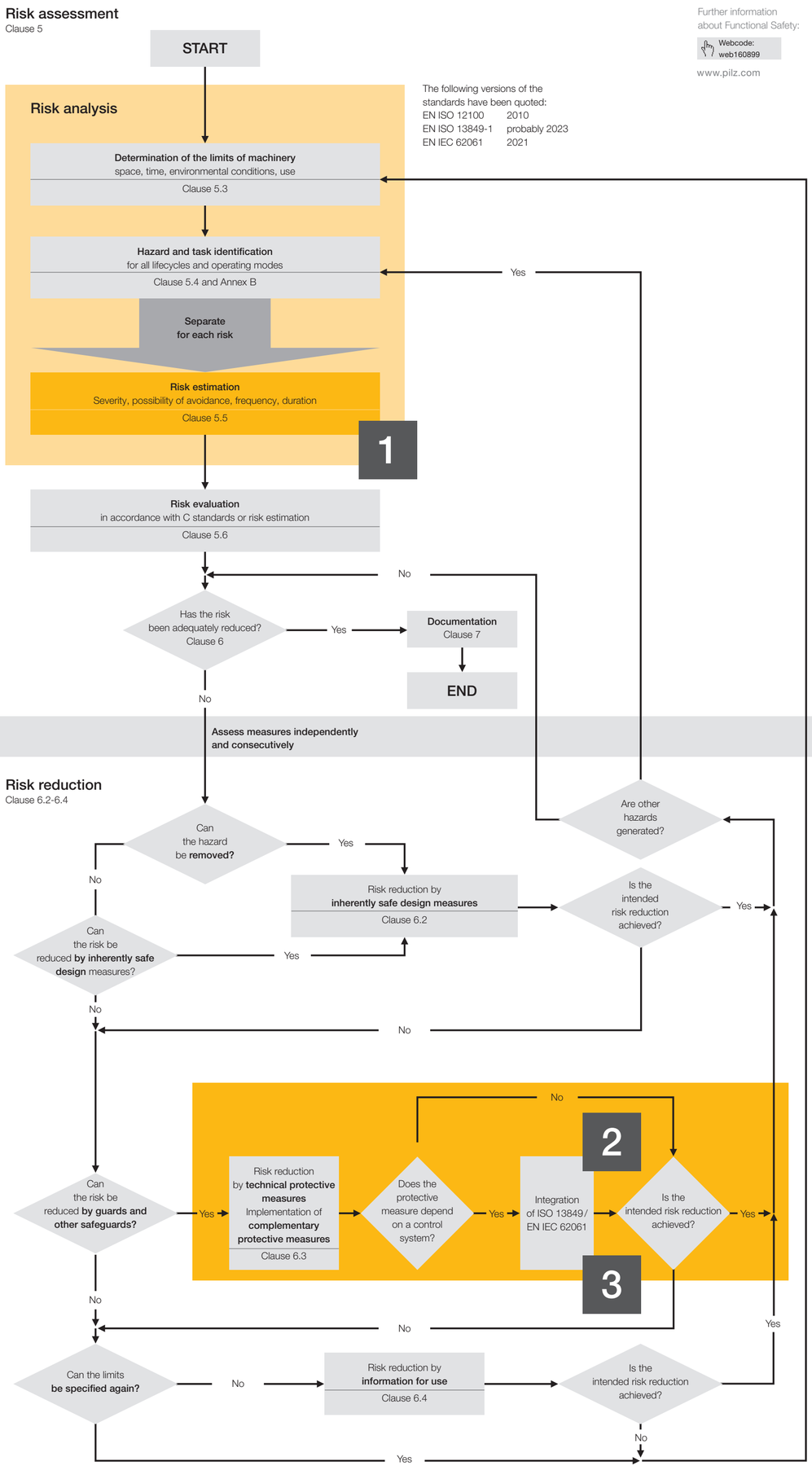
Standards Functional Safety and Risk Assessment
EN ISO 12100, ISO 13849 and EN IEC 62061

