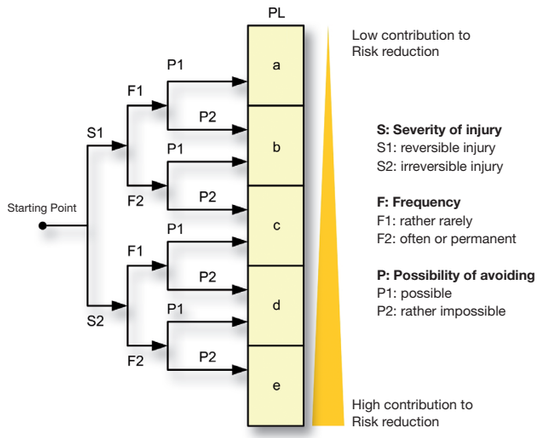
Risk graph and evaluation
Safety classification

Risk graph according to ISO 13849

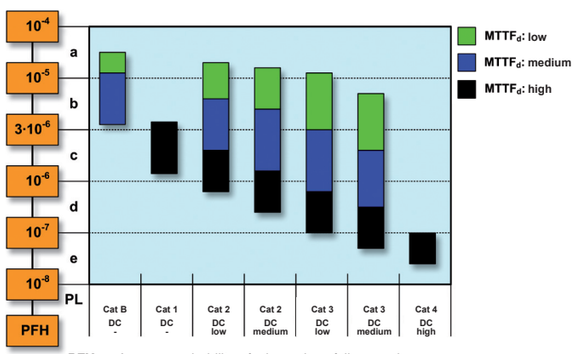


S: Severity of injury
S1: reversible injury
S2: irreversible injury

F: Frequency
F1: rather rarely
F2: often or permanent

P: Possibility of avoiding
P1: possible
P2: rather impossible

Performance Level (PL) according to ISO 13849

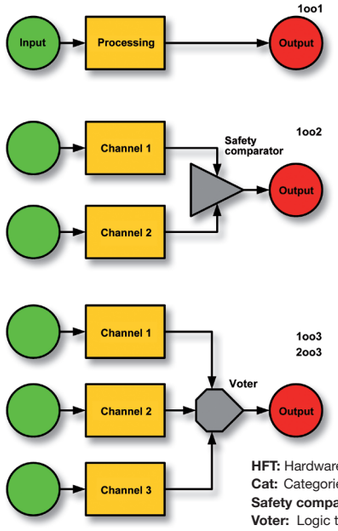


PFH: Average probability of a hazardous failure per hour
$MTTF_d$: Mean Time to Failure (dangerous)
DC: Diagnostic coverage

$MTTF_d$ for each channel		DC	
	$MTTF_d$ (in a)		DC in %
low	3 to < 10	none	< 60
medium	10 to < 30	low	60 to < 90
high	30 to < 100	medium	90 to < 99
impossibel	100 or more	high	99 or more

Structure Hardware Fault Tolerance
Safety requirements
Comparisons of parameters to standards

Safety structures, HFT



XooY:
X: Number of channels for switch-off
Y: Number of existing channels

1oo1:
One-channel structure
HFT = 0 (Cat: B to 2)

1oo2:
Two-channel structure
HFT = 1 (Cat: 3 and 4)

1oo3, 2oo3:
Multi-channel structure
HFT > 1

HFT: Hardware Fault Tolerance
Cat: Categories according ISO 13849
Safety comparisons: Switch in the safe state
Voter: Logic that follows the majority

Safety Integrity, Standard Comparison PFH, PFD, Requirements

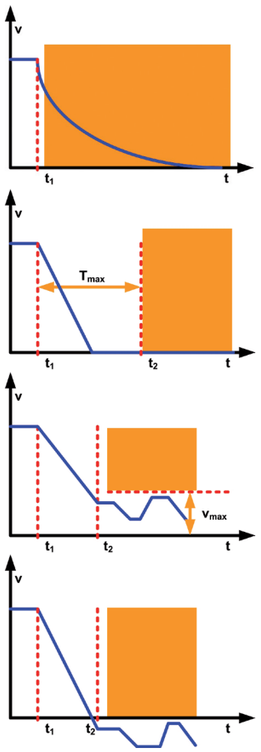
Safety Integrity (Type B) according to IEC 61508				SIL / PL (ISO 13849)	
	HFT				
SFF	0	1	2	SIL	PL
< 60%	-	SIL 1	SIL 2	1	b, c
60% - < 90%	SIL 1	SIL 2	SIL 3	2	d
90% - < 99%	SIL 2	SIL 3	SIL 4	3	e
99% - < 99%	SIL 3	SIL 4	SIL 4	4	-

Requirement according to IEC 61508, Type B (partly unknown failure performance)
Comparison SIL / PL (IEC 61508 / ISO 13849)

