SHARING COMPETENCE

Pfannenberg
ELECTRO-TECHNOLOGY FOR INDUSTRY

Realize norm-conforming functional safety

Norm situation: functional safety

Machine industry

Electric
Hydraulic
Pneumatic
Mechanical

EN ISO 13849

IEC 62061

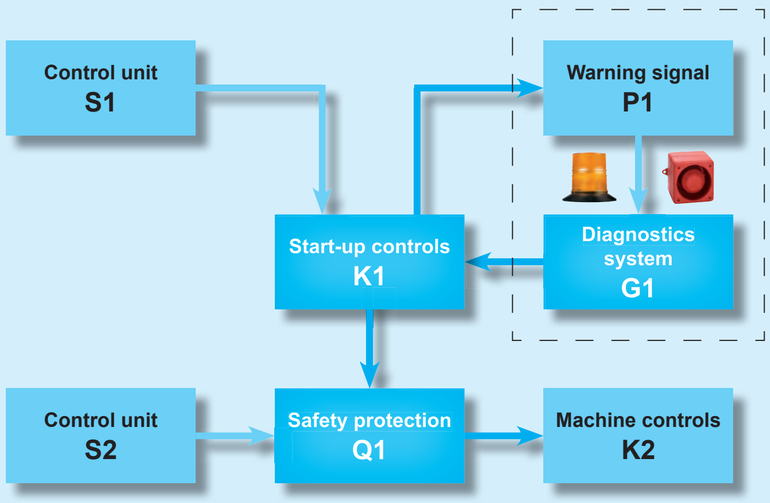
IEC 61508

Process industry

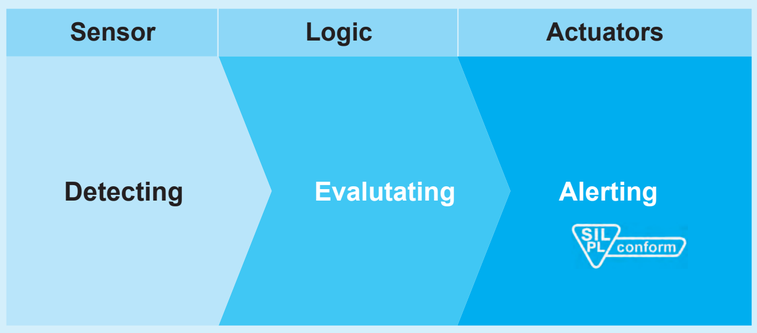
IEC 61511

Electric
Electronic
programm. electronics
(E/E/PE)

Machine safety e.g. start-up warning



Safety Loop

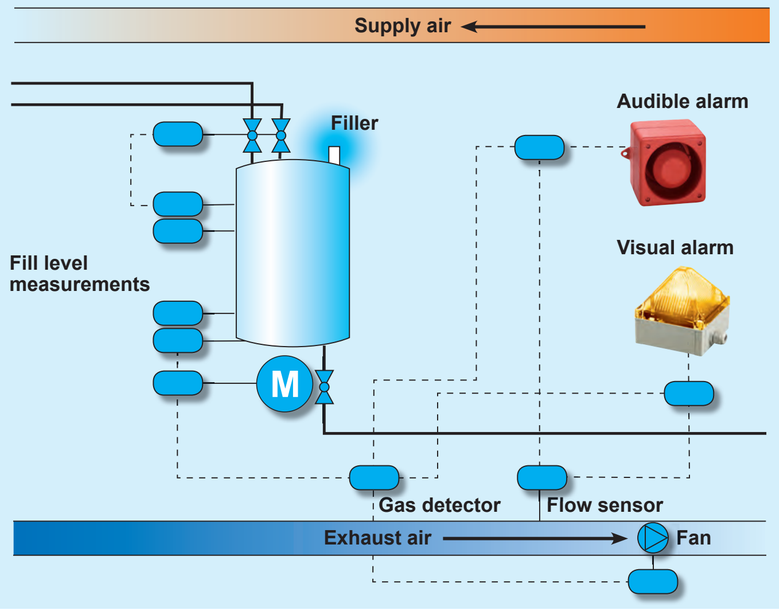


Actuators conform 100% to SIL/PL:

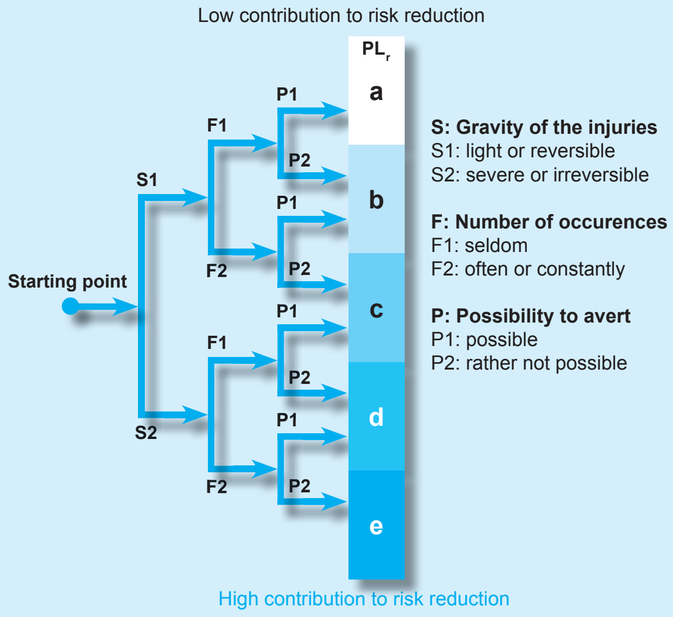
Quadro and PMF Flashing lights

DS Sounder

Process safety e.g. gas leak alarm



Risk factor according to DIN EN ISO 13849

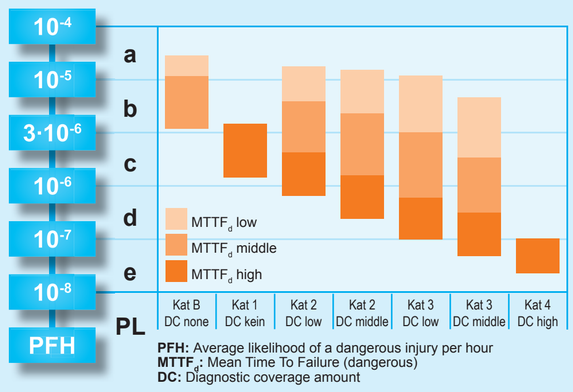


S: Gravity of the injuries
S1: light or reversible
S2: severe or irreversible

F: Number of occurences
F1: seldom
F2: often or constantly

P: Possibility to avert
P1: possible
P2: rather not possible

Performance Level (PL) according to DIN EN ISO 13849



PFH: Average likelihood of a dangerous injury per hour
MTTF$_d$: Mean Time To Failure (dangerous)
DC: Diagnostic coverage amount

MTTF$_d$ for each channel		DC	
	MTTF$_d$ (in a)		DC in %
low	3 up to < 10	none	< 60
middle	10 up to < 30	low	60 up to < 90
high	30 up to < 100	middle	90 up to < 99
not possible	ex 100	high	ex 99

Characteristics

Portion of safe failures (SFF), Diagnostic coverage amount (DC)

$$SFF = \frac{\lambda_s}{\lambda_{ges}} \text{ without diagnostic} \qquad SFF = \frac{\lambda_s + \lambda_{dd}}{\lambda_{ges}} \text{ with diagnostic}$$

$$DC = \frac{\lambda_{dd}}{\lambda_d} \qquad SFF = \frac{\lambda_s + DC \cdot \lambda_d}{\lambda_s + \lambda_d}$$

$$\lambda_{ges} = \lambda_s + \lambda_d \qquad \lambda_d = \lambda_{dd} + \lambda_{du}$$

s: safe
d: dangerous
dd: dangerous detected
du: dangerous undetected

Safety integrity, norm comparison, PFH, PFD, requirements

Safety integrity (type B) according to IEC 61508				SIL/PL (ISO 13849)	
	HFT				
SFF	0	1	2	SIL	PL
< 60%	–	SIL 1	SIL 2	1	b, c
60% up to < 90%	SIL 1	SIL 2	SIL 3	2	d
90% up to < 99%	SIL 2	SIL 3	SIL 4	3	e
99% up to > 99%	SIL 3	SIL 4	SIL 4	4	–

Requirements according to IEC 61508, Type B (in part, unknown failure characteristics)
Comparison SIL/PL (IEC 61508/ DIN EN ISO 13849)

SIL	PFH(d)	PFD(d)
	in 1/h	
1	$<10^{-5}$	$< 10^{-1}$
2	$<10^{-6}$	$< 10^{-2}$
3	$<10^{-7}$	$< 10^{-3}$
4	$<10^{-8}$	$< 10^{-4}$

Characteristics (IEC 61508)
SIL Safety Integrity Level
SFF Portion of safe failures
PF Failure likelihood
PFH PF per hour
PFD PF per requirement

Lexicon A–P

β (beta-Factor or rather, Common Cause Factor)
Measure for the CCF; portion of failures, which have a common cause.