PILZ
THE SPIRIT OF SAFETY

EN ISO 12100
Risk assessment and risk reduction



Further information about Functional Safety:
Webcode: web160899
www.pilz.com

The following versions of the standards have been quoted:

EN ISO 12100	2010
EN ISO 13849-1	probably 2023
EN IEC 62061	2021

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

ISO 13849-1

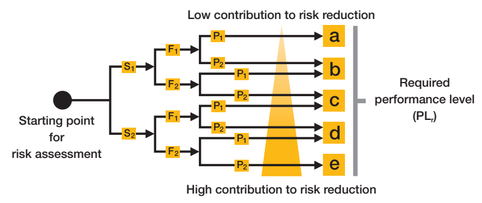
Safety of machinery – Safety-related parts of control systems: Part 1: General principles for design

EN IEC 62061

Safety of machinery – Functional safety of safety-related control systems

2 PL_r 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 or limiting harm**
  P_1 = Possible under specific conditions
  P_2 = Scarcely possible
- **A low probability can reduce the PL, by one level**

Determination of the parameter P – Factors	A	B	C
Use of the machine by	Skilled person	Unskilled person	
Speed of the part that can create a hazardous event	Low or very low speed event	Medium speed event	High speed event
Spatial possibility to withdraw from the hazard	Possible in more or equal to 50 % of the cases	Possible in less than 50 % of the cases	Not possible
Possibility of recognition of the hazard/ awareness of the hazard	Possible in more or equal to 50 % of the cases	Possible only in less than 50 % of the cases	Not possible
Complexity of the operations	Low complexity or no interaction	Medium to High complexity	
if "C" is selected OR "B" is selected at least 3 times; avoidance "P2": # „C" >=1; #"B" >=3 ➔ P2 if "C" is not selected AND "B" is selected at most 2 times; avoidance "P1": # „C" =0 AND #"B" <=2 ➔ P1			

Determination of the required Safety Integrity Level (SIL)

Frequency and duration	Fr > 10 min	Fr ≤ 10 min	Probability of hazardous event	Pr	Avoidance	Av
≥ 1 per h	5	5	Very high	5		
< 1 per h to ≥ 1 per day	5	4	Likely	4		
< 1 per day to ≥ 1 per 2 weeks	4	3	Possible	3	Impossible	5
< 1 per 2 weeks to ≥ 1 per year	3	2	Rarely	2	Possible	3
< 1 per year	2	1	Negligible	1	Likely	1

Consequences	Severity Se	Class Cl = Fr + Pr + Av									
		3	4	5	6	7	8	9	10	11	12	13	14	15
Death, losing an eye or arm	4	SIL 1		SIL 2			SIL 2			SIL 3			SIL 3	
		PL b	PL c	PL d			PL d			PL e			PL e	
Permanent injury, losing fingers	3			OM			SIL 1			SIL 2			SIL 3	
				PL a			PL b		PL c	PL d			PL e	
Reversible injury, medical attention	2	No SIL (or PL) required					OM			SIL 1			SIL 2	
							PL a			PL b		PL c	PL d	
Reversible injury, first aid	1	OM: Other Measures								OM			SIL 1	
										PL a			PL b	PL c

Example for calculating the class Cl:
For a specific hazard with an 'Se' assigned as 3, an 'Fr' as 4, a 'Pr' as 3 and an 'Av' as 5 then: Cl = Fr + Pr + Av = 5 + 4 + 3 = 12