SIL	PFH(d)	PFD(d)		Critical values (IEC 61508)
	in 1/h	on demand		
1	$< 10^{-5}$	$< 10^{-1}$		**SIL** Safety Integrity Level
2	$< 10^{-6}$	$< 10^{-2}$		**SFF** Safe Failure Fraction
3	$< 10^{-7}$	$< 10^{-3}$		**PF** Failure Probability
4	$< 10^{-8}$	$< 10^{-4}$		**PFH** PF per hour
				PFD PF on demand

Safety-related drive functions

Safe drives, motion functions



STO: Safe Torque Off

The drive coasts to a stop without further commutation

SS1: Safe Stop 1
Safe stopping

The drive is down-regulated and separated from the torque

SS2: Safe Stop 2
Safe operating stop

Like SS1, yet with standstill monitoring

SLS: Safely Limited Speed

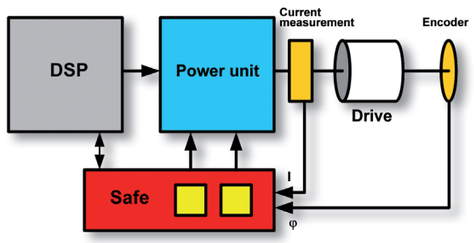
On exceeding the maximum speed the drive is switched off

SDI: Safe Direction

On deviating from the preset direction of rotation the drive is switched off

Monitoring area: marked orange

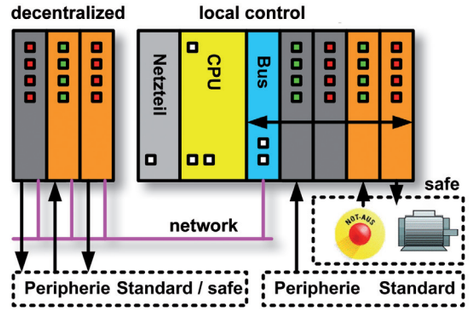
Monitoring principle:



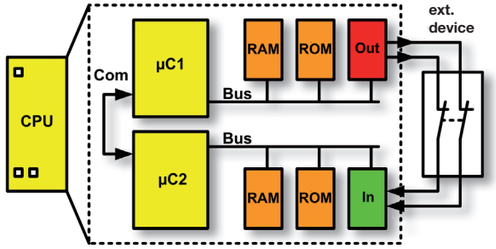
Safe controls and networks

Safe programmable logic controller

1. Complete system (PLC)



2. Safe CPU (1oo2) with switching device



3. Safe bus systems (Faults/Measures)

Fault \ Measure	Sequential number	Timestamp	Time expectation	Confirmation	Identifier	Data integrity	Redundancy	Data redundancy (response)
Repetition	●	●	■	■	■	■	●	■
Loss	●	■	■	●	■	■	●	■
Insertion	●	■	■	●	●	■	●	■
Wrong sequence	●	●	■	■	■	■	●	■
Corruption	■	■	■	●	■	●	■	■
Delay	■	●	●	■	■	■	■	■
Coupling (s/ns)	■	■	■	●	●	■	■	●

Terms & Abbreviations
Contact

SIL Safety Integrity Level	Classification of the safety integrity according to IEC 61508 und IEC 62061
PL Performance Level	Classification of safety-related functions to fulfil a safety requirement
Category	Classifcation of resistance to faults according and ISO 13849
PFH Probability Failure per Hour	Dangerous failure rate per hour (= λ_{du}, in 1/h)
PFD Probability Failure per Demand (Low Demand)	Failure probability in relation to the number of demands
λ Failure Rate	Indicated in fit
MTTF Mean Time to Failure	Mean time until the occurrence of a fault (=1/λ)
fit Failure in Time	Failures in 10^9 hours
DC Diagnostic Coverage	Diagnostic coverage (percentage of detected faults during a test
SFF Safe Failure Fraction	Fraction of the safe failure rate to the entire failure rate.
HFT Hardware Failure Tolerance	Critieria for immunity from failures
CCF Common Cause Failure	Failures that occur due to a common cause

innotec
... reaching your safety goals

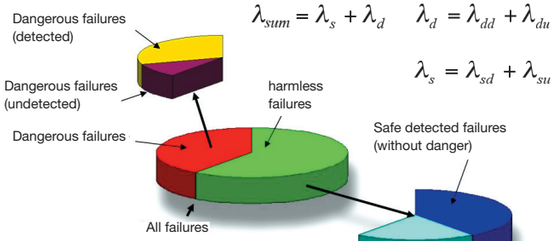
innotec GmbH
Heinrich-Wildung-Weg 3
D-21224 Rosengarten
Tel.: +49 (0)4105-1559182
Fax: +49 (0)4105-1559183
info@innotecsafety.de
www.innotecsafety.de

innotec GmbH
Salurner Straße 16
A-6020 Innsbruck
Tel.: +43 (0)512-583320
Mobil: +43 (0)664-73031 881
info@innotecsafety.com
www.innotecsafety.at