CCF (Common Cause Failure)
Failure due to common cause.

DC (Diagnostic Coverage)
Measure for the effectiveness of the diagnostic, which can be defined as the relationship of the failure rate of the recorded dangerous failures and the failure rate of the total dangerous failures.

DC$_{avg}$
Average diagnostic coverage.

HFT (Hardware Failure Tolerance)
Ability of a SRECS of a system or system element to complete a required function during the presence of a failure or breakdown.

KAT (Category)
Setting of the safety-related components of the controls with relation to their resistance against failures and the respective behavior following, which is attained according to the structure of the component alignment, the failure recognition and/or their dependability.

λ
Average probability of a failure.

λ$_D$
Rate of dangerous failures.

λ$_S$
Rate of safe failures.

MTTF$_d$ (Mean Time To Dangerous Failure)
Average time / mean time to a dangerous failure.

Muting
By-pass function: a compliant time-limited override of the safety function with additional sensors.

PFH / PFH$_d$ (Probability of [Dangerous] Failure per Hour)
(dangerous) failures per hour during continuous use.

PFD (Probability of Failure per hour on Demand)
Failure probability when safety function is triggered / activated.

PL (Performance Level)
Discrete Level, which specifies the ability of safety-related control components to execute safety function under predictable conditions.

PL$_r$ (Performance Level, necessary)
To attain a necessary risk minimization for safety functions.

Hierarchical arrangement of the EN Norms

Excerpt of the relevant norms for the use of visual and acoustic signaling units

Basic safety norm
e.g. EN ISO 12100

Type A Norms
General design guidelines and basic definitions for machines

Safety group norm
e.g. EN ISO 13849-1
EN 62061

For example:

Type B Norms

EN 61310	Indication, matking and actuation
EN 981	System of acoustic and visual alarm signals and information signals
EN 842	Visual danger signals
EN ISO 7731	Alarms for public areas and workplaces

Engineering standard

For example:

Type C Norms

EN 15093/15094	Rolling machines	**EN 692/693**	Presses
EN 415	Packaging machines	**EN 1034**	Paper machine
EN ISO 11111	Textile machines	**EN 1248/1247**	Casting machine
EN 1010	Printing machine		

Lexicon R–Z

Risk
Combination of the probability of loss / damage occurrence and the extent of the damage.

SFF (Safe Failure Fraction)
Portion of safe failures, portion of the total failure rate of a sub system, which does not cause a dangerous failure.

Safety function
Machine function, which if fails, automatically increases the risk (the risks).

SIL (Safety Integrity Level)
Discrete step / stage (one of four possible) to specify the safety integrity of the safety function, which is assigned to the E/E/PE-System. The SIL 3 (SIL 4 in the process industry) is the highest step / stage and SIL 1 is the lowest.

SIL$_{CL}$ (SIL-standard limitation)
Maximum SIL, which can utilized for a SRECS-sub-system with regards to the structural constraints and system safety integrity.

SRCF (Safety Related Control Function)
A SRECS executed control function with a defined integrity level, which is designated to maintain the safe condition of the machine or to prevent the immediate increase of risk.

SRECS (Safety Related Electronic Control System)
Electronic control system of a machine, whose failure immediately increases risk.

SRP/CS (Safety Related Part of Control System)
Portion of a control, which reacts to safety-related incoming signals and generates safety-related outgoing signals.

T$_1$ (Repeat test)
Recurring test in order to detect failures in a safety-related system so that, if necessary, the system can be brought back into a "like new" condition or as close as possible according to the practical factors. Technically speaking, a recurring test is not possible for most units.

T$_M$ (Service life)
Time-span covering the use of the SRP/CS.

Pfannenberg GmbH Werner-Witt-Straße 1 · D-21035 Hamburg · Phone +49 40 734 12-0 · Telefax +49 40 734 12-101 · sales.support@pfannenberg.com · www.pfannenberg.com