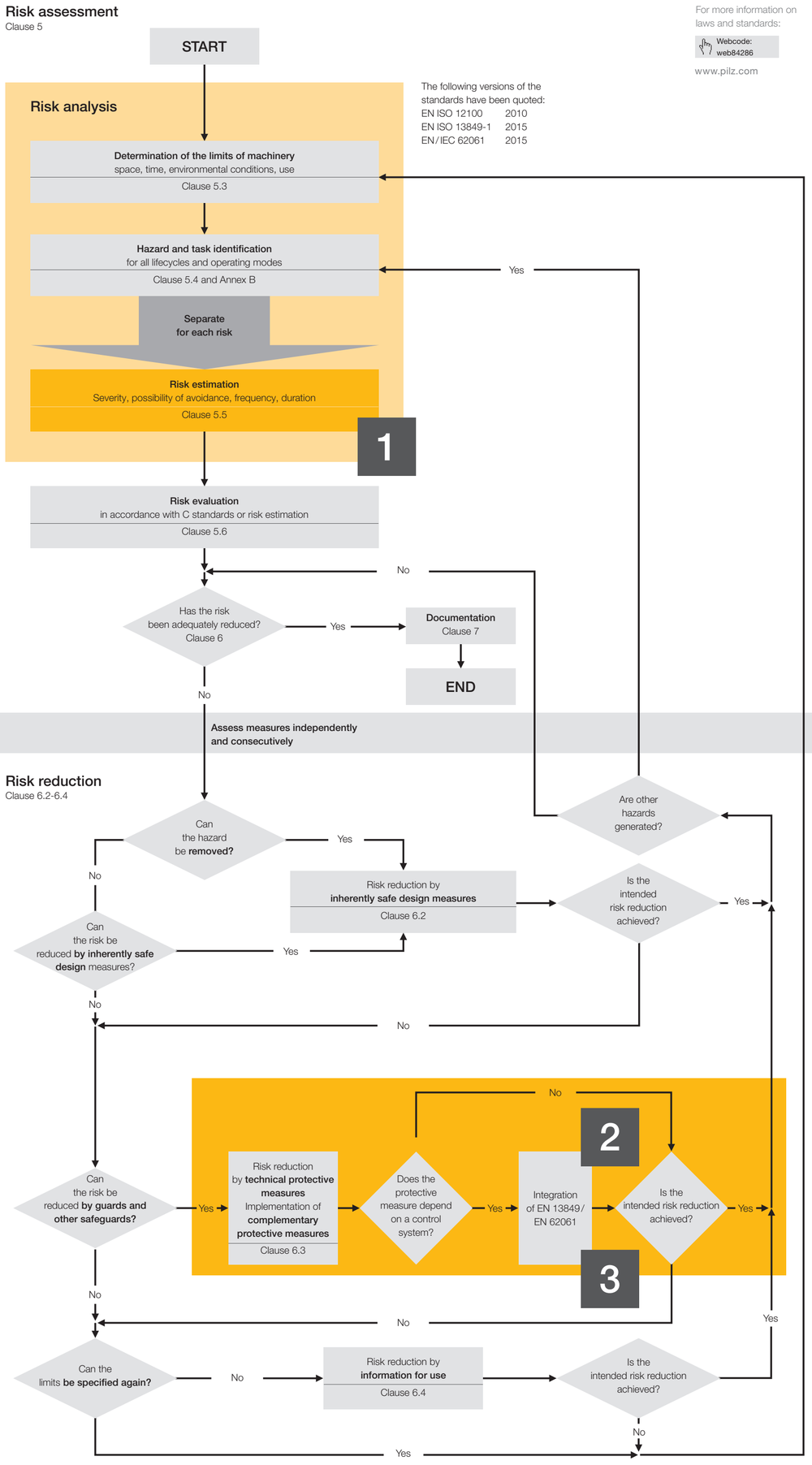
Functional safety
EN ISO 12100, EN ISO 13849 and EN/IEC 62061

PILZ
THE SPIRIT OF SAFETY

EN ISO 12100
Risk assessment and risk reduction



For more information on laws and standards:

Webcode: web84286

www.pilz.com

The following versions of the standards have been quoted:

EN ISO 12100	2010
EN ISO 13849-1	2015
EN/IEC 62061	2015

1 EN ISO 12100

Risk assessment based on the following risk parameters for each danger zone

Risk	is a function of	Severity	+	Probability of occurrence
with regard to the hazard to be considered		of the possible injury that results from the hazard to be considered		**Frequency and duration** of exposure to the hazard **Likelihood** of the hazard occurring **Avoidability** or limit