CONTROL SYSTEMS · DRIVES · NETWORKS · RAILTECHNOLOGY · MACHINES · PLANTS · ELEVATORS · TRANSPORTSYSTEMS · SOFTWARE · ORGANISATION · DOCUMENTATION

Parameters
Formulas
Calculations

1. Failure distribution



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

$$\lambda_s = \lambda_{sd} + \lambda_{su}$$

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

$$PFH = \lambda_{du}$$

(For single channel structure)

2. Parameters

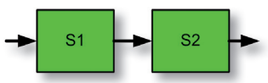
Safe Failure Rate (SDFF), Diagnostic Coverage (C)

$$SFF = \frac{\lambda_s}{\lambda_{ges}}$$ without diagnosis $$SFF = \frac{\lambda_s + \lambda_{dd}}{\lambda_{ges}}$$ with diagnosis

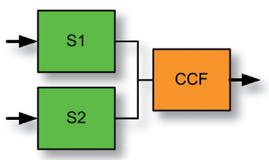
$$DC = \frac{\lambda_{dd}}{\lambda_d} \qquad SFF = \frac{\lambda_s + DC \cdot \lambda_d}{\lambda_s + \lambda_d}$$

MTTF, λ, 1-channel, 2-channel Systems with diagnosis (according to EN 62061)

$$MTTF = \frac{1}{\sum \lambda_i} \qquad \lambda_i = \lambda_1 + \lambda_2 + \ldots + \lambda_n$$



$$\lambda_{du} = \lambda_{d1} \cdot (1 - DC_1) + .. + \lambda_{dn} \cdot (1 - DC_n)$$



$$\lambda_{du} = (1-\beta)^2 \cdot (F_1 \cdot \frac{T_2}{2} + F_2 \cdot \frac{T_1}{2}) + \beta \cdot \frac{\lambda_{d1} + \lambda_{d2}}{2}$$

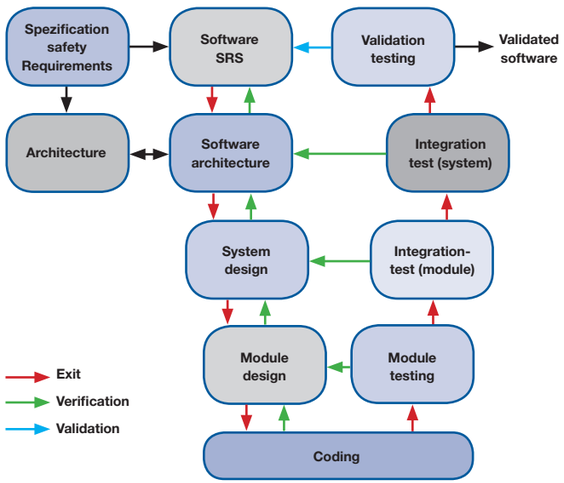
$$F_1 = \lambda_{d1} \cdot \lambda_{d2} \cdot (DC_1 + DC_2)$$

$$F_2 = \lambda_{d1} \cdot \lambda_{d2} \cdot (2 - DC_1 - DC_2)$$

ß: Common Cause Failures (CCF)
T1: Proof testing interval
T2: Diagnosis testing interval
S1, S2: Subsystems

V-Model
Methods & Organisation

V Model, Development Life Cycle



SRS: Safety Requirement Specification
Validation: Proof that the requirements are correct.
Verification: Proof that the requirements are correct implemented

Methods & Organisation

FMEA	Failure mode and effects analysis
- **System-FMEA**	Analysis of failures within the system (e.g. using hard or software)
- Process-FMEA	Analysis of failures that occur within the process (e.g. production, maintenance or change)
Calculation of RPZ Risk Priority Number	Product of 3 rating numbers (e.g. risk, probability, severity)
Fault Tree (FTA, Fault Tree Analysis)	Presentation of failure structures failure scenarios
Simulation	Examination using a model (also mathematical) to allow a conclusion about the actual situation
Calculation (of the parameters)	Mathematical calculation of the parameters for safety classification (e.g. HFT, λ, CCF, DC, PFH and PFD)
Safety lifecycle	Consideration of all phases of a product (e.g. concept, development, production, testing, during service, maintenance, change, after service
Safety Assessment	Examination of the quality assuring measures within an organisation

SafetyFirst

The essentials of safety engineering

- Risk assessment
- Safety classifications
- References between standards
- Safety parameters
- Maschines
- Plants
- Controls
- Sensors and actuators
- Drive systems
- Bus systems
- Definitions
- Formulas

innotec