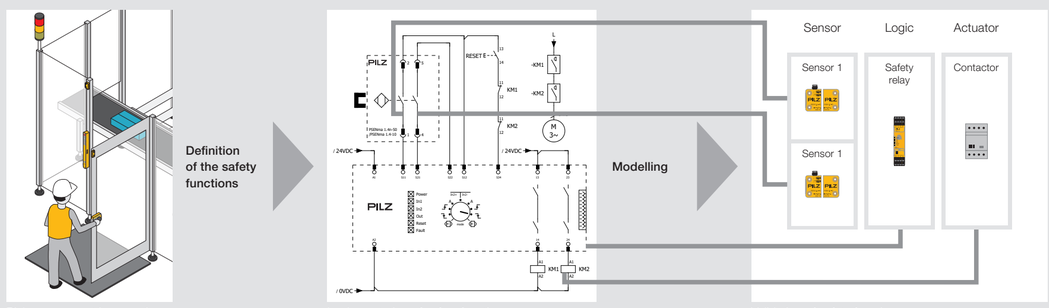
3 Calculation of safety function failure rate

Necessary safety performance data

ISO 13849-1		Unit type			EN IEC 62061	
Data provided by the manufacturer	Data determined by the designer				Data provided by the manufacturer	Data determined by the designer
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**	Components not subject to wearing	Sensors	$MTTF_D$	DC, CCF, Subsystem type
$B10_D$	DC, CCF, Category, n_{op}		**With** wearing components	Emergency stops, relays, switches, valves	$B10_D$	DC, CCF, Subsystem type, n_{op}

Evaluation procedure

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



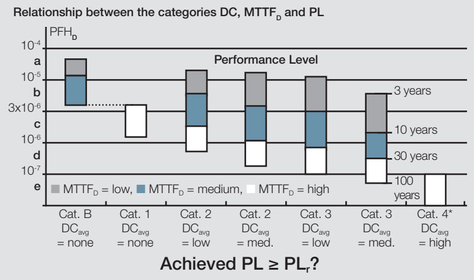
Risk assessment in accordance with EN ISO 12100
Implementation of safety functions
Validation of safety functions

Specification of categories – in this case on the sensor subsystem, for example

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

Performance Level (PL_r) in accordance with ISO 13849-1

Relationship between the categories DC, $MTTF_D$ and PL



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

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

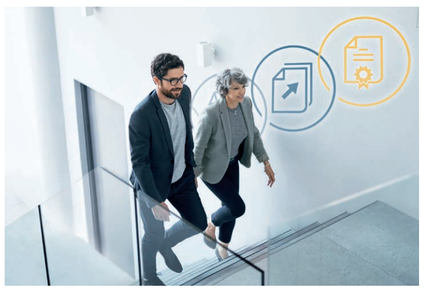
Safety Integrity Level	Probability of a dangerous failure per hour (PFH)
3	PFH < 10^{-7}
2	PFH < 10^{-6}
1	PFH < 10^{-5}

Achieved SIL ≥ required SIL?

Glossary of terms

- **Architecture**
  Specific configuration of hard-ware and software elements in a safety-related control system (SCS)
- **B_{10D}**
  Number of cycles of products before 10% of the product range fails "dangerously"
- **Category**
  Classification of the subsystem in respect to its resistance to faults and the subsequent behaviour in the fault condi-tion 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 of the effectiveness of diagnostics, which is detemined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures
- **DC_{avg}**
  Average diagnostic coverage
- **Fault**
  Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function
- **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 a safety-related part of a control system
- **$MTTF_D$**
  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**
  Average rate of dangerous failure
- **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 three) for describing the capability to perform a safety function where SIL 3 has the highest level of safety integrity and SIL 1 has the lowest
- **Safety-related control system (SCS)**
  Part of the control system of a machine which implements a safety function by one or more "subsystems"
- **Subsystem**
  Entity of the top-level architec-tural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function

The measures outlined on this sheet are simplified descriptions and are intended to provide an overview of the standards EN ISO 12100, ISO 13849-1 and EN IEC 62061. Detailed understanding and correct application of all relevant standards and directives are needed for validation of safety circuits. As a result, we cannot accept any liability for omissions or incomplete information.



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.

Further information on Machinery Safety services:
Webcode: web225977
www.pilz.com

8-8-en-3-125, 2025-07, Printed in Germany © Pilz GmbH & Co. KG, 2025