EN ISO 13849-1

Applicable for electrical, electronic, programmable electronic, hydraulic, pneumatic, mechanical systems

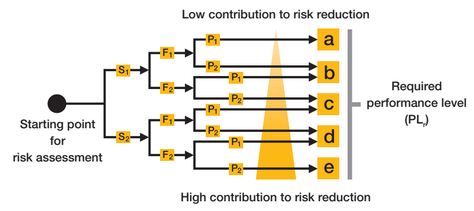
EN/IEC 62061

Applicable for electrical, electronic, programmable electronic systems

2 PL and SIL determination for each safety function

Determination of the required performance level (PL_r)

- **S – Severity of injury**
  S_1 = Slight (normally reversible injury)
  S_2 = Serious (normally irreversible injury including death)
- **F – Frequency and/or duration of exposure to a hazard**
  F_1 = Seldom to quite often and/or the exposure time is short
  F_2 = Frequent to continuous and/or the exposure time is long
- **P – Possibility of avoiding the hazard**
  P_1 = Possible under specific conditions
  P_2 = Scarcely possible
- **Probability of occurrence of the hazardous event**
  A low probability can reduce the PL_r by one level



Determination of the required Safety Integrity Level (SIL)

Frequency and duration	Fr > 10 min	Fr ≤ 10 min
≤ 1 hour	5	5
> 1 hour – ≤ 1 day	5	4
> 1 day – ≤ 2 weeks	4	3
> 2 weeks – ≤ 1 year	3	2
> 1 year	2	1

Probability of hazardous event	Pr
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Avoidance	Av
Impossible	5
Possible	3
Likely	1

Consequences and severity	Se	Class Cl = Fr+Pr+Av 3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			OM	SIL 1	SIL 2
Reversible, first aid	1				OM	SIL 1

OM = other measures recommended

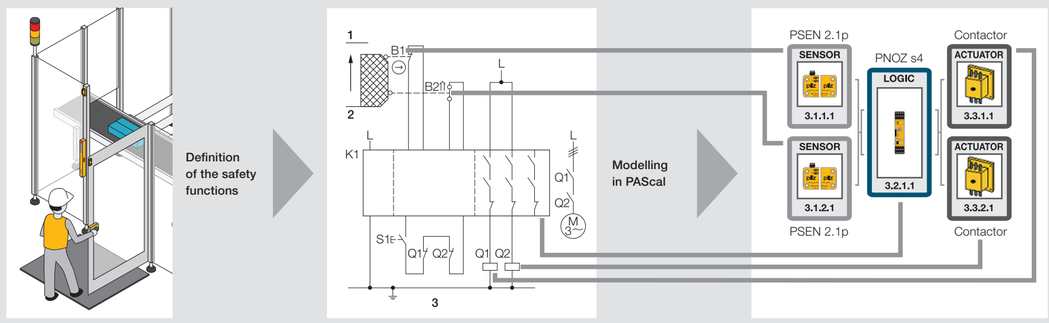
3 Calculation of the safety function (e.g. with PAScal®)

Necessary safety performance data

EN ISO 13849-1 Data provided by the manufacturer	EN ISO 13849-1 Data provided by the user	Unit type			EN/IEC 62061 Data provided by the manufacturer	EN/IEC 62061 Data provided by the user
PFH, PL Category, T_M	-	Units with internal diagnostics		Safety control, safety relay	PFH SIL T_M	–
$MTTF_D$	DC, CCF, Category	Units without internal diagnostics	No wearing components	Sensors	$MTTF_D$ λ_d λ_s	DC, CCF, Subsystem type
$B10_d$	DC, CCF, Category, n_{op}		With wearing components	EMERGENCY STOPs, relays, switches, valves	$B10_d$ λ_d λ_s	DC, CCF, Subsystem type, n_{op}

PAScal® calculation tool

From the machine … **… to the safety function …** **… to their assessment in PAScal.**

