) of functional safety components. The aim is that valid SI parameters will be provided in a database by the TÜV Rheinland.

The entire sector is working on defining and publishing these parameters. Mechanical engineers who want to have their machines certified in accordance with the new EN ISO 13849-1 now are pushing manufacturers to provide the relevant parameters. However, in many cases they cannot rely on the quality of the parameter values received. A harmonised database which can be relied upon is the order of the day.

How does this benefit you?

Lenze will provide you with the relevant safety-related parameters verified by the TÜV Rheinland. Lenze is actively involved in the development of a database of valid SI parameters which will be available world-wide and which you will be able to rely on in the future for the provision of accurate parameters.



Lenze

Lenze

Drive-based Safety

11:47:51

19.02.20

Sicher abgeschaltetes Moment

Sicherer Stopp 1

Sicherer Stopp 2 / Sicherer Betriebslauf

Sicher begrenzte Geschwindigkeit

Sichere Maximalgeschwindigkeit

Betriebsart

Gen. über Lenze

Appendix | Safety standards

Abbreviations

Abbreviation	Term	Explanation
B_{10d}		Number of cycles, up to 10% of components fail as dangerous
λ	Failure rate	
λ_S		Failure rate in the case of non-hazardous failures
λ_d		Failure rate in the case of hazardous failures
CCF	Common cause failure	
DC	Diagnostic coverage	
DC_{avg}	Diagnostic coverage average	
	Designated architecture	Of a SRP/CS
HFT	Hardware fault tolerance	
MTBF	Mean time between failures	
MTTF	Mean time to failure	
$MTTF_d$	Mean time to dangerous failure	
MTTR	Mean time to repair	(always much shorter than the MTTF)
PFH	Probability of failure per hour	
PFH_D	Probability of dangerous failure per hour	
PL	Performance level	Ability of safety-related parts to execute a safety function under foreseeable conditions in order to achieve the expected reduction in risk
PL_r	Performance level required	
SIL	Safety integrity level	
SILCL	Safety integrity claim limit	

Useful Web links

Directives (EU)	European Union legislative provision can be accessed directly and free of charge here.	http://eur-lex.europa.eu
Lists of standards	EU Official Journal BAuA: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Federal Institute for Occupational Safety and Health) VDMA: Verband Deutscher Maschinen- und Anlagenbauer (German Engineering Federation)	http://www.baua.de http://www.vdma.org
Software tool for determining PLs to EN ISO 13849-1	BGIA: Berufsgenossenschaftliches Institut für Arbeitsschutz in St. Augustin (Institute for Occupational Safety and Health)	http://www.dguv.de/bgia/de/prs/softwa/sistema/index.jsp#
Functional safety management (FSM)	TÜV Rheinland ASI: Automation – Software – Information technology	http://www.tuvasi.com
Notified testing laboratories	BAuA: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Federal Institute for Occupational Safety and Health) Up-to-date list of notified certification bodies in Europe	http://www.baua.de/de/Geraete-und-Produktsicherheit/Geraete-und-Produktsicherheit.html?__nnn=true
Publishers of standards, German-speaking	DIN: Deutsches Institut für Normung e.V. (German Institute for Standardization)	http://www.din.de
Publishers of standards, international	IEC ISO CENELEC CEN	http://www.iec.ch http://www.iso.org http://www.cenelec.eu http://www.cen.eu



Lösung mit Drive-based Safety

Solution using Drive-based Safety

Geringere Systemkosten
Lower system costs

- ▶ keine externe Sicherheitstechnik-Hardware erforderlich
No external safety engineering hardware required
- ▶ weniger Verdrahtungsaufwand
reduction in wiring
- ▶ weniger Platzbedarf
reduction in space requirement



It's good to know | why we are there for you



"Our customers come first. Customer satisfaction is what motivates us. By thinking in terms of how we can add value for our customers we can increase productivity through reliability."



Lenze drive and automation solutions

"We will provide you with exactly what you need – perfectly co-ordinated products and solutions with the right functions for your machines and installations. That is what we mean by 'quality'."



"Take advantage of our wealth of expertise. For more than 60 years now we have been gathering experience in various fields and implementing it consistently and rigorously in our products, motion functions and pre-configured solutions for industry."



"We identify with your targets and strive towards a long-term partnership which benefits both sides. Our competent support and consultation process means that we can provide you with tailor-made solutions. We are there for you and can offer assistance in all of the key processes."



You can rely on our service. Expert advice is available 24 hours a day, 365 days a year, in more than 30 countries via our international helpline: 008000 24 Hours (008000 2446877).

www.Lenze.com

13340000