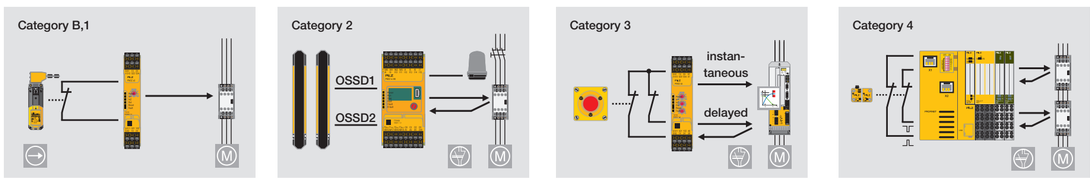


Risk assessment in accordance with EN ISO 12100

Implementation of safety functions

Validation of safety functions in PAScal

Specification of categories – examples of solutions

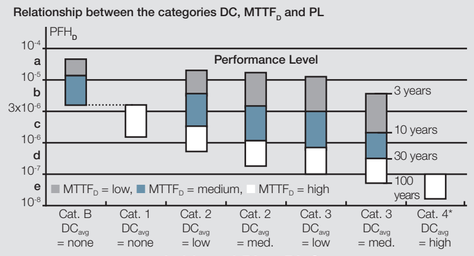


The solutions illustrated here are provided purely by way of example.

Probability of a dangerous failure per hour – comparison PL / SIL

Performance Level (PL) in accordance with EN ISO 13849-1

Relationship between the categories DC, $MTTF_D$ and PL



Achieved PL ≥ PL_r?

* In Cat. 4, $MTTF_D$ up to 2,500 a is possible

Safety Integrity Level (SIL) in accordance with EN / IEC 62061

Safety Integrity Level.	Probability of a dangerous failure per hour (PFH_D)
3	$10^{-8} \le PFH_D < 10^{-7}$
2	$10^{-7} \le PFH_D < 10^{-6}$
1	$10^{-6} \le PFH_D < 10^{-5}$

Achieved SIL ≥ required SIL?

Glossary of terms

- **B_{10d}** Number of cycles of products before 10% of the product range fails "dangerously"
- **Category (CAT)** Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability
- **CCF** Common cause failure
- **Diagnostic coverage (DC)** Measure for the effectiveness of diagnostics, may be determined as the ratio of the failure rate of detected dangerous failures and the failure rate of total dangerous failures
- **DC_{avg}** Average diagnostic coverage
- **Fault** State of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources
- **λ** Average probability of failure
- **λ_D** Dangerous failure rate
- **λ_S** Safe failure rate
- **Mission time** Period of time covering the intended use of the SRP/CS
- **$MTTF_D$** Mean time to dangerous failure
- **n_{op}** Mean frequency of operation per annum
- **Performance level (PL)** Discrete level to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions
- **Performance level, required (PL_r)** Performance level (PL) in order to achieve the required risk reduction for each safety function
- **PFH_D** Probability of dangerous failure per hour
- **Risk** Combination of the probability of occurrence of harm and the severity of that harm
- **Safety function** Function of the machine whose failure can result in an immediate increase of the risk(s)
- **Safety Integrity Level (SIL)** Discrete level (one out of a possible four) for specifying the safety integrity of the safety functions to be allocated to the E/E/PE system, where SIL 3 (SIL 4 in the process industry) has the highest level of safety integrity and SIL 1 has the lowest
- **Safety validation** Confirmation by examination and by provision of a certificate stating that special requirements for a specific intended use are met
- **SRCF – Safety-Related Control Function** Control function implemented by an SRECS with a specified integrity level that is intended to maintain the safe condition of the machine or to prevent an immediate increase of the risk(s)
- **SRECS** Safety-Related Electrical Control System
- **SRP/CS – Safety-Related Part of a Control System** Part of a control system that responds to safety-related input signals and generates safety-related output signals
- **Subsystem** Entity of the top-level architectural design of the SRECS where a failure of any subsystem will result in a failure of a safety-related control function
- **Verification** Confirmation by examination and by provision of a certificate stating that the requirements of the specification are met

Range of plant and machinery lifecycle services

We support you in the optimum global application of safety strategies. Benefit from consulting and engineering: from risk assessment through to the declaration of conformity. Our international qualification programme guarantees enhanced success through professional development.

PAScal® Safety Calculator – Calculation software for verifying functional safety

Determine the safety levels of safety functions with ease - with the Safety Calculator PAScal you have a handy calculation tool to verify functional safety in accordance with EN ISO 13849-1 and EN / IEC 62061.

Webcode: web150431

Download the current version: www.pilz.com

International hotline +49 711 3409-444

8-8-en-3-125, 2020-01, Printed in Germany © Pilz GmbH & Co. KG, 2020